Integration of Biometrics and PIN Pad on Smart Card

CHUNLEI YANG

A thesis submitted to The Newcastle University in partial fulfilment of the degree of Doctor of Philosophy in the School of Electrical, Electronic & Computer Engineering

School of Electrical, Electronic & Computer Engineering

Newcastle University

January 2011

Abstract

Secure payment is the basis of electronic commerce (e-commerce). A large amount of electronic payments are made via POS (point of sale) terminals using smart cards and legitimate users are usually authenticated by PIN. The security design of POS terminals and authentication methods are increasingly becoming concerns of e-business. The major aims and objectives of this industrially oriented research are to investigate a new solution at system level to improve the security of current POS payment systems. The contributions of this thesis include several aspects: 1) An in-depth literature survey has been undertaken. The security threats of current POS terminals and available countermeasures have been systematically investigated. The main existing problems have been identified. 2) An innovative scheme, the so-called Supercard, which integrates PIN pad, biometrics and the smartcard, has been proposed. Approaches based on this scheme can meet security challenges posed by attacks such as visual and channel PIN attacks, display attacks, and fake-machine attacks. The scheme also has advantages to prevent the cryptographic key being disclosed by channel or side channel attacks. 3) The Supercard scheme has been examined specifically to improve fingerprint biometrics security. The Capture & Match on Card scheme and corresponding authentication protocol has been designed with the advantage of preventing biometric channel attacks. Biohash is adopted to protect the biometric template. 4) Keystroke dynamics, as a behaviour biometric to strengthen PIN authentication, has been investigated under the specific conditions of a highly limited number of keystrokes. 5) The multimodal signals of PIN, fingerprint and keystroke dynamics have been studied through fuzzy-logic-based information fusion.

Declaration

No portion of the work referred to in the thesis has been submitted in support of an application for another degree or qualification of this or any other university or other institute of learning.

Signature of Chunlei Yang

Date: 10 January 2011

Publications

In the course of completing this thesis, the contents of a number of chapters have already been published by the author.

These are:

- Chunlei Yang, Guiyun Tian, Steve Ward. *Biometric Based Smart Card for Security.* Proceedings of ICETE'05", the 2nd International Conference on E-business and Telecommunication Networks, 2005, Reading, UK, pp.240-246.
- Chunlei Yang, Guiyun Tian, and Steve Ward. *Security systems of point-of-sales devices.* The International Journal of Advanced Manufacturing Technology. ISSN 0268-3768. April 2006, Springer London, pp.799-815.
- Chunlei Yang, Guiyun Tian, and Steve Ward. *Multibiometrics authentication in POS application.* School of Computing and Engineering Researchers' Conference, 2006. University of Huddersfield, pp.1-6.
- Guiyun Tian Chunlei Yang, Jingzhuo Wang, Steve Ward. *Wireless sensor network for e-manufacturing.* Proceedings of e-ENGDET2006, 5th International Conference on e-Engineering & Digital Enterprise Technology, 16th -18th August, 2006, Guiyang, China.
- Chunlei Yang, Guiyun Tian and Said Boussakta. *Keystrok dynamic and fingerprint multibiometrics authentications.* 3rd Information and Partnering Forum on Safety and Security Systems in Europe, 19th - 20th June 2008, Potsdam, Germany.
- *Smart card with integrated display and keypad,* in procedure of patent application.

Abbreviations

AES		Advanced Encryption Standard
ABS		Acrylonitrile Butadiene Styrene
BGA		Ball Grid Array
CEN		the European Committee for Standardization
CMOC		Capture & Match On Card
COC		Capture On Card
COS		Smart Card Operating Systems
COTS		Commercial Off-The-Shelf
DES		Data Encryption Standard
DFA		Differential Fault Analysis
DoS		Denial of Service
DPA		Differential Power Analysis
DUKPT		Derived Unique Key Per Transaction
EC		Elliptic Curve
ECC		Elliptic Curve Cryptography
ECDH		Elliptic Curve Diffie-Hellman key agreement scheme
ECDLP		Elliptic Curve Discrete Logarithm Problem
EEPROM		Erasable Programmable Read-Only Memory
EER		Equal Error Rates
EMI		Electromagnetic Interference
EMV		Europay International, MasterCard International and Visa International
ESD		Electrostatic Discharge
FAR		False Acceptance Rate
FIPS		Federal Information Processing Standards
FPGA		Field Programmable Gate Arrays
FRR		False Rejection Rate
LVQ		Learning Vector Quantization
MOC		Match On Card

OFET	Organic Field Effect Transistor
PC	Polycarbonate
PCB	Printed Circuit Board
PCI	Payment Card Industry
PED	PIN Entry Device
PIN	Personal Identification Number
POS	Point of Sales
RBFN	Radial Basis Function Network
RSA	Ronald L. Rivest, Adi Shamir and Leonard Adleman
SMD	Surface Mounted Devices
SQUID	Superconducting quantum interference devices
SRAM	Static Random Access Memory
SVM	Support Vector Machine
UML	Unified Modelling Language
VHDL	Very High Speed Integrated Circuit Hardware Description Language
WFMT	Wavelet and Fourier Mellin Transform

Symbols

C	Ciphertext
E	An elliptic curve over the field
$E(F_q)$	The set of all points on an elliptic curve E defined over F_q and including the point at infinity Q
F_2^m	The finite field containing 2^m elements, where m is a positive integer
F_p	The finite field containing p elements, where p is a prime
gcd(x,y)	Greatest common divisor. The largest number that divides evenly into each of a given set of numbers.
K_M	Master key
K_S	Session key
mod	Modulo
O	A special point on an elliptic curve, called the point at infinity.
p	An prime number
P	An elliptic curve point
q	The number of elements in the field F_q
Q	An EC public key
$x \bmod n$	The unique remainder r, $0 \le r \le n-1$, when x is divided by n. For example, 23 mod 7=2
$X \oplus Y$	Bitwise exclusive-or of two bit strings X and Y of the same bit length
$\equiv$	identical to
d	A private key of asymmetric cryptography

Acknowledgements

My greatest thanks are reserved for those who helped me the most in the past six years.

I would like to express my gratitude for the support, guidance and patience to my supervisor, Professor Guiyun Tian. His attention to detail, quest for excellence, and love for perfection has inspired me to give my best. He has helped greatly to develop my research skills and philosophy. I am deeply indebted to him for making the Ph.D. experience a memorable one. My second supervisor Prof. Said Boussakta from Newcastle University has supported and helped me to finish this thesis.

Prof. Dr. Reinhard Völler, my external supervisor, always encouraged me move forward. He ensured that I kept on track and was incredibly helpful in guiding me through the whole programme.

Ingenico, the company I worked for, initiated and provided financial aid to the research at first stage. Former CEO of Ingenico Group Mr. Gehard Compain and chief architect Mr. Michel Dargent encouraged and supported me to join this programme.

My family members, Fenfang, Congcong and Anteng belief in my abilities and me has allowed me to achieve my goals and go far beyond my expectations. My family have given up all family holiday plans during past several years because of this thesis. My old parents are always proud of me and encourage me to achieve further. I will especially memorise the love of my father forever, although he passed away before he can see that I finally finish my study.

Final thanks to all rest people whose names are not listed here, they have also supported me during this thesis written.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1. Introduction

This chapter provides the project background, general information and summarises the contributions of this thesis.

1.1 Background

Electronic commerce, commonly known as e-commerce or eCommerce, consists of the buying and selling of products or services over electronic systems such as the Internet and other computer networks. The amount of trade conducted electronically has grown extraordinarily with the increase in eCommerce. Meanwhile, card payment devices are rapidly evolving and becoming ubiquitous as a method of e-payment to support eCommerce. Security is more important than ever with the need to ensure the integrity of the payment process and protect the privacy of individuals using Point of Sale (POS) devices. The card (magnetic card or smart card) and PIN (Personal Identification Number) play important roles in payment. Magnetic cards use magnetic material to store some information for machine-identification, but it cannot prevent data copy or manipulation. Therefore, magnetic cards no longer meet today's security challenge, and they are gradually being replaced by IC cards, also known as smart cards [1][2]. The smart card, a French invention, has an embedded CPU and memory. The smart card has the capability to record and modify information in its own non-volatile memory and the security data can be well protected by the operation system and hardware measures. These features make the smart card a powerful and practical tool against unauthorised data access and copying [3].

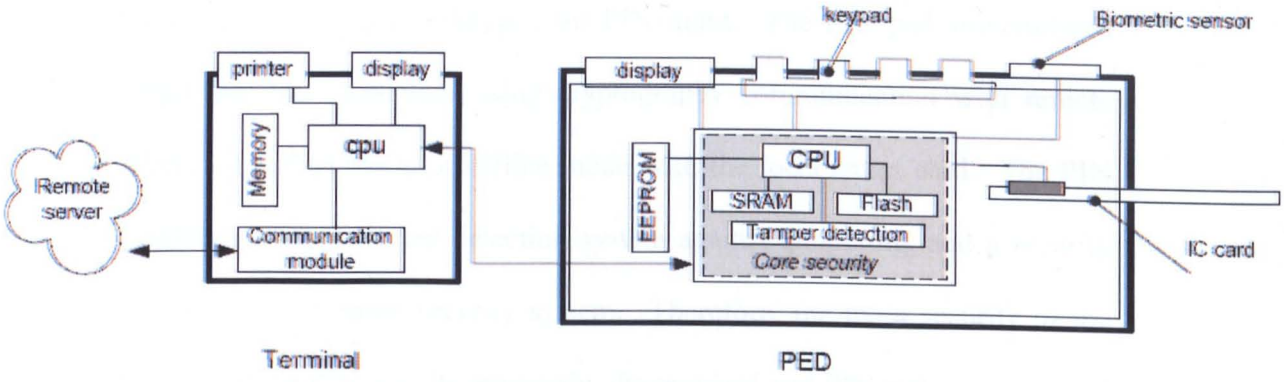
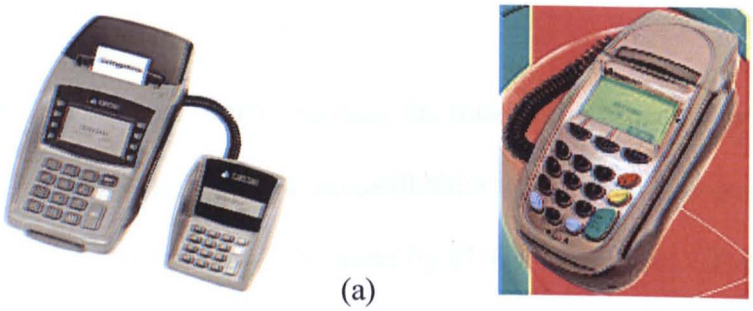


Figure 1: Diagram of POS System



(a) (b)

Figure 2: Integration of terminal and PIN pad

(a) Separate Terminal and PIN pad (b) Integrated Terminal and PIN pad

Machines that accept card payments at the Point of Sale are called POS terminals. They are widely used in shops, hotels or even in taxis. A typical secure POS system diagram is illustrated in Figure 1 and a corresponding product in market from Ingenico [4] is shown in Figure 2. The secure POS system consists of a terminal and a PIN pad (PIN Entry Device). In many cases, the terminal and the PIN pad are combined into one physical machine body. The terminal normally has the functions of entering the payment amount, printing receipts, etc. It has various communication modules and plays the role of a communication bridge between the bank system and the PIN pad. Normally there is no high security requirement on the terminal because all sensitive data passing through the terminal have been encrypted in advance, either in the PIN pad or in a remote server. The PIN pad typically has slots to accept smart

cards and magnetic cards, and a keypad for PIN input. The PIN pad authenticates both the card and the cardholder using cryptography communication with remote bank systems, i.e. online mode or offline mode with the local smart card. The PIN pad also includes a sophisticated detection system against tampering, and a security core inside controls the entire security system. Therefore, the main security of the POS system lies in the PIN pad. Increasingly, the terminal and PIN pad are integrated into one physical body, as illustrated in Figure 2 (b). Thereafter, in this thesis we use the word "terminal" to represent the general integrated device of the terminal and PIN pad.

In the POS system, before starting the transaction, three authentications must be done, namely the legitimacies of the cardholder, the card and the payment terminal. The cardholder authentication can be done by PIN or biometrics. The PIN is known only by the cardholder and can be input through terminal keypad and sent for approval to the card issuer. Instead of by PIN, more recently the cardholder can also be authenticated by providing a fingerprint or other biometrics. The legitimacy of the card can be proven by checking the unique card number and its corresponding encrypted secret data, which is stored by the card issuers (banks). Similar to the card authentication, the legitimacy and integrity of the terminal can be decided by checking the unique number and its corresponding encrypted data, which is stored by payment network providers (acquirers). Obviously, if the cryptographic keys are disclosed, all encrypted data are no longer secure.

In short, two types of security information need to be especially well protected: the cardholder PIN/biometrics and the cryptographic keys. The keys used in information encryption/decryption are stored in the SRAM or registers inside the terminal. The cryptographic algorithms used in the payment system must be public

and well known such as the RSA (Rivest-Shamir-Adleman) [5] or DES (Data Encryption Standard) [6]. The only confidentiality involved in the encryption/decryption process is the key. Therefore, common attacks as well as countermeasures primarily target the cryptographic keys and user PINs. The terminal must be able to protect the PIN and detect attacks by adversaries. Any penetration or unauthorised modification shall cause an immediate and automatic erasure of all keys and other sensitive data [7].

There are two cardholder authentication methods in POS systems, i.e., PIN-based authentication and biometric-based authentication. The PIN-based method is the most popular one. The approach of PIN authentication has many advantages, e.g. it is simple, stable and easy to update or revoke. Nevertheless, security can be easily breached in these systems when a PIN is divulged to an unauthorised user or an impostor steals a card; furthermore, simple PINs are easy to guess by an impostor and difficult PINs may be hard to recall by a legitimate user [8]. Meanwhile there are many attacks, which can disclose the PIN. For example, a PIN can be disclosed by visual observation (eyes or a camera) at the time the cardholder is keying the PIN numbers on a PINpad, or by monitoring different characteristics that change during the transaction, e.g. using electromagnetic radiation noise, beep sounds produced by the different keys or fluctuations of the power consumption [9]. Instead of non-intrusive attacks, there are many intrusive attacks which can disclose the PIN by accessing the inside of the PINpad, e.g. by installation of a tapping bug connected to the keyboard matrix and recording the communication via a smart card reader [10]. Currently, the visual PIN leakage is commonly prevented by building a physical visual shield around the keypad. A higher visual shield is more secure, but it makes the PIN input more inconvenient. In the field of preventing penetration attacks, some

security mechanisms are harder to implement, because a standard PINpad case cannot be built from very hard materials like steel, nor can it be built as a closed system, because although this would resist penetration, an open slot is required for smart card insertion. Common countermeasures which deploy micro open-alarm switches against the unauthorised opening could be defeated by methods of bypassing, e.g., silver ink injection.

For a long time, people have tried to find a new method to replace the PIN-based authentication technology. The emergence of biometric methods has addressed the problems that plague traditional verification methods. Biometrics refers to the automatic verification of a claimed identity by using certain physiological or behavioural traits associated with the person [8]. By using biometrics, it is possible to establish a verification based on 'who you are', rather than by 'what you possess' (e.g., a smart card) or 'what you remember' (e.g., a PIN). As illustrated in Figure 3, biometric systems make use of fingerprints, hand geometry, iris, retina, face, hand vein, facial thermograms, signature, voiceprint, gait, palm print, etc. to establish a person's identity [8][11]. Although biometric systems have their limitations [13], they have an edge over traditional security methods in that it is much more difficult to lose, steal or forge biometric traits; furthermore, they facilitate human recognition at a distance (e.g., face and gait) [14].

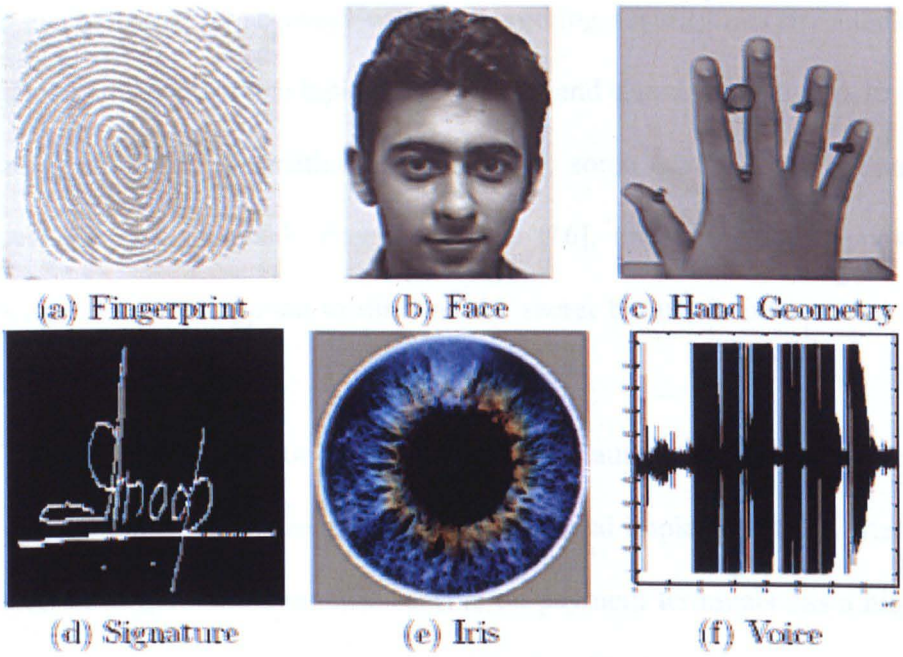


Figure 3: Examples of some of the biometric traits used for authentication

Figure 4: Example of a POS terminal with a fingerprint sensor

Biometrics cannot replace the PIN method completely as it has its innate disadvantages; for example, it is hard to revoke, is susceptible to impersonation attacks and it cannot currently provide 100% correct identification rate [13]. For example, a fake finger can be created without great difficulty to fool many fingerprint sensors [15]. Currently, biometric sensors are designed and installed with a payment terminal (machine). Security risks exist in this kind of configuration. For instance,

after the machine case is accessed without triggering security alarms, attackers can apply channel attacks, like line taping, interception and signal replacement, to disclose the security biometric information. Furthermore, some advanced crypto-analytical techniques, like so-called side channel attacks [16], and in particular, power and timing analysis, can be applied to disclose the secret biometric information without machine penetration.

Therefore, using PIN or biometrics alone for authentication systems may not be particularly high security from the view of technical implementation. Meanwhile, the location of keypad and biometric sensors on payment terminals has a higher risk of being attacked. Previous research [17] has indicated that biometric methods can be combined with PIN and smart card technology to improve security. The payment industry is seeking new solutions to improve the security. In this thesis, we want to extend such research.

1.2 Aims and Objectives

The research was initiated and partially funded by Ingenico Group, one of the leading providers of payment solutions. For over 25 years, it has delivered over 15 million POS terminals that have been deployed across 125 countries. Ingenico [4] wants a prospective study to understand the future development of payment devices. The author, who was a senior research engineer in the Advanced Technology Department of Ingenico Group, initiated this work. The aim of the work was to gain an in-depth understanding of POS terminal security and to investigate potential advanced solutions which can enhance that security. The study results will be used as a reference for R&D development, as well as for marketing strategies.

The major aims and objectives of this research are:

- To identify the major security problems of the current POS systems.
- To propose a new framework for enhancing security, especially preventing the PIN visual leakage and fake terminal attacks which for a long time have been recognised as fundamental threats.
- To investigate the integration of biometric technology in POS systems. To determine which types of biometrics are useful and how they can be integrated together to improve the user authentication process.
- To evaluate the new system through experimental tests.

With the nature of industrially oriented research in mind, the following requirements need to be taken into account:

- User convenience. e-payment is part of daily life for millions of people of different ages, educational backgrounds, etc. The proposed security solution shall not be detrimental to user convenience.
- Cost-effective. Payment terminals are massive products. The new solution to reinforce the current payment security should be affordable.

1.3 Thesis Contributions

A few of the challenges presented in the earlier section will be addressed later. In this thesis, new proposed schemes are presented to improve the security of e-payment. Threats, which have been addressed by our proposed approaches, are listed in Table 8-1 of Chapter 8.

The major contributions of this thesis are as below.

- An in-depth literature survey on POS terminals has been undertaken. The security threats and available countermeasures have been

systematically reviewed. The main existing problems have been identified.

- A novel scheme, the so-called Supercard, which integrates PIN pad, biometrics and smartcard, has been proposed to provide a new system-level solution. This scheme is able to solve fundamental challenges such as visual and channel PIN attacks, display attacks, and fake-machine attacks.
- The security of fingerprint biometrics has been reinforced by a new Capture & Match on Card (CMOC) scheme based on Supercard. The corresponding authentication protocol is investigated. Biohash is adopted to protect the biometric template.
- Studies on keystroke dynamics as behaviour biometrics to strengthen the PIN authentication has been done under the specific conditions of highly limited numbers of keystrokes. The research results can be applied to the Supercard or a conventional POS. The experimental and evaluation results are presented.
- Based on the Supercard platform, fuzzy-logic-based information fusion has been studied in an effort to integrate the multimodal signals of PIN, fingerprint and keystroke dynamics to make a comprehensive authentication.
- A potential vulnerability of electromagnetic attack has been discovered. In terms of hardware implementation, preliminary investigations have been conducted on how to protect the key store unit. New approaches are proposed which exploit the features of BGA packages, or features of ceramic fragility, hardness and electric isolation.

The results of this research can be applied not only to POS systems, but also to internet security applications, e.g. user login and online payment.

Publications of research through journals, conferences and patent applications are detailed in the list of PUBLICATIONS.

1.4 Thesis outline

In the subsequent chapters, a detailed description of each of these contributions is provided. The thesis structure is outlined below.

Chapter 2 is a systematic survey of the current research in the area of POS security, mainly on aspects of hardware and systems. Attacks and countermeasures around PIN and key disclosures are also reviewed.

Chapter 3 presents the research methodologies. Based on the analysis of the identified problems, a new scheme known as Supercard is proposed. System cryptography algorithms are selected using comparison studies. The novelties and advantages of the Supercard are elaborated with application scenarios. Proposals are given on improving the tamperproof package of the key store unit through a BGA solution and ceramic solution. Major problems are identified including the new potential electromagnetic attack.

In Chapter 4, the Supercard is further studied in the domain of how to improve the security of fingerprint biometrics. Advantages and disadvantages of different biometrics are compared with application, and the CMOC structure is proposed to improve the security.

In Chapter 5, the Supercard investigation is extended by applying the keystroke dynamics as behaviour biometrics to strengthen the PIN authentication. The theoretical background and experimental results are presented.

Chapter 6 describes how to fuse the multimodal signals from fingerprints, keystroke dynamics, and the risk level of transactions. The fuzzy-logic-based information fusion is applied and experimented. At the end, a flexible and adaptive decision system is investigated.

Chapter 7 describes the development of a Supercard demonstration system. The software design and implementation are also presented.

Chapter 8 is the summary and plan for further work. The threats that have been addressed by our proposed approaches are listed in Table 8-1.

The documentation of Supercard's industrial implementation is attached as an appendix.

Chapter 2. Literature Survey

This chapter conducts a comprehensive literature survey on the security of POS products. Threats and available countermeasures are investigated with the target of identifying the major problems.

2.1 Introduction of POS Security

Security is more important than ever to ensure the security of e-commence. As introduced in the previous chapter, in the POS payment system, two types of security information need to be especially well protected: the cardholder PIN/biometrics and the cryptographic keys. The PIN is entered using a keypad. The keys used in information encryption/decryption are stored in the SRAM or registers inside the terminal. Common attacks as well as countermeasures target primarily the cryptographic keys and user PINs. The terminal must be able to protect the PIN and detect adversary attacks. Any penetration or unauthorised modification shall cause an immediate and automatic erasure of all keys and other sensitive data [7].

The security of a POS system has its own specialties. Firstly, POS devices are embedded systems [17]. Implementing security in embedded systems is dramatically different from that of full-featured personal computers. Even with today's advanced technology, embedded systems have severely limited resources: embedded CPU speed is much slower than that of a personal computer, for example, and volatile and non-volatile storage is usually much smaller. For example, a POS payment device has a 40MHz processor, 1M RAM and 2M Flash memory. Meanwhile, embedded systems often perform periodic computations to run control loops in real time. A delay of a fraction of a second can cause a loss of control-loop stability, hence

embedded systems become vulnerable to attackers designed to disrupt system timing [19]. Another feature of embedded systems is cost sensitivity; several dollars can make a big difference for mass production in the market. Consequently, some security approaches with computational requirements, which can be implemented in personal computers, will be too complex to implement in an embedded system.

Secondly, the POS devices directly involve a high volume of financial transactions. They have far higher risks than other civilian secure apparatuses such as pay-TV decoders and mobile phones. POS security devices must be compliant with many strict bank transaction standards and industry security specifications. Not only is the communication protocol far more complicated, but also the hardware and the physical design have higher demands. For instance, according to new security regulations in the POS industry [7][20], peripherals like the smart card, display and keypad must be controlled directly by a security core. Triple-DES and RSA cryptographic algorithms, which require high computation power, shall be supported [21]. The shape, design and the position of the smart card reader in the POS device are included in the security spectrum with specific requirements. Meanwhile, a comprehensive and sophisticated tamper-proof system must be carefully implemented. With more and more sophisticated attack methods being developed [24][25][26], the security design becomes the most challenging job of the POS system.

Thirdly, compared with the security implementation of a smart card [24], which has been widely studied in depth, implementations in POS devices have specific constraints. (1) The production volume of smart cards is huge and the card is held by each cardholder, so the average cost of security development for each card is relatively low. In contrast, the POS devices are only deployed on sites where transactions occur. Meanwhile, the security standards and marketing requirements

vary from country to country and from bank to bank. Consequently, the production volume of POS devices with a specific configuration is far less than that of smart cards; it ranges typically from several thousand to one hundred thousand for each batch and type. (2) In a smart card, the whole control system is integrated into one small chip, the size of which is only several square millimetres. Many modern semiconductor technologies and measures can be applied to protect it, such as scrambling the memory and bus or covering a protective layer over the whole chip, for example [24]. However, it is not easy to implement such measures to protect the POS security. In the POS system, the security requirements evolve quickly, and for reasons of flexibility and cost, most of the POS providers still use generic CPU core, memory chips and other discrete components. It is not always practical to build the whole security system into one ASIC (Application Specific Integrated Circuit). Additionally, the POS security system requires more physical space for powerful processors, more memory and various peripheral components; as a result, the secure area in a POS system is much larger than that of a smart card. (3) The smart card is held by cardholders personally and carefully while the POS system is deployed in public locations. The adversary can get far more potential benefits from compromising a POS device than compromising a card. This is because one compromised card will affect only one user, but one compromised POS system will jeopardise all of its users.

Therefore, in terms of security, the POS device has its own unique set of difficulties and specialities. Nevertheless, it has not drawn as much attention as it should have. Very few papers focus on POS security, especially in the physical and hardware implementation spectrum. This research attempts to give a systematic security study of POS devices by identifying weak points, introducing some practical

implementations and proposing further research. It focuses on the hardware and physical security fields, primarily, although logic security is also referred to.

The rest of the chapter is organised as follows: Section 2.2 and Section 2.3 elaborate the security issues of the terminal peripherals and the security core unit. Practical implementations are presented in Section 2.4. Section 2.5 overviews some standards related to POS security, cryptographic algorithms, and physical approval programs.

2.2 Peripherals Security

Terminal security means to effectively prevent the disclosure of PIN, keys and sensitive data. Referring to Figure 5, according to the different security requirement levels, the terminal entity can be defined and divided into two parts, or two layers. The first layer is the *peripheral layer*. It includes the case and peripherals such as keypad, smart card reader and biometric sensors if present. The second layer is the *core security layer*, as illustrated within the dashed line in Figure 5. The security measures deployed in the peripheral layer primarily prevent the disclosure of the PIN. The peripheral layer also constitutes the first defence for the second layer, i.e. core security, while the security measures deployed in the core security layer primarily prevent the disclosure of the keys. Therefore, the security requirements in the core security layer are higher than that in the peripheral layer. For the purpose of clarity, peripheral security and core security will be investigated separately. The rest of this section focuses on common attacks, measures and existing problems of peripheral security. The next section investigates attacks, measures and problems of core security.

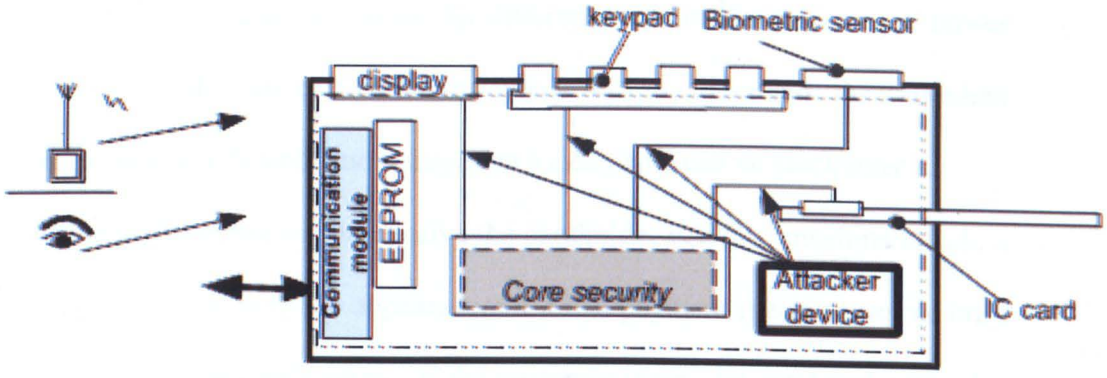


Figure 5: Terminal structure illustration

2.2.1 Attacks on Peripherals

The terminal has peripherals such as the keypad, the smart card reader and the display (recently it may also include biometric sensors), all of which belong to members of the security system and need to be protected. According to whether the terminal cases need to be accessed, the attacks can be classified into two categories: non-intrusive attacks and intrusive attacks.

2.2.1.1 Non-intrusive Attacks

It is evident that the PIN can be disclosed by visual (eyes/camera) observation while the cardholder is inputting the PIN numbers in a payment device. Even at a distance from the PIN keypad, the keying PIN can be observed by simply using binoculars or a telescope [27]. It is important to emphasise the threat of visual observation attack, because it is a very common means of PIN leakage that is hard to prevent. Moreover, this is not a highly demanding type of attack, technically, thus adversaries who have no prior knowledge of security can carry it out.

A PIN can also be remotely disclosed by monitoring physical signals during a transaction, e.g. electromagnetic radiation (with the help of a radio device with an

antenna), noise, beep sounds produced by different keys or fluctuations of power consumption, etc. In the case of membrane keyboards or touch screens, for fraudulent PIN capture purposes, a flexible and transparent touch panel can be stuck over it.

Another well-known way to deceive the cardholder is a fake machine attack; a forged payment machine with the appearance of a real payment machine can be built and put in place to cheat cardholders. If the customer inserts his card and enters his PIN in a fake machine, it will record the PIN and some user information.

Most computer devices and systems, output devices (e.g. LCD display) and input devices share the same data bus. This means that if a connector or display signal lines are easily accessible to an attacker from outside, then the PIN or other data from the input device can be recorded from the output device.

2.2.1.2 Intrusive Attacks

If an attacker can access the inside of devices, by installing a tapping bug that is connected to the keyboard matrix or cable, they can record the communications and get the PIN which can then be used in replay attacks. Meanwhile, since many smart cards have no ability to make decryption computation, for such cards, the PIN that is inputted from the keypad cannot be encrypted before it is sent to the smart card for authentication; consequently, the plaintext PIN can be obtained from the I/O lines of the smart card reader.

Provided the attacker can imitate the display message either from the outside or the inside, by an attack method where the terminal is not visibly damaged, it is dangerous. The reason is that the cardholder will not realise that the terminal has been manipulated and the cardholder will be falsely instructed. Performing a

sensitive task such as entering a PIN during an unsafe running mode [20] will cause a PIN disclosure.

2.2.2 Countermeasure for Peripherals Attacks

Corresponding to the non-intrusive and intrusive attacks, there are two protection types.

2.2.2.1 Non-intrusive PIN Leakage Protection

The most effective way (or the only available way currently) to prevent visual PIN leakage is to build a non-transparent physical barrier, or a so-called *privacy shield* around the keypad [27]. Obviously, a higher privacy shield can better prevent disclosure. Also PIN keypads should be designed without flat surface keyboards (e.g. a membrane) as these are susceptible to attacks like adding a flexible and transparent capture layer.

In addition, hardware designers should aim to protect the activity on the keyboard matrix, the I/O line of the IC card interface or any associated hardware, as the PIN information can be revealed by electromagnetic radiation monitoring [20]. If the PIN entry is accompanied by audible tones, then the tone for each entered PIN digit must be indistinguishable from the tone of any other entered PIN digit.

2.2.2.2 Intrusive Attack Protection

Theoretically, if the device case is strong and hard enough to resist attacks, it is a tamper-resistant device. Unfortunately, this category countermeasure is hard to implement in a terminal device due to practical constraints of weight and cost. The majority of terminal cases are made of plastic materials such as ABS (Acrylonitrile Butadiene Styrene) or PC (Polycarbonate). To detect attempts to open the case,

sensors are needed to issue open-alarm signals. Once an open alarm is triggered, the security system will stop the terminal service automatically. Afterwards, unless the terminal is returned to the manufacturer and resumed under security control, it will no longer be able to work properly. Correspondingly, it would not be able to instruct the cardholder to input the PIN.

However, in reality, the detect sensors cannot be deployed everywhere and normal micro open-alarm switches can also be bypassed. To always keep the keys and the security detective system in an active state during a normal transportation and storage period, an internal battery supplies the power of the terminal security system. As a result, the limitation of the battery supply is that strict, active techniques of ultrasonic or infrared space detectors cannot be exploited [28]. The terminal case cannot be similar to a closure, although this would be more effective at resisting penetrations, because there has to be an open slot for smart card insertion. A skilled attacker will not try to open the case because they know it will easily trigger the open alarm. They cut or drill through the case from the bottom plastic part or the rear part to avoid opening the case directly, or by injecting silver ink (electric conductive) to bypass the open-alarm switches so that they can access the device without triggering the security alarm. In such a case, customers will still use this device and give their PIN.

2.2.3 Problem Analysis

As we have just discussed, anti-penetration of terminal peripherals is very difficult in practice. A reasonable anti-penetration system can only be realised by a comprehensive and careful design of a sensor detecting system, a proper layout of components, dedicated PCBs, etc. Some practical implementation examples will be presented later in Section 2.4.

The problems are concentrated on the PIN keypad and the PIN transmission channel, i.e. from the keypad to the core security package. If we can find a solution to physically remove the keypad and correspondingly the transmission channel out of the terminal, the security can be improved dramatically. This is the basic idea of our proposed Supercard solution, which will be elaborated in the next chapter.

2.3 Core Security

This section provides an overview of a typical core security unit. Attacks are described in sections 2.3.1. Countermeasures are explained in section 2.3.2.

2.3.1 Attacks of Key Disclosure

One disclosed PIN would put an individual cardholder at risk. However, the disclosure of cryptographic keys, which are stored in the core security unit of the terminal, can put all transactions via this terminal at risk, even in a DUKPT (Derived Unique Key Per Transaction) based system. Therefore, key attacks are much more dangerous than PIN attacks. Consequently, the protection requirement of core security is much higher than that of peripherals.

A typical structure of a core security part in a terminal is illustrated in Figure 6. The whole core security area is encapsulated in a small package (shown in the dashed line closure) and filled with epoxy resin. Inside the device, there are sensitive components such as CPU, SRAM and Flash. It also includes tamper detection circuits. The power supply is backed up with a battery to keep the keys in the volatile memory and to ensure that the tamper detective circuit is always active.

According to whether the protection package or security chip needs to be accessed, the attacks can be classified into two categories: non-intrusive attacks and intrusive attacks.

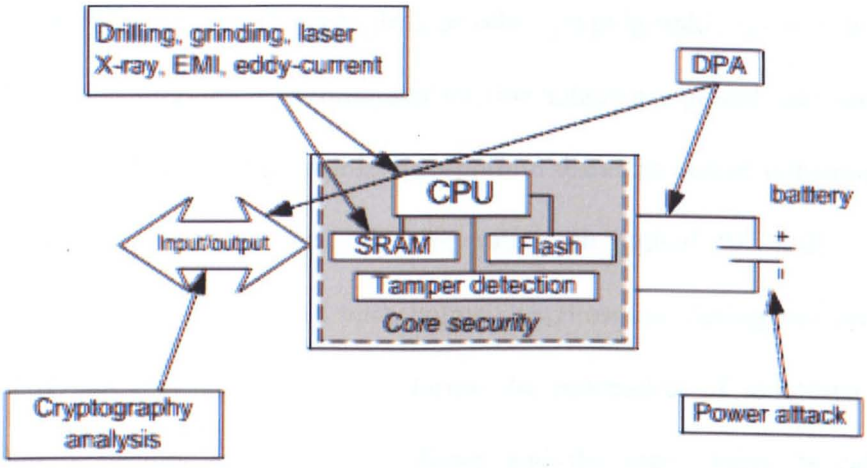


Figure 6: Illustration of core security structure and attacks

2.3.1.1 Non-intrusive Attack

When a cryptographic system is running, accompanying the data transformation, some physical signals, i.e. time, power consumption or electromagnetic signals, change correspondingly and are often used as leakage sources to detect security information. These signals can be measured from outside of the cryptographic chip rather than from its communication channel, and non-intrusive and powerful attacks based on these methods are also called *side channel* cryptanalysis. Typical non-intrusive attacks including Differential Power Analysis (DPA), electromagnetic analysis, timing attacks, Differential Fault Analysis (DFA), and condition changing attacks will be investigated below.

(1) DPA Attack

Differential power analysis (DPA) is a class of attack discovered by Cryptography Research Inc [29]. This attack is able to extract secret keys and compromise the security of smart cards or other cryptographic devices by analysing their power consumption. It measures the instantaneous power consumption of a device while it runs a cryptographic algorithm: a different power consumption when operating on logical "1" compared to operating on logical "0" [30]. The power consumption is first determined with help of oscilloscope during the processing of known key and it is then measured during the processing of unknown key. The measuring is usually repeated many times and the mean value is calculated to eliminate the noise. After measuring is complete, the difference is determined and hence the unknown key can be deduced [29].

(2) Electromagnetic Analysis

Theoretically, electromagnetic analysis is a process similar to a DPA attack. By measuring the electromagnetic radiation of the CPU, conclusions can be drawn about the internal sequence of events taking place on the microcontroller. Superconducting quantum interference devices (SQUIDs) can be used to measure magnetic fields of low extension and strength. The evaluation can be carried out in a manner that is analogous to DPA. Karine Gandolfi et al. [31] experimentally attempted such an attack. They tried to analyse the electromagnetism conducted on three different CMOS chips, which have different hardware protections and cryptographic algorithms of a DES, an alleged COMP128 and a RSA. In all cases, the complete key material was successfully retrieved.

(3) Timing Attacks

The performance characteristics of a cryptosystem typically depend on both the

encryption key and the input data (e.g., plaintext or ciphertext). Cryptosystems often take slightly different amounts of time to process different inputs. By carefully measuring the amount of time required to perform key operations, attackers may be able to find the key.

Paul Kocher described this type of attack in a 1996 publication [32] that focussed particularly on time dependencies of RSA and DSS. Even today, it is still a powerful attack. The 2003 paper [33] by Brumley and Boneh presented that they can use "timing attacks" remotely (three routers and multiple switches distant from the server) and extract a 1024-bit RSA private key from an OpenSSL 0.9.7 server. Their experiment broke the common beliefs that timing attacks are only applied in the context of poor computation hardware tokens such as a smart card.

(4) DFA Attack

In September 1996, Boneh et al. announced a new type of cryptanalytic attack against RSA public key cryptosystems on tamperproof devices. Later, Biham and Shamir published their new attack, called DFA, which can get a secret key from DES cryptosystems [34]. More details on how this attack works were revealed in [35].

The basic idea is to give certain physical effects (e.g., ionising or microwave radiation) to a sealed tamperproof device; one can induce, with reasonable probability, faults at random bit locations in a tamperproof device at some random intermediate stage in the cryptographic computation. The faults in the random bit locations do not influence the code itself, i.e., the program itself does not crash, and only some of the values it operates upon are affected. It is further assumed that the attacker is in physical possession of the tamperproof device and that he/she can repeat the experiment with the same private key by applying external physical effects to obtain

outputs due to faults. By analysing a series of different fault results, the key can be disclosed [36].

There are many variations of such attacks, one example being the Optical Fault Induction Attacks, described by Sergei Skorobogatov and Ross Anderson in 2003 [38]. In such an attack, a regular flashlight is flanged to the camera adapter of a conventional light microscope, then it is used to flash a very limited area of the RAM of a microcontroller and cause faults. The background of such attack is that the semiconductor transistor is sensitive to ionizing radiation – whether caused by nuclear explosions, radioactiveisotopes, X-rays or even intensive light. By depackaging the chip to get access to the chip surface (but the passivation layer of the chip remains intact, no require electrical contact to the metal surface) such 'semi-invasive' attack can be conducted. Refer to Figure 7.

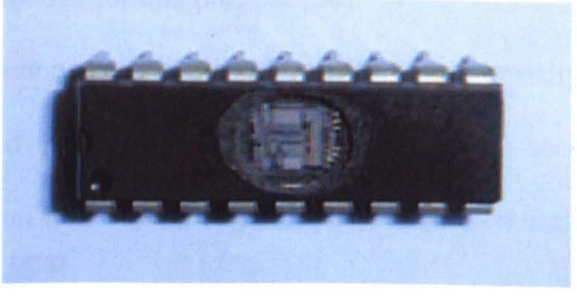


Figure 7: Depacaged microcontroller to apply optical DFA

(5) Condition Changing Attacks (temperature, voltage, frequency, EMI/RFI)

The majority of electronic components perform within specific conditions of voltage, temperature, EMI, etc. Moving outside of such required ranges can cause the system to malfunction. If the intruders can make security circuits inactive by giving extreme conditions, they can access sensitive data without triggering the alarm. For example, immersing the device in liquid nitrogen can cause the temperature to suddenly reach -l95°C [28]. Likewise, if an attacker can control the system frequency,

conclusions can be drawn regarding the RAM frequency content by halting the clock frequency and analysing the RAM with the help of electron beam testers.

2.3.1.2 Intrusive Attacks

If the attack has the ability to successfully access the core security area, the main goal will no longer be to record the PIN (of course it is easy to do), but the keys. Usually the keys and the secret data are kept in the volatile memory (e.g. SRAM) inside a tamper-responsive enclosure. On detection of a tampering event, the volatile memory chips will be powered down or even shorted to ground [37][38], then the stored data will be erased.

Obviously if the adversary can access key storage chips without triggering the security alarm, the intact key remains in memory and it can be obtained easily using the read-out circuitry provided for that purpose [38].

The security components like SRAM and CPU are normally protected by an epoxy-resin-encapsulated package. The common method to access the sensitive components is to drill, mill, and grind or plane the potted area until it is sufficiently close enough to the target and then by proceeding more carefully using fine tools. For instance, the data bus can be bugged with microprobe needles. In order to successfully attack in these ways, knowledge of the layout of the PCB and the associated components is desirable, and this can be accomplished using X-Rays, so that the drilling procedure may then be undertaken more accurately [28].

A more serious problem is that data in volatile memory will not really disappear immediately after power down [28] [37][38] due to some characteristics of the semiconductor. Even if the data have been "erased" after triggering an alarm signal, there are still some possibilities of restoring it. If the time that the data remains after powering down exceeds the time required by an opponent to open the device and

power up the memory, then the protection mechanisms will fail. More details about remaining data are as follows:

(1) Data Remanence in Semiconductor Devices

Taking the advantages of some effects of a semiconductor, there is a variety of ways in which stored data can leave traces of its existence [38]. These include the effects of electrical stress on ionic contaminants (electromigration) and hot-carrier effects, which can be used to recover overwritten data or data from memory from which the power has been removed. Electromigration effects, which can be used to determine, after indefinite periods of time, which type of signal was most commonly carried by a particular part of a circuit. The latter is useful in recovering information such as the bit patterns of keys stored in special-purpose cryptographic devices. Since the physical device is modified, the bits can be recovered in an arbitrary amount of time, even if the memory cells they were stored in have been successfully erased and trapped charges have bled away.

(2) Low Temperature Data Remanence

In the 1980s, it was found that low temperatures could increase the data retention time of SRAM up to many seconds or even minutes. With the devices available at that time, it was found that increased data retention started at about −20°C and increased as temperatures fell further [40]. This means that at temperatures below −20°C, the contents of SRAM can be 'frozen'.

Sergei Skorobogatov repeated some experiments to establish the temperature dependency of data retention time in modern SRAM devices in 2002 [37]. The results indicated that data remanence for dangerous periods and the phenomenon of part of data remanence are widespread, even at temperatures above 20°C . It is important to note that parts of the sensitive data that remain can also lead to a security catastrophe

because the attacker can get the remaining part by attacking it with brute force. Obviously, the more data that remain, the higher the probability is of the system being attacked by brute force.

Without direct contact to IC pins electrically, there are still some techniques that can extract data from the semiconductor's memory (ranging from registers through RAM to FLASH). What these techniques have in common is the use of semi-invasive probing methods to induce measurable changes in the analogue characteristics of the memory cells of interest [41]. The basic idea is that when a memory cell, or read-out amplifier, is scanned appropriately with a laser, the resulting increase in leakage current depends on its state; the same happens when we induce an eddy current in a cell. Researchers have demonstrated their practicality by reading out DES keys stored in RAM without using the normal read-out circuits.

2.3.2 Countermeasures for Key Disclosure Attacks

Following the identified attacks on the core security above, the countermeasures and existing problems will be explored here.

To deter attacks, one basic strategy of security countermeasures is to make attackers feel that the risks far outweigh the benefits of the attack. No single countermeasure can meet all of the challenges, and securing a system requires more than simply adding encryption processors and a hard physical case. The security design must be treated as a system design and it needs integrated approaches [43][44].

2.3.2.1 Common Countermeasures

To prevent condition-changing attacks, appropriate sensors such as temperature, voltage and frequency can be employed to detect the changes. Once the

predefined ranges have been exceeded, the transaction system will be shut down in a controlled way. The sensors, however, must be carefully protected to avoid being disabled easily by adversaries.

DPA attacks, from a hardware point of view, can be prevented by power randomisation, which adds a random noise artificially, or an active power filter to get steady power or detachable power supplies [45]. Unfortunately, such reductions generally cannot reduce the signal size to zero, as an attacker with an infinite number of samples will still be able to perform DPA on the (heavily degraded) signal [29]. From a software point of view, DPA can be prevented by introducing random waiting periods to the processor, by using a constant execution path code, or by choosing operations that leak less information in their power consumption and state transitions [24].

To prevent the data remanence attacks, complete data destruction is required. All storage cells can be actively purged by overwriting with all `1's, and then all `0's, at least three times in rapid succession, followed by shorting of the power supply input pins of the device to ground.

In cases of extreme sensitivity, it is possible that the only acceptable method of destroying the data is by non-reversible physical destruction of the storage devices themselves [28]. Measures which can effectively prevent timing attacks include using noise-free cryptographic algorithms, i.e. the time for encrypting and decrypting is independent of the input values, or adding a cryptographic coprocessor to dramatically shorten the encryption/decryption time [24][38].

The basic principle of DFA is to give certain physical effects, e.g., ionising or flashlight, microwave radiation, to induce faults by individual key bit modification. Therefore cutting the physical attack paths with a physical shield, which is able to

withstand radiation and ionising, can effectively increase the security. Some precautionary measures can be implemented in the cryptographic algorithms. For instance, attacking a random number in front of the plaintext that is to be encrypted [24] results in the encryption of different data by the crypto-algorithm and therefore causes different results. Another example is to calculate the crypto-algorithm twice and compare the two results. If the results are identical, no attempt was made to corrupt any bits from the outside.

2.3.2.2 Using Commercial CryptoProcessors

Some security systems utilise commercial CryptoProcessors to improve security. There are several popular products on the market. For example, Dallas DS5002 series from MAXIM have hardware encryption functions and use encrypted external memories. They are designed to meet the physical security requirements of FIPS140 (Federal Information Processing Standards) and Common Criteria certifications. They detect intrusion of the chip's cryptographic boundary and the CRC-16/32 generator provides strong error detection of memory contents [46][47]. Another popular CryptoProcessor comes from IBM. The IBM 4758 was the first device to obtain a FIPS 140-1 Level 4 validation, the highest level of commercial cryptographic certification currently available. Dyer and colleagues [48] presented a design retrospective of IBM's 4758 physically secure coprocessor for protecting both data and computation in potentially hostile environments. In addition to providing physical protection, it encompasses the equally challenging problems of securely downloading applications into the secure environment and remotely identifying and authenticating the embedded device.

However, having a cryptoprocessor does not mean that the system is safe. Work in [49] reported a protocol attack on the Dallas DS5002 series processors,

which use encrypted external memory. The attack can search through the range of encrypted instructions until an output instruction is recognised by its effects. This is then used to tabulate the encryption function. Bond and Anderson's paper [50] describes protocol flaws in the IBM 4758 secure coprocessor. These flaws make it possible to extract application secrets without actually opening the tightly sealed, FIPS-certified device. It demonstrated that a certified, physically secure device is not a security panacea. The article also pointed out attacks that exploit the mathematical properties of protocol flaws instead of the protocol implementation flaws.

Meanwhile, the ever-evolving POS security leads to a higher integration and flexibility trend of security systems: more and more peripherals, e.g. smart card readers and displays, need to be directly controlled by the core security unit, and their interfaces become part of the core security unit. However, the generic commercial CryptoProcessors are expensive and lack flexibility, e.g., most generic security processors lack smart card driving support, and in many cases, display driving support as well. Normally flexibility regarding the key size was not offered either.

2.3.2.3 Using FPGA to Improve Security

Many hardware security researchers have started to use FPGA (Field-Programmable Gate Arrays) [51][52]. FPGAs are hardware programmable platforms; they typically use program languages like Verilog or VHDL. Users can define a special hardware structure of CPU, memory and control circuits. Therefore, FPGA is a flexible platform to provide hardware arithmetic acceleration in many cryptographic applications. Their re-configurability means that they can be re-programmed to perform the more computationally intensive operations of a range of ciphers depending on security and application requirements.

Based on FPGAs, most of the published cryptography algorithms have been successfully implemented into hardware. The paper from Saggese et al. [53] detailed a tamper-resistant hardware accelerator for RSA. They successfully integrated an RSA processor and an RSA key-store on a Commercial Off-The-Shelf (COTS) programmable board. (Xilinx Virtex-E 2000 FPGA is mounted). Work in [54] showed how to implement Elliptic Curve Cryptosystems (ECC) into Xilinx XC4085XLA FPGA.

FPGAs, however, are more suitable for applications that are still in the prototype phase [25]. Compared to general embedded CPU or ASICs, they are still too expensive for mass production. FPGAs can improve the flexibility and can be a coprocessor to improve the security performance. Nevertheless, it is not suitable to create the generic core because the final size of the silicon is too large and the cost is too high. Tamper-detection sensors, like temperature sensors or X-ray sensors, cannot be embedded. Hence, the whole security system still needs an extra security package to protect the system.

2.3.2.4 Using Self-defined Core Security Architecture

In the current market, many payment device providers such as Ingenico and VeriFone have their own secure platforms including specific hardware architectures and corresponding operation systems in order to get more flexibility, higher security and reduced costs. Security platforms such as the Unicapt 32 of Ingenico and the VeriShield of VeriFone [55] belong to the core expertise of the companies. The generic RISC processor and memories are usually employed in these systems. A number of security protections are designed to thwart physical and logical attacks on the system. This may further include a coprocessor to remove the burden of

processing cryptographic operations from the main processor to improve the performance. The security system is packed in a security package to constitute a core security unit.

The typical structure of the core security unit consists of one (or more) printed circuit boards containing a processor, memories, a tamper-detective system and peripheral interfaces, among other components. All these security elements are placed together in an area covered by a flexible protection circuit. The protection circuit is made of a plastic foil with two-sided silver ink tracks; any break in the tracks will activate self-destruction. The whole core security unit is finally placed into a plastic package and filled with epoxy resin to ward off physical attacks.

The tamper-detective system embedded in the core security unit comprises several detectors to thwart various attacks. The normal monitored parameters are: (1) Low temperature (e.g. -50°C) and high temperature (e.g. 100°C). This is to prevent attackers from disabling the protection mechanisms by freezing or heating this unit. (2) Low battery voltage and high battery voltage. These measures can prevent the attacker disabling the protection mechanism by cutting or increasing the voltage. (3) External attacks, i.e. the signal from open-alarm switches. (4) Low frequency detector, etc.

Since the solution, which covers the core security components with an extra package, has the advantages of flexibility and relatively low cost, it would exist for quite some time before other revolutionary measures can be invented.

2.4 Implementation of Countermeasures

The security in a commercial terminal device design is a trade-off between the risk of fraud and the cost of security. In this section, some practical implementation of terminal security will be presented.

2.4.1 Hardware Implementation of Countermeasures

Two categories of protection are commonly used in the terminal, namely tamper-evident and tamper-responsive [57]. If a protective method can provide obvious evidence that an attack has been attempted, this method can be regarded as a tamper-evident countermeasure. A seal label of a carton is a common example of this, because the label will be damaged after the carton has been opened. As the label can be easily covered by another label or removed under very cold temperatures, it is not suitable for terminal security. It is important to note that both merchants and cardholders are not trained to identify tamper evidence, and it is not expected that there will be frequent inspections by a trained inspector. Therefore, only evidence that is very strong and obvious can be called tamper-evident. Merchants and cardholders can stop making further transactions after they recognise tamper evidence at the terminal. Another category of protection, i.e. tamper-responsive, involves actively detecting any penetration or unauthorised modification; this causes an immediate erasure of all keys and other sensitive data. Tamper-responsive protection must be triggered by direct attacks (penetration) and by equipment failure due to environmental conditions (extreme temperatures, power), whether deliberate or accidental. Both tamper-evident and tamper-responsive methods can be jointly implemented to protect the terminal.

Generally, in practice, physical damage to the top cover of the terminal case can be regarded as tamper-evident. Any damage to the case sides can be considered as tamper-evident too, if it was observable to the cardholder in its normal operation position. Applying this rule in design can save costs because it means less security countermeasures need to be implemented against the physical attacks from the top and two sides of the case. However, the top cover of the terminal cannot always be

regarded as tamper-evident. For example, if a terminal is covered with an extra decorative layer (a plastic piece printed with colour, text, etc.) over the top surface for product aesthetics or customisation, it poses security problems, because the adversary can remove the decorative layer and then cut the top case to access the inside of the terminal. After the attack, the adversary can put back the decorative layer on the terminal surface, and there will be no tamper evidence visible. Therefore, it is more prudent to avoid designs that put any extra layer over the keypad and display. If such a design is inevitable, the removal of the surface layer shall be made detectable, e.g. by adding a sensor.

Obviously any damage to the bottom part of the case cannot be considered as tamper-evident since cardholders cannot observe it. As a result, the attacks on the bottom sides must be prevented by tamper-response measures rather than tamper-evident measures.

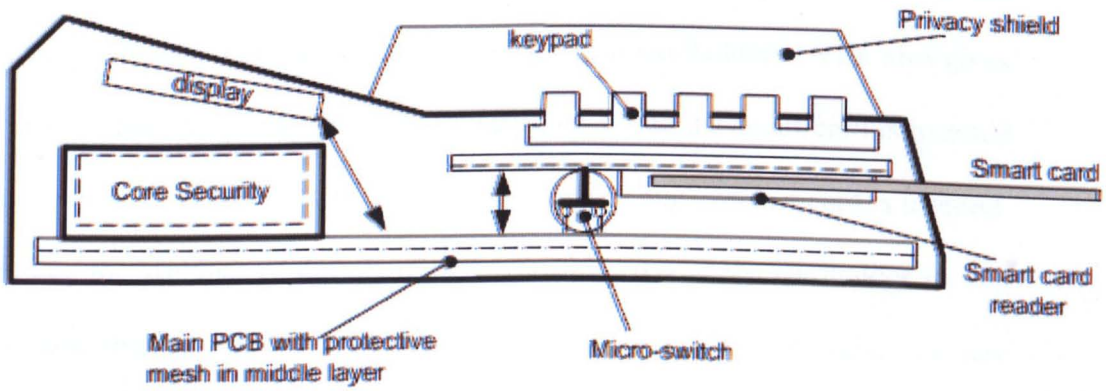


Figure 8: Lateral view of a classic terminal layout

Figure 8 is an example of the classic architecture of a terminal. The main PCB is deployed near the bottom of the case. There is an electric mesh hidden in the inner layer of the main PCB. Any drill or cut penetration will break the electric mesh which will cause a security alarm (tamper-responsive). Thus, the main PCB with

mesh constitutes a safe space over it. All security-relative components, including smart card reader, display and their corresponding connectors and cables, are located in this space. Furthermore, the connection of the cables is detectable. Removing cables from connectors will cause a security alarm.

Parts of the display signal lines are relatively easy for an attacker to access, e.g. accessing from the rear side, so the PIN can be recorded, since the keyboard signals and the display signals use the same bus lines. To prevent this attack, a bus controller (switch) is implemented to control the connection of the display data bus. With the help of this controller, the firmware can select whether those display signal lines are active or not during the PIN entry process.

There are several guidelines to be followed during terminal security implementation, as given in [20]. First, the shape of the case used to house the device's electronic components shall not be similar to commonly available products or commercially available components. This rule can increase the difficulty for the attacker to construct a duplicate terminal form to cheat cardholders. Visa also gives requirements. The slot of the smart card reader into which the smart card is inserted shall not have sufficient space to hold a PIN-disclosing "bug" when a card is inserted. The opening for insertion of the smart card is in full view of the cardholder so that any untoward obstructions or suspicious objects at the opening are detectable, e.g. any wires running out of the slot of the smart card reader to a recorder or a transmitter can be observed by the cardholder.

Second, inside the terminal, sensors must be properly deployed to detect the attack attempt of opening the case. For implementation, a wide range of sensors is available, including simple mechanical micro-switches, magnetic reed switches and permanent magnet actuators on mating surfaces, or rubber switches. Integrating the

open-alarm switches with a rubber keypad is the most popular solution. It is cost-effective and able to detect removal of external case screws or case opening.

An example is illustrated in Figure 8. On the reverse of the rubber keypad, apart from normal electric conductive tabs for numerical keys, there is an extra tab for security (which may be made of metallic materials to improve the stability). Correspondingly, several contact switches made up of copper tracks are on the keypad PCB. The security tab is pressed by the plastic case after the case is closed and the track switch is normally connected. Once the case is opened or the keypad is removed from the keypad's PCB, the security switch will be disconnected, and, in turn, it triggers a security alarm. However, such a detective switch is susceptible to short-circuiting by injecting silver ink through the rubber keypad with a needle. To prevent this kind of attack, the security switch on the PCB is surrounded with another circular track switch, which is normally open. The injected silver ink will overflow and connect the circular track switch, and then trigger a security alarm.

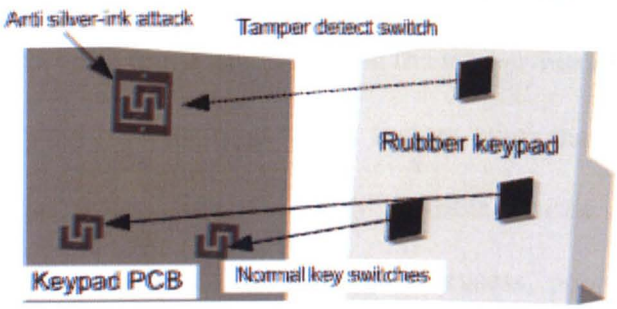


Figure 9: Integration of a tamper-detective sensor with a rubber keypad

If mechanical micro-switches are used to detect and trigger an alarm once the PCB is removed. Refer to Fig.8. Such alarm switches shall be placed far from the edges of the PCB as far as possible to increase the difficulty for attackers which may try to access and disenable the switches. A protective wall surrounding the switch shall be built to increase the difficulty of bypassing the switch.

All security components and routes must be limited to a small area on the top layer or inner layer of the PCB so that the sensitive signals cannot be measured from the bottom layer. Thus, it is a challenging job for PCB designers. The security system shall consist of SMD (surface-mounted device) components. For the multiple-layer PCB, different layers and the track routing techniques use vias to connect tracks in different layers. These vias have security risks, because the standard vias cross the PCB completely from the top layer to the bottom layer (unless using a non-standard and expensive PCB manufacturing process). Therefore, they are accessible at the bottom of the PCB. In order to decrease this risk, the vias can be hidden under IC packages at the bottom of the PCB so that the IC must be removed before the attacker can access the vias. Another solution is to create a track switch on the bottom layer of the PCB and hide the vias within the switch area, which is normally covered by conductive rubber. As a result, the rubber must be removed before the attacker can access the vias; nevertheless, the removal of the rubber will cause a security alarm. Meanwhile, this switch can be used as the case-opening alarm sensor.

Stability is another important issue regarding the tamper-response device. The phenomenon of the security system triggered by factors other than a real attack is called *false tamper detection.* There are many possible causes of false tamper detections: neutrinos, gamma ray or ESD; shocks in excess, poor design quality; quality problems during manufacturing. Any tamper-response device has the risk of false detections; they cause the terminal to be returned to the manufacturer and increase the cost. Hence, attention needs to be paid to how to reduce the occurrence of false alarms and improve the reliability of the tamper-detecting mechanisms.

2.4.2 Software Implementation of Countermeasures

Software security is as important as the hardware security measures. If untrustworthy software can be downloaded into the terminal and executed, the hardware and physical protections become useless.

Applications loaded into terminals are highly sensitive as they control most of the functionality of the terminal. Even in terminals where the majority of the security functionality is performed at the firmware level, certain application functions are inevitably security sensitive as well. These generally include prompting, selection of keys and protection against PIN-exhaustion attacks, etc. The software security control can be divided into two phases. The first phase is software development. The security is controlled by careful inspection and test during this phase. The second phase is to download the software into the terminal and execute it. During this phase, digital signature technology is employed.

As the terminal industry moves toward online security, software downloads and updates, and multi-application environments with payment, payment-related and non-payment applications are increasingly likely to run in the terminal, thus a systematic and flexible software authentication is required. For example, a chain of trust needs to be established, whereby the digital certificate that is used to verify the file is itself verified by the next digital certificate in the chain. This process continues all the way up to the "trusted root" certificate that is securely loaded into the terminal at its manufacturing facility.

The following describes an example of the software security control for the terminal prompt [56][57]. One characteristic of the software development in a secure terminal device is that the display message must be strictly controlled. Otherwise, the customer can be misled. The terminal prompt is a message appearing on the display

of a terminal that instructs the user of the terminal to perform a task. In particular, the PIN-entry message, e.g. "Please input PIN", is vitally important, because the cardholder will be instructed to input the PIN. This message can only be displayed when the terminal is in safe mode where all numeric digits are formatted into a PIN block that is then encrypted. To prevent unwanted messages from being displayed, prompt messages shall be encrypted and stored in advance and then be authenticated during calling. Furthermore, the highly sensitive PIN-entry prompts and other prompts (non-PIN-entry prompts) shall be encrypted using two different cryptographic keys. In this way, the non-PIN-entry prompts cannot be mixed with the PIN-entry prompt at the time of the PIN-entry process. Meanwhile, the non-PIN-entry prompt shall not contain a message that would cause a reasonable person to believe that it is appropriate to enter their PIN, e.g., "type PIN", "PIN Please", "Enter Secret Code".

Reviewers other than software developers shall carry out internal source code inspections. The reviewer shall verify that all required security functionality is implemented and that no unauthorised or fraudulent functionality is included. Examples of such functionality include back door access methods to code or data in the terminal, and disabling of security features such as PIN-exhaustion protection if the terminal receives a specific keystroke or input. The reviewer must also look for coding errors that can lead to problems. This includes buffer and stack overflows, and type checking. Once the software development process has been concluded, it is common that independent test institutes within the scope of a software evaluation examine the complete developed source code. The major reason for these timely and cost-intensive examinations is to exclude software faults. They also make it

impossible for a developer, for instance, to hide a Trojan horse in the application software.

Once the inspection of the submitted prompts is completed and any offending prompts are removed or suitably modified, the reviewer shall approve the set of prompts for signature, which will be verified by the terminal prior to execution of the application. Typically, two custodians (dual control) separately hold the signature key. Custodians shall verify the results again before they enter their key components into the signing tool for the prompts signature.

2.5 *Cryptography Algorithms and Security Standards*

Cryptography refers to encryption and decryption. Encryption is the process of converting ordinary plain information (plaintext) into unintelligible cipher text. Decryption is the reverse; in other words, it involves moving from the unintelligible cipher text back to plaintext. Cryptography is fundamental for secure communication, as well as for POS secure payment. In principle, all sensitive information between smart card, POS terminals and remote server shall be exchanged in an encrypted way, to prevent information disclosure. In this section, we review the implemented cryptography algorithms in a POS terminal. The applicable standards concerning POS terminal security are also investigated.

2.5.1 Cryptography Algorithms Used in POS

There are two types of algorithm used in cryptography: symmetric algorithm and asymmetric algorithm. Symmetric algorithm has the same key for both encryption and decryption. The calculation speed of symmetric algorithm is fast but it is difficult to exchange the key safely between communication parties. DES is the best-known

and most widely used symmetric algorithm in the world. The DES has a 64-bit block size and uses a 56-bit key during execution (8 parity bits are stripped off from the full 64-bit key) [60]. However, with ever-increasing computer power, 56-bit keys are too short and vulnerable to do an exhaustive search. To improve the DES security, it has become common practice to use Triple-DES with a double-length (16-byte) secret key.

The double-length-key Triple-DES encipherment algorithm (see ISO/IEC 18033-3) is the approved cryptographic algorithm to be used in the encipherment and MAC mechanisms. The algorithm is based on the (single) DES algorithm standardised in ISO 16609. Triple-DES encipherment involves enciphering an 8-byte plaintext block in an 8-byte ciphertext block with a double-length (16-byte) secret key $K = (K_L \| K_R)$ as Equation 2-1:

$$Y = DES3(K)[X] = DES(K_L)[DES^{-1}(K_R)[DES(K_L)[X]]] \quad (2\text{-}1)$$

Decipherment takes place as Equation 2-2:

$$X = DES^{-1}(K_L)[DES(K_R)[DES^{-1}(K_L)[Y]]] \quad (2\text{-}2)$$

The successor to DES can be AES (Advanced Encryption Standard). The AES algorithm based on the Rijndael algorithm was selected by NIST in October 2001 and the standard was published in November 2002. AES supports key sizes of 128 bits, 192 bits, and 256 bits [61][62]. In most circumstances, AES is faster than DES and about 2.5 times faster than Triple-DES [63][64]. The short AES key set-up time and its very low memory requirements make it well suited to restricted-space environments. More details of AES will be discussed in Chapter 3.

The asymmetric algorithm has a key pair (private key and public key). The encrypted information by one key can only be decrypted by the other, and vice versa. The most commonly used asymmetric algorithm is RSA. RSA's security hinges on the

difficulty of factoring an integer into primes [65]. The asymmetric algorithm is securer and easier for key exchange but the calculation is slower than the symmetric algorithm. In practice, asymmetric and symmetric encryptions are often jointly used. Following we briefly introduce the principle of the RSA algorithm [76].

The RSA key pair generation algorithm can be concisely presented as Table 2-1.

Table 2-1: Algorithm of RSA key pair generation:

Input: Security parameter l.

Output: RSA public key (n,e) and private key d.

1. Randomly select two primes $prime_1$ and $prime_2$ of the same bitlength $l/2$.
2. Compute $n = prime_1 prime_2$ and $\phi = (prime_1 - 1)(prime_2 - 1)$.
3. Select an arbitrary integer e with $1 < e < \phi$ and $\gcd(e,\phi) = 1$.
4. Compute the integer d satisfying $1 < d < \phi$ and $ed \equiv 1 \pmod{\phi}$.
5. Return (n,e,d).

RSA encryption use the fact that

$$m^{ed} = m \pmod{n} \tag{2-3}$$

for integers m,e,d.

Decryption works because of

$$c^d \equiv (m^e)^d \equiv m \pmod{n} \tag{2-4}$$

Therefore, the algorithm of RSA encryption and decryption can be presented as Table 2-2.

A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering. RSA is also the base of digital signature [65][67][72].

Table 2-2: Algorithms of RSA encryption and decryption

RSA basic encryption	RSA basic decryption
Input: RSA public key (n,e), plaintext $m \in [0,n-1]$. Output: Ciphertext c. 1. Compute $c = m^e \bmod n$. 2. Return (c).	Input: RSA public key (n,e), RSA private key d, ciphertext c. Output: Plaintext m. 1. Compute $m = c^d \bmod n$. 2. Return (m).

The algorithms of RSA signature and verification are presented in. The signer of a message m first computes its message digest $h = H(m)$ using a cryptographic hash function H, where h serves as a short fingperprint of m. Then, the signer uses his private key d to compute the eth root s of h modulo n: $s=h^d$ mod n. The signer tranmits the message m and its signature s to verifying party. This party then recomputes the message digest $h=H(m)$, revovers a message digest $h=s^e$ mod n from s, and accepts the signature as being valid for m provided that $h=h$. The security relies on the inability of a forger to compute eth roots modulo n [65][76].

Table 2-3: Signature generation and verification algorithms

Basic RSA signature generation	Basic RSA signature verification
Input: public key (n,e), private key d, message m. Output: Signature s 1. Compute $h=H(m)$ where H is a hash function. 2. Compute $s=h^d \bmod n$. 3. Return (s).	Input: public key (n,e), message m, signature s. Output: true or false of the signature. 1. Compute $h=H(m)$. 2. Compute $h'=s^e \bmod n$. 3. If $h=h'$ then true Else false.

Another public-key method is Elliptic Curve Cryptography (ECC), which is based on a discrete logarithm. It has gained popularity recently [54]. Compared with RSA, it appears faster and it uses smaller keys, while providing an equivalent level of security, for example, the encryption strength of 160 bit key ECC is equal to 1024 bit RSA. More details of ECC will be discussed in Chapter 5.

However, in the latest payment transaction specification EMV 4.2 [7], only RSA, DES/Triple-DES and SHA-1 are recommended as *proven algorithms*. Thus, they are the most common cryptographic algorithms used in the terminal.

Smart card transaction procedures can be outlined below according to EMV:

(1) Insert the card, select the application if multiple applications are supported.

(2) Authenticate the card (to check if the card has been manipulated).

(3) Verify the cardholder by checking the inputted PIN.

(4) Applications, Checks (Action Analysis, terminal risk management, possible issuer authentication).

(5) Close the transaction.

RSA is used in the step of card authentication and cardholder verification, if both the card and the terminal can support RSA. To prove that a card has not been modified after it has been issued, during the card manufacture, the card issuer takes some of the important data such as cardholder name and primary account number. The data are then encrypted using the private key of the card issuer [73]. The original and encrypted data are then stored on the card while the corresponding public key is released to banks/terminal manufacturers. During a transaction, the terminal reads the original data together with encrypted data from the card. Using the corresponding public key, the terminal decrypts the card data and compares it with the original data to make the decision. In this way, the fake and modified card can be detected.

As a further security measure, the public key is issued with hash values and an expiry date. The former is used to validate its accuracy while the latter is used to set an expiry date with the encrypted data. In case key validity fails, the transaction will be cancelled. Meanwhile, the length of the key will be increased periodically to meet the challenge of ever-increasing computer power. According to the key migration plan from Visa, currently a 1024 bits key is regarded as sufficient; after 2012, however, an 1152 bits key will be required and after 2016, a 1984 bits key will be required, and so on. Thus, the terminal security design must also consider the flexibility of key length and how to replace and update them in the field.

After the card authentication and the cardholder authentication have passed and a trusted channel is established, symmetric cryptographic algorithms are mainly employed to speed up the transaction. Data confidentiality is achieved using Triple-DES encryption of the data field. Triple-DES is also used in the encryption key derivation. Data integrity and issuer authentication are achieved by adding a MAC (message authentication code) to each message.

2.5.2 Security Standards related with POS Security

The smart card is becoming the number one payment card. In order to ensure that smart cards, smart card readers and smart card applications are interoperable, international standards are essential. Smart card standards originated from international standards organisations (ISO, CEN etc.). The basis is the ISO 7816 standard, which specifies physical and electrical characteristics as well as formats and protocols for information exchange between the smart card and the reader. The Comité Européen de Normalisation (CEN) is a European standard organisation. This organisation defines the CEN 726 standard - requirements for IC cards and terminals for telecommunications use [74][75]. Many standards have been developed, for financial security, especially. The government, private industry, and other organisations contribute to the vast collection of security standards. Standards related to the security of the POS terminal are listed in Table 2-4.

Table 2-4: Standards related to POS terminal security

Standards	Description
ISO 13491	Banking -- Secure cryptographic devices
ISO 9564	Banking -- Personal Identification Number (PIN) management and security
ISO 9596	Information technology -- Open Systems Interconnection -- Common management information protocol
ISO/IEC 9797	Information technology -- Security techniques -- Message Authentication Codes (MACs)
ISO 11568	Banking – Key management
FIPS 140	Federal Information Processing Standard

ANSI X3.92-FIPS 46 and ISO16609	Data Encryption Algorithm
ANSI X3.106-FIPS 81	Data Encryption Algorithm – Modes of Operation
ANSI X9.52	Triple Data Encryption Algorithm Modes of Operation
ANSI X9.9	Financial Institution Message Authentication

Based on international standards, many national and industry standards have been developed such as EMV, OpenCard Framework and JavaCard. EMV specification is a cooperative work of Europay, MasterCard and Visa, to offer common standards ensuring global interoperability between smart cards and payment terminals, regardless of the manufacturer, the financial institution, or where the card is used. Since 1992, the EMV has been continuously updated, and the latest version EMV 4.2 [7] was published in June 2008. Today it is one of the most important specifications in the POS payment industry. Now the global payment system is carrying out EMV immigration, which updates from the magnetic card to the smart card. From 2005 onwards, in order to stimulate the EMV implementation, schemes such as Visa and MasterCard no longer assume liabilities for fraudulent transactions if the payment devices are not EMV compliant.

2.5.3 Hardware Security Approval and Specifications

The history of the e-payment terminal is still less than 20 years old and there were no forced security certification requirements for terminal devices for a very long time. The security was determined and examined by the payment device manufacturers. Since security has become a crucial problem, today the situation has changed dramatically. Security approval and certification from authorised laboratories is now mandatory.

However, there are still no globally accepted physical security approvals for terminals. EMV standards and the above-mentioned security standards address very little about hardware security and terminal security. As a result, the security approval of the terminal is still left to card schemes (Visa, MasterCard, etc) and national organisations. Visa has a security approval program called Visa PED, which has a significant impact on terminal industries. Many countries have their own approval organisations such as ZKA in Germany, APACS in UK, and Interplay in the Netherlands. Among them, the ZKA is regarded as the strictest approval organisation in the field of payment device security.

In 2003, Visa announced that a terminal that accepts Visa cards must be approved and listed on its Visa PIN Entry Device Approval List after January 1st 2004. At the end of 2004, MasterCard and Visa jointly announced new aligned requirements for terminal devices: the brand new Payment Card Industry (PCI) program. The PCI program is similar in concept to the Visa PED program. However, there are significant hardware security requirements in addition to the Visa PED. The hardware security requirements for the PCI PED are similar to the ZKA requirements in Germany. From October 1st 2004, terminal device vendors must meet the PCI PIN pad security requirements. To date, the test laboratories evaluate the terminal according to the PCI requirements.

2.6 Summary and Identified Problems

This chapter has systematically undertaken a literature survey for the security system of POS payment devices. According to the different security requirement levels, we categorise attacks into two types: 1) PIN disclosure. This occurs in the peripheral layer consisting of terminal case, keypad, smart card reader and biometric sensors. These attacks are most common. 2) Key disclosure. The aim of such attacks

is to compromise the core security layer. Attacks and countermeasures around PIN and key disclosure, from simple to most sophisticated methods, are reviewed.

After investigation, we have identified several of the main challenges of the POS security system, which are outlined below:

- Two well-known but hard-to-solve threats: 1) inputting a PIN on a POS terminal can be peeked or recorded by a camera of adversary; 2) the cardholder can be easily misled by the information on a compromised or fake POS terminal.
- The most common attacks take place in the data-transferring channels of peripheral devices, such as the connecting cable of the PIN pad, the cable of the display or the cable of the fingerprint sensor. The smart card reader and its cable are susceptible to line-tapping attacks.
- The traditional PIN authentication is gradually becoming out of date. Biometrics like fingerprints can address some of the problems that exist in traditional PIN authentication, but it causes new challenges that the tradition system does not have. More biometrics need to be investigated to answer these challenges. For example, what kind of biometrics is suitable for a POS system? Can a multimodal biometrics be set up to enhance security? Can they been integrated with traditional PIN authentication?
- The key is the most sensitive information of cryptography. Most critical problems arise from the weak design of the tamperproof store unit of encryption keys. The high-intensive electromagnetic attack is a potential vulnerability.

- It is a challenging task to combine the advantages of different authentication methods comprehensively. A new, sophisticated information fusion and expert decision system need to be developed to meet the challenges of complex input information like fingerprints, PIN, stroke dynamics and risk level.

Chapter 3. The Proposed Supercard Scheme, Cryptography Algorithm and Key Unit Protection

Following the literature survey in Chapter 2, this chapter studies the new schemes and approaches to strengthen POS security. Research methodologies to address the identified problems are discussed. The Supercard scheme and security approaches based on the scheme will be illustrated. Their subsystems, i.e. PIN enhanced with biometrics and information fusion, will be further investigated in subsequent chapters.

3.1 Analysis of the identified problems

There are many challenges to solve the problems which have been identified in the previous chapter.

(1) Using a non-transparent privacy shield is probably the most popular method of preventing PIN disclosure through observations. However, all PINpad designers are being plagued by a dilemma: a lower visual shield is easier for operation and design, but it is not secure enough. A higher visual shield is more secure, but it makes the PIN input more difficult. Recently, for security reasons, the height of the privacy shield suggested by authorities has been constantly increasing. The latest suggestions are extremely strict. For example, refer to Figure 10, the privacy shield should build 270° horizontal and 45° vertical protection space which is measured from the middle of the keypad to the edge of privacy shield [56]. However, the manufacturers are struggling to keep up with user operation convenience and aesthetics. Meanwhile, this solution cannot eradicate many risks, such as line-tapping attack, for example. So today the question of how to prevent PIN disclosure by

observation has already become an impasse, and a new approach needs to be developed in the future.

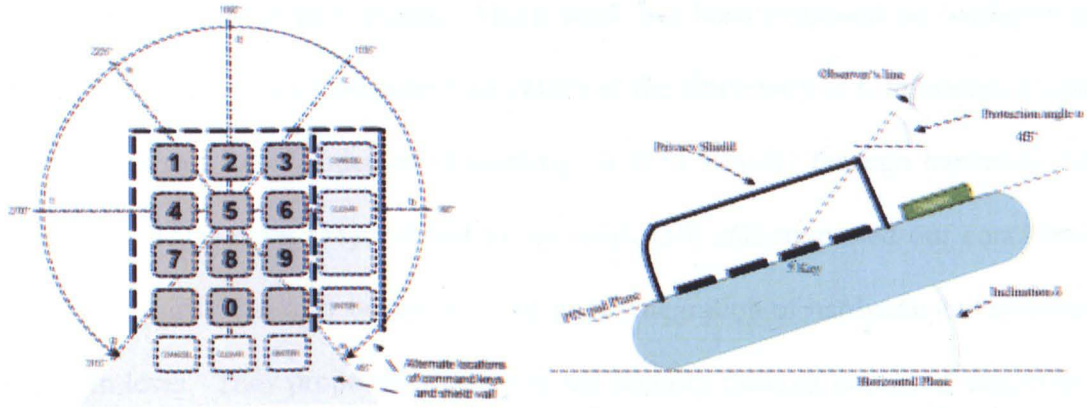


Figure 10: Guideline of building a privacy shield

More fundamentally, the risk of a physical replacement attack still exists. No matter how sophisticated the terminal security design is, a fake payment machine with the appearance of a real payment machine can be built and positioned by the attacker to cheat cardholders. If the customer inserts the card, the fake terminal will ask the cardholder to input the PIN. Since there is no signal to alert the cardholder, the common cardholder will follow the instruction and input the PIN. Straightforwardly, the PIN and some user information will be recorded by fake machines easily.

(2) To enhance the PIN or fingerprint security, a multimodal biometrics system can be setup. The comprehensive information can be processed based on the research results of information fusion.

(3) Due to the limitation of materials and cost, building a more sophisticated security package to protect the encryption keys in the terminal is becoming a very tough task for electronic and mechanical security engineers. An investigation needs to be carried out in the direction of new materials and mechanism.

Industrial and academic researchers have been trying to solve such problems. Visa, MasterCard and the leading POS providers, e.g. Ingenico, VeriFone, all have their own security research teams. Much work has been proposed on hardware or system solutions. In the Computer Laboratory of the University of Cambridge, a team led by Professor Ross Anderson is working on POS security through hardware and algorithms. Their work [58] referred to our work [10] and supported our conclusion that POS security can only be achieved by good integration of hardware and software at system level. They proposed to enhance the security through improved design and evaluation processes [58]. Killourhy et. al from Carnegie Mellon University tried to improve security through keystroke dynamics [59]. Besides the key typing rhythm, they also used cameras to analyse the finger motion. We try to solve such problems by integrating a PIN pad and biometrics with smartcard technologies.

3.2 Research Methodology

In order to address the identified problems, based on understanding the industrial and academic approaches and advanced technology available, a series of theoretical and experimental investigations are proposed.

- Study from system level all the possibilities to protect or shorten the signal-transferring channels.
- Investigate what kind of biometrics can be applied in POS and evaluate the performance individually. We have finally selected the fingerprint and keystroke dynamics as the two most suitable types of biometrics.
- Integrate different information to build a multimodal system, to check if the overall performance has been improved compared with the single modal system.

- Continual experimental assessments of system performance were made throughout the design process.

Principally and fundamentally, we have identified the radical problems of PIN disclosure that arose from two factors: the keypad is physically fixed with the terminal and the PIN is plaintext before it can be encrypted inside the core security unit. Thus, the whole PIN transmission channel has high probabilities of being attacked. In other words, if the PIN has already been encrypted before it is sent to the terminal, such problems can be prevented. Similarly, if the fingerprint sensor can be deployed elsewhere where it is more secure and easier to maintain, the biometric security can be enhanced. The above observations lead to the conclusion that the existing security structure can hardly meet the challenges it faces, and a novel security structure is expected.

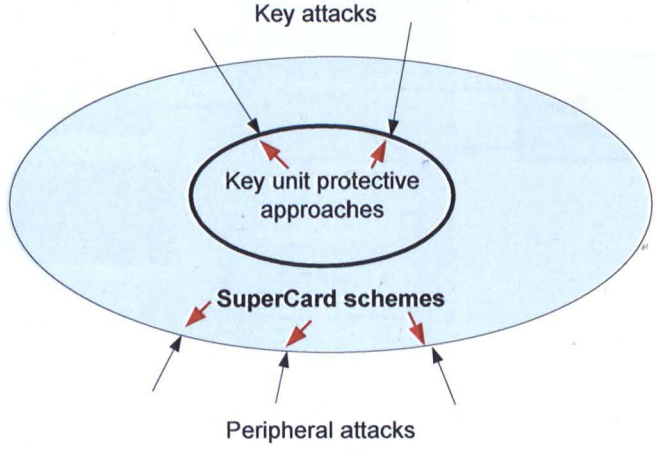


Figure 11: Supercard scheme and key unit protection

Thus, we designed a new scheme, called Supercard (as shown in Figure 11), to prevent attacks. This is based on a smart card, integrating biometrics and PIN pads. The Supercard scheme is devised to mainly defeat peripheral attacks and PIN disclosures. Meanwhile, approaches are proposed as key unit protections to defence

attacks on key and sensitive information. In the following sections, the Supercard scheme and key unit protections will be discussed.

3.3 The proposed Supercard Scheme

Based on the analysis results of the previous section and considering the aims and objectives of this research, the configuration of the proposed system is discussed as follows.

The main diagram of Supercard is illustrated in Figure 12. A PIN pad, a display and a fingerprint sensor are embedded together in the physical body of the smart card. Additionally, there is a slim battery embedded as a power supply. From a functional point of view, it is a miniature POS terminal.

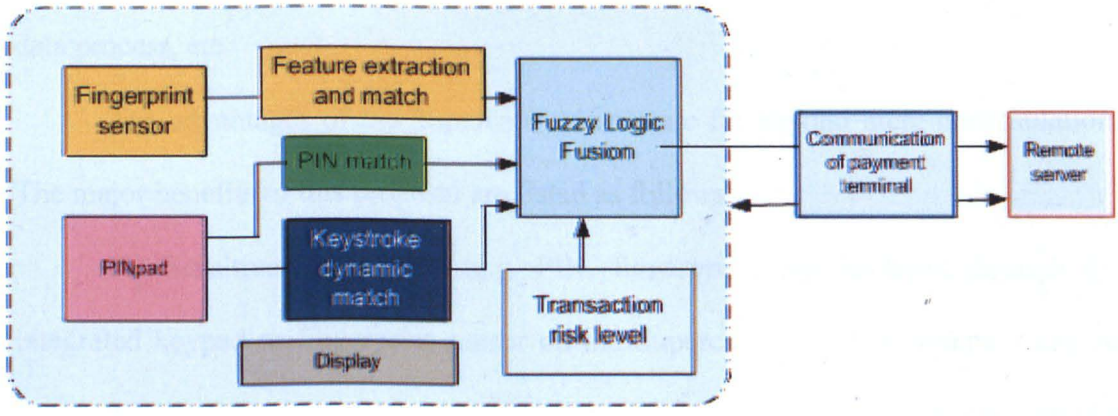


Figure 12: Main diagram of Supercard

For the simplicity of description, the system can be divided into three channels according to the different types of information. The first one is the fingerprint channel, consisting of a fingerprint sensor and the feature extraction of the fingerprint. The second one is the PIN channel, consisting of PIN pad and PIN match unit. The third is the keystroke dynamic channel, consisting of PIN pad and the keystroke dynamic match. The PIN channel and the keystroke dynamic channel have the same input device, i.e., a PIN pad. Each channel can be evaluated and experimented

individually. All signals from the different channels will be fused together through a comprehensive fuzzy-logic-based solution. More details of the channels will be investigated in the coming chapters. The fingerprint channel will be studied in Chapter 4. The PIN channel and keystroke dynamic channel will be investigated together in Chapter 5. The fuzzy-logic-based information fusion and decision-making will be studied in Chapter 6.

From a systematic point of view, the Supercard scheme encapsulates the traditional susceptible peripheral devices, such as keypad, display, sensor and all the connecting cables between them, into one closed mini smart card body. Correspondingly, such traditional "external" devices become the "internal" devices of a smart card. All communication between them can be done internally – for example, inputting the PIN, sending messages to the display, capturing the fingerprint and the data process, etc.

The advantages of the Supercard scheme are far beyond mere encapsulation. The major benefits of this proposal are listed as follows:

(1) Sensitive information (e.g. PIN, fingerprint) can be input through the integrated keypad or fingerprint sensor on the Supercard. Such information can be kept, encrypted, inside of the card temporarily. Meanwhile, the display on the Supercard can be used as a reliable interface to communicate with the cardholder. Such features can be used to find new methods in security applications. We will elaborate on these by way of case studies in Section 3.4.

(2) It increases the difficulty for channel and side channel attackers. In practice, most of the channel attacks are conducted by attackers through the installation of an electric bug or apparatus to the attacked object. A POS machine normally has a spacious plastic housing, which contains many PCBs, electric

components, etc. The wires linking the system components to each other can become potentially passive or active penetration routes. It is not difficult to find a small space in the terminal for installing an electric bug inside. In the Supercard, such typical channel threats can be eliminated. Meanwhile, the risk of being compromised through side channel attacks (crypto-analytical techniques through power, electromagnetic and timing analysis) is much lower because the power consumption and electromagnetic radiation of the Supercard is much less than the system of a conventional POS terminal.

(3) It distributes the security risk. The conventional POS terminal is fixed in one place. Once one terminal is compromised, all transactions through this terminal will be jeopardised. The Supercard scheme converts the fixed terminal into thousands or millions of "mini terminals" (Supercards) one of which is held by each cardholder privately. In a situation where one Supercard is compromised, other cardholders will be not affected.

(4) Better privacy protection. Nowadays, the fingerprint sensor is installed with the terminal machine. Although the terminal providers as well as the merchants declare, "We don't take your fingerprint images – only features", customers are unlikely to believe that when they see their fingerprints scanned by the terminal. In the Supercard, customers can input their fingerprints through their own card and the information can be pre-processed.

(5) Increased flexibility. A comprehensive authentication can be made as depicted in Figure 13. Principally, we can first classify different applications into several predefined levels according to various security requirements and transaction values. To easier the memorize of a PIN and maximum the user convenience, the author even thinks to bring the concept of PIN fuzzy match in future research. For

example if the user wants to pay a small amount of transaction like park fee, if 70% PIN numbers are matched correctly (instead of traditional 100% PIN match), the transaction can be still completed. Finally, the system will select authentication factors and set varies threshold values of the similarity degree to make the final decision. Details of this topic will be discussed in Chapter 6.

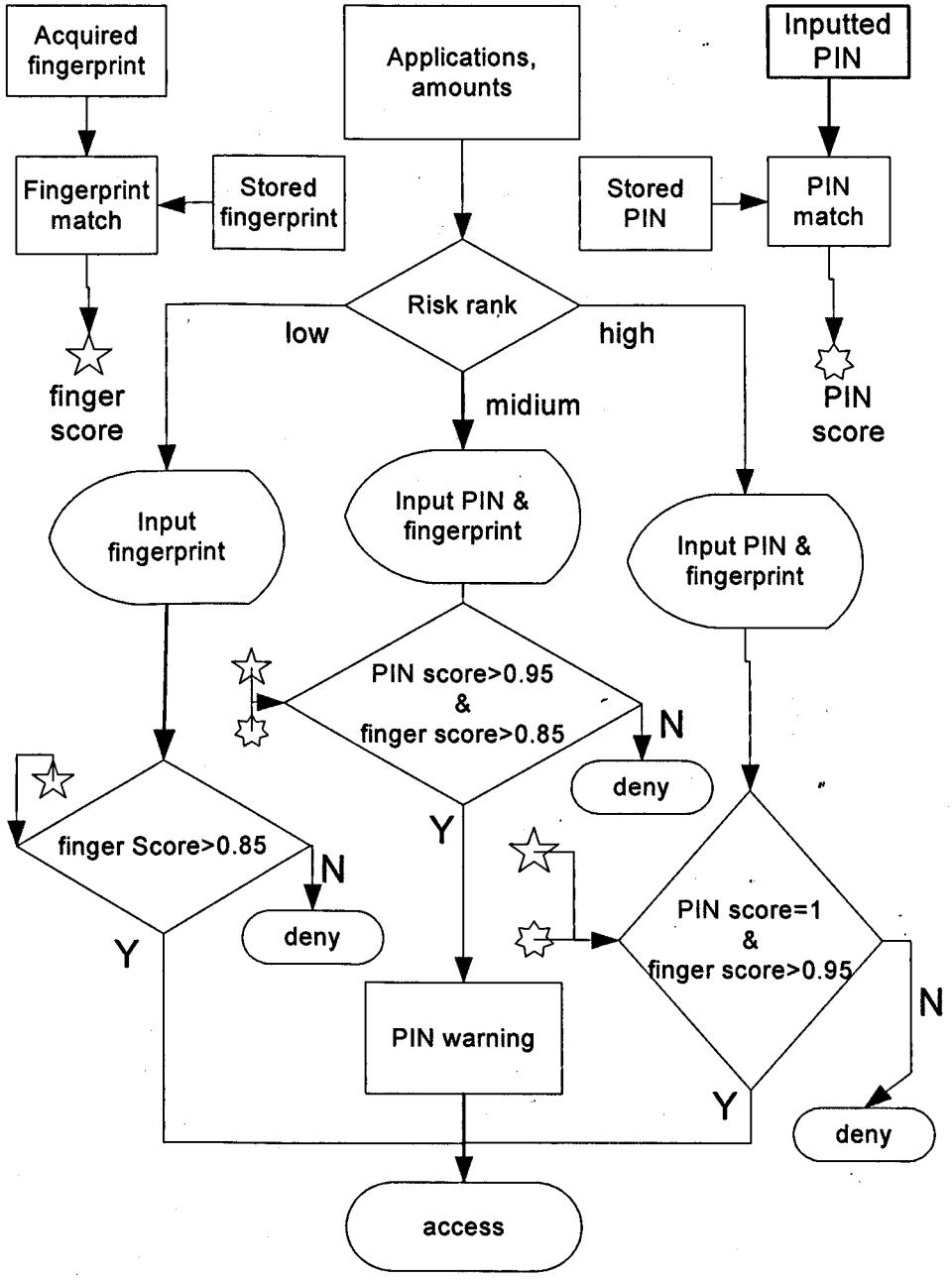


Figure 13: Supercard multiple authentication scheme

3.4 Supercard Case Studies

To better understand the advantages of the Supercard scheme which are outlined in Section 3.3, several case studies will be presented in this section, namely the PIN Medium, the Message Verifier, the Detector of Fake or Compromised Terminals, and the Tool with Multimodal Authentication. The Supercard can work in different applications and meet different security requirements.

One simulation image of the Supercard scheme is referred to in Figure 14. The keypad and the display on the card are deployed vertically to make it easier to hold. The fingers and palm can be used as a privacy shield to break the view line of other people.

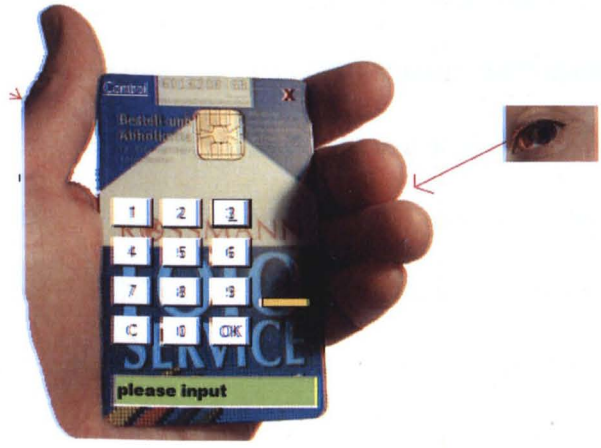


Figure 14: The embodiment of the Supercard

3.4.1 Case Study: PIN Medium

This case is envisaged to show the ability of using the Supercard to replace the conventional method of PIN inputting through the terminal PIN pad. The scenario is as follows: before the transaction occurs, the cardholder can input the PIN through the keypad on the Supercard in any place he/she feels safe; in turn, the PIN will be

encrypted and temporarily kept in the card. As additional security measures against PIN disclosure in a stolen Supercard, after the PIN is inputted and activated, if the PIN data is not read by the POS terminal, it will be deleted automatically in a predetermined time (e.g. 20 minutes). After the user brings the Supercard to the POS terminal location and inserts the card into the terminal, the encrypted PIN can be sent out for authentication [22][23].

This method can solve several fundamental security challenges in the traditional POS terminal. First, it can avoid the inputting of the PIN on a fixed POS device being observed or recorded by a camera of adversary. This is a traditional security issue but one that is but very difficult to solve. The feature of mobility of the Supercard scheme enables the cardholder to input his/her PIN on the Supercard in a safer and private space other than the fixed payment machine location. Secondly, since the keypad and the crypto unit are located together in the Supercard scheme, the connection cable between them is very short and protected by the very slim body of the Supercard (<0,8mm). It can prevent most PIN attacks, which normally can happen on a traditional POS PIN pad. Thirdly, the Supercard is normally always in the possession of the cardholder, so the cardholder will be aware of physical attacks on his card. Thus, to some extent, the Supercard is also a tamper-evidence device in this case.

Another big advantage of this proposed approach is that it can be implemented into a current POS system by modifying the authentication protocol and some software. All current POS terminals can still be used.

3.4.2 Case Study: Message Verifier

In a POS terminal, all messages shown on the display must be strictly examined and controlled, especially messages such as PIN prompt, transaction

amount, transaction results as these contain very sensitive information. Otherwise, the cardholder can be easily misled. For example, once the display of the POS device is compromised, the adversary can manipulate the message and give a message of "please input your PIN" at an unsecure stage, then he can record the PIN. Alternatively, the adversary can falsify the transaction amount, which is shown in the terminal display.

Therefore, in a POS terminal, the display belongs to important peripherals, which must be protected by hardware and software measures. The message contents are filtered and checked by the security unit. Although many efforts have been made regarding security design, as we explained in Section 2.2.1, such traditional protection measures are still not strong enough to defeat attackers. Display message protection is one of the weak points of terminal security.

The Supercard can be used as a "verifier" to solve the difficulty of display message protection. One example is illustrated in Figure 15. Let us assume the display of the terminal is manipulated by an attacker. The attacker sets 28.50EUR as the transaction amount. However, the display shows a fake message, e.g. "5.21EUR". The user will believe everything is normal and correspondingly give the PIN and confirm this transaction. Thus, this transaction will be done as 28.50EUR instead of 5.21EUR, and the user will be cheated. If similar scenarios take place with Supercard users, the Supercard will be able to check the real amount because the security unit in the Supercard will check and show the message on the card display as "28.50EUR". Once the user sees the different messages (for example, the terminal display shows "5.21EUR" but the Supercard display shows 28.50EUR), he/she will not continue this transaction.

Meanwhile, once the Supercard has detected that the communicating terminal was compromised, it will show a warning message on the card display to suggest that the user stops the transaction.

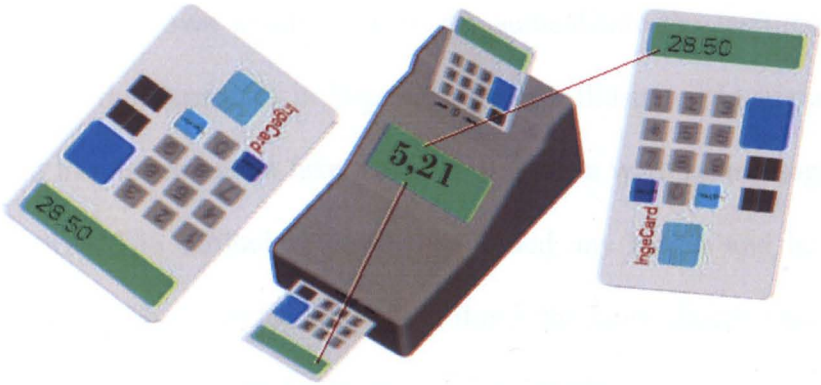


Figure 15: Message verifier and how it adapts to different insertions

3.4.3 Case Study: Detector of Fake or Compromised POS Terminals

There is one type of replacement attack on POS terminals, and it is called a fake terminal. This means that the adversary can build a fake device, which looks like a POS terminal, and put it in some locations. The display shows something like "Welcome to use card payment". After the cardholder inserts the card, the display will show "please input your PIN" etc. Since this terminal is actually fully under the control of the adversary, the inputted PIN or other information of the card can be stolen. Similar scenarios can also happen to compromised POS terminals.

Building such fake terminals does not require high technology and deep understanding of security technologies. Many common adversaries can build them with low costs. However, so far there are no effective technical measures to prevent such attacks. The card issuers or banks can only give warnings such as "do not use

your card on unsecured terminals". However, the cardholders cannot distinguish whether this terminal is a fake one.

The Supercard scheme can address this security vulnerability. Because the Supercard has its own crypto unit, it can authenticate the legitimacy of the POS terminal that the Supercard is inserted into. As illustrated in Figure 15, once the Supercard has determined a fake terminal, it gives a warning message on its display immediately. The cardholder cannot be fooled any longer and he can report the incident to the police. So far, we believe this is the most effective action against fake terminal attacks or other hardware replacement attacks.

3.4.4 Case Study: Tool with Multimodal Authentication Enhanced with Biometrics

Security systems can be categorised by factors or the number of different ways that a user is authenticated before being allowed access. As a well-known principle in security, two-factor security relies on something you alone have (e.g. a card) and something you alone know (e.g. a PIN), which is more secure than just one factor. You already use it when you get cash from an ATM machine, where the combination of the bankcard and your PIN identifies you in two ways. Security companies are also keen to promote an even more secure system known as three-factor security, which includes biometric identification to check something related to who you are, alongside what you have and know.

Actually, different applications request different authentication levels. For example, in payment application of a car parking fee, which typically amounts to several Euros, fingerprint verification is sufficient. In the case of payment for a €1000 computer, the fingerprint and the PIN need to be verified together.

In the Supercard scheme, keypad and fingerprint sensors are embedded together. Furthermore, a multi-biometrics authentication can be conducted in the Supercard scheme. Moreover, the fingerprint and the keystroke pattern (how the cardholder inputs the PIN) can also be authenticated as a behaviour biometrics factor. This is known as keystroke dynamics. There are many combination possibilities: fingerprint alone, PIN alone, fingerprint and PIN, PIN and keystroke dynamic, etc. Details will be investigated in Chapter 4 and Chapter 5.

The typical scenario for fingerprint verification is: during the transaction, the cardholder swipes the finger through the sensor, which is embedded in the Supercard. In turn, the fingerprint can be processed and authenticated directly inside the Supercard. Alternatively, depending on the implemented CPU and memory in the Supercard, if such hardware sources are limited, the fingerprint can be temporarily kept in the card. The encrypted fingerprint information can be sent out to the card reader or the remote server for minutiae extraction. The details will be encrypted again and sent back to the Supercard for authentication.

The Supercard authentication protocol can be described as Table 3-1. The Supercard issues a fresh nonce N_{sc} and sends the certificate for server authentication. The server sends back the agreed session key. The server can extract a fingerprint template, $Template_{live}$, from the received image before sending it to the Supercard for match. The keys K_{SV} and K_{SV}^{-1} are the public key and private key of the remote server respectively.

Table 3-1: The proposed Supercard authentication protocol

Supercard → Server:	$\{N_{sc}, Certificate_{sv}\}K_{SV}$
Server → Supercard:	$\{N_{sc}, K_{sess}\}K_{SV}^{-1}$

Supercard → Server:	$\{ N_{sc,}\ Fingerprint_{image} \}K_{sess}$
Server →Supercard:	$\{Hash(Template_{live}\}K_{sess}$
Supercard → Server:	*Accept / Deny*

3.5 Selection of Cryptography Algorithms

Cryptography is the base of POS security. The objective in this section is to identify cryptography algorithms, which are more suitable for the Supercard scheme.

In Section 3.3, we have briefly described the authentication involved with encryption/decryption. Currently, two cryptography algorithms are widely used in POS terminals. RSA is used as an asymmetric algorithm and DES as a symmetric algorithm for encryption/decryption. However, they are gradually becoming less able to meet today's security challenges. In this section, we investigate the cryptographies of ECC and AES, which could be more suitable for the Supercard scheme. First, we provide some background information on these two cryptography algorithms, and later a comparison will be conducted.

3.5.1 Elliptic Curve Cryptography

Let p be a prime number, and let F_p denote the field of integers modulo p. An elliptic curve E over F_p is defined by an equation of the form

$$y^2 = x^3 + ax + b \qquad (3\text{-}1)$$

where $a, b \in F_p$ satify $4a^3 + 27b^2 \neq 0 \pmod{p}$. A pair *(x,y)*, where $x, y \in F_p$, is a point on the curve if *(x, y)* satisfies the equation (3-1). The point at infinity, denoted by ∞,

is also said to be on the curve [65]. The set of all the points on E is denoted by $E(F_p)$. Figure 16 shows two examples of elliptic curves [76].

The assumed difficulty of several problems related to the discrete logarithm in the subgroup of $E(F_p)$ allows cryptographic use of elliptic curves [77]. Most of the elliptic curve cryptographic schemes are related to the discrete logarithm schemes, which were originally formulated for the usual modular arithmetic. The most popular is the Elliptic Curve Diffie-Hellman (ECDH) key agreement scheme which is based on the Diffie-Hellman scheme. ECDH is a key agreement protocol that allows two parties, each having an elliptic curve public-private key pair, to establish a shared secret over an insecure channel.

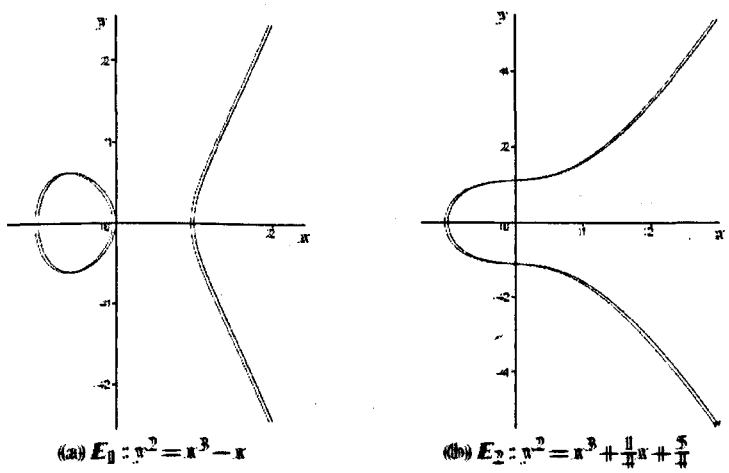


Figure 16: Elliptic curves over R

The key pair of elliptic curve cryptography can be generated as following. Let P be a point in $E(F_p)$, and suppose the P has prime order n. Then the cyclic subgroup of $E(F_p)$ generated by P *is*

$$< P >= \{\infty, P, 2P, 3P, ..., (n-1)P\} \tag{3-2}$$

A private key is a integer d that is selected uniformly at random from the interval $[1, n-1]$, and the corresponding public key is $Q = dP$.

The elliptic curve encryption scheme can be briefly presented as following [65]. A plaintext m is first represented as a point M, and then encrypted by adding it to kQ where k is a randomly selected integer, and Q is the intended recipient's public key. The sender transmits the points $C_1=kp$ and $C_2=M+kQ$ to the recipient who use her private key d to compute

$$dC_1=d(kP)=k(dP)=kQ \tag{3-3}$$

and thereafter recovers $M=C_2-kQ$.

Table 3-2: Algorithms of elliptic curve encryption and decryption

Encryption	Decryption
Input: Elliptic curve domain parameters *(p, E, P,n)*, publick key *Q*, plaintext *m*. Output: Ciphertext (C_1, C_2).	Input: Domain parameters *(p, E, P,n)*, private key *d*, ciphertext (C_1,C_2). Output: Plaintext *m*.
1. Represent the message *m* as a point *M* in $E(F_p)$. 2. Select $k \in_R [1,n-1]$ 3. $C_1=kP$, $C_2=M+kQ$. 4. Return (C_1, C_2).	1. Compute $M=C_2-dC_1$. 2. Extract m from *M*. 3. Return *(m)*

3.5.2 AES Cryptography

Each AES cipher has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. Considering the limitation of the computer power in the Supercard, we will only take the key sizes of 128 bits in our system [122].

The AES algorithm is divided into four different phases, namely SubBytes, ShiftRow, MixColumn and AddRoundKey, which are executed in a sequential way

forming rounds. The encryption is achieved by passing the plain text through an initial round, nine equal rounds and a final round. In all the phases of each round, the algorithm operates on a 4×4 array of bytes (called the State). In Figure 17 we can see the structure of this algorithm [78].

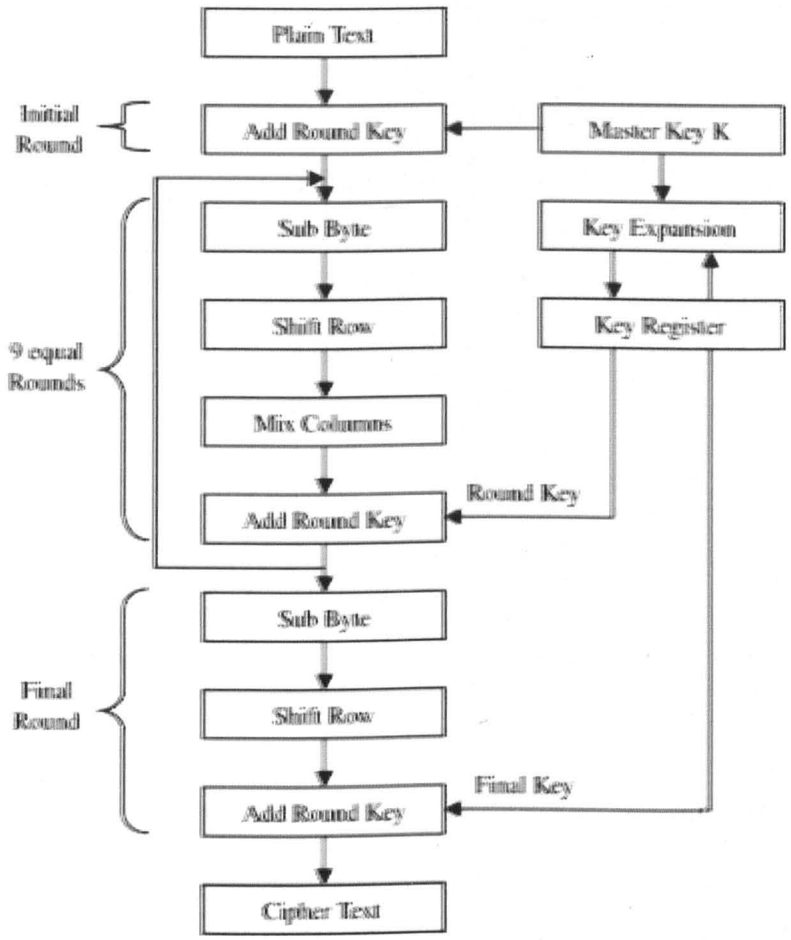


Figure 17: Structure of the AES algorithm

The first is a SubBytes process. The inputted plaintext will be separated into 128 bytes segments, each segment is arranged in a rectangular array known as a State.

The SubBytes transformation is a non-linear byte substitution that operates independently on each byte of the State using a substitution-predefined table known as an S-box. The S-box is constructed by composing two transformations. First, take

the multiplicative inverse in the finite field GF(2^8), and the element {00} is mapped to itself. Then, apply the following affine transformation over GF(2) [122]:

$$b_i = b_i \oplus b_{(i+4) \bmod 8} \oplus b_{(i+5) \bmod 8} \oplus b_{(i+6) \bmod 8} \oplus b_{(i+7) \bmod 8} \oplus c_i \tag{3-4}$$

For $0 \le i < 8$, where b_i is the i^{th} bit of the byte b, and c_i is the i^{th} bit of a byte c with the value $\{01100011\}$. Here and elsewhere, a prime on a variable indicates that the variable is to be updated with the value on the right.

In matrix form, the affine transformation element of the S-box can be expressed as [78]:

$$\begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \tag{3-5}$$

In the `ShiftRows` transformation, the bytes in the last three rows of the State are cyclically shifted over different numbers of bytes (offsets). The first row, $r = 0$, is not shifted. Specifically, the `ShiftRows` transformation proceeds as follows:

$$s_{r,c} = S_{r(c+shift(r,Nb)) \bmod Nb}' \text{ for } 0 < r < 4 \text{ and } 0 \le c < Nb, \tag{3-6}$$

Where the shift value $shift(r, Nb)$ depends on the row number, r, as follows (recall that Nb=4): $shift(1,4)$=1; $shift(2,4)$=2; $shift(3,4)$=3.

The `MixColumns` transformation operates on the State column by column, treating each column as a four-term polynomial. The columns are considered as

polynomials over GF(2^8) and multiplied modulo $x^4 + 1$ with a fixed polynomial $a(x)$, given by:

$$a(x) = \{03\}x^3 + \{01\}x^2 + \{02\} \tag{3-7}$$

This can be written as a matrix multiplication. Let $s'(x) = a(x) \otimes s(x)$:

$$\begin{bmatrix} s'_{o,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{o,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix} \quad \text{for } 0 \le c < Nb \tag{3-8}$$

Because of this multiplication, the four bytes in a column are replaced by the following:

$$\begin{aligned} s'_{0,c} &= (\{02\} \bullet s_{0,c}) \oplus (\{03\} \bullet s_{1,c}) \oplus s_{2,c} \oplus s_{3,c} \\ s'_{1,c} &= s_{0,c} \oplus (\{02\} \bullet s_{1,c}) \oplus (\{03\} \bullet s_{2,c}) \oplus s_{3,c} \\ s'_{2,c} &= s_{0,c} \oplus s_{1,c} \oplus (\{02\} \bullet s_{2,c}) \oplus (\{03\} \bullet s_{3,c}) \\ s'_{3,c} &= (\{03\} \bullet s_{0,c}) \oplus s_{1,c} \oplus s_{2,c} \oplus (\{02\} \bullet s_{3,c}) \end{aligned} \tag{3-9}$$

In the `AddRound` transformation, a Round Key is added to the State by a simple bitwise XOR operation. Each Round Key consists of *Nb* words from the key schedule. Those *Nb* words are each added into the columns of the State, such that

$$[s'_{0,c}, s'_{1,c}, s'_{2,c}, s'_{3,c}] = [s_{0,c}, s_{1,c}, s_{2,c}, s_{3,c}] \oplus [w_{round+nb+c}] \quad \text{for } 0 \le c < Nb \tag{3-10}$$

where $[w_i]$ are the key schedule words and *round* is a value in the range $0 \le round \le Nr$. In the Cipher, the initial Round Key addition occurs when $round = 0$, prior to the first application of the round function. The application of the `AddRoundKey` transformation to the *Nr* rounds of the Cipher occurs when $1 \le round \le Nr$ [122].

For the key length of 128 bits, 10 rounds need to be done and each round uses a different key, which is expanded. The final round does not include the MixColumns.

3.5.3 Algorithm Comparison

Compared with RSA and Triple-DES algorithms, the ECC and AES algorithms have advanced features, which can be outlined as below.

- Less Memory and space requirement.

Both ECC and AES have advantages in terms of resource requirements. The ECDLP (elliptic curve discrete logarithm problem) algorithm of ECC leads to a very strong security with relatively small keys. When the key becomes smaller, the memory needed to store the keys is smaller.

An RSA chip designed to do modular multiplication of 512-bit numbers has about 50,000 transistors, while a chip designed to perform arithmetic has about 100,000 transistors [34]. With the current technology, these devices are too large to be placed on a smart card. By comparison, a chip designed to do arithmetic in F_{2m} (the basement of ECC), where m is about 200, would have less than 15,000 transistors, and would occupy about 15% of the 25 mm^2 area assigned for the processor. Another advantage to be gained by using elliptic curves is that each user may select a different curve E, even though all users use the same underlying field K [106]. Table 3-1 is from Certicom [107], and compares the size of the system parameters and selected key pairs for the different systems.

Table 3-3: Space requirement of RSA and ECC key

	System parameters (bits)	Public key (bits)	Private key (bits)
1024-bit RSA	n/a	1088	2048
160-bit ECC	481	161	160

- Higher Security Level

ECC is becoming more popular because of the reduced number of key bits required in comparison to other cryptosystems (for example, a 160-bit ECC has roughly the same security strength as 1024 bit RSA). Meanwhile the AES uses

128/192/256 bits keys, so it is much harder to crack than its predecessor DES that is only 56 bits. Table 3-2 compares the different key size in RSA and ECC.

Table 3-4: Key size: Equivalent strength comparison

Time to break (in MIPS years)	RSA key size (in bits)	ECC key size (in bits)	RSA/ECC key size ratio
10^4	512	106	5 : 1
10^8	768	132	6 : 1
10^{11}	1024	160	7 : 1
10^{20}	2048	210	10 : 1
10^{78}	21000	600	35 : 1

- Lower Computing Processing Required

ECC reduces the processing times very much because of the nature of actual computations (especially in the case of GF(2^k) where there are no modular operations). Other systems normally need a dedicated crypto coprocessor to do the computations. The coprocessor has the problem of increasing both the area and the cost. In the case of ECC, the algorithm can be implemented in the available CPU with no additional hardware.

Therefore, we decided to use ECC and AES cryptographies in the Supercard applications. In the applications, as illustrated in Figure 18 [107], ECC is used as the key agreement between the Supercard and remote server through the communication model of the POS terminal, or it is used in the key generation. AES is employed as the symmetric key cryptography for fast secure data communication, after the key is determined by the ECC.

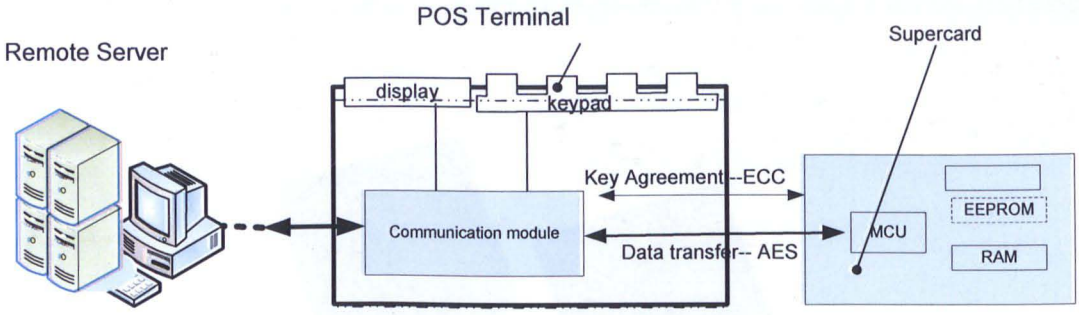


Figure 18: ECC and AES cryptography in the Supercard

3.6 Approaches to Protect the Key Unit

As identified in Chapter 2, the hardware design of a tamper-proof key store unit is the weakness of the current POS terminal. The key is the most sensitive information in cryptography. The Supercard scheme presented in this chapter mainly protects against peripheral attacks and PIN disclosure. In order to enable the mutual authentication between the POS terminal and the Supercard, the POS terminal still needs a crypto-unit to conduct the encryption and decryption. That means the crypto-key store unit in the traditional POS terminal still needs to be protected, even in the Supercard scheme. As investigated in Section 2.3, most critical problems arise from the weak design of the tamperproof store unit of encryption keys. Differing from the common current countermeasures, which have been investigated in Section 2.3.2, in this section, we suggest several practical methods on how to improve the security of key store units from a hardware point of view.

3.6.1 Security Chips Built with BGA Package

More and more large-scale integrated circuits use the BGA (Ball Grid Array) package. Unlike common IC packages such as SOP (Small Outline Package) and QFP (Quad Flat Package) where pins are deployed along the chip boundaries only, BGA packages lay out the pins in a grid format on the back of the package. The BGA

package can be made with a large number of high-density pins, thus it offers dramatic board area savings.

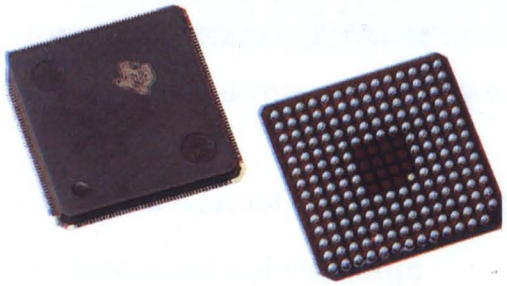


Figure 19: Illustration of a BGA package

We suggest applying the concept of BGA to protect the crypto-processor and key unit. For security applications, the more interesting BGA feature is that some security-sensitive pins can be "hidden" in the central area under the chip (refer to Figure 20). The crypto-processor and the key unit are integrated together and encapsulated into one BGA package. In the package, one protective layer can be built by utilising some available semiconductor technologies. The most security-sensitive pins are deployed in the central area. Meanwhile, in the multiple-layer printed circuit board side, a protective layer (detective mesh as described in Section 2.3.2) is integrated to protect penetration from beneath. All security-sensitive lines are deployed under the PCB protective layer. Finally, after the BGA package is soldered with the top side of PCB, the security sensitive pins and lines become very difficult to access from outside. Thus, many intrusive attacks on key disclosure can be prevented by this scheme.

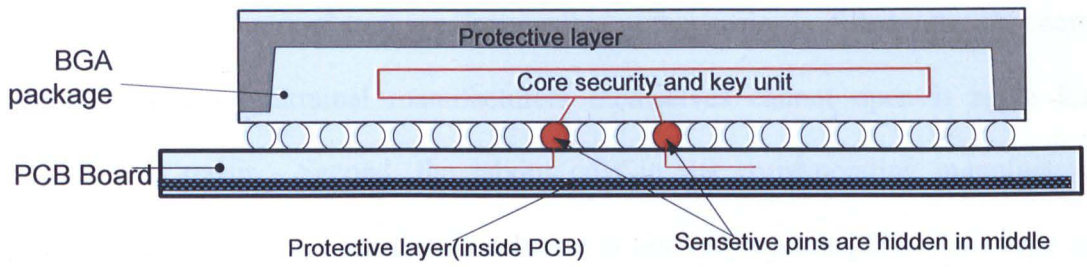


Figure 20: The suggested BGA-based security package

3.6.2 Ceramic-based Tamperproof Package

The construction of a suitable security package to protect sensitive data is a long-term expectation in the security device industry. In 1996, Clark [28] also explicitly emphasised the necessity for new security package research and this was his major conclusion after his security survey. The explosive growth of POS schemes has led to research in the area of low-cost tamper resistant modules but with high security. Either the unit cost is so low that the secure components can be thrown away if they fail, or the tamper resistant mechanisms are reusable, allowing their return to the factory for maintenance. Unfortunately, so far there is still no breakthrough in this field. The research on a new electromechanical tamperproof package is still quite a meaningful job.

The security of the core unit can be improved by putting all high security components into one chip (an all-in-one solution) and protecting this chip by using the latest microelectronic technologies, e.g. the BGA package, as presented in the last section. However, from another side, the one-chip solution means inevitably losing much flexibility. It can be hard to synchronise with ever-evolving security requirements as well as various customer demands. The huge R&D cost of the large ASIC is not affordable for small terminal providers.

In the current POS design (refer to Section 2.3.2), usually the epoxy resin is used to fill in the security package. This epoxy method has big disadvantages: first,

the manufacturing procedures are irreversible; after resin is filled into the core security unit, even terminal manufacturers themselves cannot open it again for inspection or repair. Second, the labour cost in the corresponding manufacture procedures is expensive. Third, this solution is not very secure [28]. This type of package cannot stand X-ray, electromagnetic attack, and the epoxy resin can be melted or removed by some chemical methods or advanced tools.

To address the challenges of the security package, here we propose a ceramic-based solution (refer to Figure 21). The package is made of high-purity 99.8% aluminium oxide ceramic. The inner surface of the package is fully printed with electric conductive wires. The wires constitute a protection mesh. Once one wire is broken, the alarm system will be triggered. The ceramic has features of high hardness, fragility and electric isolation. It can stand many physical and chemical attack methods.

Compared with the current resin-filled solution, this proposed ceramic package has many advantages: 1) It is more difficult to attack. 2) It is reusable. Since no resin filling is required, the ceramic package can be removed by the manufacturer to repair some security components. 3) It is cost-effective. Assembling the ceramic package on a printed circuit board is easier than assembling a traditional one.

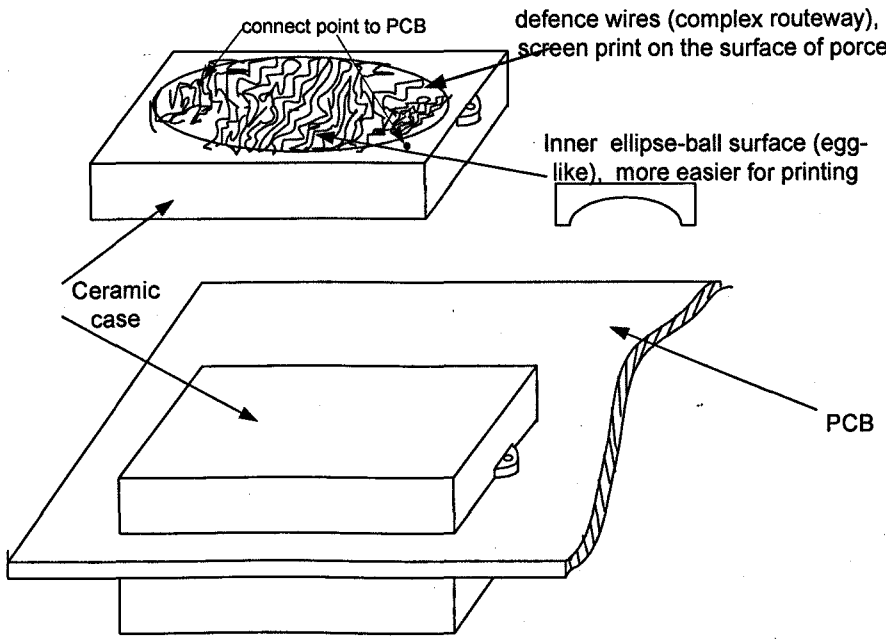


Figure 21: Ceramic-based tamperproof package

3.6.3 The Potential Electromagnetic Vulnerability

In this section, we want to introduce a concern about the potential for high-intensive electromagnetic attacks. As discussed in Section 2.2., the electromagnetic radiation of a security system can be measured by an attack to disclose security information. Actually, the electromagnetic radiation is a question with a dual character. On the one hand, electronic devices will emit electromagnetic radiation to the outside; on the other hand, the electronic devices are sensitive to electromagnetic disturbances from outside, too.

Radio Frequency Interference (RFI) can induce unwanted currents, which cause various disturbances. In addition, current high-performance integrated circuits (ICs), such as microprocessors, have very small feature sizes and are clocked at frequencies well into the GHz range while operating at reduced voltage levels. Although this has improved the ability and performance of modern systems, it has also increased their susceptibility to RFI [42]. Figure 22 shows an example. The transient spikes in the data input to the latch (the D signal in the diagram) are not

transmitted to the latch's output. The latch's internal state and thus its output will be whatever data value is seen at the latch's input during the shaded window surrounding a rising clock edge. Setup and hold time violations cause the latch to become metastable, in which the latch's state becomes undefined for an undefined length of time [42].

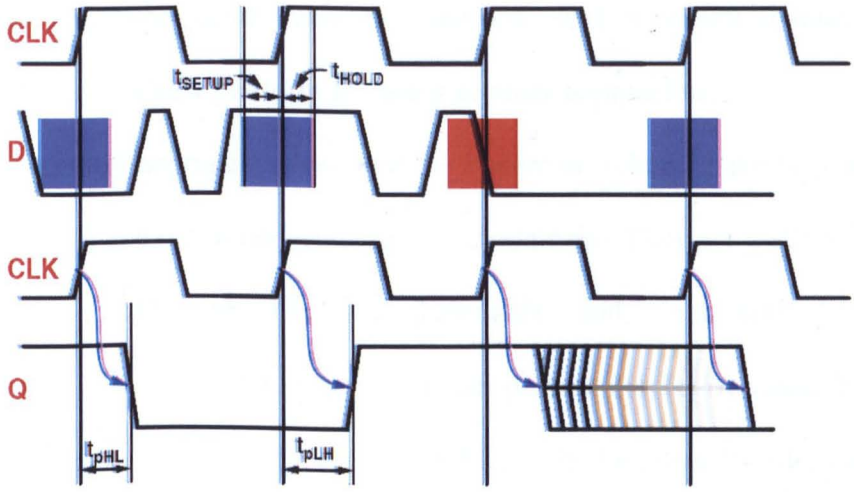


Figure 22: Example of the CPU metastability caused by RFI

Theoretically, this vulnerability can be utilised by the attacker to paralyse the security system by generating an extremely strong electromagnetic field, e.g. by the help of medical equipment such as Magnetic Resonance Imaging (MRI). Under extreme electromagnetic conditions, the CPU and security program would not run properly, so the security alarm can be disabled. If this threat is true, it will be very dangerous to the whole security industry.

To the author's knowledge, we are the first to explore these security concerns on payment security. No work has ever discussed this kind of attack, and it has not yet been specified in current terminal security requirements. Although we have not managed to prove this attack by experiments due to limitations to this research, we propose that some serious experiments and investigations need to be carried out on this issue.

3.7 Conclusion

Many attacks to POS systems attempt to disclose PINs and keys. In this chapter, we have proposed a novel Supercard scheme to address threats on PIN and POS peripherals. By taking the advantages of encapsulating a PIN pad, display and fingerprint sensor into smart card, the sensitive information, e.g. PIN, fingerprint and prompt messages are acquired, transferred and processed in securer channels. Thus, the Supercard offers a new platform for many security approaches.

Four security approaches based on the Supercard scheme have been presented to defeat attacks that exist in conventional POS terminals. They are the PIN Medium, Message Verifier, Detector of Fake Terminals, and Tool with Multimodal Authentication. The PIN Medium approach can prevent attacks of visual disclosure, non-intrusive attacks and intrusive attacks on PIN. The Message Verifier can defend against display manipulation attacks. The Detector of Fake Terminals can help the cardholder being cheated by a fake terminal. The Tool with Multimodal Authentication can offer a flexible platform of authentication to improve the overall security.

To protect the crypto key unit through hardware more effectively, two methods, namely the BGA package solution and ceramic-based tamperproof package solutions, are proposed as new approaches. The former solution exploits the semiconductor technology to encapsulate the crypto-processor and key unit into one-chip, hide them and risk pins in the BGA package. Together with the currently available electronic detector circuits, the highly secure units and their pins become very difficult for adversaries to access. In cases where the crypto-processor and key unit cannot be integrated into one chip, the solution of a ceramic-based tamperproof package can be applied. It exploits the ceramic features of fragility, hardness and

electric isolation. With the protection of the printed protective mesh on the package, the secure units and their pins covered by the package become safer.

The electromagnetic attack has been discovered as a potential vulnerability for security devices. We argued that threats exist if the security unit can be paralysed by the generation of an extremely strong electromagnetic field. The modern security CPU works in high GHz frequencies, and when operated at reduced voltage levels, their susceptibility to radio frequency interference is increased. Once the CPU stops working because of the strong magnetic interference generated by the adversary, it will not be able to detect normal access attacks and the security system will be subverted.

On the subject of cryptography algorithms, we argued that the ECC and AES cryptography algorithms are more suitable than RSA and DES. The comparison study indicated that the ECC and AES algorithms use less memory. They have higher security levels at the equivalent key length and require a less complex computing process.

To further study the Supercard, in the following chapters the channels in the Supercard will be investigated. The fingerprint biometric channel will be detailed in Chapter 4. The PIN pad channel and keystroke dynamics channel will be studied together in Chapter 5. The information fusion based on fuzzy logic will be studied in Chapter 6.

Chapter 4. Fingerprint for the Supercard

In this chapter, the Supercard scheme will be further investigated, focusing on fingerprint biometrics and their feature extraction for security identification.

Biometrics is increasingly integrated into POS systems. Biometrics refers to the automatic identification or verification of living persons using their enduring physical or behavioural characteristics. Biometric personal authentication uses data taken from measurements of a person's body, such as fingerprints, faces, irises, retinal patterns, palm prints, voice, signature, DNA, and so on [8]. Biometric systems also introduce an aspect of user convenience that may not be possible using traditional security techniques. For instance, in the PIN authentication method, the user might forget the password, requiring the system administrator to intervene and reset the password for that user. A Meta Group study reports that a password-related help desk call may cost as much as $30 in terms of support staff time and money [97]. Maintaining, recollecting, and remembering passwords can be a tedious and expensive task in such a PIN-based system. By comparison, biometrics has features of "not be lost or forgotten, unique". It is widely used in security or devices that require privacy.

In a Supercard, one fingerprint sensor is embedded which enables it to capture and process the fingerprint data inside of the card (see Figure 12). In the following section, we present more specifically how to integrate the fingerprint into the Supercard, i.e. the fingerprint channel into the Supercard.

4.1 Background

As shown in Table 4-1, different biometric technology has its advantages and weaknesses [98]. For instance, retina scanning requires a laser to be shone onto the back of the eyes and the unique characteristics of the retina are measured. The retina is an extremely stable form of biometrics because it is 'hidden' and not subject to wear. The system is hard to fool because the retina is not visible and cannot be faked easily. However, it is a potential risk to health and the invasive nature is unattractive to customers. Face recognition is a quite natural method, but in practice, it is strongly affected by lighting, pose and expression. It also needs high computation power and the embedded system cannot meet this requirement. Therefore, thinking comprehensively based on the factors of accuracy, cost, convenience and marketing, fingerprint is convenient, proven, miniaturised and inexpensive, and it has the best potential for a mass-market authentication schema. Figure 23 is a POS terminal with a fingerprint sensor.

Table 4-1: Comparison of common biometrics

Type	Merits	Weakness
Iris	High accuracy, hard to fool	Large and expensive equipment
Face	Non-invasive, no physical interaction with sensor needed	Low accurateness, affected by lighting & face position
Finger-print	Convenient, well-developed, inexpensive, high potential for miniaturization	Accuracy depends on fingerprint quality, Finger subject to wear
Voice	Non-invasive and natural	Subject to wide variation, hard to detect recorded voice
Retina	Stable, hard to fool	Invasive, not well tested, expensive

Figure 23: POS terminal with fingerprint

The biometrics verification may be formally posed as follows: given an input feature vector X_Q and a claimed identity I, determine if (I, X_Q) belongs to ω_1 and ω_2, where ω_1 indicates that the claim is true (a genuine user) and ω_2 indicates that the claim is false (an impostor). Typically, X_Q is matched against X_I, the biometric template corresponding to user I, to determine its category. Thus,

$$(I, X_Q) \in \begin{cases} \omega_1 \; if \; S(X_Q, X_I) \geq \eta, \\ \omega_2 \; otherwise, \end{cases} \tag{4-1}$$

where S is the function that measures the similarity between X_Q and X_I, and η is a predefined threshold. Therefore, every claimed identification is classified as ω_1 and ω_2 based on the variables X_Q, I, X_I and η, and the function S.

In a typical biometrics-based personal authentication, fingerprint authentication uses a four-step process including capture, extraction, comparison and matching [99]. The pre-stored minutiae for matching during an enrolment are also called the template. Two techniques are used to decide if the verification data really corresponds with the reference data. One is based on minutiae matching (local details) and the other is based on pattern matching (global structure). Minutiae matching is more commonly used. Figure 24 illustrates how to extract fingerprint minutiae.

Figure 24: Fingerprint minutiae extraction

There are two common ways to implement a biometric system according to the different places of storing templates and matching: online and offline. Online means the fingerprint templates are stored and matched in a centralised server computer. This solution has advantages in terms of management and rapid system update; however, a stable communication is always needed and it will increase the cost and slow down the transaction. Offline means the authentication can be done locally because the template is stored and matching is finished locally. This solution can verify identity without complex communication infrastructures and can cut costs. It is especially important in mobile application and at sites away from the communication line. The vital question for offline solutions is how to store the template securely. A smart card can be an ideal solution to address these questions. It can operate both online and offline.

The smart card has the capability to record and modify information in its own non-volatile memory and the security data can be well protected or 'hidden' by the operating system and hardware. These features make the smart card a powerful and practical tool against unauthorised data access and copy [1][3]. More and more technologies are integrated with the smart card. The PKI (public key infrastructure) has reinforced the smart card's security and makes the smart card an ideal place to carry varying degrees of sensitive information. In the past few years, biometric and smart card technology has been combined together in some applications [100]. As illustrated in Figure 25, a terminal with a fingerprint sensor captures the fingerprint

and extracts the minutiae, and then the extracted minutiae are sent to the smart card to match with the stored fingerprint templates in the smart card. The process is called *match-on-card* (MOC) and the card is called a biometric card [101].

The rest of the chapter is organised as follows: the principle of fingerprint verification is described in Section 4.1. Section 4.2 analyses the general security of the fingerprint authentication system, namely attacks and countermeasures. Sections 4.3, 4.4 and 4.5 describes the proposed system, including architecture, protocol and an adaptive decision algorithm. Section 4.7 is a conclusion and future work description.

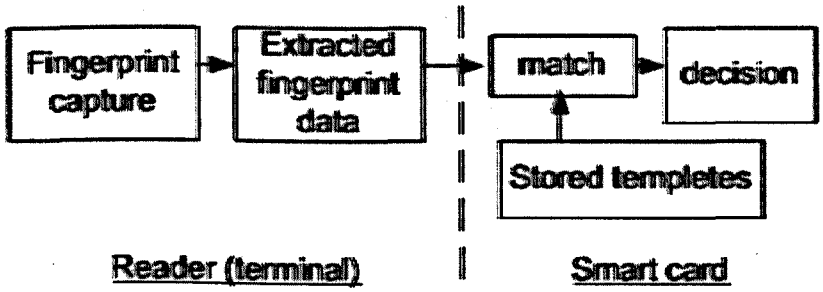


Figure 25: Diagram of Match-on-Card process

Fingerprints are identified by their special features such as ridge endings, ridge bifurcation, short ridges, and ridge enclosures, which are collectively called the minutiae. The fingerprint administrator uses the method of greyscale ridge tracing backed up by a validating procedure to extract the minutiae of fingerprints. In a fingerprint, each minutia is represented by its location (x, y) and the local ridge direction φ. Figure 26 shows the attributes of a fingerprint's minutiae. The process of minutiae detection starts with finding a summit point on a ridge, and then continues by tracing the ridge until a minutia, which can be either a ridge ending or bifurcation, is encountered [103].

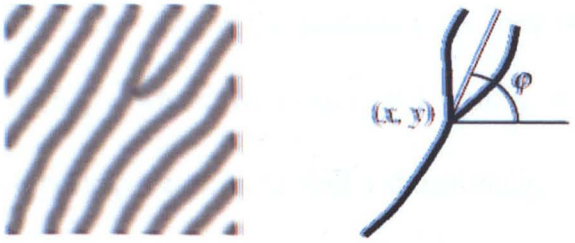


Figure 26: A minutia's attributes

The direction angle φ at point x mentioned above is computed as follows. A 9×9 neighbourhood around x is used to determine the trend of grey level change. At each pixel $u = (u_1, u_2)$ in this neighbourhood, a gradient vector $v(u) = (v_1(u), v_2(u))$ is obtained by applying the operator $h = (h_1, h_2)$ with

$$h_1 = \frac{1}{4}\begin{bmatrix} -1 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 1 \end{bmatrix}, \quad h_2 = \frac{1}{4}\begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & -1 \end{bmatrix} \tag{4-2}$$

to the grey levels in a neighbourhood of u. That is,

$$v_1(u) = \sum_y g(y)h_1(y-u), \quad v_2(u) = \sum_y g(y)h_2(y-u) \tag{4-3}$$

where y runs over the eight neighbouring pixels around u and $g(y)$ is the grey level of pixel y in the image. The angle φ represents the direction of the unit vector t that is orthogonal to all gradient vectors v. That is, t is chosen so that $\sum_u (v,t)^2$ is minimised [103].

The primary purpose of the fingerprint recognising system is to calculate the matching degree of the target fingerprint with the images in a database and to decide if it belongs to a particular individual. One method of calculating this matching degree is based on fuzzy evolutionary programming technique and can be described below [103].

Consider two fingerprints that are represented by their sets of minutiae, $A=\{a_1,K,b_m\}$, $B=\{b_1,K,b_n\}$, where $a_i=(x_i,y_i,\alpha_i)$ and $b_j=(u_j,v_j,\beta_j)$, for $1\le i\le m$, $1\le j\le n$. The principal task is to find a transformation $F=(s,\theta,\delta x,\delta y)$ that transforms the set of minutiae A into the set B.

Here, s represents a scaling factor, θ an angle of rotation, and $(\delta x,\delta y)$ a translation in the xy-plane. Thus, the transform $F(p)=(x',y',\alpha)$ is defined by:

$$\begin{bmatrix} x' \\ y' \\ \alpha' \end{bmatrix} = s \begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & \frac{1}{s} \end{bmatrix} \begin{bmatrix} x \\ y \\ \alpha \end{bmatrix} + \begin{bmatrix} \delta x \\ \delta y \\ \theta \end{bmatrix} \tag{4-4}$$

Based on above transformation, the matching degree of two fingerprints can be determined.

4.2 Security Study of Fingerprint System in POS

Besides the performance issues, people have been concerned with the security of biometric systems since the very beginning. Our discussions here will focus on the fingerprint system and its applications in smart cards.

4.2.1 Fingerprint System Security

A generic biometric data-processing model is shown in Figure 27. Within this model, following the data process from sensor until application, we identify nine basic biometric attacks (Attack 1; . . . ; 9) that plague biometric-based authentication systems. For simplicity, the enrolment of the fingerprint template is not included, although that is quite an important link of the whole biometrics security system.

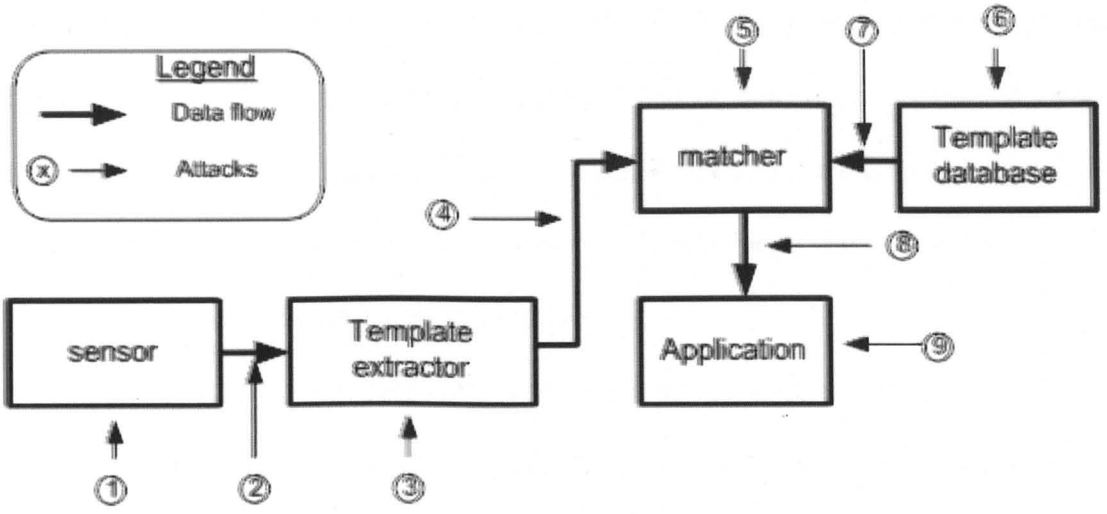


Figure 27: Illustration of biometric attacks

Typically, Attack 1 can be an *impersonation attack* where the attacker uses a fake fingerprint to fool the sensor. Attacks 2, 4, 7 and 8 belong to *channel attacks* for which the attacker can use line taping, intercept the biometric data or use previous recorded signal to replay attacks. Besides these direct channel attacks, some advanced crypt-analytical techniques, so called *side channel* attacks, also pose serious threats to biometric systems, even to the channels that are encrypted. For instance, by analysing the power dissipation or the timing of encryptions in device, encrypted information inside can be deduced [104]. Attacks 3, 5, 6 and 9 fall into the categories which attack the inside software or secure keys (if the cryptographic technology is employed for secure data transmission). Below, more details about attacks and countermeasures will be examined.

A fake finger attack is a serious threat to biometric authentication systems, since this type of attack directly exploits the intrinsic weakness of biometrics: easy to capture and hard to revoke. When fingers touch an object, the chemicals in finger sweat may be absorbed into that object, the work in [15] being a good example. There are new chemicals which can restore the absorbed sweat quite nicely.

Afterwards, a fake finger can be made to fool the biometric system. With the ongoing development of technology, a latent fingerprint can be detected and captured easily and a very sophisticated fake finger can be made; for example, a fake print made from gelatine, which is low-cost, electrically quite like real flesh, can already fool many optical, capacitive pressure-based sensors [15].

Theoretically, each data transfer channel is susceptible to channel and side channel attacks if it is not well protected. The typical attacks can be a replay attack, resubmission of an old digitally stored biometric signal, or an electronic impersonation. More specifically, like in Attack 2, after the features have been captured by the sensor, if the sensor and the extractor hardware have a long and exposed channel (e.g. connected with cables), this captured data can be replaced with a different synthesised feature set. In Attack 4 the minutiae can be replaced. In Attack 7, the templates from the stored database, which are sent to the matcher, can be altered before they reach the matcher. In Attack 8, the final decision of the matching module can be overridden.

From a software perspective, the compiled source code stored in the system is susceptible to de-compilation and reverse engineering, which means the program can be read and analysed. Therefore, if the security mechanism is merely based on some tricks in the program, it will be easily subverted by analysing the program and designing some actions to avoid triggering the security mechanism. If the adversary can install a Trojan horse into the biometric system, some information will be disclosed to the attacker, etc.

4.2.2 Countermeasures for Biometric Attacks

Based on the above threat analysis, some countermeasures can be taken to improve security.

A multi-modal sensor can be an effective way to prevent a fake finger attack. In a multi-modal sensor, for example, in addition to capturing a fingerprint, the warmth and pulse can also be detected. Like some advanced sensors, instead of taking a static picture of the surface of the finger, it reads the fingerprint from the live layer below the surface of the skin. This method ensures that the device will acquire the fingerprint despite varying skin moisture levels; abrasion of the fingerprint from harsh chemicals or friction like rubbing; and common contaminants such as lotion, grease, or smoke. This subsurface-imaging approach thereby eliminates the surface-based recognition failures common with surface-imaging fingerprint sensors based on capacitive, thermal, optical, or pressure-sensing techniques.

Several solutions can improve the system security. 1). As proposed in the paper by Nalini et al. [80], "Image based challenge/response method", the matcher unit generates a pseudorandom challenge for the transaction and the sensor unit acquires a signal at this point of time and computes a response to the challenge based on the new biometric signal. 2). *WSQ* (Wavelet Scalar Quantization)-*based data hiding.* This uses data-hiding techniques to embed additional information directly in compressed fingerprint images to guard against replay attacks. 3). Cancellable biometrics. This refers to the intentional and systematically repeatable distortion of biometric features in order to protect sensitive user specific data [81]. The methods fall into two categories of biometric salting and non-invertible transforms. The transform can be down in a way of keyless in some cases. However, such measures can hardly meet high security requirements or reach high recognition accuracies. Fundamentally, if the hardware of storing the encryption key or biometric template is not secured, the whole system cannot reach a high security level.

To prevent the fingerprint template from being revealed and to ease the match at less computation costs, Jin et al. [82] proposed a Biohashing method. In this case, the biometric template is stored in a non-original format. Indeed, the template is built through an irreversible hash function known as Biohashing. Even if the adversary can get a Biohashing template, he cannot obtain the original biometric template. Biohashing methodology can be decomposed into two components: (a) an invariant and discriminative integral transform feature of the fingerprint data, with a moderate degree of offset tolerance. This would involve the use of an integrated wavelet and Fourier–Mellin transform framework (WFMT) as reported in Ref [82]. In this framework, the wavelet transform preserves the local edges and noise reduction in the low-frequency domain after the image decomposition, and hence makes the fingerprint images less sensitive to shape distortion. In addition to that, the reduced dimension of the images also helps to improve the computation efficiency. FMT produces a translation, rotation in plane and scale invariant feature. The linearity property of FMT enables multiple WFMT features to be used to form a reference invariant feature and hence reduce the variability of the input fingerprint images. (b) A discretisation of the data via an inner-product of tokenised random number and user data. The Biohashing progress is depicted in Figure 28 [82].

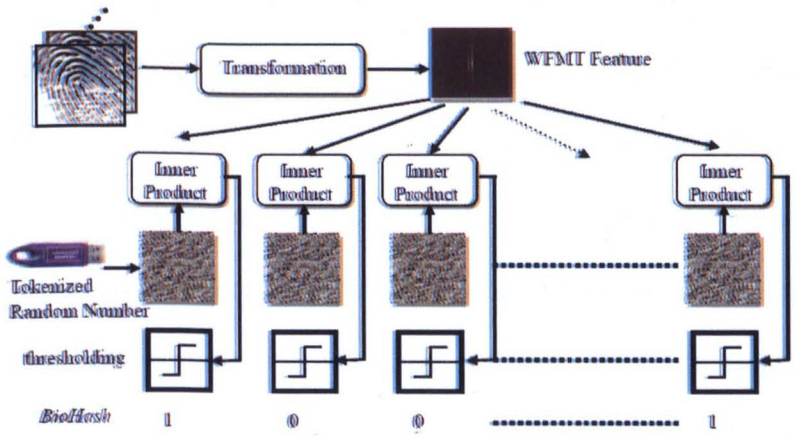


Figure 28: Biohashing progress

Indeed, the essential protection is to seal as many of the system components as possible into a tamper-proof device, including the data transmission channels. If some channels cannot really be sealed, then cryptographic technology shall be employed to ensure data integrity and confidentiality. The security key must be very well protected. Following these philosophies, the combination of biometrics, PIN and smart card can be an attractive solution.

4.3 The Biometric CMOC Scheme

As an extension of the Supercard, which we proposed in last chapter, here we examine our proposed biometric CMOC scheme in the Supercard. Purely from a hardware point of view, compared to the Match-On-Card (MOC) solution, which is developed by previous researchers, the CMOC solution has a fingerprint sensor with a smart card body so that the fingerprint can be acquired directly from the Supercard. Meanwhile, a Biohashing template, as previously mentioned, is stored in the Supercard. The template is derived from the original biometric template with wavelet transformation and irreversible hash functions. Based on that, a specific securer authentication protocol will be detailed in Section 4.5.

The benefits of this proposal are listed as follows:

(1) It will increase the difficulty for attackers. In practice, attackers only need to install an electric bug or apparatus to the attacked object. A terminal machine (card reader) normally has a spacious plastic housing, which contains many PCBs, electric components, etc. The wires linking the system components to each other can become potentially passive or active penetration routes. It is not difficult to find a small space in the terminal for installing an electric bug inside. However, if the fingerprint sensor is integrated with the smart card, all these electric elements can be packed into one

very thin plastic package, or even be integrated into one single chip and interlinks can be hidden.

(2) Distribute the security risk. The adversary can get far more potential benefits from compromising a terminal security system than compromising a single card. If the biometric sensor in a terminal is compromised, it will jeopardise all its users, thus distributing the sensor to the cards can distribute the risk.

(3) Protect the privacy and increase the flexibility. Nowadays, the sensor is installed with the terminal machine. Although the terminal providers as well as the merchants declare that "we don't take your fingerprint images – only features", it is hard to believe when the customers see their fingerprints scanned by the terminal. Meanwhile, if the card has a biometric sensor itself, it can improve the flexibility and customers can use and benefit from the potential advanced biometric technology everywhere. Meanwhile, the Biohashing template protects the privacy very well. An embodiment of the biometrics Supercard is illustrated in Figure 29. Later in this chapter, the envisioned architecture and procedures will be presented.

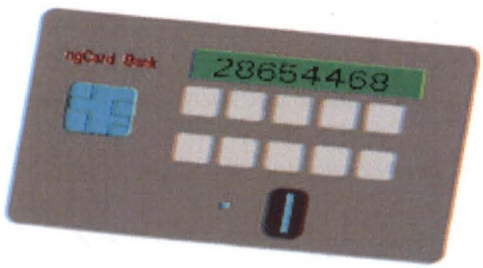


Figure 29: Supercard with fingerprint swiping sensor

For our system experiments, a swipe-type fingerprint sensor AES2510 from AuthenTec Inc has been selected, not only for its small size and low cost, but for security. It uses a radio frequency (RF) imaging technique that allows the sensor to generate an image of the shape of the live layer of the skin that is buried beneath the

surface of the finger. Thus, it can better prevent attacks like a gelatine fake finger. AuthenTec promised to offer a smaller and cheaper version of swipe fingerprint later.

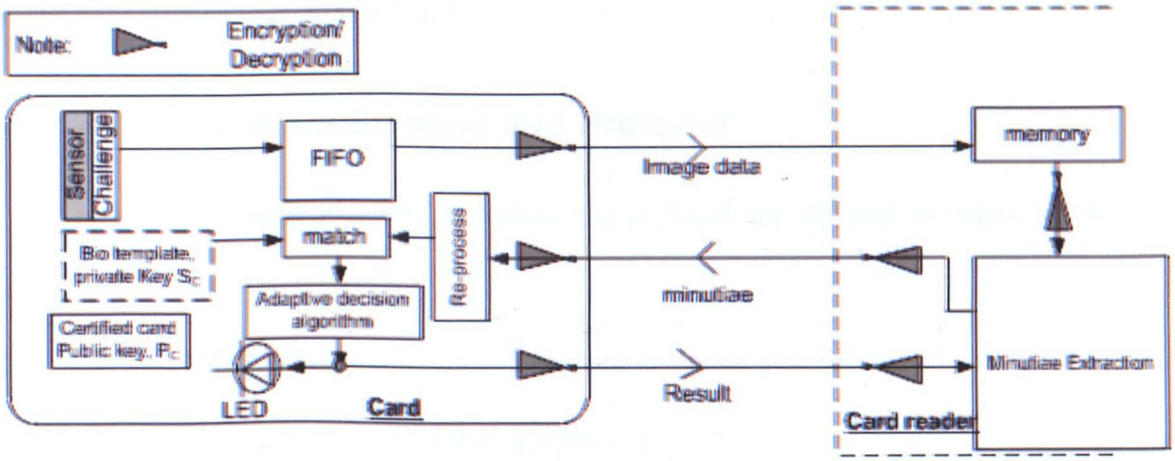


Figure 30: Architecture of biometric Supercard

4.4 Architectural Description

The structure of the biometric supercard system is illustrated in Figure 29. Theoretically, since the fingerprint sensor has been integrated with the Supercard, the whole process of fingerprint capture, feature extraction and matching can be done inside the card. This is the best option from a security point of view. However, because the normal embedded processor of the smart card, as well as the memory, can hardly fulfil the requirements of complex image processing, it will be more realistic to remove the tasks of fingerprint minutiae extraction to the POS terminal side, which normally has a more powerful CPU. The swipe fingerprint sensor reads the finger line by line, generates a challenge and sends the data to FIFO (first in, first out) via parallel or DMA (direct memory access) communication. The data in FIFO will be encrypted and directly sent out to the memory of the POS terminal. After the image capture is completed, the image data will be decrypted and the minutiae will be

extracted before it is sent back to the smart card for verification. In addition, the display in the Supercard can change the role of the smart card from a passive and 'dumb' card to an active one, e.g., it can indicate some serious edicts to improve security as well as user convenience.

4.5 Authentication Scheme and Protocol

The whole authentication procedure and protocol are outlined as below in six steps:

1. Fingerprint feature extraction and biohash template generation:

$fingerprint_{Template}=\Psi\{ WFMT(fingerprint) \}$

Here *WFMT* denotes Wavelet and Fourier–Mellin Transformation. Ψ denotes the discretisation operation. Before the cardholder gets the Supercard, the card issuer will first store the fingerprint biohash template in the Supercard, together with the PIN template.

2. Insert the card into the card reader to get power. For the best security, if the hardware configuration of the Supercard (e.g. CPU speed and memory size) is strong enough, after the fingerprint is captured by the Supercard sensor, the feature extraction and the live Biohashing fingerprint template can be computed in a similar way to step 1 by $Fingerprint_{live}=\Psi\{ WFMT(fingerprint)\}$, and the process can skip the steps 3 to 5 and directly go to step 6. In this case, no signal needs to be sent out the premier of Supercard.

Considering the cost and implementation limitations, if the hardware configuration of the Supercard itself is not strong enough, the card reader, which has better hardware resources, can be utilised to undertake the computation task of fingerprint feature extraction. The below steps will be needed.

3. Mutual authentication using PKI technology between the Supercard and the POS reader [73].

The authentication protocol between the Supercard and the POS reader will start. The Supercard will send a nonce N_{sc}, i.e. random data to the POS card reader. The random data N_{sc} can be used through the communication to prevent replay attack (as shown in Figure 31). The card issuer uses its issuer private key S_I to certify the card public key P_C, and saves the certified P_C in a readable area of the smart card. The card private key S_C and the fingerprint template are saved in the 'hidden' area in the smart card. Therefore, they cannot be copied or read out by an external card reader.

The issuer public key P_I is distributed to the card reader. Therefore, the card reader can use P_I to verify that the card's P_C was certified by the issuer, and use P_C to verify the digital signature of the card data. Therefore, in this way the terminal can confirm that the card is original and has not been modified. On the other hand, to determine whether the card reader is genuine, the card can check the certification of the card reader. In case the above mutual authentication fails, the application will be cancelled and both the card reader display and the card will indicate the error message, i.e. the display on the Supercard will show a warning message. This is an important feature because it can detect a fake terminal, which is made by an adversary to cheat the user.

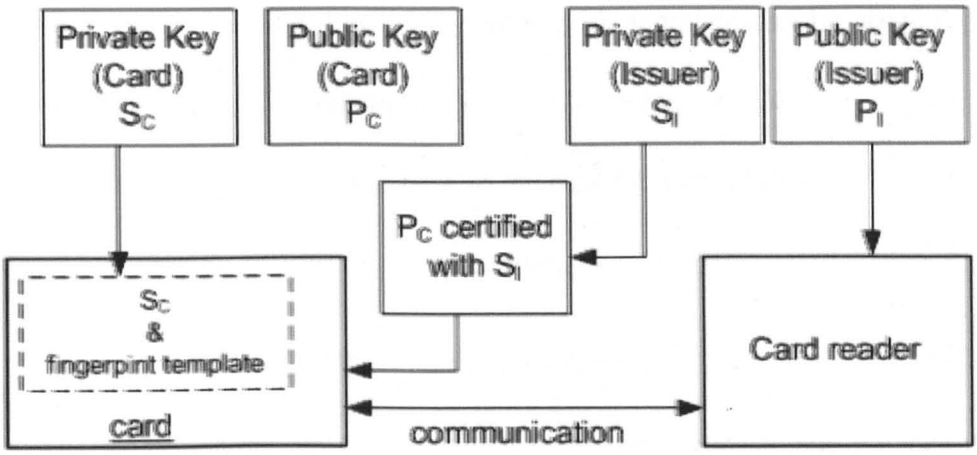


Figure 31: Diagram of dynamic data authentication

4 Session key generation

A session key can be used as a secure key for the encrypted communication between the card and the reader (e.g. AES encryption). The session key derivation function in both the card and the reader, generates a unique session key *Ks* for each ICC application transaction as per the following method. The system first generates unique Master Keys K_M from the user's primary account number and an Issuer Master Key, and then *Ks* can be derived from K_M, ATC (Application Transaction Counter) using diversification data R.

$$K_M := F\ (Primary\ Account\ Number,\ Issuer\ Master\ key) \qquad (4\text{-}5)$$

$$Ks := F\ (K_M, ATC)\ [R] \qquad (4\text{-}6)$$

The session key will be used through the whole communication. The nonce, session key and PIN will be encrypted and sent to the POS terminal.

$$\text{Supercard} \rightarrow \text{POS reader:} \quad \{\{|N_{sc}, K_s|\}_{PIN}\}_{K_I} \qquad (4\text{-}7)$$

5 Fingerprint capture and Biohashing

The fingerprint sensor reads the finger image. The mixed data are sent to FIFO, and after AES-encryption, using the session *Ks*, they are sent out to the memory of the card reader. After fingerprint reading is complete, the stored image

can be decrypted. The live biohashing fingerprint template can be computed in a similar way to step 1 by $Fingerprint_{live}=\psi\{ WFMT(fingerprint) \}$

It can be encrypted and sent back to the card for authentication.

Supercard →POS reader: $\{\|N_{sc}, fingerprin\|\}_{Ks}$ (4-8)

POS reader→ Supercard: $\{\|N_{sc}, fingerprin_{live}\|\}_{Ks}$ (4-9)

6. The Supercard decrypts the received fingerprint biohash and matches it with the stored template.

$$fingerprint_{live}=fingerprint_{template}?$$

7. Match the acquired $fingerprint_{live}$ with the hidden fingerprint template $fingerprint_{template}$ in the smart card and generate a similarity score. The final decision comes from an adaptive algorithm. The decision is encrypted and sent to the card reader. The result will be indicated both in the card reader display and in the Supercard display. This is a special measure because the conventional way is just to send it either to the card or the card reader. In this way, even if the attacker faked a result in the card reader and the card reader display shows that the operation is right, the LED on the smart card will start to flash and give a warning.

4.6 System Evaluation

The security features of the aforementioned CMOC system and the proposed protocol are evaluated and discussed as follows.

1. Strength of protection on the biometric template. In traditional schemes, the user's biometric template is directly stored into smart cards, thus they may be obtained by the adversary under attacks [69]. In our scheme, a biohash fingerprint template instead of the normal fingerprint template is stored in the Supercard. Even if the biohash template is revealed, the

adversary cannot obtain the real fingerprint due to the irreversibility of the biohash algorithm. In addition, the revealed biohash cannot be used in other biometric applications, because of the different applications which usually have different biohashes. Furthermore, by re-registering the Supercard, the user can generate a new biohash to cancel the revealed one easily.

2. Channel attack resistance, guessing attack resistance and denial-of-service attack resistance. In Table 4-2 we have compared our solutions with previous schemes, which were proposed by other researchers of smart card security.

Table 4-2: Security comparison of smartcard-based schemes

	Khan [71]	*Lee [70]*	*Our Scheme*	
Channel attack resistance	no	no	Yes	Sensor is integrated as an internal component
Session key	no	no	Yes	Each session has a unique key for AES
Mutual authentication	Yes	no	Yes	Before the session starts
DoS attack resistance	Yes	yes	Yes	Authentication is carried inside of card

4.7 Conclusion

Fingerprints and their features have been used as biometrics which can be integrated and which reinforce our Supercard solution. One of the main merits of our CMOC biometric Supercard is that the fingerprint image data can be transferred and processed inside of the closed secure channel and places of Supercard.

The new authentication protocol has been developed by me in this chapter correspondingly. Compared to traditional biometric authentication in the remote server or "Match-on-Card", we do not need to store any fingerprint image in the

remote server nor in the smart card. Instead, we store a biohash template in the Supercard and the authentication is carried out inside of the Supercard between two biohash data. This solution has not only enhanced security and distributed the risks, but also shortened the time of authentication. Meanwhile, our protocol is a practical protocol and it has considered the potential limitations of card hardware configuration. The feature extraction is designed to be done securely inside of the POS terminal, which normally has a more powerful processor.

Most of the smart-card-based schemes excessively depend on the tamper resistance of smart cards, so in these schemes biometric templates or passwords' hash values are stored directly onto smart cards, regardless of the information extracting attacks [68] on smart cards. Our scheme has remedied these security pitfalls. Since the fingerprint sensor is integrated in the Supercard, thus there is no space for an adversary to install electronic bugs to intercept data. It can effectively prevent the typical channel attacks and side channel attacks, guessing attacks and Dos attacks. The conducted system evaluation and security analysis support the advantages of our scheme.

Chapter 5. Keystroke Dynamics to Strengthen PIN Authentication

This chapter studies the feasibility and merits of adapting keystroke dynamics as behaviour biometrics to improve the hardness of PIN security.

5.1 PIN Authentication

A standard PIN pad layout of a POS terminal is illustrated in Figure 32 [73]. The PIN pad comprises the numeric and 'Enter' and 'Cancel' command keys. If necessary, the command key for 'Clear' may also be present. The numeric layout of the PIN pad shall comply with ISO 9564. The key for '5' shall have a tactile identifier (for example, a notch or raised dot) to indicate to those whose sight is impaired that this is the central key from which all others can be deduced.

The method of traditional PIN authentication is simple. The PIN is inputted through a keypad and then it is encrypted in the crypto-unit of the PIN pad. The encrypted PIN will be sent out to the remove server for authentication. In other words, before the PIN is encrypted, it is in plaintext and prone to being attacked.

Figure 32: Standard POS terminal layout

The PIN authentication is stable but prone to being disclosed and forgotten; the biometric authentication is not forgettable but is sensitive to impostor attacks and is unable to reach a perfect recognition rate. If a hybrid system and an adaptive algorithm can be built based on the biometric and PIN fusion, a better trade-off can be reached between security and convenience. As illustrated in Figure 33, a high-level security system needs to be based on three factors: token factor (e.g. a card), knowledge factor (e.g. PIN) and features factor (e.g. a fingerprint or keystroke pattern). There is no possibility of replacing one with another entirely. Theoretically, even a perfect biometrics system can also not completely replace the knowledge-based authentication method, e.g. PIN. Therefore, it is foreseen that biometrics cannot replace the PIN authentication completely in the short or medium term. A realistic solution can be to combine different authentication methods or to reinforce the PIN by biometrics.

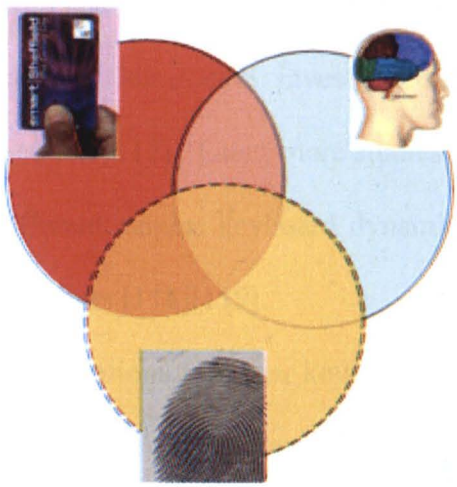


Figure 33: Three factors of a high-security system: token, knowledge and feature

The multimodal authentication decision system can strengthen the traditional PIN method and offer a flexible solution. For example, for a high value payment, 100% PIN correspondence and high commensurate numbers of features of fingerprint are required. For a lower value payment, if specific numbers of fingerprint features have been commensurate, the payment can be done. This has the practical effect of reducing the number of legitimate users coming back to the bank asking for service because their cards are locked due to wrong input of the PIN more often than the allowed amount of times. Decreasing the possibilities of such accidents can save management cost for banks.

5.2 Keystroke Dynamics

Keystroke pattern is one type of behaviour biometric that identifies an individual based on their unique typing rhythm. The premise behind keystroke pattern is that each individual exhibits a distinctive pattern and cadence of typing. As early as 1980, researchers have been studying the use of habitual patterns in a user's typing behaviour for identification. Gaines et al. investigated the possibility of using keystroke timings for authentication [117]. Later, more studies were done. Keystroke pattern is known by a few different names: keyboard dynamics, keystroke analysis, typing biometrics and typing rhythms [118][119].

Most studies have used durations between keystrokes (latencies) as features for user verification, but some have also used keystroke durations (the time a key is held down) [120], as shown in Figure 34 and Figure 35. The classification methods used include traditional statistic techniques, Bayesian classifiers, neural networks and fuzzy systems. Bleha et al. [121]tried detecting the keystroke pattern of users' "usernames" for user verification and reached FRR 8.1% and FAR 2.8%. Obaidat

and Sadoun [123] made a comprehensive study of different classification methods that can be used with keystroke patterns. It was noted that keystroke durations gave better results than latencies between keystrokes, but using both measurements together gave the best results. The best results were achieved by neural methods of Fuzzy ARTMAP (a generalisation of adaptive resonance theory networks (ART) with fuzzy set theory operations), RBFN (Radial Basis Function Network) and LVQ (Learning Vector Quantization) [125].

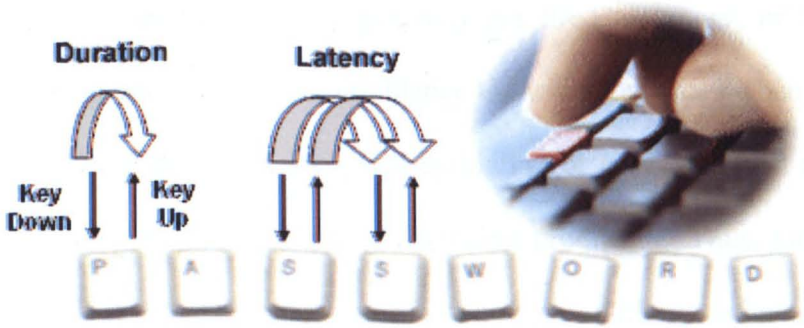


Figure 34: Illustration of keystroke dynamic detection (duration and latency)

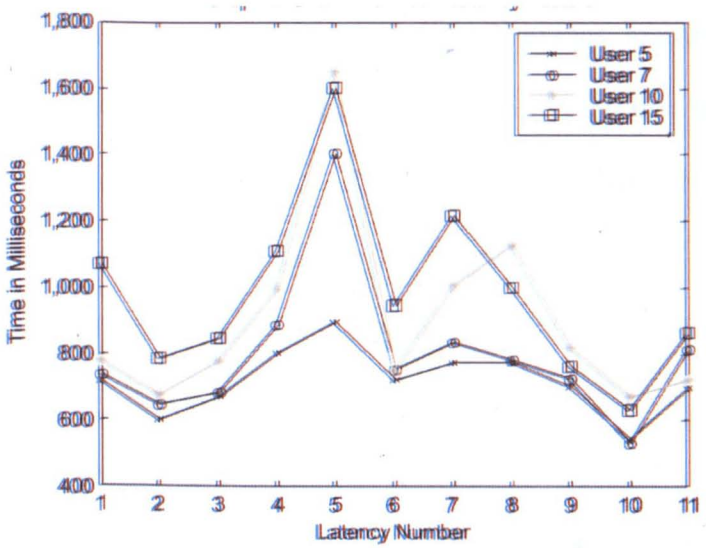


Figure 35: A graph to show the mean latency vector

The main advantage of keystroke dynamic is the simplicity of implementation. Unlike other biometric systems, which may be expensive to implement, the attractive

advantage of a keystroke pattern is that it requires almost no extra hardware expense. The only hardware required is the keyboard.

Nevertheless, user authentication through keystroke characteristics remains a difficult task. The reason is quite understandable: physiological features such as face, retinal and fingerprint patterns are strongly stable over time, unlike behavioural features such as writing and keystroke patterns [114]. One of the major problems that keystroke dynamics runs into is that a person's typing varies substantially during a day and between different days. People may get tired, or angry, or have a beer. A person's typing may bear little resemblance to the way he types when he is well rested. Because of these variations, there will be high error rates to almost any system, with both false-positives and false-negatives being produced. Thus, currently the main application of keystroke pattern is proposed as an auxiliary authentication technique in computer network security, rather than as the normal method for user authentication.

Several observations can be made based on previous research works on keystroke dynamics. 1) Keystroke authentication requires typing in a relatively long segment of text to get distinct features. 2) A person's typing may vary substantially from time to time. It is very hard to get a perfect verification rate. 3) For people working daily before a computer, and for well-known, regularly typed strings, better recognition results can be achieved.

The rest of this chapter is organised as follows. The method of how to adapt keystroke pattern into POS is studied in Section 5.3. The preliminary experimental system and test results are presented in Section 5.4. The conclusion and future works are summarised in Section 5.5.

5.3 Adapting Keystroke Pattern into POS Applications

Our major objective is to apply keystroke dynamics to strengthen PIN authentication. Unfortunately, previous study results on keystroke dynamics that are based on computers and networks cannot be directly applied to POS systems due to some specialities of the PIN pad.

POS devices and its applications have specialities. First, unlike a computer keyboard which has 26 alphabetic characters keys, 10 numerical keys and other character and function keys, the keypad of a POS device has only 10 numerical keys (0-9) and 3 command keys, namely Enter, Clear and Cancel. As a matter of fact, the layout and position of the numerical keys are strictly specified by standards (refer to Figure 32). The PIN is typically inputted by one finger with small movements within a highly limited pad boundary. Second, a typical strong password in computer, "tie.5Roanl", contains more than 7 characters, a capital letter, a number, and punctuation [115]. It offers more features for keystroke analysis. However, the typical length of a PIN in a POS system is 4-6 digits only. Thus the number of key strokes is highly limited, which means very few features are available for keystroke pattern analysis. Actually, this is the biggest challenge for pattern verification. Thirdly, the European Standard for Access Control (EN 50133-1) requires a commercial biometric system to have a 0.01% miss rate and <1% false alarm rate. A POS system expects even higher in some case because it is involved with payment transactions. Due to the reasons given above, applying authentication based on a natural or unintentional keystroke pattern will be much more difficult in the POS applications than in a normal computer network.

To enable the keystroke dynamic to become a viable solution under the conditions of very limited keystrokes, features are expected to be more

distinguishable. Our approach to address this problem is explained below. Instead of casual or untrained key typing, we let cardholders intentionally build their special typing patterns. For example, the cardholder can type in the PIN "1234" with his predefined preferred typing pattern: Key "1" (hold 10ms)-(release for 80ms)-"2" (hold 60ms)-(release for 150ms)-"3" (hold 65ms)-(release for 80ms). This means he has built special pattern features with a very short press on Key "1" and a long interval between "2" and "3", and he tries to remember these features. Such deliberate typing patterns can be more consistent and distinguishable, thanks to the features of POS applications, namely a simple and fixed layout and limited number of keystrokes.

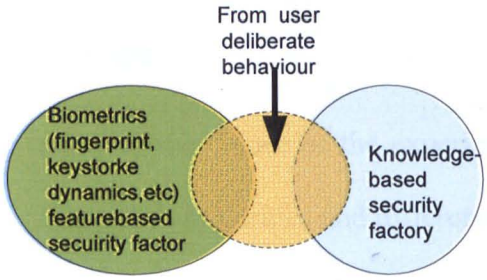


Figure 36: Deliberate keystroke is a combination of feature-based and knowledge-based factors

Indeed, these deliberately built typing patterns actually do not purely belong to the traditionally defined biometrics any longer, which refer to natural features or behaviours. Users must intentionally memorise some special behaviour. Therefore, it is already a combination of feature-based security factors and knowledge-based security factors. Thanks to this hybrid feature, it offers the possibility to better replace the PIN method, which is a knowledge-based method. In practice, to make a better trade-off between security and user convenience, a prompt (message) can be shown on the display to help to memorise the keystroke pattern. The prompt can be

defined by the user themselves, as they prefer. The prompt can have direct or indirect connections with the real keystrokes pattern. A timer progress bar can be shown to help the user better follow his own pattern.

The user will be authenticated by both the PIN and keystroke dynamics. Assume the impostor knows the PIN shall be "1234". Due to the wrong typing pattern, the impostor still will not be able to access the payment system.

This procedure is similar to traditional PIN inputs, thus it can be quite acceptable. However, remembering some simple behaviours is easier than to memorise a real, more complicated PIN, especially with the assistance of prompt messages. Additionally, in case the keystroke pattern is disclosed, it can be updated (a feature which normal biometrics lack).

5.4 Experimental Studies

The profiles collected over the course of the experiment were represented as N-dimensional feature vectors. The similarities and differences were calculated using the normalised Euclidean distance and non-weighted maximum probability measures.

5.4.1 Data Collection

The performance results reported here are based on a database of profiles collected over a period of four weeks. After a prototype system was built, 15 people were invited to join preliminary keystroke pattern tests. They were divided into two groups: group A (five members) and group B (10 members). Group A were regarded as genuine users and group B were regarded as impostors.

In our experiment, we only tested the extreme cases: we assumed that the impostor already knew which keys to press and the sequence that needed to be stroked, but the impostor did not know the user-typing pattern. Meanwhile, the prompt

message was identical for all users. A progress bar, which was controlled by a 100ms timer, was shown on the display as a reference to help the user manage the duration and latency time. An example is given in Figure 37.

Figure 37: Example of prompt, timer bar and real keystrokes

Table 5-1: Sample of tested keystrokes

Total Attempts	Designed Keystrokes	Feature Dimension	Designed Features
675	222	7	Simple short keystrokes, the same position and the same key
675	123	7	Neighbouring and consequent keys
675	649	7	Keystrokes in a clutter, short
675	55555	11	Long but simple keystrokes, the same position and the same key
675	12345	11	Long neighbouring and consequent keys strokes
675	67853	11	Keystrokes in a clutter, long

During enrolment, group A members were asked to input numbers according to our given tables, which were also public to group B (thus members of group B also knew what to input). However, group A members had to design individual typing patterns, which would not be told to the others. After they had 10 different keystroke patterns, a typing pattern template was built. Testing data were recorded in 15

different sessions separated by at least three days. Each participant in each session inputted three different keystroke patterns as in Table 5-1. The "Feature dimension" is counted by each key duration and latency, plus the Enter key. For example the keystrokes "222" consist of 3 durations, 2 latencies and 1 latency and duration of the Enter key, so totally it is 7 features. The data collected from other members of group A were used to attack each other. Thus, more than 4,075 data sets were created.

5.4.2 Classification Algorithms

Initially the Euclidean distance measure, as per equation 5-1, was used and then the Non-weighted Probability was applied, as per equation 5-2, similar to the experiment in [126]. Both the keystrokes' latencies and duration are acquired to build N-dimensional feature vectors for keystroke pattern analysis. Let R = $[r_1; r_2, r_3; ...; r_N]$ and U= $[u_1; u_2, u_3; ...; u_N]$, with R representing the reference vectors (template) and U representing unknown feature vectors. Then the following classifiers are used for recognition.

- Euclidean distance measure

"Similarity" is based on the Euclidean distance between the pattern vectors [116]. The Euclidean distance between the two N-dimensional vectors U and R is defined as per equation 5-1:

$$D(R,U) = \left[\sum_{i=1}^{N} (r_i - u_i)^2 \right]^{\frac{1}{2}} \qquad (5\text{-}1)$$

$i = 1, 2, 3, \ldots, N$, where N = number of pattern vectors.

- Non-weighted probability

Let U and R be N-dimensional pattern vectors as defined previously. Furthermore, let each component of the pattern vectors be the quadruple (μ_i, σ_i, o_i, x_i),

representing the mean, standard deviation, number of occurrences, and data value for the i^{th} feature. The score can be calculated between a reference profile R and an unknown profile U as equation 5-2 [8][126]:

$$Score(R,U) = \sum_{i=1}^{N} \frac{1}{O_{u_i}} \left[\sum_{i=1}^{o_{u_i}} \Pr ob\left(\frac{X_{ij}^{(u)} - u_{ri}}{\sigma_{r_i}}\right) \right] \quad (5\text{-}2)$$

O_{ui} – number of occurrences of u_i

$X_{ij}^{(u)}$ – value of j^{th} occurrence of u_i

μ_i – mean of the i^{th} of u_i

5.4.3 Results Analysis

Our findings are reported in Table 5-2. False acceptance rate (FAR) and false rejection rate (FRR) are both presented.

Table 5-2: Test results after applying Euclidean Distance Measure and Non-weighted Probability

Item	Designed Keystrokes	Feature Dimension	Euclidean Distance Measure		Non-weighted Probability	
			FAR	FRR	FAR	FRR
1	222	7	3.6%	1.8%	3.2%	1.7%
2	123	7	2.4%	2.2%	2.1%	2.0%
3	649	7	1.9%	1.8%	1.9%	1.8%
4	55555	11	2.6%	2.5%	2.3%	2.4%
5	12345	11	2.2%	2.3%	2.3%	2.0%
6	67853	11	1.5%	2.9%	1.3%	2.7%

We observed that the keystrokes "222" of item 1 have relatively high FAR at 3.5%, and the keystrokes "67853" of item six have relatively low FAR at 1.5%. This can be explained by the fact that keystrokes "222" have only three keystrokes, thus the imposters can relatively easily guess the keystrokes style. Meanwhile, all

keystrokes are on the same position, and no finger movements between keys are necessary. Therefore, the genuine user can concentrate more to perform his designed typing style and get lower FRR at 1.8%. As a comparison, the keystrokes "67853" have five irregular movements, thus the user can concentrate less on his style and get higher FRR 2.9%. On average, the probability classifier performs better than the Euclidean distance classifier, with a slight increase in computation.

Previous studies [114][117] indicate that keystroke durations give better results than latencies between keystrokes. In accordance with that, the equation 5-2 can be modified to a weighted probability as in equation 5-3. We gave higher weights on keystroke duration than that of keystroke latencies. In our experiment, we assigned the preliminary weight of keystroke duration $W_{du} = 0.6$ and the weight of keystroke latency $W_{la} = 0.4$. The score was calculated as equation 5-3 where $i = 1...\frac{N}{2}$.

$$Score(R,U) = \sum_{i=1}^{2i-1} \frac{W_{du}}{O_{u_i}} [\sum_{i=1}^{o_{u_i}} \Pr ob(\frac{X_{ij}^{(u)} - u_{ri}}{\sigma_{r_i}})] + \sum_{i=1}^{2i} \frac{W_{la}}{O_{u_i}} [\sum_{i=1}^{o_{u_i}} \Pr ob(\frac{X_{ij}^{(u)} - u_{ri}}{\sigma_{r_i}})] \quad (5\text{-}3)$$

The comparisons between non-weighted probability and weighted probability are depicted in Figure 38. The performance is improved by about 3.12%. Our results support the suggestion that keystroke durations give more recognisable features and latencies.

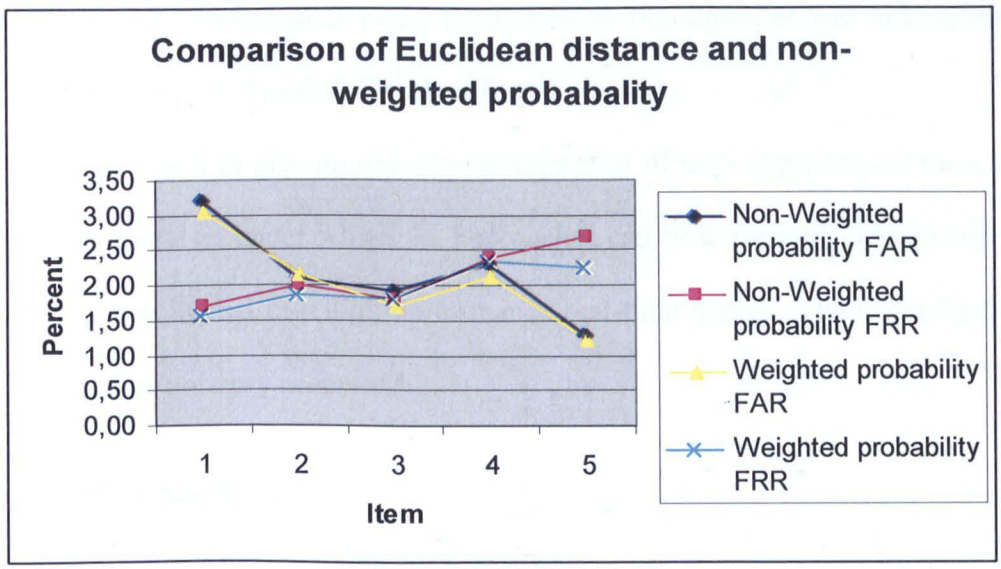


Figure 38: The comparison of FAR & FRR between non-weighted probability and weighted probability

To take the experiment further, we considered using other methods. Bayesian-like classifiers [126] were also tried in our experiment. The approach aims to characterise the performance of the feature-based technique as a function of the number of classes to be discriminated. It is assumed that the feature vectors are distributed with the person who maximises the probability of the measurement vector. The classifier is defined as follows:

Let x_i be the feature vector, σ_i the interclass dispersion vector and ω_i the weight vector, and then the distance of two feature vectors x_i and x_i' are expressed as:

$$\Delta^{\alpha}(x,x') = \sum \omega_i \left(\frac{|x_i - x_i'|}{\sigma_i}\right)^{\alpha} \qquad (5\text{-}4)$$

The feature vectors, $x_1, x_2, ..., x_n$, are derived from keystrokes. The value of α can be adjusted to achieve more robustness – the net effect is a slight improvement in recognition for values of close to one rather than two, as justified by the Gaussian

assumption. The performance using the Bayesian-like classifier was approximately 1.8% over the weighted probability classifier.

It is difficult to give an objective comparison of each approach, as there is no large unified data set under which the approaches can be compared. Meanwhile, the data were not collected in a high-performance real-time system. The accuracy of the data is therefore not very accurate.

5.5 Conclusion

Keystroke dynamics is studied in this chapter in consideration of the special features of a POS PIN pad. We argue that although the use of a behavioural trait (rather than a physiological characteristic) as a sign of identity has inherent limitations, when implemented in conjunction with traditional PIN schemes, keystroke dynamics allows the design of more robust authentication systems than traditional PIN-based alternatives alone.

Compared to its applications in a computer, the major difficulty to adapt keystroke dynamics to a POS terminal is that too few features can be collected. Since the typical PIN is very short, the number of keystrokes is highly limited, typically four to six keystrokes, which means very few features are available for keystroke pattern analysis. This obstacle can be overcome through our proposed approach, which is to let the user intentionally build his special preferred pattern, e.g. by long pressing on specific keys, or by making long intervals between two specific keys. In this way, the limited features of keystroke dynamics become more distinguishable, hence the performance of authentication can be improved.

Different classifiers in pattern recognition of keystroke dynamics achieve correct identification in diverse ways. Compared to the classifier of Euclidean distance measure, probability classification performs better overall. The weighted

probability classification has about 3.12% better performance than non-weighted probability. The results of weighted probability were concluded in the case of assigning 0.6 for key duration and 0.4 for key latency. The performance using the Bayesian-like classifier was approximately 1.8% over the weighted probability classifier. Our research results are not limited to the case of the Supercard scheme. They can also be extended to normal POS terminals and all PIN authentication through a keypad.

Overall, our results validate and suggest that it is possible to use keystroke dynamics to improve the security of payment. Our experiments are based on the hypothesis that the impostors know the PIN. If the PIN is unknown and the keystroke pattern is used as an additional authentication method, the security level of the payment system can be much higher.

To address the issue that keystroke patterns change gradually and unintentionally, e.g. due to the user growing older or becoming more and more familiar with the key layout, an adaptive algorithm is required to have a gradual learning function, which can modify the keystroke dynamic template gradually. The learning ability is the advantage of the neural networks. Building a hybrid neuro-fuzzy logic system could be a very interesting method to use to extend our research.

Chapter 6. Fuzzy-Logic-Based Decision System

Correct decision making in the security sector mainly depends on information, which is received from multiple sources. Often, the information is insufficient, unreliable and contradictive. For example, in the Supercard scheme, fingerprint authentication suggests that the cardholder is a genuine one but the keystroke dynamics authentication suggests the cardholder is a fake one. In such cases with multiple information from different modalities, what kind of decision should be made? To answer this question, this chapter will study information fusion by applying different methods, namely weighted average fusion and fuzzy logic fusion.

6.1 Introduction

Security in payment is becoming more and more complicated. Different applications and different authentication methods are applied, e.g. PIN, biometrics, and multibiometrics. As we have discussed in chapter 4, a multibiometric system refers to the fusion of multiple biometric features, e.g. detecting face, voice and signature together to identify a person. Multibiometric systems have also been approved to be able to help achieve an increase in performance that may not be possible using a single biometric indicator [126][128]. On the other hand, diverse information increases the difficulty of making the right decisions.

The same challenges are posed on our proposed multibiometrics Supercard, which we have discussed in the previous chapters. How to fuse information in the Supercard becomes an unavoidable topic. The typical Supercard authentication procedure is illustrated in Figure 39. It works as follows: depending on different risk levels of transaction (e.g. amount of transaction), different authentication scenarios

can be applied. In a typical high-security scenario, to authenticate whether the user is legitimate, the traditional PIN will be checked first. If the PIN does not match, the normal PIN-authentication mechanism, without consulting the biometrics component, will reject the user. If the PIN does match, the biometrics component will provide a supporting recommendation that verifies that the user is legitimate; that is, the user will be required to swipe through a fingerprint sensor on the card. Furthermore, keystroke patterns during PIN input will also be checked. A keystroke pattern is a biometric that identifies an individual based on their unique typing rhythm (the stop time on a key and the interval between two successive keys). Finally, the system performs an information fusion to give a comprehensive match score.

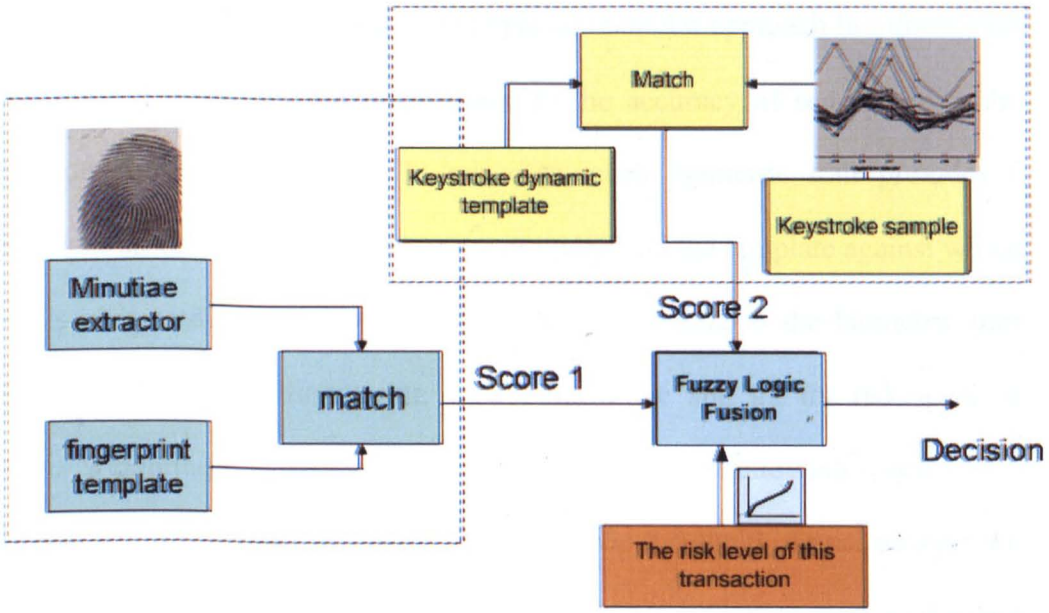


Figure 39: Multiple-modal authentication system based on multiple biometric features and the risk level of transaction

6.2 Levels and Schemes of Information Fusion

Generally, there are various levels of fusion for combining multiple biometric systems: (a) fusion at the feature extraction level, (b) fusion at the matching score level, (c) fusion at the decision level [129]. The fusion at the matching score level can

be conducted as follows: each system provides a matching score indicating the proximity of the feature vector with the template vector. These scores can be combined to assert the veracity of the claimed identity. These techniques attempt to minimise the FRR for a given FAR [13]. Since the match score is the most important indicator for the final decision (accept or reject), this kind of fusion technology plays a critical role in the whole biometric system.

A variety of fusion schemes have been described in the literature to combine these various scores. These include majority voting, sum and product rules, k-NN classifier, SVM (Support Vector Machine), decision trees, Bayesian methods, and fuzzy logic.

The weighted average scheme is a simple and popular approach in information fusion. Usually the weights are proportional to the accuracy of sensors or to the credibility of sensor information. In our case, each biometric trait provides a matching score based on the input feature set provided and the template against which the input is compared. These scores are weighted according to the biometric trait used, for example, w_1 for fingerprint, w_2 for keystroke and w_3 for risk level of transaction. Weighting the matching scores can be done in the following ways:

1) Weighting all traits equally and using a user-specific threshold. Equal weights are assigned to the fingerprint, keystroke and transaction risks and a new score is obtained as

$$S_{fusion} = \sum_{k=1}^{3} \frac{1}{3} S_k \qquad (6\text{-}1)$$

2) User-specific weights. In order to reduce the importance of less reliable biometric traits and increase the influence of more reliable traits, here we assign each user

different weights for different traits as equation 7-2, $w_1 + w_2 + w_3 = 1$ (where w_1 is for fingerprint, w_2 for keystroke and w_3 for risk level of transaction).

$$S_{fusion} = w_1 S_1 + w_2 S_2 + w_3 S_3 \qquad (6\text{-}2)$$

The SVM (Support Vector Machine) scheme is based on the principle of Structural Risk Minimisation [130]. Classical learning approaches are designed to minimise the empirical risk (i.e. error on a training set) and therefore follow the empirical risk minimisation principle. This principle states that better generalisation capabilities are achieved through a minimisation of the bound on the generalisation error. We assume that we have a data set D of M pints in a n dimensional space belonging to two different classes, $+1$ and -1.

$$D = \left\{ \left(x_{k,y_k} \right) | k \in \{1...M\}, x_k \in R^n, y_k \in \{+1,-1\} \right\} \qquad (6\text{-}3)$$

A binary classifier shall find a function f that maps the points from their data space to their label space.

$$f : R^n \rightarrow \{+1,-1\}$$
$$x_k \mapsto y_k$$

The optimal separating surface can be expressed as:

$$f(x) = sign(\sum_i \alpha_i y_i K(x_i, x) + b) \qquad (6\text{-}4)$$

where $K(x, y)$ is a positive definite symmetric function, b is a bias estimated on the training set, and α_i is the solution of the following Quadratic Programming problem:

$$\begin{cases} \min_A W(A) = -A^t I + \frac{1}{2} A^t DA \\ \sum_i \alpha_i y_i = 0 \cdot and \cdot \alpha_i \geq 0, where \\ (i,j) \in [1...M] \times [1...M] \\ (A)_i = \alpha_i \\ (I)_i = 1 \\ (D)_{ij} = y_i y_j K(X_i, X_j) \end{cases} \quad (6\text{-}5)$$

There are some advanced schemes known as artificial intelligence (AI). Neural networks, fuzzy logic and genetic algorithms are regarded as the main types of AI. AI exploits the tolerance for imprecision, uncertainty, and partial truth to achieve tractability, robustness, and low solution cost. In many systems, the information from different sources is insufficient, unreliable and contradictive. Commercially available equipment using fuzzy logic is proliferating tremendously.

Fuzzy logic is being applied in many and varied fields, from a washing machine to mission-critical train control. Fuzzy logic uses multivalued logic to model problems that deal with ambiguous data. It is a generalisation of the traditional bivalent logic, which states that any premise can be either true or false, but not both. The statement "The result of fingerprint match is good" is ambiguous, because where can the line for "good" be drawn? Fuzzy logic holds that everything is a matter of degree; for example, the match score "3.1" of keystroke biometrics belongs 50% to the set of bad and 28% to the set of moderate.

In this chapter, we will focus on the scheme of fuzzy-logic-based information fusion in the application of the Supercard. Section 3 describes the implementation of fuzzy logic. Section 4 presents the fuzzy function, membership and the definition of fuzzy rules. Our experimental prototype is demonstrated and comparisons of different

information fusion schemes will be discussed in Section 5. Conclusions and future works are summarised in Section 6.

6.3 Apply the Fuzzy Logic into Supercard Information Fusion

Fuzzy logic is a powerful tool due to the fact that most of human reasons a concept formation to the use of fuzzy rules. Fuzzy logic can simplify implementation and reduce hardware costs. In addition, conventional techniques in most real-life applications require complex mathematical analysis and modelling, floating-point algorithms, and complex branching. They typically yield a substantial size of object cost, which requires a high-end DSP chip to run. Fuzzy logic enables you to use a simple rule-based approach, which offers significant cost savings, both in memory and processor class.

The fuzzy expert system consists of different processes. The first is fuzzification, which converts the crisp values into a fuzzy linguistic level by the definition of fuzzy sets and membership functions. If-then rule statements are used to formulate the conditional statements that comprise fuzzy logic. Following that, the fuzzy rules are applied and Mamdani or Sugeno's fuzzy inference method is executed, which will lead to an output. After aggregating all outputs, the defuzzification process will be executed to extract a numerical value for the final output.

6.4 Definition of Variables, Membership and Fuzzy Rules

Three inputs have been defined for our fuzzy system. See Figure 41. The first input is the `fingerprint_match_score`, which comes from the result of fingerprint match. It is mapped to a scope [0,10]. Three linguistic level terms are

defined as fuzzy sets: {bad, moderate, good}. For example, for score=3.5 is 0.27 bad, 0.5 moderate and 0.0 good.

The second input is keystroke_match_score, which comes from the result of keystroke pattern match. The data are also mapped into the scope [0,10]. Our experiment and previous researches suggested that keystroke recognition is less precise, thus we only use two sets: {bad, good}. The risk level of transaction is the third input, transaction_risk_level, with two sets: {low, high}.

The system output is the final match score, which is the most important indicator for the final decision (accept/reject). It has four subsets: {very bad, bad, good, very good}.

To fuzzify inputs to a degree of membership between 0 and 1, membership functions must be defined. The fingerprint_match_score can be represented by

$$F = [F_1, F_2, F_3] \tag{6-6}$$

where F_{1-3} are the three subsets of this variable i.e. bad, moderate and good. For example, the F_1 member function can be defined as

$$F_1 = \sum_{i=1}^{N} \mu_{F1}(x_i)/(x_i) \tag{6-7}$$

where x_i is the element of fuzzy subset F_1 and $\mu_{F_1}(x_i)$ is its corresponding membership value with respect to the fingerprint_match_score. For the purpose of simplicity, triangular shape trimf is selected to describe this membership function. The other inputs can be defined with similar methods as above.

Before applying the fuzzy operator and implication method on inputs, If-Then rules must be defined.

Considering a set of rules, R_1, R_2... R_n:

R1: IF $(x \in A_1)$ AND $(y \in B_1)$ AND $(z \in C_1)$ THEN $(s \in D_1)$

R2: IF $(x \in A_2)$ AND $(y \in B_2)$ AND $(z \in C_2)$ THEN $(s \in D_2)$

...

Rn: IF $(x \in A_n)$ AND $(y \in B_n)$ AND $(z \in C_n)$ THEN $(s \in D_n)$

where the A_1, B_1, C_1, D_1 represent the subsets of `fingerprint_match_score`, `keystroke_match_score`, `transaction_riskLevel` and `final_match_result` respectively.

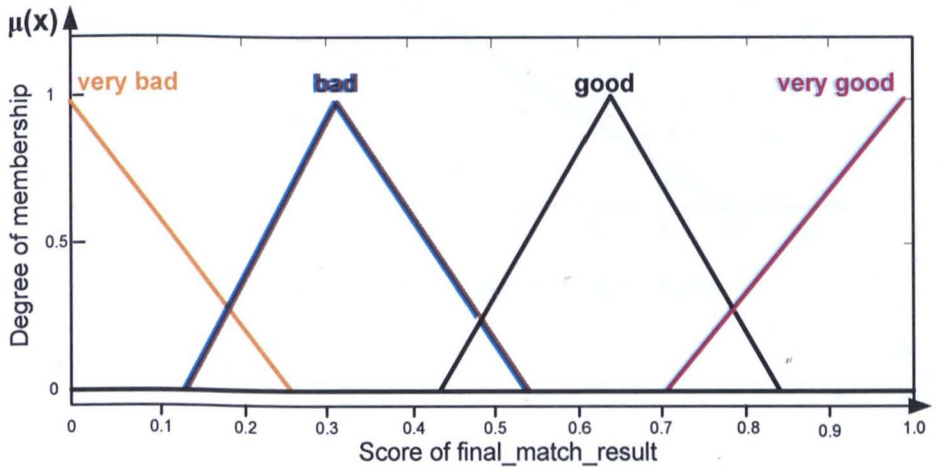
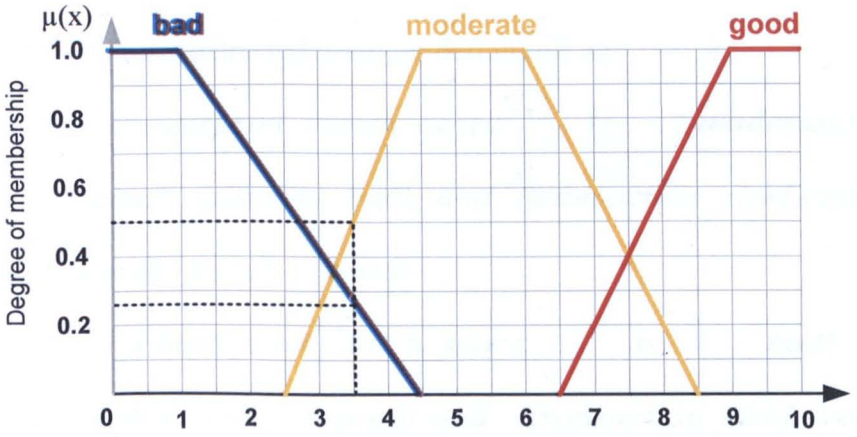
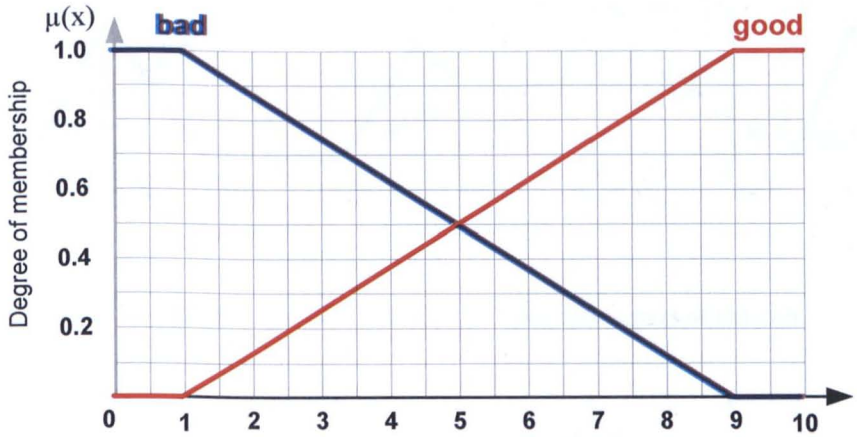


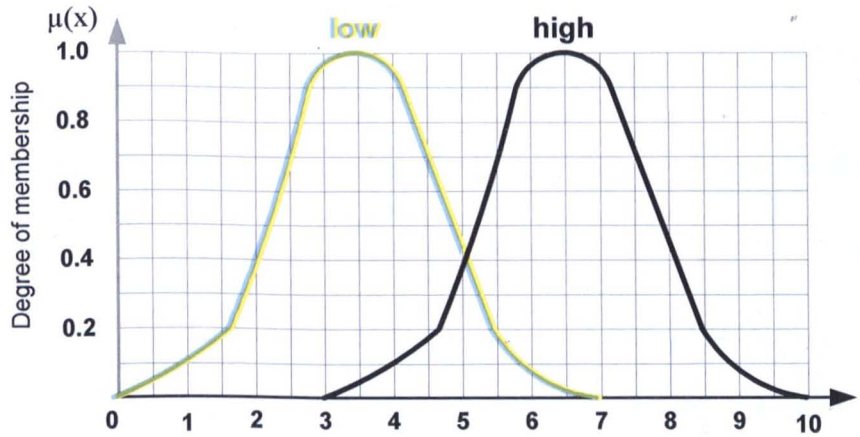
Figure 40: The output of the fuzzy fusion system: final_match_result



(a) input variable: fingerprint_match_score



(b) input variable: keystroke_match_score



(c) input variable: transaction_riskLevel

Figure 41: Membership functions for the three inputs and the output: (a) fingerprint_match_score; (b) keystroke_match_score; (c) transaction_riskLevel; (d) final_match_result

Overall, 16 fuzzy rules have been selected to associate the inputs with the output. Example rules extracted from our definitions are:

*If (Fingerprint_match_score is **moderate**) and (Keystroke_match_score is **bad**) and (transaction_riskLevel is **low**) then (final_match_Result is **good**)*

*If (Fingerprint_match_score is **bad**) and (Keystroke_match_score is **good**) and (transaction_riskLevel is **high**) then (final_match_result is **very bad**)*

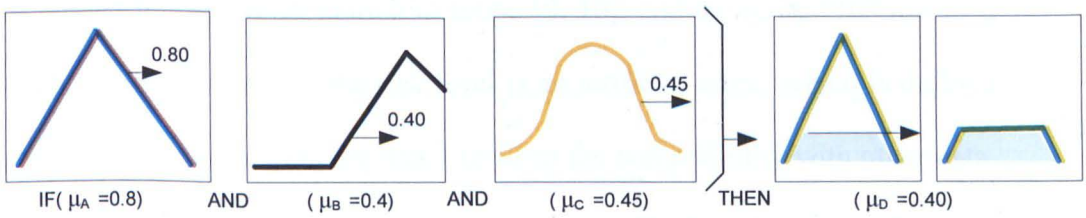


Figure 42: Implication operator AND to the consequent part of the rule

A general fuzzy operation can be demonstrated as:

$$\begin{aligned} m = &\{(F_{11},P_1)\oplus(F_{21},P_1)\oplus\cdots(F_{N1},P_1)\} \\ &\otimes\{(F_{12},P_2)\oplus(F_{22},P_2)\oplus\cdots(F_{N2},P_2)\} \\ &\otimes\cdots\{(F_{1M},P_M)\oplus(F_{2M},P_M)\oplus\cdots(F_{NM},P_M)\} \end{aligned} \tag{6-8}$$

where the symbols $\oplus$ and $\otimes$ represent fuzzy aggregators of union and intersection type, respectively. $F_{ij}(1 \le i \le N, 1 \le j \le M)$ represents the j^{th} feature extracted from the i^{th} signal and *Pj* its admissible position on the waveform [131]. In our application, we just applied the MIN and MAX operations to replace them, as depictured in Figure 42.

Finally, to finish the defuzzification and get a numerical value of `final_match_refult`, the centroid method is used by applying equation 7-6:

$$X = \frac{\int xf(x)dx}{\int f(x)dx} \tag{6-9}$$

where $f(x)$ is the vertical extent of the object at abscissa x.

6.5 Experiments and Results

The experimental database of our information fusion experiments consisted of matching scores obtained from three different modalities – fingerprint, keystroke pattern and risk level for transaction. Among them, the fingerprint and keystroke pattern are biometric data which belong to scope [0, 10], and the score "10" means a perfect match. As a comparison, the risk level is an artificial score, which is defined by us according to the transaction amount. To keep the compatibility with other data, the score of the risk level is controlled in the same scope [0,10], where the "0" means that there is no transaction risk. The mutual non-dependence of the biometric indicators allows us to assign the data of one user to another.

The database itself was constructed as follows: for the fingerprint experiment, we use an FMV2004 fingerprint database [118], which contains 880 impressions from 30 volunteers, together with the Grfinger development kit. The experiment equipment is shown in Figure 43. The keystroke data were achieved from the system as described in Chapter 5. The transaction risk was defined according to the transaction amount.

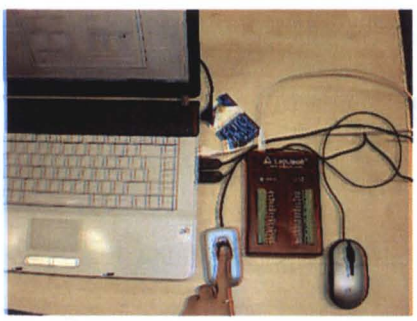


Figure 43: Photo of the test system

Our experiments try to identify the different performance between single biometrics (fingerprint or keystroke), equal and individual weighted fusion schemes. The value of Equal Error Rates (EER) will be measured as a comparison benchmark. The value EER indicates that the proportion of false acceptances is equal to the proportion of false rejections as shown in Figure 44. The lower the equal error rate value, the higher the accuracy of the biometric system.

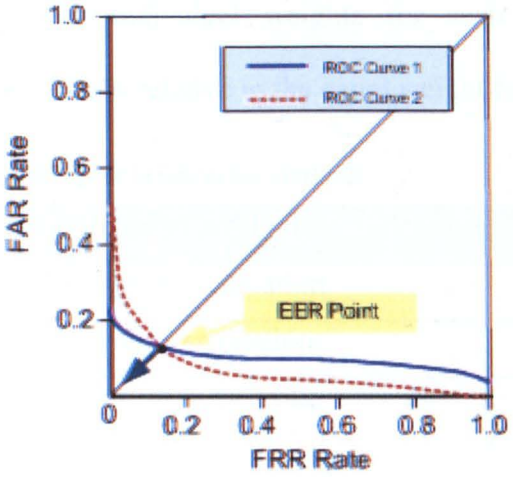


Figure 44: Explanation of EER point

The results of the equal error rates, which we obtained from our tests, are shown in Table 6-1. Items 1 and 2 are the results when fingerprint or keystroke verification is applied alone. Item 3 is the result from equal weighted factors with a combination of fingerprint and keystroke verification, as per equation 6-1.

Item 4 in Table 6-1 was achieved according to equation 6-2. The values of the individual weights are given in Table 6-2. The values were optimised according to the user's personal characteristics. For example, w_1 is assigned to the user No.6 as 0.2, a very low value. The main reason is that we note that the ridge details of this

user are not very clear, and therefore the minutiae-matching algorithm of the fingerprint cannot provide correct matching scores. Similarly, the user No.2 has a very small weight attached to the keystroke biometric, because this aged user has an unstable keystroke style, but she has a clear fingerprint. These demonstrate the importance of assigning user-specific weights to the individual biometric trait. The resulting performance is indicated by the ROC curve in Figure 45. By the equal weighted fusion of the fingerprint and keystroke, the system shows a marked improvement of 18.4% relative to the fingerprint verification only. By the fusion of fingerprint and keystroke with individual weights for each user, the system performance can be improved 21.6% relative to the equal weight fusion scheme.

Table 6-1: Results from different verification methods

Item	Verification method	EER
1	Fingerprint verification	3.80%
2	Keystroke verification	17.36%
3	Fingerprint+Keystroke (equal weighted)	3.10%
4	Fingerprint+Keystroke (individual weighted)	2.43%

Table 6-2: Weights for different traits of ten users

User #	Weight for fingerprint w1	Weight for keystroke w2
1	0.6	0.4
2	0.8	0.2
3	0.7	0.3
4	0.3	0.7
5	0.7	0.3
6	0.2	0.8
7	0.4	0.6
8	0.5	0.5
9	0.6	0.4
10	0.8	0.2

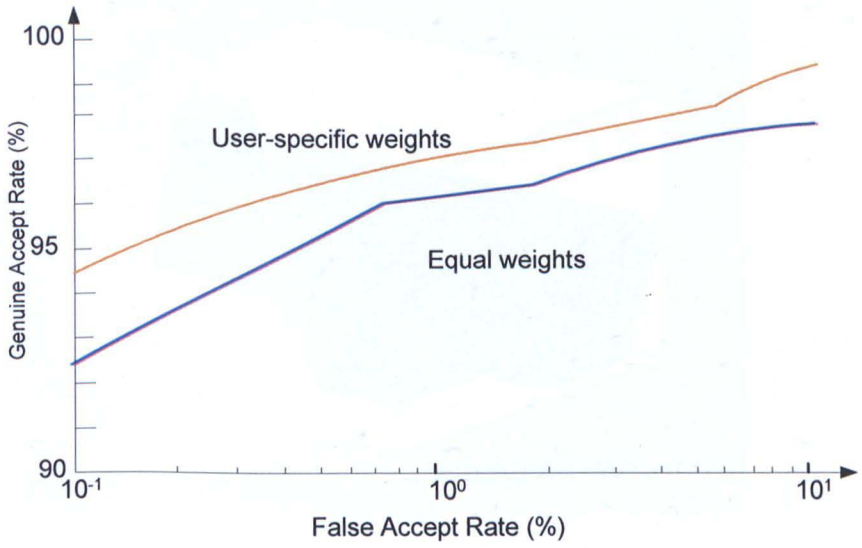


Figure 45: Comparison of equal weights and user-specific weights

It seems that the weighted individual fusion scheme has good performance. However, the disadvantage of this fusion is that we must know the characteristics of each individual clearly in advance, and his/her behaviour must be stable. Obviously, it is not very practical since each bank gets new customers daily, and normally customers want to start to use their payment card immediately. Meanwhile, in complicated situations, the performance of the weighted solution is not good enough.

Our fuzzy logic system has been described in Section 3 and Section 4. We used threefold cross-validation based on the verification data to optimise the parameter values of the Gaussian combination membership functions in the fuzzy sets. The verification set is divided into three equal portions. Each portion is used in turn for testing while the other two are used for optimising the system. The fuzzy system achieved an equal error rate (EER) of 2.62%, and it corresponded a further improvement of 8% relative to fusion with the weighted average scores. The influences of fingerprint and keystroke biometrics have been given in Figure 46.

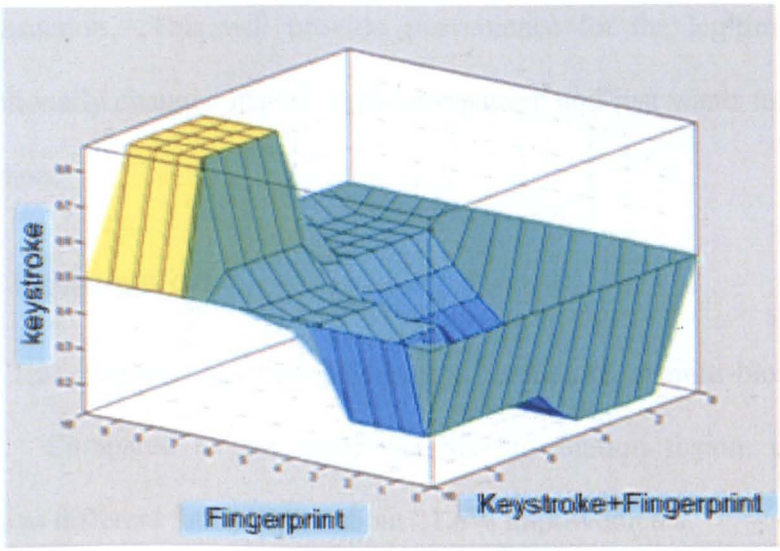


Figure 46: Influence of fingerprint and keystroke biometrics to the match result

Meanwhile, it is observed that our proposed fuzzy-logic-based system does a better trade-off of security and user convenience. For instance, in a case where the `fingerprint_match_score` is 8.83, the `keystroke_match_score` is 1.54, and the `transaction_riskLevel` is 9.87, this means that the fingerprint verification is good; however, the keystroke verification is very bad and the transaction risk is high (e.g. 5000EUR). The fuzzy system generates a `final_match_result` of 0.38, which will prevent this transaction from finishing. This mechanism will prevent a scenario where the impostor fakes a fingerprint and gets the PIN number of a legitimate user, as he/she still cannot finish a big transaction because he/she does not know the right keystroke pattern. In another case (`fingerprint_match_score` is 4.21, `keystroke_match_score` is 2.75, `transaction_riskLevel` is 1.54), both biometrics scores are not very high which will result in a "rejection" in a traditional system. However, our system considers that the risk level of this transaction is low (e.g. 100EUR), and the system

will still generate a `final_match_result` of 0.74 which will still grant for finish the transaction. This will provide convenience for the legitimate user who has unintentionally changed his/her keystroke pattern and just wants to make a low-value transaction.

6.6 Conclusion

This chapter presented information fusions of a multi-biometric verification system. Compared to the equal weights information fusion, using user-specific weights to different factors gave about 21.6% improvements.

Fuzzy logic fusion generated a further improvement of 8% relative to fusion by weighted average scores. The fuzzy logic approach can enhance the consistent information, and at the same time, attenuate the conflict information extracted from all match scores. It is based on three factors: (1) feather of fingerprint, (2) feather of keystroke, and (3) the risk level of the transaction. Member functions and 16 fuzzy rules were defined. We proposed the use of fuzzy logic decision fusion, in order to account for the complex user characteristics.

A trend is growing in visibility related to the set of fuzzy logic in combination with neurocomputing and genetic algorithms. Among various combinations, the one that has highest visibility is a so-called neuro-fuzzy system. In a neuro-fuzzy system, the explicit knowledge representation of fuzzy logic is augmented by the learning power of simulated neural networks. Actually, in our system, the learning function is also essential. For instance, compared with fingerprint, the keystroke pattern is a much less discernible biometric because of its lack of consistency. As the customer becomes more and more familiar with the layout of the PIN input device (PIN-pad), his or her typing style will be gradually and unintentionally changed. To address this issue, an adaptive algorithm is required to have a gradual learning function, which can

modify the keystroke pattern template gradually. Thus, our further work will try to build a hybrid neuro-fuzzy logic system to further improve the performance of our system.

Chapter 7. Development of Supercard Demonstration system

To build a real prototype of the proposed Supercard requires the involvement of semiconductor industries. Many new components, e.g. the slim and flexible display or the slim fingerprint sensor, are still in the development stage and the manufacturers are reluctant to offer detailed information and support. Due to such constraints, it is almost impossible to build a real prototype during this study. Thus we set the target of this simulation to simulate and demonstrate the Supercard operation.

7.1 Demonstration Setup

In this section, we first define the design requirements. Afterwards, the software structures are described in Unified Modelling Language (UML).

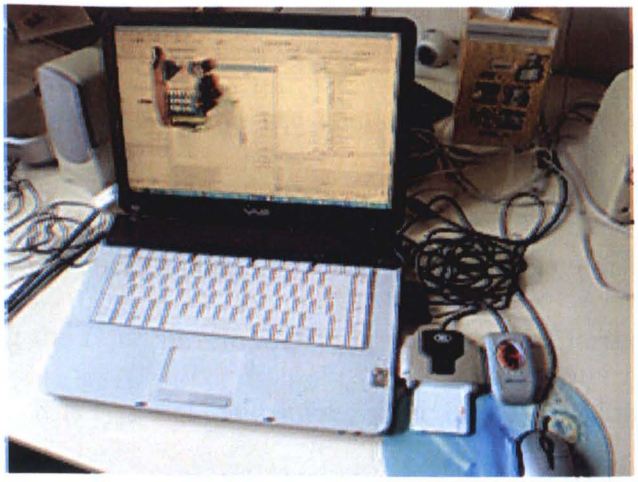


Figure 47: Picture of our prototype and experiment system

The system consists of a computer, fingerprint sensor and smart card reader as in Table 7-1.

Table 7-1: Main equipments in experiments

Items	Description	Specification
Fingerprint sensor	Microsoft Fingerprint Reader connection: USB 1.0, 1.1 or 2.0	Optical Resolution: 512 DPI Image size: 355x390 pixels Colours: 256 levels greyscale
Smart card reader	ACR38 USB 2.0 full speed interface to PC	- Read and write all microprocessor cards with T=0 or T=1 protocols - ISO7816-1/2/3 compatible smart card interface - Support 1.8V. 3V and 5V MCU cards
Notebook	Sony VAIO VGN-FS415M	Intel Pentium 1.73G, 512M RAM Windows XP Version 2002

We assume that studying the Supercard can last many years and the concept can be proven by many people and aspects. Thus, we want to build a flexible and portable demonstration system. The Microsoft .NET framework provides the ability to quickly build, deploy, manage, and use connected, security-enhanced solutions with web services. As an important member of .NET, C# is a modernised object-oriented language-taking benefit of the .NET Framework. A major benefit of C# is that it is able to bring the rapid development paradigm of VB to the world of C++ developer [133][134]. It is type-safe and solves some of the traditional problems for C and C++ programmers: memory leaks, difficulty writing multithreaded applications, static linking, illegal pointer references, overly complex multiple-inheritance rules, and so on.

C# implementation has the above-mentioned advantages and it can also be integrated in other systems more rapidly and in a more agile manner. Moreover, the author had some experience in this language before this project. Therefore, we selected C# as the simulation language.

7.2 Analysis of the Demonstration System

The basic requirements of the Supercard demonstration program are:

- A friendly and easy-to-understand user interface. The interface shall be close to the envisioned Supercard.
- Able to simulate basic functions, e.g. PIN enrolment, PIN verification, issuing error and warning messages.
- The fingerprint can be acquired from the fingerprint sensor. Minutiae can be extracted and depictured clearly in the interface. The fingerprint enrolment and verification function can be dealt with by many experimenters. The verification finally can generate a similarity score in the scope of 0-100.
- The keystroke pattern recognition can be demonstrated. It can record each keystroke and analyse the style of the keying. The different level of difficulties can be set by the user. The keystroke recognition can be integrated with the PIN function. Finally, a keystroke match score between 0-100 can be shown.
- Most application scenarios and advantages of the Supercard can be demonstrated clearly based on this simulation.

Additionally, the following requirements are considered during the simulation program design. The design is driven by several key concerns: reusability, portability and safety.

Reusability: software reuse is the key to significant gains in productivity. Software assets, or components, from requirements and proposals, to specifications and designs, to test suites – anything that is produced from a software development effort can potentially be reused.

Portability: application must be portable across many machines and compliers.

Reliability: the IEEE defines reliability as "The ability of a system or components to perform its required functions under stated conditions for a specified period of time". The simulation program must be robust and stable under the required specifications.

Flexibility: the degree of correctness of a system may decrease as time passes. The user requirements or the system environment can instantly change, affecting the system. The Supercard system modules must therefore be designed to be as flexible as possible, so that they are easy to change and adapt. The developer must always anticipate new requirements later on.

Software safety: software hazards can be identified, tracked and controlled. Hazardous functions (data and commands) can be prevented to ensure safe operation within a system.

Simplicity: the Supercard implementation should be simple, not complex. It must be easy to learn and use.

The Unified Modelling Language (UML) is developed as a graphical language for visualising, specifying, constructing, and documenting the artefacts of a software-intensive system. The Unified Modelling Language offers a standard way to write a system's blueprints, including conceptual things such as business processes and system functions, as well as concrete things such as programming language statements, database schemas, and reusable software components [135]. UML is a

widely recognised and used modelling standard. Thus, we try to use some UML concepts to design our simulation system.

7.3 GUI Design and Use Case Diagram

Use case diagram of UML is used to represent an external view of the whole Supercard simulation program. A use case is a set of scenarios combined together by a common user goal. It is a description of a system's behaviour as it responds to a request that originates from outside of that system [136] (see Figure 48). A user can simulate it to input the numerals and commands through the card keypad.

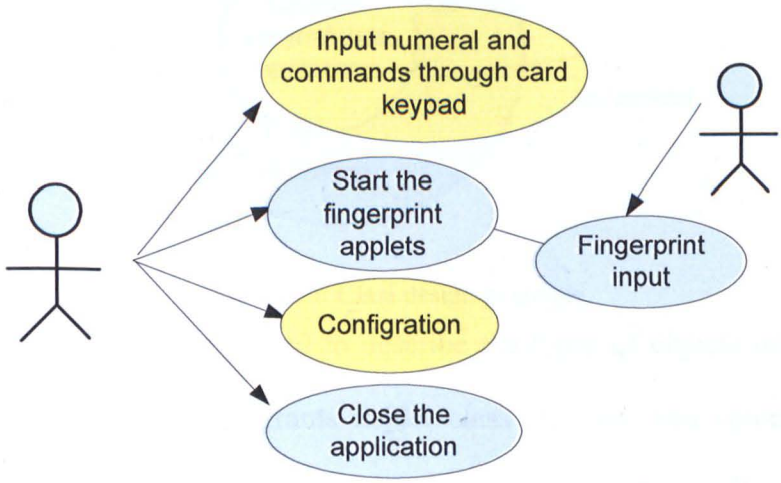


Figure 48: Use case diagram of a Supercard

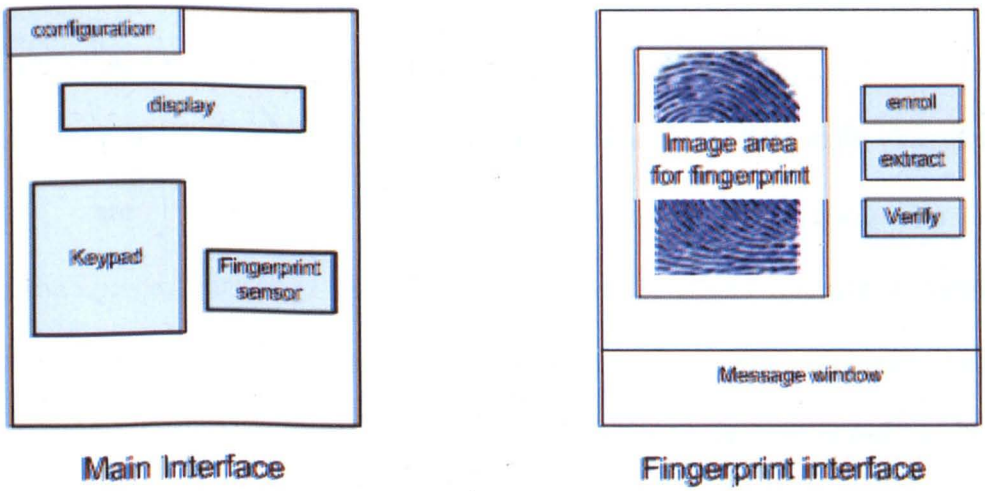


Figure 49: Interface design

The user interface handles the user interaction. It should be very concise and easy to understand. The minimum components present on the interface can be one numerical keypad plus several command keys like OK or Cancel, one small display and one symbol of a fingerprint sensor. To enable the user to make some basic configuration, a small "Config" button can be presented on that, too.

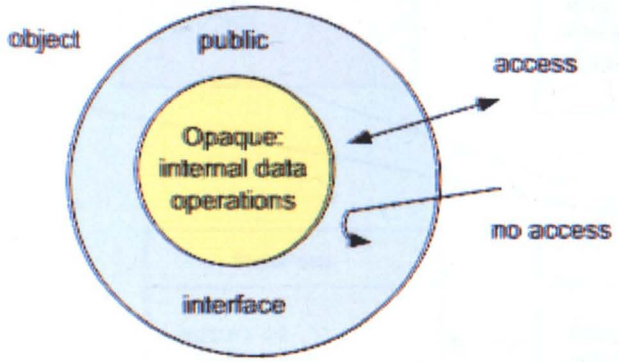


Figure 50: Class design principle

Class diagrams are widely used to describe the types of objects in a system and their relationships. Class diagrams model class structure and contents using design elements such as classes, packages and objects. Figure 50 describes the class design principle [138]. Mutable fields, which can be modified, always belong to the implementation; immutable fields can belong to the interface. The public interface can be accessed and the internal data operations cannot be accessed.

The conceptual class diagram is depicted as Figure 51. The main classes in Supercard are `Config`, `DecisionCenter`, `PINanalysis`, `StrokeAnalysis`, plus class `Form1`, `formMain` and `formOption` which control the user interfaces. The fingerprint implementation part includes class ImageConverter, DBClass, and Util. Relative methods are gathered in the

corresponding class. For example, the class `Util` includes methods `Enroll()`, `ExtracTemplat()` and `Verify(int, ref int)`.

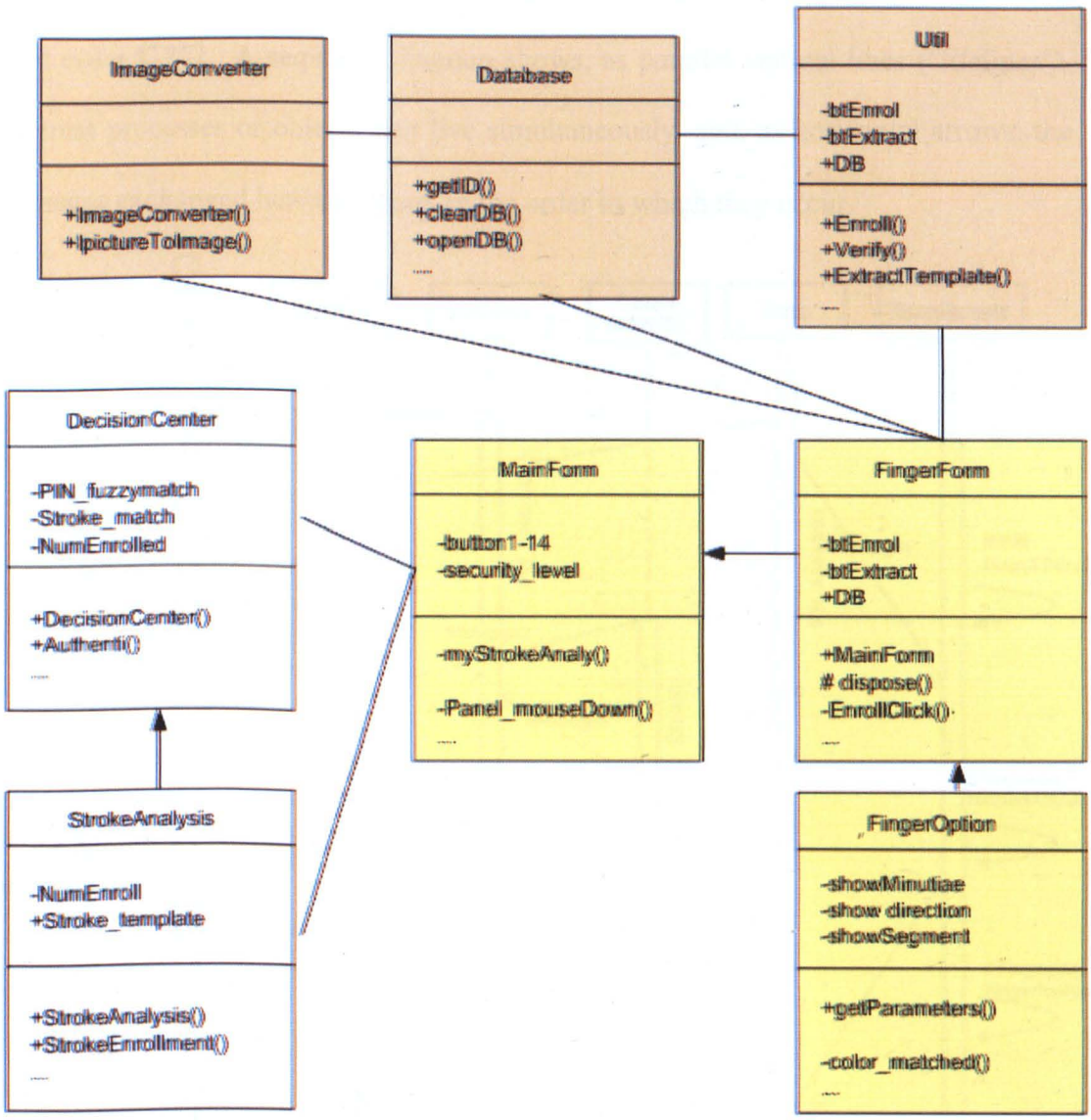


Figure 51: Class diagram

7.4 Sequence Diagram

The sequence diagram also plays an important role in software analyses and design. A sequence diagram (also called interaction diagram) is a UML construct of a Message Sequence Chart. It shows how processes operate with one another and in what order [137]. A sequence diagram shows, as parallel vertical lines ("lifelines"), different processes or objects that live simultaneously, and, as horizontal arrows, the messages exchanged between them, in the order in which they occur.

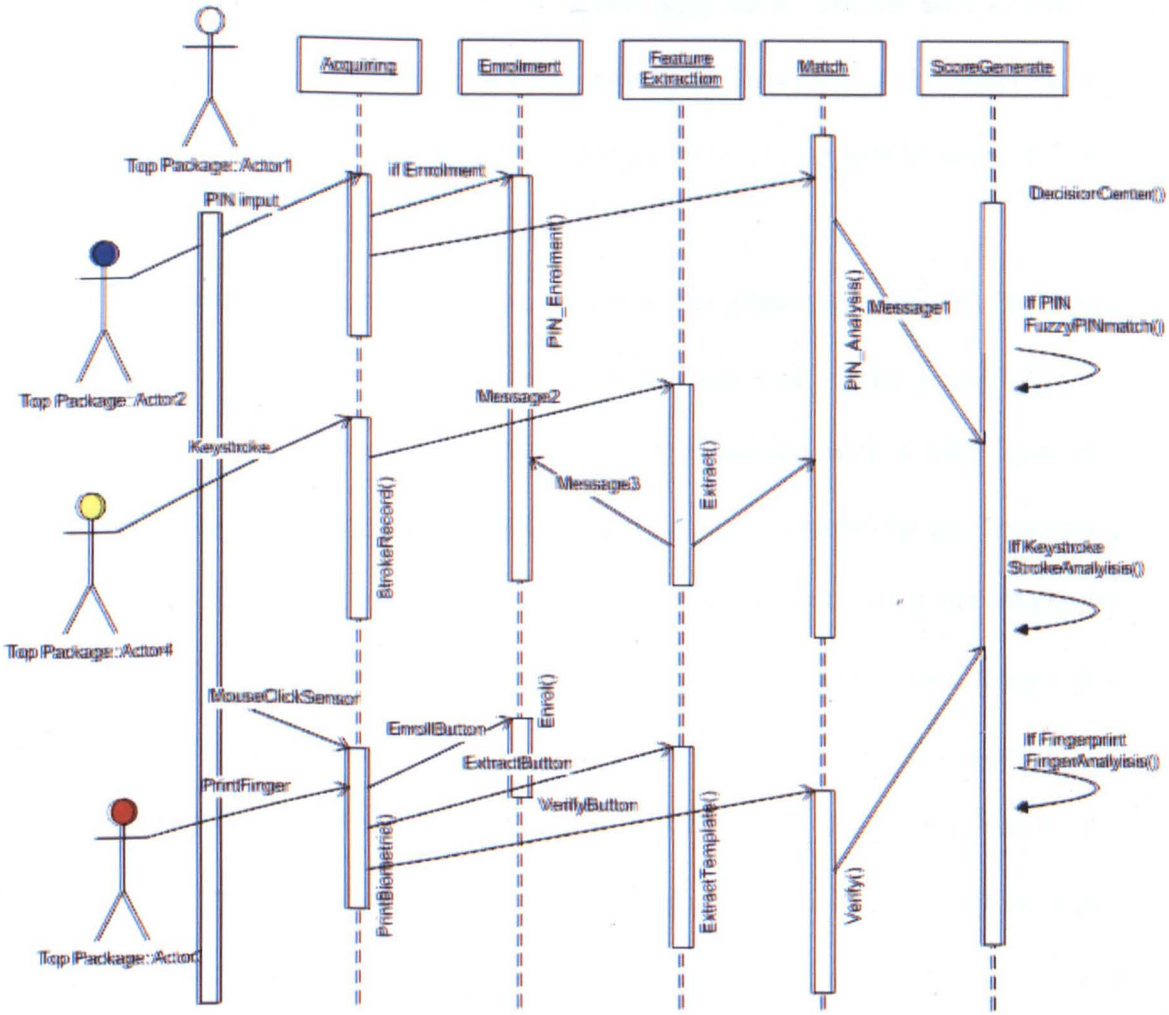


Figure 52: Supercard sequence diagram

The sequence diagram of the Supercard is illustrated as Figure 52. After the main user interface is initiated, the user can decide what kind of authentication to start.

Typically, it will start with a PIN enrolment which is controlled by method `PIN_Enrolment()` to get a PIN template. Afterwards, the system can perform the simple PIN authentication by math with the later-inputted PIN and with the template in method `PIN_Analysis()`.

In the case of keystroke pattern simulation, all the keystroke information (number, duration, latencies) will be recorded by method StrokeRecord(). The recorded information can be used by method `Extract()` to get the keystroke pattern. A template of keystrokes can be accordingly built. For the later keystroke, the keystroke pattern can be matched by method `PIN_Analysis()`. After calling the `DecisionCenter()` and `StrokeAnalysis()`, a match score for the keystroke recognition can be generated.

If fingerprint authentication is necessary, the fingerprint interface can be called by a double mouse click on the sensor symbol on the card. After a user (Actor3) prints a finger on the external sensor, which is connected with a USB port, the fingerprint image will be acquired and shown on the window. In the fingerprint interface, there are three basic function buttons. The Enrolment button can trigger the method `Enrol()` to build a template. The Extract button can trigger the `ExtractTemplate()` to find the fingerprint minutiae (ridges, valleys) and afterwards depict them with a special colour. By clicking the Verify button, the method `Verify()` can be trigged to match the minutiae of the latest input fingerprint image with the template. It can automatically call the `DecisionCenter()` and `FingerAnalysis()` to make a calculation for the similarity, to give a match score of 0-100. If an "Automatic" option is enabled, the fingerprint acquiring, extraction, verification and score generation will be finished at once.

It is also possible in the `DecisionCenter()` to combine the different match methods of PIN, keystroke and fingerprint to generate a final comprehensive score (information fusion).

7.5 Implementation and Verification of the Demo

Corresponding to the software designs, in the coming sections, the implementation will be discussed.

A graphical user interface has been developed as the main interface of the Supercard (see Figure 53). The user interface seems like a smart card held in one hand. The background of the interface is transparent and the interface can be dragged freely, thus it looks very close to a real application. The Supercard has a small LED display, keypad, and a sweeping fingerprint sensor. All application functions are behind this interface. Some implemented classes are shown in Figure 54.

Figure 53: Graphical user interface to simulate the Supercard

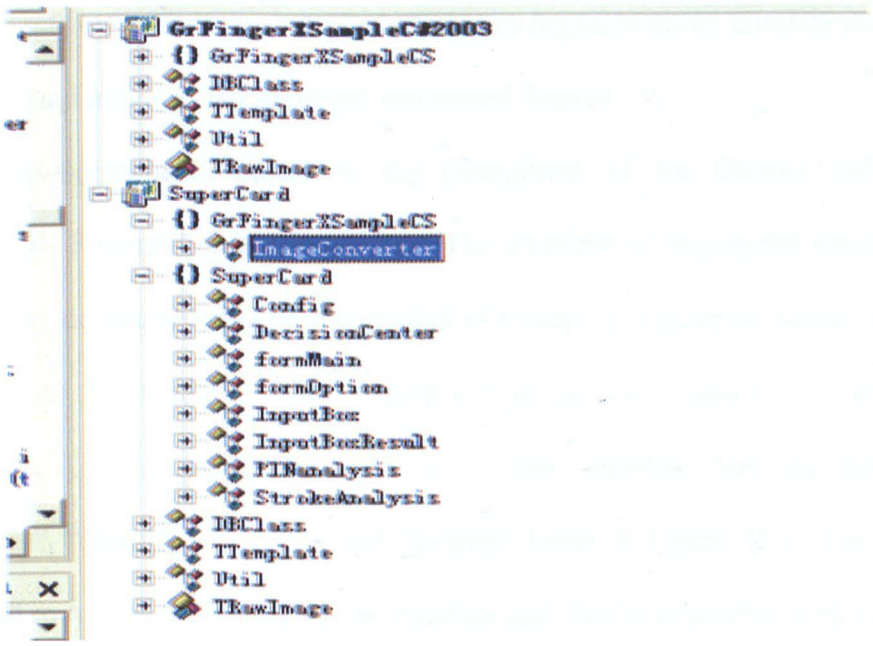


Figure 54: Class diagram

The fingerprint "Catch&Match" function has been implemented as follows. The fingerprints can be input through the Microsoft fingerprint reader. Another possibility is to read images from the FVC2004 Fingerprint database, which was used as a benchmark for different algorithms [118]. Mainly we use the DB3 from the database. The images in the DB3 database were acquired from a thermal sweeping sensor (Atmel FingerChip), and the image size is 300x480, 512dpi. This is quite close to the situation of our application.

The database comes from ninety people as volunteers for providing fingerprints. Volunteers were randomly partitioned into three groups of 30; each group was assigned to a DB and therefore to a different fingerprint scanner. Each volunteer was invited to present him/herself at the collection place in three distinct sessions, with at least two weeks' time separating each session. The forefinger and middle finger of each hand (four fingers total) of each volunteer were acquired by interweaving the acquisition of the different fingers to maximise the differences in

finger placement [118]. This database includes some impressions to simulate extreme skin distortion and rotation, and dried and moistened fingers.

The development is based on the component of the Griaule GrFinger Fingerprint SDK Recognition Library [140]. The interface of fingerprint simulation can be called by double clicking on the symbol of sweeping fingerprint sensor on the Supercard, to invoke the `button1_MouseDown(object sender, System.Windows.Forms.MouseEventArgs e)`. The interface has the function buttons "Enrol", "Identify", "Verify" and "Extract" (refer to Figure 55). The Enrol button is used to record a user fingerprint template and Verify is used to verify a new input fingerprint with the specific template, which was recorded during the enrolment. The minutiae can be automatically extracted and depicted.

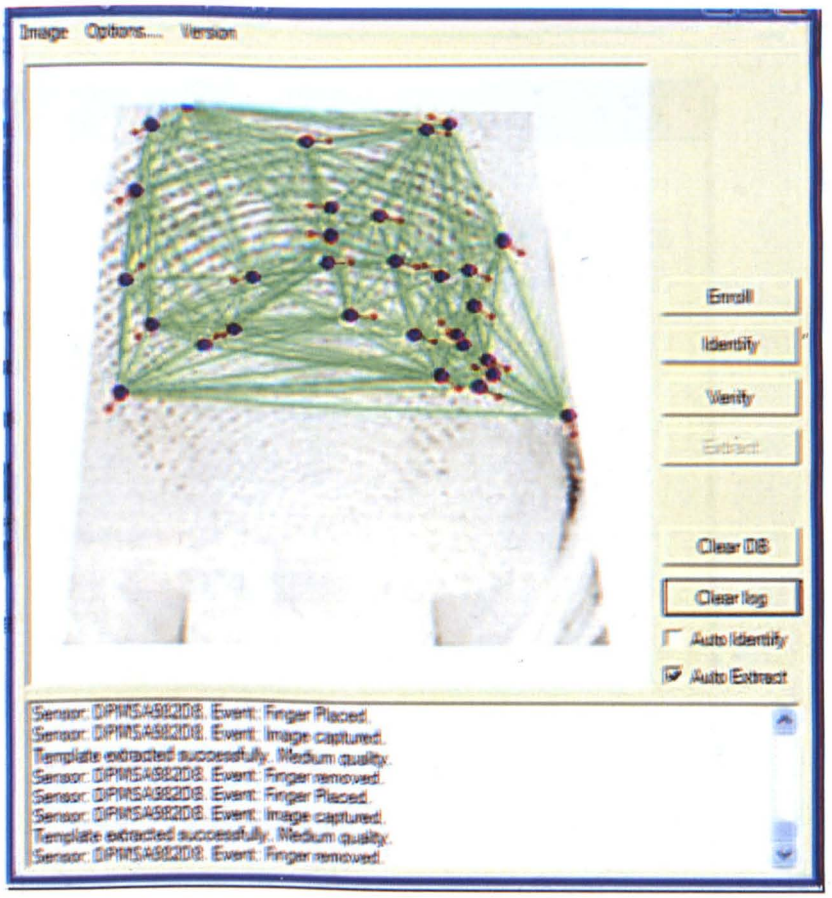


Figure 55: Fingerprint simulation interface

The extracted features (minutiae) can be depicted with different colours, which can be set up by the user. The verification functions are governed by two important parameters: threshold and rotation tolerance. The threshold is the minimum score needed to state that two fingerprints do match. The default value is 45 for the identification process and 25 for the verification process, ensuring a 1% FRR. The rotation tolerance defines the maximum acceptable angle variation (in degrees) between two fingerprints being compared that will result in a match. This value is valid in both clockwise and counter-clockwise directions, so the maximum value that can be set is 180. Depending on the verification results, finally a match score in the scope of 0-100 will be generated. 100 means perfectly matched and 0 indicates nothing is matched.

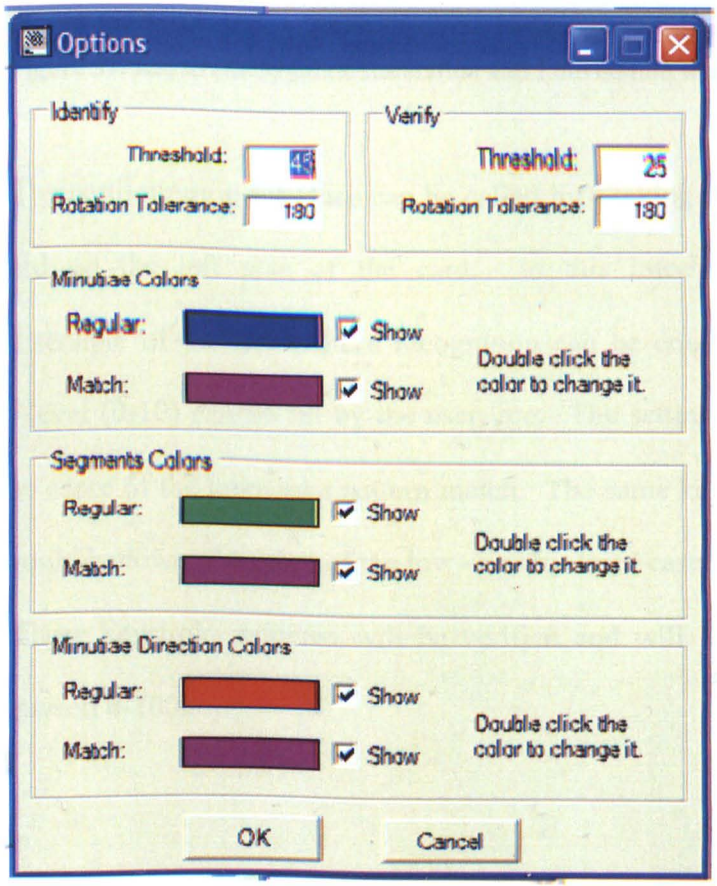


Figure 56: Configuration interface of the fingerprint recognition

The "keystroke dynamics" function has been implemented as follows. In order to check the style of the PIN input, each key pressed time and the interval between the two keys shall be recorded. This can be realised by calling the function `button1_Click(object sender, System.EventArgs e)`. For convenience purposes, at least two small information windows shall appear in the graphic user interface. The down window shows the recorded template – the time interval of the key pressed and the next key. The up window shows the new pattern.

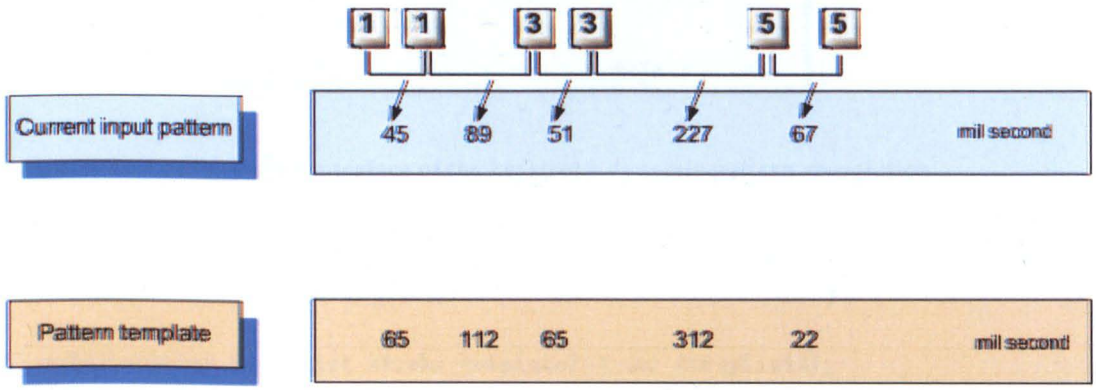


Figure 57: Keystroke dynamic simulation and information windows

The configuration interface can be called by clicking the text "Control" which is located on the left side of the card. In this interface, the enrolment and enable/disenable of the key pattern recognition can be controlled. Meanwhile, the security level (0-10) can be set by the user, too. The setting of a security level will affect the score of the keystroke pattern match. The same keystroke input, the match score, would be lower than that of the low-security-level case.

These keystroke patterns will be verified and will finally generate a match score between 0-100.

Figure 58: Configuration interface of the keystroke dynamic pattern recognition

An example source code is given.

```
public static ArrayList stroke_template2 = new ArrayList();
Form1 myForm;


//public int[] iaStroke_Template = new int[20];

public StrokeAnalysis()
{
    //
    // TODO: Add constructor logic here
    //
}

//match the typing pattern and generate a score of match result
//the scroe scope is 0--100, 0: no match, 100:perfect match
//return: 0: OK  1: failed
public int fuzzyStrokeAnalysis(ArrayList strokeInput)
{
    int StrokeScore=0;

    //if the template is empty, use the default template
    if (stroke_template.Count ==0)
    {
        for (int j=0; j < stroke_Template_default.Length; j++)
            stroke_template.Add(stroke_Template_default[j]);
    }

    if (strokeInput.Count != stroke_template.Count)
        return 0;
```

Since software implementation is not the main target of this thesis, we will not elaborate on it here. The system diagram is shown in Figure 59.

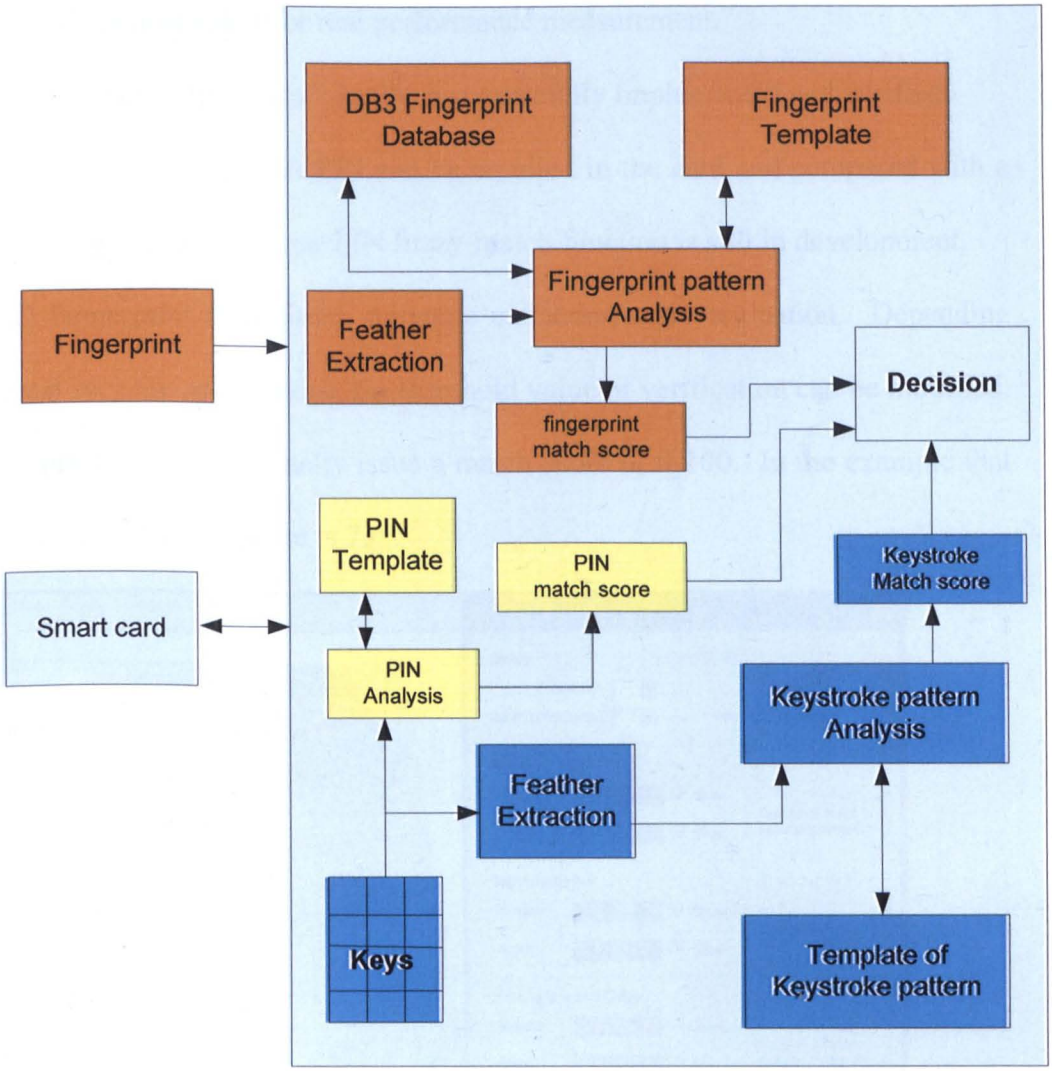


Figure 59: Implementation and function diagram

The envisioned Supercard will work in a special smart card environment with many unusual components which are not commercially available yet. Meanwhile, some common technologies like encryption/description have been widely implemented in smart card industries. It is not very meaningful to make a big effort to repeat such implementation in this thesis project. Thirdly, our prototype was developed based on a PC. The differences between a PC and the new smart card are

huge in terms of CPU and memory. Therefore, due to the specialities of this project, the developed prototype is primarily for demonstrating the functionalities and the security structure, instead of for real performance measurement.

The following functions have been successfully implemented and verified.

(1) PIN verification. A PIN can be enrolled in the card and compared with a PIN that is inputted later. A new PIN fuzzy-match function is still in development.

(2) Fingerprint acquisition, minutiae extraction and verification. Depending on different security applications, the threshold value of verification can be modified. The fingerprint system can finally issue a match score of 0-100. In the example that is given below, the match score is 73.

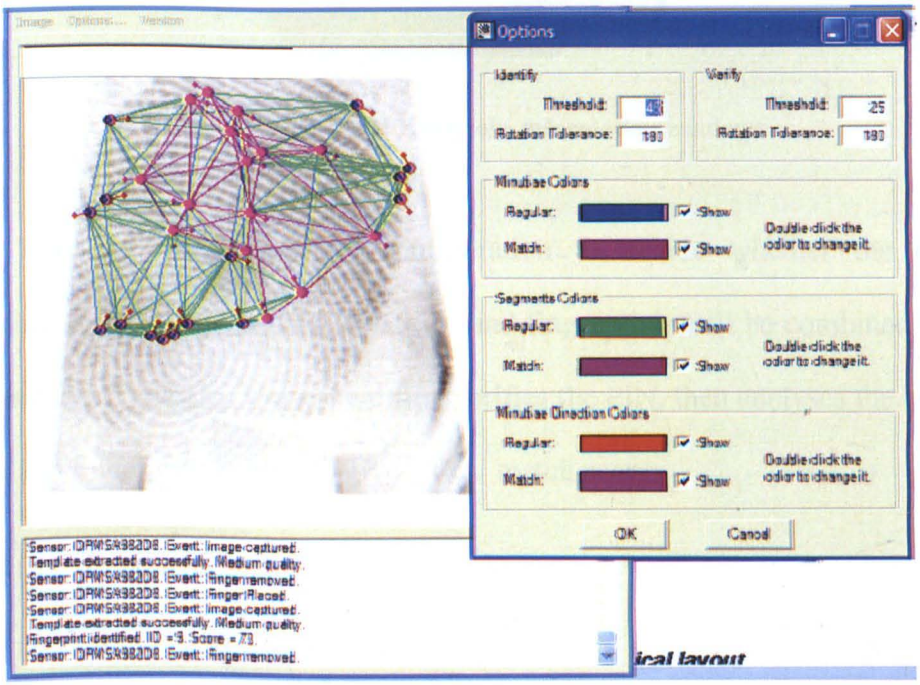


Figure 60: Fingerprint system configuration

(3) Keystroke pattern recognition. Detailed keystrokes can be recorded and the pattern can be extracted successfully. In the graphic interface, we have created two small fields to show the values of the template and the current inputs. Finally, the

keystroke pattern will be analysed to issue a match score of 0-10 as shown in Figure 61.

Figure 61: Keystroke information windows

The user can make the configuration to decide whether the different authentication methods of PIN, keystroke and fingerprint shall be combined together or separately. Typically, the system first verifies the PIN, then analyses the keystroke pattern and fingerprint pattern to give a final match score.

Chapter 8. Conclusion and Further Work

After investigation of several proposed techniques for Supercard and system integration, in this chapter we summarise the conclusion of the research and propose further work based on the study.

8.1 Conclusions

The goal of this research project was to explore how to improve the security of POS terminals at system and application level. We analysed its security in depth mainly on hardware security implementations. We investigated the anti-tampering mechanism of the current POS terminal and showed that the most critical vulnerabilities arise because of poor integration of physical, cryptographic and procedural protection. Based on the current security structure, the PIN pad, the PIN transmission channel and the storage unit of the keys were identified as the fundamental weaknesses. The current tamper-evidence and tamperproof designs are not sufficient to protect them. The major conclusions of the thesis are summarised in the paragraphs below:

1. The proposed Supercard scheme is based on the concept of minimising the POS terminal and combining it with the smart card. This can address many critical security issues of the POS terminal. The Supercard can work as a mini trustable security interface to acquire sensitive information. The scheme also distributes the security risks. The scheme can be represented as four specific approaches to defeat some common but hard-to-prevent attacks.

(i) The "PIN medium" approach can replace the conventional method of PIN inputting through the terminal PIN pad. This method has several advantages. Firstly, it can avoid the PIN being inputted from a fixed POS device, where it could be peeked or recorded by the camera of an adversary. The features of mobility of the Supercard scheme enable the cardholder to input his/her PIN on the Supercard in a safe and private space other than the fixed payment machine location. The PIN can be encrypted before it is sent out of the Supercard. Secondly, since the keypad and the crypto unit are located together in the Supercard scheme, the connection cable between them is very short and protected by the very slim body of the Supercard (<0,8mm). Thirdly, the Supercard is normally always in the possession of the cardholder and the adversary hardly gets a chance to manipulate it. Another big advantage is that the Supercard scheme can be implemented in the current POS system by just modifying the authentication protocol.

(ii). The "Message Verifier" approach was designed to prevent the cardholder from being fooled by manipulated messages. The typical "display" attack scenarios can be prevented. The crypto-unit in the Supercard can authenticate the message and show the right message on the display of the Supercard. Once the cardholder is aware of the difference, he can stop the transaction and avoid being cheated.

(iii). The "Detector of fake or compromised POS terminals" approach has been devised to defeat fake terminal attacks. This type of attack can be carried out through building a fake device, which looks like a POS terminal to cheat and steal the PIN as well as card information. The Supercard scheme can prevent such attacks because its crypto-unit can authenticate the legitimacy of the

POS terminal and give a warning message on the Supercard display immediately.

(iv). The "Tool with multimodal authentication enhanced with biometrics" was designed to meet high-level authentication through a combination of different factors. Through this security tool framework, the PIN and keystroke dynamics have been combined for further development.

2. The security of the fingerprint system can be improved by applying the proposed Supercard scheme. The CMOC approach is based on the Supercard to address vulnerabilities in a biometric payment system. The integrated sensor and encapsulated channel can respond to the threats of channel attacks. The applied biohash template can better protect the privacy as well as prevent the adversary from revealing the real biometric. According to the new authentication protocol based on the Supercard, the fingerprint acquisition, data transferring, feature extraction and patter match etc are all conducted inside the secure Supercard channels. In the case of computing demanding tasks, e.g. feature extraction which cannot be done inside of the Supercard, they can be encrypted and sent out to POS. In all cases, secure communication between Supercard and POS terminal can be built. Thus the CMOC scheme can defeat most biometric channel attacks (the attacker uses line taping, intercepts the biometric data or uses previously-recorded signals to replay attacks) and side channel attacks (by analysing the power dissipation or timing of encryptions in the device to disclose the encrypted information) which exist in a conventional POS terminal.

3. Keystroke dynamics can be used as a behaviour biometric to strength the PIN security in the Supercard or POS terminal. Our studies on keystroke dynamics to reinforce authentications have led to the following conclusions:

(i) Implementing keystroke dynamics in a POS system is feasible and no extra hardware needs to be implemented. The main obstacle lies in the highly limited number of keystrokes and low distinguishability. These difficulties are caused by the specialities of PIN pad, e.g. the typical PIN is short and inputted through a numerical pad. We argue that the distinguishability of features can be improved by users intentionally building specific typing patterns.

(ii) The rates of FAR and FRR are relative to the difficulties of selected PIN, e.g. length and complexity of finger movement over the pad. The best results from our experiment are FAR 1.3% and FRR 1.7%, which are still far too poor to meet the high accuracy requirements of payment authentication. Keystroke dynamics can only be used as an auxiliary authentication method.

(iii) The weighted probability classification (in case of assigning 0.6 for key duration and 0.4 for key latency) has about 3.12% better performance than the non-weighted probability between non-weighted probabilities.

4. The multimodal authentication resources in Supercards or terminals can be integrated through fuzzy-logic information fusion. We have investigated the fusion of fingerprints, keystroke patterns, PIN and risk levels through fuzzy logic. Different match results are first mapped to a score of 0-10, and afterwards, 16 fuzzy-logic rules are defined. Following that, the fuzzy rules are applied and Mamdani's fuzzy inference method is executed, which will lead to an output. After aggregating all outputs, the defuzzification process will be executed to extract a numeric value for the final authentication result. Meanwhile, information fusion by weighting individual biometric traits has been investigated. The improvement has been observed by this method.

5. Disturbing the core security unit by generating extremely strong electromagnetic fields can be a potential vulnerability of the tamperproof design of a key unit in POS. This issue is first raised by this thesis research. Under extreme electromagnetic conditions, if the security CPU is out of order even just for a very short time, or the security software cannot run properly, the security alarm can be disabled and the encryption keys or sensitive data can be read out. In terms of hardware implementation, preliminary investigations have been conducted on how to protect the key store unit. New approaches are proposed which exploit the features of the BGA package, or features of ceramic fragility, hardness and electric isolation.

As a summary, the attacks or threats which have been addressed by the proposed approaches in this thesis are listed below in Table 8-1.

Table 8-1: Security threats addressed by our proposed approaches

Description of Attacks or threats	**Addressed Degree** (5★ is well addressed)	**Approach and Remark**
PIN visual disclosure through peek or camera record (refer to Section 2.2.1)	★★★★★	PIN medium (refer to Section 3.4.1)
PIN disclosure through remote monitoring, electromagnetic radiation, noise, beep sounds, or by putting transparent membrane on keypad to record PIN (refer to Section 2.2.1)	★★★★★	PIN medium (refer to Section 3.4.1)
Build a fake terminal to steal PIN, biometrics and card information (refer to Section 2.2.1)	★★★★★	Detector of fake terminal (refer to Section 3.4.3)
PIN disclosure through line tapping (refer to Section 2.2.1)	★★★★★	PIN medium (refer to Section 3.4.1)
Cardholder is cheated by manipulated messages shown in terminal display (refer to Section 2.2.1)	★★★★★	Message Verifier (refer to Section 3.4.2)
Intrusive attacks on core security tamperproof package (refer to Section 2.3.1)	★★★	BGA package and ceramic-based package (refer to Section 3.6.1 and 3.6.2)
Potential high-intensity electromagnetic attacks on core security	★	Discovered by us (refer to Section 3.6.3)

(refer to Section 3.6.3)		
The weakness of cryptography algorithms (refer to Section 2.5.1)	★★	Update to ECC and AES (refer to Section 3.5.3)
Biometric channel attacks: use line taping, intercept the biometric data (refer to Section 4.2.1)	★★★★★	CMOC scheme (refer to Section 4.3)
Biometric replay attacks: use previously recorded signal to replay	★★★★	CMOC scheme (refer to Section 4.3)
Attacks on biometric templates Concerns on customer privacy (refer to Section 4.2.1)	★★★★	CMOC scheme (refer to Section 4.3)
PIN authentication alone is not strong enough (refer to Section 5.1)	★★★	Reinforced with fingerprint (refer to Section 4.3)
PIN authentication alone is not strong enough (refer to Section 5.1)	★★★★	Reinforced with keystroke dynamics (refer to Section 4.3)
Fingerprint authentication alone is not strong enough (refer to Chapter 6)	★★★	Reinforced with keystroke dynamics and PIN to build multimodal system (refer to Chapter 6)
Difficulty in making the right decision based on multimodal authentication (refer to Chapter 6)	★★★★	Fuzzy-logic-based information fusion (refer to Chapter 6)

8.2 *Future Research*

Our research has investigated POS security in the context of more secure protocols, tamperproof boxes and biometrics. In spite of this attention, the problems of POS security continue to harbour plenty of challenges for modern society. I conclude this thesis by suggesting possible ways in which the research presented here may be expanded in order to bring the Supercard from concept to a successful product.

1. The Supercard requires more software and hardware resources than the current smart card. The most suitable microprocessor, memory type and size need to be specified. Power supply and power management can be hard issues. We have made some preliminary investigation from hardward and system level on this topic in APPENDICES A: Feasibility Study of the Supercard on Industrial Implementation. Meanwhile the software operation system must be enhanced to meet the challenges of the Supercard.
2. For the keystroke pattern recognition in payment systems, the typing style of the user will be gradually and unintentionally changed (e.g. after the customer becomes more and more familiar with the key layout). To address this issue, an adaptive algorithm is required to have a gradual learning function, which can modify the keystroke pattern template gradually. The learning ability is the advantage of neural networks. Building a hybrid neuro-fuzzy logic system can be very interesting work to extend our research.
3. For the traditional terminals, an electromagnetic attack can be a very dangerous threat. In Section 2.3, we posed the risk that if attackers generate a very strong electromagnetic field to paralyse the CPU of the security unit, they can break a tamperproof box without triggering the alarm. Due to the limitations of equipment, we have not carried out this research. However, after discussions with several senior security engineers in POS security, we feel this threat is real and very dangerous. To the author's knowledge, most people still ignore this risk and there are no official requirements against such attacks. Thus, research on this topic shall be set up.
4. We used fuzzy logic to perform the information fusion. The result meets our original target. However, the parameters as well as the profile curves need to

be further optimised. Fusion at the matching score level is the most popular approach to multibiometrics due to the ease in accessing and consolidating the scores generated by multiple matchers. Fusion at the feature extraction (representation) level is expected to be more effective due to the richer source of information available at this level. However, it would be difficult to concatenate two incompatible feature sets like the keystroke pattern and minutiae points of fingerprints. Therefore, more studies are required.

References

[1] P. Peyret, G. Lisimaque and T.Y. Chua, 'Smart cards provide very high security and flexibility in subscribers management', IEEE Transactions on Consumer Electronics, Volume 36, Issue 3, 1990, pp. 744–752.

[2] D. Sternglass, 'The future is in the PC cards', IEEE Spectrum 296, 1992, pp. 46–50.

[3] David M'Raïhi and Moti Yung, 'E-commerce applications of smart cards', Computer Networks, Volume 36, Issue 4, 16 July 2001, pp. 453-472.

[4] Ingenico Group, Payment terminal manufacturer, Website. www.ingenico.com.

[5] R.L. Rivest, A.Shamir, and L. Adleman, 'A method for obtaining digital signatures and public key cryptosystem', Commun. Of the ACM, 21:120-126, 1978.

[6] National Bureau of Standards, 'Data Encryption Standard', Federal Information Processing Standards Publication 46, January 1977.

[7] EMV 4.2, The latest specification published by Europay, MasterCard and Visa. It consists of four books. They can be downloaded from http://www.emvco.com.

[8] Arun Abraham Ross. 'Information Fusion in Fingerprint Authentication'. PhD Thesis. Department of Computer Science & Engineering, Michigan State University. 2003.

[9] Chunlei Yang, Guiyun Tian and Steve Ward, 'Biometric Based Smart Card for Security', Proceedings of ICETE'05", the 2nd International

Conference on E-business and Telecommunication Networks, Reading, UK, 2005.

[10] Chunlei Yang, Guiyun Tian, and Steve Ward, 'Security systems of point-of-sales devices', the International Journal of Advanced Manufacturing Technology, Volume 34, Number 7-8, Springer London. ISSN 0268-3768. April 2006.

[11] J. L. Wayman, 'Fundamentals of biometric authentication technologies', International Journal of Image and Graphics, vol. 1, no. 1, 2001, pp. 93-113.

[12] A. K. Jain, R. Bolle, and S. Pankanti, eds., 'Biometrics: Personal Identification in Networked Society', Kluwer Academic Publishers, 1999.

[13] L. O'Gorman, 'Seven issues with human authentication technologies', in Proc. of Workshop on Automatic Identification Advanced Technologies (AutoID), Tarrytown, New York, Mar 2002, pp. 185-186.

[14] George Walner, 'A biometric solution is ideal at the point of sale', Biometric Technology Today, Volume 10, Issue 3, 31 March 2002, pp. 7-8.

[15] T. Matsumoto, H. Matsumoto, K. Yamada and S. Hoshino, 'Impact of Artificial Gummy Fingers on Fingerprint Systems', Proceedings of SPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, 2002.

[16] Benoît Chevallier-Mames, Mathieu Ciet, Marc Joye, 'Low-Cost Solutions for Preventing Simple Side-Channel Analysis: Side-Channel Atomicity', IEEE Transactions on Computers, June 2004, pp. 760-768.

[17] G. Hachez, F. Koeune, and J.-J. Quisquater, 'Biometrics, access control, smart cards: a not so simple combination', in Proc. 4th Smart Card

Research and Advanced Applications Conference (CARDIS 2000), pp. 273-288.

[18] Patrick Schaumont and Ingrid Verbauwhede, 'Domain-Specific Codesign for Embedded Security', Computer, April 2003, pp. 68-74.

[19] Philip Koopman, 'Embedded System Security', Computer, July 2004, pp. 95-97.

[20] Visa international service association, 'PIN Management Requirement: PIN Entry Device Security Requirements Manual', March 2004, Version 3.0a.

[21] RSA Laboratories homepage, http://www.rsasecurity.com.

[22] Doron Av and Staine Shlomo, 'Method and device for providing secure of an electronic authorization/credit card', USA patent application number: US20030363779 20030916, 2004.

[23] European Card, 'MasterCard's chip authentication programme makes its mark in Europe and Brazil', European Card Review. January/February 2004.

[24] Wolfgang Rankl, 'Overview about attacks on smart cards, Information Security Technical Report', Volume 8, Issue 1, March 2003, pp.67-84.

[25] Ross Anderson and Markus Kuhn, 'Low Cost Attacks on Tamper Resistant Devices, Proceedings of the 5th International Workshop on Security Protocols', Springer-Verlag LNCS No.1361, April 1997, pp.125

[26] D. Boneh, 'Twenty years of attacks on the RSA cryptosystem', Notices of the American Mathematical Society (AMS), Vol. 46, No. 2, 1999, pp. 203-213.

[27] Berni Dwan, 'Research review', Network Security, Volume 2004, Issue 3, March 2004, pp. 17-18.

[28] Andrew J Clark, 'Tamper Resistant Systems in Cryptographic Equipment', Eurocrypt '87, Amsterdam, Springer-Verlag, 1987.

[29] P. Kocher, J. Jaffe and B. Jun, 'Differential Power Analysis, Advances in Cryptology', Crypto 99, Proceedings, Lecture Notes In Computer Science Vol. 1666, M. Wiener ed., Springer-Verlag, 1999.

[30] T.S. Messerges, E.A. Dabbish and R.H. Sloan, 'Examining Smart-Card Security under the Threat of Power Analysis Attacks', IEEE Transactions on Computers, May 2002, pp. 541-552.

[31] Gandolfi, K., Mourtel, C. and Oliver, F., 'Electromagnetic Analysis: Concrete Results', CHES 2001, vol. 2162 of Lecture Notes in Computer Science, Springer-Verlag, 2001, pp. 251-261.

[32] P. Kocher, 'Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems', Advances in Cryptology - Crypto 96 Proceedings, Lecture Notes In Computer Science Vol. 1109, N. Koblitz ed., Springer-Verlag, 1996.

[33] David Brumley and Dan Boneh, 'Remote Timing Attacks Are Practical', 12th USENIX Security Symposium, Washington, DC, USA, August 4-8, 2003.

[34] M. Matsui, 'The First Experimental Cryptanalysis of the Data Encryption Standard', Advances in Cryptology: Proceedings of CRYPTO '94, Springer-Verlag, August 1994, pp. 1-11.

[35] Eli Biham and Adi Shamir, 'Research announcement: A new cryptanalytic attack on DES', posted to cypherpunks@toad.com, October 18, 1996.

[36] Feng Bao, Robert Deng, Yongfei Han, Albert Jeng, Desai Narasimhalu and Teow Hin Nagir, 'New Attacks to Public Key Cryptosystems on Tamper proof Devices', 29 Oct. 1966.

[37] Sergei Skorobogatov, 'Low temperature data remanence in static RAM', Technical Report No. 536, University of Cambridge, June 2002.

[38] Sergei Skorobogatov and Ross J. Anderson, 'Optical Fault Induction Attacks', Springer-Verlag Berlin Heidelberg , LNCS 2523, pp. 2–12, 2003.

[39] Peter Gutmann, 'Data Remanence in Semiconductor Devices', 10th USENIX Security Symposium, Washington, D.C., USA , August 13–17, 2001.

[40] Sean W. Smith and Steve Weingart, 'Building a High-Performance, Programmable Secure Coprocessor', Computer Networks, 31, April 1999, pp. 831–860.

[41] David Samyde, Sergei Skorobogatov, Ross Anderson and Jean-Jacques Quisquater, 'On a New Way to Read Data from Memory', First International IEEE Security in Storage Workshop, Greenbelt, Maryland, December 11 - 11, 2002.

[42] Hongxia Wang, Samuel V. Rodriguez, Cagdas Dirik, and Bruce Jacob, 'Electromagnetic Interference and Digital Circuits: An Initial Study of Clock Networks', IEEE International Symposium on Electromagnetic Compatibility, 2006.

[43] RJ Anderson, 'Why Cryptosystems Fail', Communications of the ACM v 37 no. 11, Nov 94, pp 32-40.

[44] Bart Kienhuis, Ed F. Deprettere, Pieter van der Wolf and Kees Vissers, 'A Methodology to Design Programmable Embedded Systems', SAMOS: Systems, Architectures, Modeling, and Simulation, LNCS 2268, Springer, 2001, pp. 18-37.

[45] Thomas S. Messerges, 'Power Analysis Attack Countermeasures and Their Weakness', CEPS-Communication, Electromagnetic, Propagation & Signal Processing Workshop, October 12, 2000.

[46] Dallas Semiconductor, 'DS5240 High-Speed Secure Microcontroller Data sheet', 2007.

[47] S. Janssens, J. Thomas, W. Borremans, P. Gijsels, I. Verbauwhede, F. Vercauteren, B. Preneel and J. Vandewalle, 'Hardware/Software Co-Design of an Elliptic Curve Public-Key Cryptosystem', Proc. Workshop Signal Processing Systems, IEEE CS Press, 2001, pp. 209-216.

[48] Joan G. Dyer, Mark Lindemann, Ronald Perez, Reiner Sailer, Leendert van Doorn, Sean W. Smith and Steve Weingart, 'Building the IBM 4758 Secure Coprocessor', Computer, October 2001 pp. 57-66.

[49] R. Anderson and M. Kuhn, 'A Cautionary Note of Tamper Resistance', Proc. 2nd Usenix Workshop Electronic Commerce, Usenix, 1996, pp. 1-11.

[50] Mike Bond and Ross Anderson, 'API-level Attacks on Embedded Systems', Computer, October 2001, pp. 67-75.

[51] Hun-Chen Chen and Jui-Cheng Yen, 'A new cryptography system and its VLSI realization', Journal of Systems Architecture 49, 2003, pp. 355–367.

[52] Philip Hunter, 'Hardware-based security: FPGA-based devices, Computer Fraud & Security', Volume 2004, Issue 2, February 2004, pp. 11-12.

[53] G.P. Saggese, L. Romano, N. Mazzocca and A. Mazzeo, 'A tamper resistant hardware accelerator for RSA cryptographic applications', Journal of Systems Architecture, Volume 50, Issue 12, December 2004, Pages 711-727.

[54] M. Ernst, B. Henhapl, S. Klupsch and S. Huss, 'FPGA based hardware acceleration for elliptic curve public key cryptosystems', The Journal of Systems and Software, Volume 70, 2004, pp. 299–313.

[55] VeriFone, 'Securing Trust in the Payment Industry', technical white paper, April 2003.

[56] Visa international Service Association, 'Visa online PIN device Derived Test Requirements', Version 3.0, November. pp. 33-43.

[57] Visa international Service Association, 'Visa offline PIN entry device derived test requirements', version 1.0, 2002.

[58] Saar Drimer, Steven J. Murdoch and Ross Anderson, 'Thinking inside the box: system-level failures of tamper proofing', Technical Report Number 711 Computer Laboratory UCAM-CL-TR-711 ISSN 1476-2986, 2008.

[59] Killourhy S. Kevin and Maxion A. Roy, 'Comparing Anomaly-Detection Algorithms for Keystroke Dynamics', In International Conference on Dependable Systems & Networks., Lisbon, Portugal, 2009, pp.125-134.

[60] Tom Kean, 'DES Key Breaking, Encryption and Decryption on the XC6216 Ann Duncan', IEEE Symposium on FPGAs for Custom Computing Machines, April 1998, Napa Valley, California, pp. 310.

[61] J. Irwin and D. Page, 'Using Media Processors for Low-Memory AES Implementation', Proceeding of the IEEE International Conference on Application-Specific Systems, Architectures, and Processors (ASAP'03), June 2003, pp. 144.

[62] William E. Burr, 'Selecting the Advanced Encryption Standard National Institute of Standards and Technology', Security & Privacy, Volume 1, No.2, April 2003, pp. 43-52.

[63] Linda Dailey Paulson, 'US picks new encryption standard', Computer, Volume 33, No. 12, December 2000, pp. 20-23.

[64] W. Diffie and M.E. Hellman, 'Exhaustive cryptanalysis of the NBS data encryption standard', Computer, Volume 10, 1977, pp. 74-84.

[65] Cormen, Thomas, Charles Leiserson and Ronald Rivest, 'Introduction to Algorithms', MIT Press and McGraw-Hill, ISBN 0-262-03293-7, pp. 881–887.

[66] B.S. Kaliski, Jr, 'RFC 1319: The MD2 Message-Digest Algorithm', RSA Laboratories, April 1992.

[67] R.L. Rivest, 'The MD4 message digest algorithm', Advances in Cryptology -- Crypto '90, Springer-Verlag, 1991, pp. 303-311.

[68] W.C. Ku and S.M. Chen, 'Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards'. IEEE Trans. On Consumer Elect., Volume 50, 2004, pp.204-207.

[69] Xiaomin Wang and Wenfang Zhang, 'An efficient and secure biometric remote user authentication scheme using smart cards', 2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, DOI 10.1109/PACIIA.2008.382913, 2008.

[70] J.K. Lee, S.R. Ryu and K.Y. Yoo, 'Fingerprint-based remote user authentication scheme using smart cards', Electronics Letters, Vol.38, 2002, pp.554-555.

[71] M.K. Khan, J.S. Zhang and X.M. Wang, 'Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices', Chaos Solitons & Fractals, Volume 35, 2008, pp.519-524.

[72] R.L. Rivest, 'RFC 1321: The MD5 Message-Digest Algorithm', Internet Activities Board, 1992.

[73] EMV group, 'Integrated Circuit Card Specification for Payment System', EMV Book2- Security and key Management, December 2000, pp.7-8 and pp. 66-69.

[74] Giampaolo Bella, Fabio Massacci and L. C. Paulson, 'The verification of an industrial payment protocol: the SET purchase phase', 9th ACM Conference on Computer and Communications Security, 2002, pp. 12–20.

[75] Giampaolo Bella, 'Inductive Verification of Smart Card Protocols', J. Computer Security Volume 11, Issue 1, 2003, pp.87–132.

[76] Darrel Hankerson, Alfred Menezes and Scott Vanstone, 'Guide to Elliptic Curve Cryptography', ISBN 0-387-95273-X, Springer-Verlag, 2004.

[77] Certicom Research, 'Standards for Efficient Cryptgraphy',SEC 1: Elliptic Curve Cryptography, version 1.0, September 2000.

[78] Christof Paar and Jan Pelzl, 'The Advanced Encryption Standard', Chapter 4 of 'Understanding Cryptography, A Textbook for Students and Practitioners', Springer, 2009.

[79] David Naccache, David M'Raïhi, 'Cryptographic Smart Cards', IEEE Micro, 1996, pp. 14-24.

[80] Nalini K. Ratha, Jonathan H. Connell and Ruud M. Bolle, 'Biometrics break-ins and band-aids', ELSEVIER, Pattern Recognition Letters 24, 2003, pp.2105–2113.

[81] S. Hirata, and K. Takahashi, 'Cancellable biometrics with perfect secrecy for correlation-based matching'. Lecture Notes in Computer Science, 2009, pp. 868-878.

[82] Andrew Teoh Beng Jin, David Ngo Chek Ling and Alwyn Goh, 'Biohashing: two factor authentication featuring fingerprint data and tokenised random number', Pattern Recognitions, Volume 37, 2004, pp. 2245-2255.

[83] IBM, secure credit card, USA patents Number: US-06641050.

[84] Yamamoto Hiroyasu, Koibuchi Misako and Shimizu Takakuni, 'Secure credit Card', Patent application number: US2002019939(A1).

[85] Heeger, MacDiarmid and Shirakawa, 'The electronic structures of Image –polyacetylene', Chemical Communication, Volume 29, Issue 4, 1977, pp.578.

[86] John K. Borchardt, 'Developments in organic display', Material Today, Volume 7, Issue 9, September 2004, pp.42-46.

[87] Kazuhiro Kudo, 'Organic light emitting transistors', Current Applied Physics 5, 2005, pp. 337–340.

[88] Michel Grimm, 'Power Tools, Alarm/Security, Medical Equipments', Industrial Applications of Batteries, 2007, pp. 573-615.

[89] John L. Warren and Theodore H. Geballe, 'Research opportunities in new energy-related materials', Materials Science and Engineering, Volume 50, Issue 2, October 1981, pp. 149-198.

[90] Lucia Vittoria Mercaldo, Maria Luisa Addonizio, Marco Della Noce, Paola Delli Veneri, Alessandra Scognamiglio and Carlo Privato, 'Thin film silicon photovoltaics: Architectural perspectives and technological issues', Applied Energy, Volume 86, Issue 10, October 2009, pp. 1836-1844.

[91] Jun Chen and Chi-sun Poon, 'Photocatalytic construction and building materials: From fundamentals to applications', Building and Environment, Volume 44, Issue 9, September 2009, pp. 1899-1906.

[92] Ioannis Hadjipaschalis, Andreas Poullikkas, and Venizelos Efthimiou, 'Overview of current and future energy storage technologies for electric power applications', Renewable and Sustainable Energy Reviews, Volume 13, Issues 6-7, August-September 2009, pp. 1513-1522.

[93] K.R. Genwa, Arun Kumar and Abhilasha Sonel, 'Photogalvanic solar energy conversion: Study with photosensitizers Toluidine Blue and Malachite Green in presence of NaLS', Applied Energy, Volume 86, Issue 9, September 2009, pp. 1431-1436.

[94] J. H. Schön, A. Dodabalapur, Ch. Kloc and B. Batlogg, 'A Light-Emitting Field-Effect Transistor', Science, Volume 290, 2000, pp.963-965.

[95] J. H. Schön, Ch. Kloc and B. Batlogg, 'High-Temperature Superconductivity in Lattice-Expanded C60', Science, Volume 293, 2001, pp. 2432-2434.

[96] G. Schmid, 'All-organic thin film transistors', Polyscene workshop, Leuven, Belgium. June 2002.

[97] R. Yasin, 'Password pain relief', Information Security Magazine, April 2002.

[98] Rodrigo de Luis-García, Carlos Alberola-López, Otman Aghzout and Juan Ruiz-Alzola, 'Biometric identification systems', Signal Processing, Volume 83, Issue 12, December 2003, pp. 2539-2557.

[99] S King, G Y Tian, S King, D Taylor and S Ward, 'Cross-Channel Histogram Equalisation for Colour Face Recognition', Lecture Notes in Computer Science, 2003, 2688:454-461.

[100] L. Chunhsing and L. Yiyi, 'A flexible biometrics remote user authentication scheme', Computer Standards & Interfaces, Volume 27, Issue 1, 2004, pp 19-23.

[101] Editor, 'Match on card system for IT security', Biometric Technology Today, Volume 11, Issue 7, 2003, pp.3-4.

[102] Davide Maltoni, Dario Maio, Anil K. Jain and Salil Prabhakar, 'Handbook of Fingerprint Recognition', ISBN: 978-1-84882-253-5, Springer, 2009.

[103] Tu Van Le, Ka Yeung Cheung and Minh Ha Nguyen, 'A Fingerprint Recognizer Using Fuzzy Evolutionary Programming', Proceedings of the 34th Hawaii International Conference on System Sciences, 2001.

[104] Zhang Tao, Fan Mingyu and Fu Bo, 'Side-Channel Attack on Biometric Cryptosystem Based on Keystroke Dynamics', Proceedings of The first international symposium on data, Privacy, and E-Commerce. IEEE Computer Society, 2007.

[105] AuthenTec, the manufacture of mini fingerprint sensor in USA and China. Website: www.authentec.com.

[106] H. Hara, M. Sakurai, M. Miyasaka, S. Tam, S. Inoue and T. Shimoda, 'Low temperature polycrystalline silicon TFT fingerprint sensor with integrated comparator circuit', Solid-State Circuits Conference, Proceeding of the 30th European, Sept 2004, pp.403– 406.

[107] Certicom, a leading company in Elliptic Curve Cryptography products, Website: http://www.certicom.com.

[108] Damien Dessimoz, Jonas Richiardi, Christophe Champod and Andrzej Drygajlo, 'Multimodal Biometrics for Identity Documents. Research Report Version 2.0.', PFS 341-08.05, European biometrics portal, 2006.

[109] 'Bundesdatenschutzgesetz (Federal Data Protection Act)', Germany, Stand 15, Novemer 2006.

[110] Bundesamt, Bundesamt für Sicherheit in der Informationstechnik, Website: http://bsi.bund.de

[111] P. Rosenzweig, A. Kochems, and A. Schwartz, 'Biometric technologies: Security, legal, and policy implications', Legal Memorandum, vol. 12, 2004, pp.1–10.

[112] S. Prabhakar, S. Pankanti, and A. K. Jain, 'Biometric recognition: Security and privacy concerns', IEEE Security and Privacy, vol. 1, no. 2, 2003, pp.33–42.

[113] Chunlei Yang, Guiyun Tian, and Steve Ward, 'Multibiometrics authentication in POS application', School of Computing and Engineering Researchers' Conference, University of Huddersfield, Dec 2006.

[114] Francesco Bergad Ano, Daniele Gunetti and Claudia Picardi, 'User Authentication through Keystroke Dynamics', ACM Transactions on Information and System Security (TISSEC). Volume 5, Issue 4 2002, pp.367 – 397.

[115] Kevin S. Killourhy and Roy A. Maxion, 'Comparing Anomaly Detectors for Keystroke Dynamics', in Proceedings of the 39th Annual International Conference on Dependable Systems and Networks (DSN-2009), Estoril, Lisbon, Portugal, June 29-July 2, 2009. IEEE Computer Society Press, Los Alamitos, California, 2009, pp. 125-134.

[116] Adams Kong, David Zhang and Mohamed Kamel, 'A survey of palmprint recognition', Pattern Recognition, Volume 42, Issue 7, July 2009, pp. 1408-1418.

[117] R. Gaines, W. Lisowski, S. Press and N. Shapiro, 'Authentication by keystroke timing: some preliminary results', Rand Rep. R-2560-NSF, Rand Corporation, 1980.

[118] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman and A. K. Jain, 'FVC2004: Third Fingerprint Verification Competition', Proc. International Conference on Biometric Authentication (ICBA), Hong Kong, July 2004, pp. 1-7.

[119] Anil K. Jain, Sarat C. Dass and Karthik Nandakumar, 'Can soft biometric traits assist user recognition?', Proceedings of SPIE Defense and Security Symposium, Orlando, April 2004.

[120] Chunlei Yang, Guiyun Tian and Said Boussakta, 'Keystrokdynamic and fingerprint multibiometrics authentications', 3rd Information and

Partnering Forum on Safety and Security Systems in Europe, Potsdam, Germany, 19th - 20th June 2008.

[121] S. Bleha, C. Slivinsky, B. Hussien, 'Computer-access security systems using keystroke dynamics', IEEE Transactions on Pattern Analysis and Machine Intelligence, Volume 12, 1990, pp. 1217–1222.

[122] National Bureau of Standards, 'Specification for the Advanced Encryption Standard (AES)', Federal Information Processing Standards Publication 197, November 2001.

[123] M.S. Obaidat and B. Sadoun, 'Verification of computer users using keystroke dynamics', IEEE Transactions on Systems, Man and Cybernetics, Volume 27, 1997, pp. 261–269.

[124] L. Osadciw, P. Varshney, K. Veeramachaneni, 'Improving personal identification accuracy using multisensor fusion for building access control applications', Information Fusion, Volume 2, 2002, pp.1176– 1183.

[125] Chen Change Loy, Weng Kin Lai and Chee Peng Lim, 'Keystroke Patterns Classification Using the ARTMAP-FD Neural Network', Intelligent Information Hiding and Multimedia Signal Processing, Volume 1, Issue 32, Nov. 2007, pp. 61– 64.

[126] Fabian Monrose and Aviel D. Rubin, 'Keystroke dynamics as a biometric for authentication', Future Generation Computer Systems, Volume 16, 2000, pp.351–359.

[127] Peter J. Huber, Robust Statistics (Wiley Series in Probability and Statistics), ISBN-10: 0471418056. 1981.

[128] C. W. Lau, B. Ma, M. Helen, Y.S. Moon and Yeung Yam, 'Fuzzy Logic Decision Fusion in a Multimodal Biometric System', Proceedings

of the 8th International Conference on Spoken Language Processing (ICSLP), Korea, October 2004.

[129] Arun Ross and Anil Jain, 'Information fusion in biometrics', Pattern Recognition Letters, Volume 24, 2003, pp. 2115–2125.

[130] S. Ben Yacoub, Y. Abdeljaoued and E. Mayoraz, 'Fusion of Face and Speech Data for Person Identity Verification', IDIAP research report, IDIAP-RR99-03, 1999.

[131] G. de Ru Willem and H. P. Eloff Jan, 'Enhanced Password authentication through Fuzzy Logic', IEEE Expert, November/December 1997, pp. 38-45.

[132] A. Hejlsberg, S. Wiltamuth, and P.Golde, 'The C# programming language: covers new C# 2.0 features', Addison-Wesley, Beijing, 2003.

[133] P. Drayton, B. Albahari, and T. Neward, 'C# in a nutshell', O'Reilly, ISBN: 0-596-00181-9, 2003.

[134] J. Puvvala and A. Pota, '.NET for Java developer: migrating to C#', Addison-Wesley, ISBN-10: 0672324024, 2003.

[135] Grady Booch, Ivar Jacobson and Jim Rumbaugh, 'OMG Unified Modeling Language Specification', Version 1.3, First Edition: March 2000. Retrieved 12 August 2008.

[136] M. Flowler, 'UML distilled: a brief guide to the standard object modelling language', Addison-Wesley, ISBN-10: 020165783X, 2004.

[137] Grady Booch, James Rumbaugh and Ivar Jacobson, 'Unified Modeling Language User Guide', 2nd Edition, ISBN: 0321267974, 2005.

[138] James Rumbaugh, Ivar Jacobson and Grady Booch, 'The Unified Modeling Language Reference Manual', 2nd Edition, Addison-Wesley, ISBN: 020130998, 2008.

[139] F. Esser, 'Java 2: Patterns, Idioms, Java-Zertifizierung', Galileo Computering (open books), 2001.

[140] Providor of GrFinger Fingerprint SDK Recognition Library, Website: www.grfinger.com/index.php.

[141] M. David and Y. Moti, 'E-commerce applications of smart cards', Computer Networks, Volume 36, Issue 4, 2001, pp. 453-472.

[142] Editor, 'Biometrics secure loan application', Biometric Technology Today, Elsevier, Volume 12, Issue 7, p. 3.

APPENDICES A: Feasibility Study of the Supercard on Industrial Implementation

To evaluate how realistic my proposed Supercard is, a preliminary feasibility study needs to be conducted. This is critically important, especially because our research was initialised by Ingenico Group, the terminal provider I worked for. This section investigates the feasibility of building a smart card with embedded display, keypad and power based on current available technologies and new technologies in the near further. Mainly, the embedded power supply and display are studied. The differences between silicon-based and organic polymer-based technologies are shown and the latter is concluded as the future of card development. The whole investigation is conducted comprehensively in terms of technical concept, manufacture and marketing factors. Current availabilities and limitations and possible future solutions are also explored.

To turn the Supercard concepts into products, there are still many obstacles in both marketing and technical terms. A successful realisation is constrained by:

- The computation ability of the micro CPU and power supply.
- The limitations of the smart card's mechanical characteristics. Physical and electrical characteristics of smart cards are defined in ISO 7816.
- Anti-bending and lifetime. The cards are supposed to be carried in a wallet and work for longer than three years.
- Cost. This is a crucial issue. The degree of acceptance is largely dependent on the price.

The rest of the document is organised as follows: Section A.1 and Section A.2 study the currently available methods and the limitations of embedding displays and

power supplies on a smart card. Section A.3 investigates the possibility of embedding a fingerprint sensor in a smart card. Section A.4 observes the developments of organic technology relative to smart cards. The last section is the conclusion.

A.1 Embedded Display

Obviously, the major difficulties of the Supercard mainly reside in the integration of display and power.

The requirements for a display to be included in a smart card are thinness, flexibility, robustness, lightness and low power consumption. Conventional displays use glass as a substrate, hence they are heavy, fragile and thick. Obviously, they are not suitable to be embedded. The recently developed organic display, however, is a promising technology to address these requirements. Organic material is relatively low cost and can be deposited onto almost any substrate, both rigid and flexible. Since discovery of conductive polymers by Heeger, MacDiarmid and Shirakawa in the 1970s [85], which earned them the 2000 Nobel Prize in chemistry, much progress has been made on polymer semi-conducting technology. It is possible to build the whole device on flexible plastic foils to get a thin, light and flexible display.

The key material of an organic display is the organic emitter layer. This semiconducting organic layer must contain a material with conjugated π-bonds, but can be either a small molecule crystalline phase (small molecule OLEDs or SMOLEDs) or a polymer (polymer OLEDs or POLEDs). In 1990, Friend and co-workers at the University of Cambridge created a low-voltage electroluminescence in an organic device with a polymer, poly (p-phenylenevinylene), as the organic emitter [86]. Rapid advances in materials and manufacturing technology are making organic light-emitting diodes (OLEDs) the leading technology for a new generation of displays. The main players in this field include Cambridge Display Technology, E Ink,

Philips, Sony, DuPont, and Eastman Kodak. An informative review paper regarding OLED has been done by John K. Borchardt [86].

The typical smart card application requires only segmented 8-digits, about $4cm^2$, and a monochromic display with a lifetime of about five years. Applying POLED on smart cards has the lowest technical risk compared with E-paper or TV display applications that require large, full colour and high resolutions. Several companies have developed prototypes. In the 2004 Carte exhibition (Paris), Philips showed a prototype card with a bi-stable organic display (refer to Figure A-1). A bi-stable display needs power only when the state is changing, and the state can be kept for a quite long time without power, thus the power consumption can be very low. In addition, OLED panels emit light only from the necessary pixels rather than the entire panel. Therefore, power consumption is 20-80% of that of LCDs [86]. It is forecasted that when sufficient OLED production volume is achieved, prices shall drop to 10-40% less than LCDs. The company MicroD developed one prototype in 2005. See Figure A-2.

Figure A-1: A colour polymer flexible OLED from Philips

Figure A-2: A prototype card with display from MicroD

There are still important areas in which POLED technology needs to improve before it is mature enough for mass production, including increased electroluminescence efficiency and longer operating life. The limited lifetime is largely due to its reactions with the ambient oxygen, CO_2 and moisture. Therefore, industrialisation and encapsulation is a key issue.

A.2 The embedded power supply

Below we study another major challenge of the integration solution: power supply in the Supercard. The candidates for an embedded power supply are:

- Solar cells. Currently limited to low efficiency, this technology requires that the object be used in full light, unless it is used in combination with a rechargeable cell.
- Primary lithium. The power density is about 15mW/cm^2. Ultra-thin vapour-deposited lithium rechargeable battery. Very low power density but possible integration directly on several substrates (even silicon) [88].
- Paper-printed battery. This is developed by Power Paper Ltd. The combined battery materials of zinc and manganese dioxide are like printer's ink, which can be printed on many materials, and it does not require a hard metal case [89]. The cost of basic materials is very low but the deliverable energy is highly limited. It is more suitable for applications like Smarter Luggage Tags.

The power supplier from a photovoltaic (PV) cell is preferred. Single crystal is the original PV technology that was invented in 1955 [90]. It can supply endless

energy. It is environmentally friendly and needs almost no maintenance. Therefore, it has attracted great research interests.

The current photovoltaic market is dominated by single crystal silicon, polycrystalline silicon, and inorganic thin film. The efficiencies range from about five percent for low-cost thin film materials to about 24 percent for high-quality silicon crystal. Photovoltaic cells based on single crystal silicon or polycrystalline have high efficiency and durability; however, they are very fragile as well as expensive and they cannot be directly deployed on a smart card. Although the thin-film photovoltaic can be flexible and relatively cost effective, it has the features of low efficiency and quick degradation. Even for a low-end 8-bit microcontroller in smart cards, e.g. PIC 16F84CPU, it typically needs 2mA at 5V, 4MHz. A flexible thin-film photovoltaic cell with an area of 0.79" x 0.4" (20mm x 10mm) has an approximate output of 0.45 Volts @ 50 mA, 0.01" thick. Here, the rated current 50mA is under the conditions of outdoor sunlight. When indoors or under office light, the performance of photovoltaic cells is very poor. Theoretically, photovoltaic cells can have series or parallel connection to offer a high voltage as well as a big current; nevertheless, the available area that can be used for this is highly limited. Therefore, normally it cannot supply sufficient energy for smart card application. The combination of a photovoltaic cell and a mini rechargeable battery is possible but the cost is unacceptable.

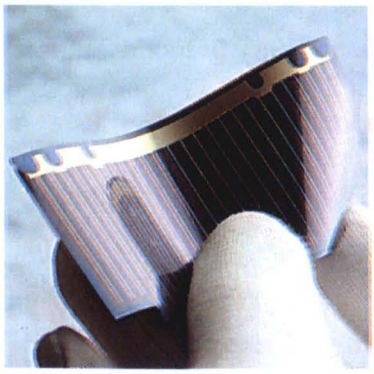


Figure A-3: A thin-film flexible solar cell

An interim conclusion can be made: based on current smart card and conventional PV technology, the PV cell is not a suitable solution [91]. The system power consumption must be dramatically decreased. The market requires a less expensive technology.

There have been notable advancements in terms of decreasing the cost of thin-film solar cell (refer to Figure A-3). One reason why a conventional solar cell is expensive is that it requires complicated processes, e.g. deposition of other inorganic materials, as well as expensive manufacturing technologies (vacuum deposition, photolithographic, etc) like normal silicon IC. Through a combination of fundamental research and development programs and external contractual efforts, there are two techniques for flexible solar cell designs, which have a low fabrication process: one is based on an all-polymer/organic material approach and the other is a dye-sensitised, organic/inorganic material hybrid approach. In the all-polymer approach, the researchers combined two organic materials – an electron-donating material and an electron-accepting material – to make a percolating structure with two interpenetrating networks [92].

The solar cell has been successfully employed in calculators for many years because the low-end calculator needs less power. For example, with a calculator system (CPU: KI1724A LCD: 10+2 7-segment LCD display, 128byte RAM and 22K ROM), the power consumption is about 0.7mW at operating. Hence, to realise dynamic password generation, such a "simple" function on a smart card with high energy limitation, a proposal as outlined in Figure A-4 can be made which integrates the calculator circuit into smart cards. In addition to the conventional smart chip that contains a CPU, RAM, EEPROM itself, the card has a dedicated low-end calculator processor (e.g. KI1724A) which is low-speed but optimised for power consumption.

The processor contains a small-size RAM and a power management circuit, among other components. The solar cell power will only supply to the calculator circuitry (1.5V, 200-300μA) to accomplish some limited tasks like dynamic password generation. The conventional smart card chip (with a powerful CPU and peripherals) need not be powered unless the card is connected to a card reader for a transaction.

Nevertheless, the weak system described above cannot support a strong mechanism (a secure OS and hardware) against sophisticated attacks. The fundamental way out for concept realisation lies in dramatically and systematically decreasing power consumption and cost. The rapid developments in organic material and physics appear to make this the most promising technology to address these requirements. In the previous part of this paper, organic developments in flexible displays and photovoltaic cells have been covered. More organic applications around smart cards will be investigated in the next section.

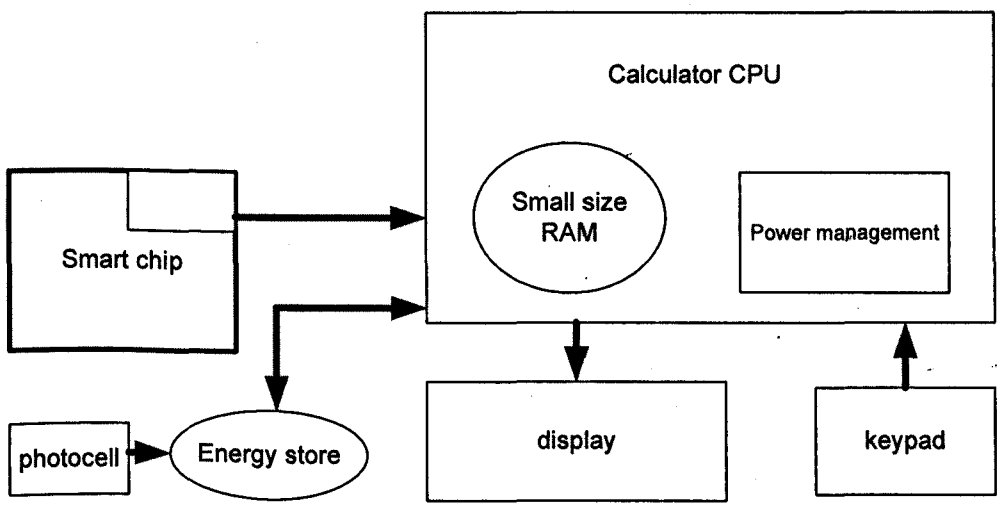


Figure A-4: Combing smart card circuit and calculator circuit

In recent years, much progress has been achieved in miniaturisation and increasing the lifespan of extremely thin lithium batteries. In the short term, the super-slim lithium battery is the most realistic solution. There are several companies that can offer commercially available products, especially integration with cards.

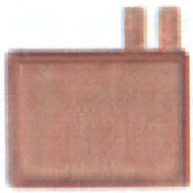


Figure A-5: A lithium card battery from VATRA

Figure A-5 is a special slim card battery from VATRA (non-rechargeable). The material is manganese dioxide and lithium, wrapped with a copper package and sealed. Typical capacity is 25mAh (@0.03mA, cut off: 2V @20°C). The thickness is 0.4mm and the dimensions are 29mm x 25mm. There already exist rechargeable super-slim lithium batteries. Charging can be done while the card is in use in a card reader for other applications; however, the recharged energy is quite limited in a short transaction period (about 40s). The development of quick charging technology is still under way. There are two major problems: the first is high cost. Such a battery alone needs 1-2€. It is not suitable for a price-sensitive massive market. The second problem is self-discharge and limited energy, e.g., capacity retention is 90% after 45 days of storage.

A.3 Embedded fingerprint sensor in card

In this section, we will briefly investigate the feasibility of integrating a fingerprint sensor on the Supercard. The feasibility of this solution relies on two issues: (1) whether the physical shape of the sensor allows it to be integrated into a card, and (2) the cost of such a sensor.

A biometric sensor, or a fingerprint sensor to be specific, also known as a fingerprint reader, is a fingerprint image capture device. The types of fingerprint sensor available are static capacitive type 1, static capacitive type 2, dynamic capacitive, optic reflexive, optic transmissive with a fibre optic plate, acoustic (ultrasound), pressure sensitive, thermal line, and capacitive and optical line. All the

types of fingerprint sensors are generally known as optical, semiconductor, and ultrasound sensors. Among all these sensors, semiconductor sensors are considered to be low cost, optical sensors are considered to have a high degree of stability and reliability, while ultrasound sensors are very precise and fraud-free, though expensive to implement.

Thanks to the ever-evolving research and improvements in biometric sensors, especially the new silicon swipe fingerprint sensor, this proposed work becomes more realistic than ever. These sensors when embedded in compact systems like laptops, mice and cellular phones provide a small contact area for the fingertip. For example, a company called AuthenTec [105] has published a one-swipe fingerprint sensor EntrePad1510 as a comical product. Figure A-6 shows its size and Figure A-7 shows a typical application in a block diagram. Physically, it uses a 48 Ball Grid Array (BGA) package with a size of 5mmx13.8mm. The thickness is 1.2mm. It is close to the requirements of being integrated into the smart card, with a thickness of 0.8mm. The cost of such a sensor is already less than four US dollars. The fragile sensor can be protected by a thin metal sheet that goes around it.

On another side, such sensors sense only a limited portion of the fingerprint. This complicates the problem of matching impressions due to the lack of sufficient minutiae information [105]. Generally, pattern-based matching algorithms give a better performance than minutiae-based algorithms.

Figure A-6: EntrePad1510 swipe fingerprint sensor

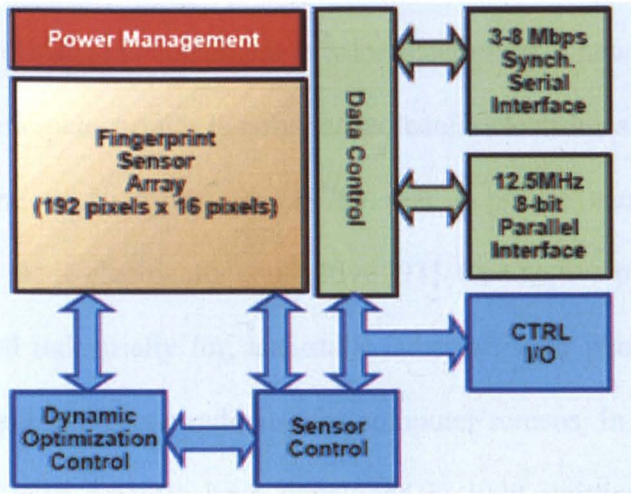


Figure A-7: EntrePad 2510 Application Block Diagram

Seiko Epson has developed a paper-thin fingerprint sensor measuring 0.2mm thick [106]. The fingerprint sensor's ultrathin profile means it can easily be incorporated into a Supercard. When touched, the sensor reads fingerprint patterns based on the faint electric current emanating from the user's fingertip. The company aims to commercialise the sensor by 2010. The prototype is illustrated in Figure A-8.

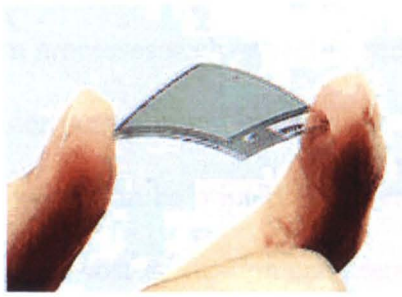


Figure A-8: Prototype of the thin and flexible fingerprint sensor from Seiko Epson

A.4 Implementation based on organic polymer electronics

Today's generation of smart cards depend on conventional silicon chips (processor, memory, etc.). Despite many advances in silicon chip technology, the cost-saving space is limited. Not only is the silicon wafer expensive, but also the fabrication process needs vacuum and photolithographic, high temperature, etc.

Parallel to the classical development in microelectronics, a new promising and growing area within microelectronics is polymer/molecular electronics. This new area is an outcome of the discovery in the 1970s that a plastic can, after certain modifications, can be made electrically conductive [93]. Conductive plastics are used in, or being developed industrially for, anti-static substances for photographic film, and shields against electromagnetic radiation for computer screens. In addition, semi-conductive polymers have recently been developed in light-emitting diodes, solar cells and as displays in mobile telephones. During the last few years, a surprising number of new devices using organic materials or conjugated polymers as an active component (e.g. a transistor) have been reported. Thus, polymer can be a material for isolation, conductors as well as semiconductors. These very interesting electrical and mechanical properties enable an electronic device completely based on cheap and flexible polymer substrates.

Another important feature is that the polymer material has high solvability like ink. High-yield fabrication processes such as reel-to-reel, inkjet printing and spin casting can be carried out under normal room temperature. That means that organic electronic components and circuitry can be printed as we print a book, while the low price of the raw materials and low-cost fabrication can dramatically decrease the cost of the device. In addition, the organic electronics can work in low voltage with very

low power consumption. The coming decade may indeed become the age of organic electronics.

Actually, the organic polymer electronics can be extended to the field of transistor, electric circuit and memory field. A transistor is the basic component of electronic circuitry. Moore's prediction over 27 years ago that the semiconductor industry would be able to double the number of transistors per chip every 18 months still holds today. As alternative methods to reach low cost, much progress has been made in organic thin film transistors [87].

Although the mobility of polymer thin film transistors (PTFTs) is 1 order of magnitude lower than the mobility of small molecule based TFTs (motilities of ≥1cm2/Vs were achieved for pentacene TFT by several groups, it is interesting because spin casting and printing methods can be employed for low-cost fabrication based on polymeric materials. A few groups and companies such as the group of Prof. Jackson from Penn-State University, Philips, Infineon, and Plastic Logic have presented integrated systems on flexible substrates. For example, the group of Dr. De Leeuw at Philips has presented integrated circuits based on several hundred TFTs.

The realisation of large-scale integrated circuits requires a stable process technology, so that TFTs with identical properties can be produced. Second, the process has to be uniform over the entire substrate. Third, the thermal expansion of the polymeric substrates leads to additional constraints, which has to be considered during the device design and the manufacturing process. Very little has been published about the issue of reliability and stability of organic and polymeric TFTs. Large integrated circuits using inkjet printing of the active material have not been presented.

There is still a long way to go before a high-end processor or large-scale complex control circuit can be built, but polymer electronics can satisfy the simple logic as the application of dynamic generation card soon.

Conventional RAM memory is expensive and volatile while Flash memory is slow and has a limited number of read/write cycles. The memory of the future shall be low cost, low power, easy to integrate and non-volatile. Various companies are working on a polymer-based memory using a polymer material sandwiched between two metal electrodes. The memory cell behaves like a Ferroelectric memory. The storage element can be combined with CMOS-based read-out electronics. Memory devices like organic bi-stable elements have been developed.

Existing RF identification tags use a silicon die interconnected with an antenna on paper or a flexible foil. The price of existing crystalline silicon-based RF tags ranges from 0.3-0.5 US dollar. 50% of the cost of the systems is determined by the interconnection between the silicon die and the antenna [96]. By using organic materials and processing technologies, the price of the RF tag can be distinctly reduced, and the same technology can be integrated into smart cards.

We strongly believe many advanced application concepts based on smart cards will finally be realised with the maturity of polymer technology in the near future. We believe that, in the near feature, the Supercard can be realised as in Figure A9. The processing circuit and memory element, display, photovoltaic cell and RF circuit are all made from plastic organic material. Since the system power consumption is very low in this case, the organic photovoltaic cell is efficient enough to recharge during the short periods when the card is removed from your wallet. The final price can be even cheaper than today's simple calculator can.

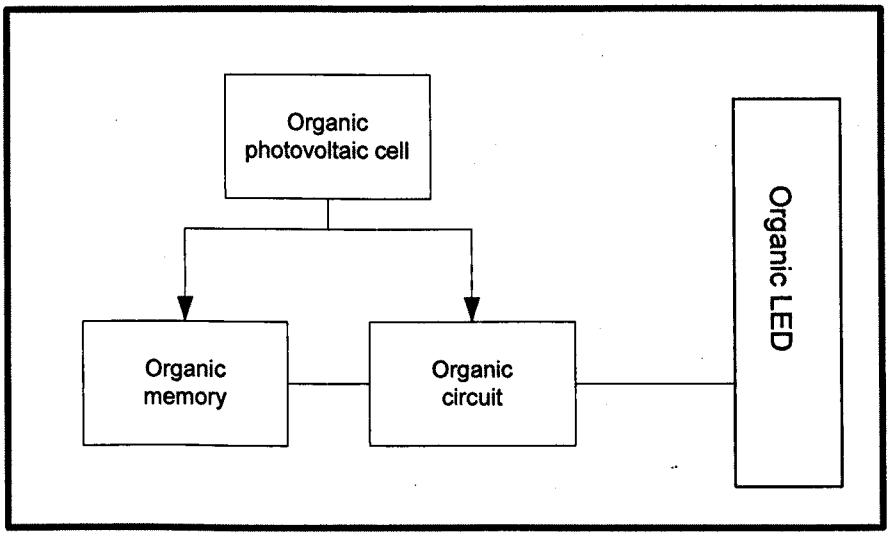


Figure A-9: An organic polymer Supercard

The further work in organic polymer microelectronic moves in two directions: the fundamental physical properties and fabrication process [93]. Despite an explosive growth in practical advancement, the fundamental physical properties of organic semiconductors are only poorly understood. Organics resist description by the simple band theory that so successfully explains the optical and electrical properties of inorganic materials. Organic semiconductors do not fit comfortably in a molecular picture that considers electronic states of individual molecules but ignores the formation of extended states. Therefore, some research institutes, e.g. the Princeton Center for Organic Electronics (P-COE), aim at achieving a fundamental understanding of optical and electronic processes in organic semiconductors. On the other hand, with the major objectives of high-volume production and low-cost processing of organic polymer technology, a project called PolyApply has been conducted since 2004 by 20 leading European industrial enterprises as well as renowned academic and research institutes.

A.5 Summary

To summarise, the major observations of feasibility are to build a prototype of Supercard is realistic today. The document indicates today's feasibilities and constraints. The display, power supply and fingerprint sensor are discussed in relative detail. The thin flexible polymer OLED display appears to be the best candidate of the Supercard display. The super-slim lithium battery has been identified as the most mature technology to be integrated into a Supercard. A better solution can be a combination of a lithium battery and a thin-film flexible solar cell. In the field of fingerprint sensors, the mini swipe sensor from AuthenTec and the big slim sensor from Seiko Epson are suggested.

In the near future, we believe, the cost obstacle will be removed when organic electronic technologies become ripe. Today's generation of smart cards and electronic devices depend on conventional silicon technologies (processor, memory, etc.). Despite many advances in silicon chip technology, the cost-saving space is limited. Not only is the silicon wafer expensive, but also the fabrication process needs vacuum and photolithographic. The new organic-based (especially the polymer-based) electronics offer the possibility that the components and circuit can be 'printed' (or inkjet printed) under low-requirement conditions, similar to the way we print on paper.