HIGHLY ROBUST BIOMETRIC SMART CARD DESIGN

Afzel Noore
Department of Computer Science and Electrical Engineering
West Virginia University, Morgantown, WV 26506-6101

Abstract -- ***An architecture of a highly reliable smart card is proposed. Dual on-chip biometric fingerprint sensors, implemented with different technologies, are integrated with the smart card architecture for increased security and reliability.***

Index Terms -- Smart cards, Biometrics.

I. INTRODUCTION

As smart cards become more and more pervasive in e-commerce and m-commerce applications the concern for security and reliability are profound. The wide acceptability of smart cards for consumer applications in cellular telephones, internet, wireless or mobile networks, and ATMs has propelled the development of advanced architectures, and the need for highly reliable personal authentication systems. Fig. 1 shows the architecture of a smart card.

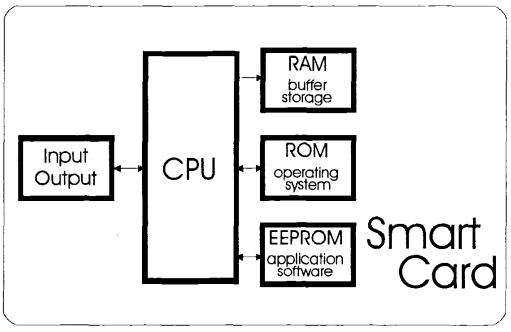


Fig. 1 Basic architecture of a smart card

A smart card has an embedded microprocessor, several types of memory, and an input/output port. It can handle arithmetic computations, logic decisions, read and write operations, authentication algorithms, and communication protocols. Smart cards store information inside the card in contrast to magnetic stripe cards where the information is encoded externally making it is susceptible to fraud and misuse.

such as encryption algorithms and communication protocols. The EEPROMs store application programs written in the assembly language of the embedded microprocessor. The file system used in the EEPROM is a simple hierarchical structure with only one master file serving as the root of the file system on each smart card. A master file may contain several sub files. Data stored in the EEPROM can be changed by the microprocessor using an on-chip charge pump, eliminating the need for a separate external power supply for programming. The I/O port of a smart card is primarily used for communication and authentication. Data transfers occur in bytes or blocks in an asynchronous half-duplex mode. Smart cards store access codes, passwords, and public and private keys used in encryption and authentication.

To ensure interoperability, smart cards must conform to specific physical attributes, electrical characteristics, communication protocols, and encryption standards. Existing smart card standards are based on ISO 7816 [1]. The ISO 7816 smart card standard consists of several parts as shown in Table 1. However, most of the smart card manufacturers conform to ISO parts 1, 2 and 3 to maintain ISO compliance.

Table 1 ISO 7816 smart card standard

ISO 7816	Standards
Part 1	Physical characteristics.
Part 2	Dimension and location of the contacts.
Part 3	Electronic signals and transmission protocols.
Part 4	Inter-industry commands for interchange.
Part 5	Numbering system and registration procedure for application identifiers.
Part 6	Inter-industry data elements.
Part 7	Inter-industry commands for Structured Card Query Language (SCQL).
Part 8	Security related inter-industry commands.
Part 9	Additional inter-industry commands and

light, x-rays, electromagnetic interference, electromagnetic fields, static electricity, mechanical strength, heat dissipation, etc. Part 2 of the ISO 7816 standard relates to the physical dimensions of a smart card. Figure 2 shows the dimensions of a smart card, along with eight electrical contacts on the front face of the card. The function for each contact assignment is described in Table 2.

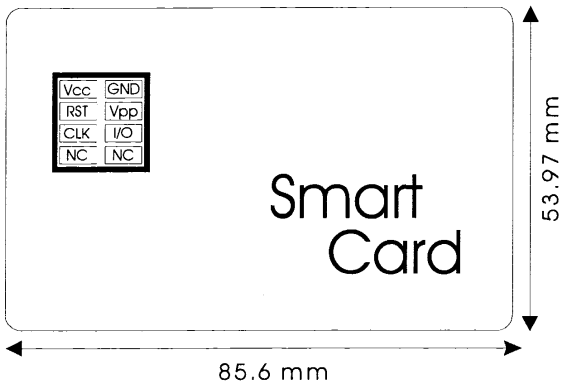


Fig. 2 Dimension and contact pins of a smart card

Table 2 Smart card pin functions

Pin	Function
Vcc	DC power is supplied to the microprocessor in the smart card.
RST	Reset pin is used by external device to initiate reset sequence.
CLK	External clock is supplied to the microprocessor in the smart card.
NC	Reserved for future use.
GND	Common electrical ground between the smart card and the external device.
Vpp	Used rarely (because of internal circuitry) to program the EEPROM.
I/O	Input/Output line is used in half-duplex communication mode.
NC	Reserved for future use.

Part 3 of the ISO 7816 standard defines the initialization, power-up sequence and half-duplex communication protocols between the smart card and the external device. The initialization operation always results in the sending of an answer-to-reset (ATR) from the smart card to the external device. The ATR is a string of characters returned from the card indicating a successful power-up sequence. The total length of the ATR sequence is limited to 33 bytes. If the ATR is not returned in the prescribed time, the external device begins a sequence to power down the card. Part 4 describes more complex protocols for error-free communication between the external device and the smart card.

II. Smart Card Authentication

To provide access to sensitive information stored on the smart card, it is critical to implement reliable authentication procedures. Passwords sent over networks without encryption can be intercepted and will compromise the security of data transfers. Smart card manufacturers widely use the standard ANSI data encryption and message authentication algorithms to ensure that cards receive and send data in a reliable and secure environment. Secure authentication is implemented using *public key* and *private key* cryptography along with encryption and decryption algorithms. The sender's public key is used to encrypt data for transmission. The private key, which is unique to the recipient, is used to decode the original data. Private keys are stored in the smart card. Authentication can be initiated either by the smart card or the reader application software. The procedures below describe the steps involved during an authentication initiated by the smart card and an authentication initiated by the external reader software application.

smart card initiates authentication

begin
{
card initiates authentication command to reader;
card and reader identify common encryption algorithm;
reader sends a random encrypted number to card;
card uses private key to encode the random number;
card sends the decrypted data back to reader;
reader verifies the random number it generated;
if a match is detected, card identity is validated;
}
end

smart card reader application initiates authentication

begin
{
reader sends authentication command to card;
reader and card identify common encryption algorithm;
card sends a random encrypted number to reader;
reader uses private key to encode the random number;
reader sends the decrypted data back to card;
card verifies the random number it generated;
if a match is detected, reader request is validated;
}
end

Authentication procedures described above ensure that the personal identification numbers (PINs), passwords or private keys are securely stored inside the smart card and are not accessible to anyone. Public and private key cryptography enhances the reliability of secure transactions. However, smart cards are vulnerable to compromise because the existing smart card architecture and authentication procedures do not verify if the person using the smart card is the true owner of the card. Smart cards using secure keys can associate an identity of a valid card but cannot confirm that the individual using the card is the

rightful owner performing the desired transaction. As a result smart cards are not reliable and secure without positive user identification during the authentication process. The proposed smart card architecture described in Section III uses biometric sensors to authenticate the smart card and its user.

III. BIOMETRIC SMART CARD DESIGN

In this section dual biometric sensors are embedded in the architecture of a smart card. Biometric sensors use human physiological or behavioral characteristics to uniquely verify an individual's identity. Common biometric characteristics used for identification purposes include: hand geometry, finger geometry, fingerprint, iris feature, retinal pattern, facial features, voiceprint, signature, keystroke dynamics, vein pattern, thermal image, ear shape, and DNA, etc. [2] Biometric sensors used for smart card applications must be small, reliable, and cost effective. Fingerprint identification technology has matured over the years and vendors are developing on-chip fingerprint sensors for many security applications. These sensors use thousands of tiny sensors to measure the ridges and valleys of a fingerprint. Special identification algorithms then verify if the fingerprint sample matches the digitally encoded characteristics of the actual owner stored in the smart card memory.

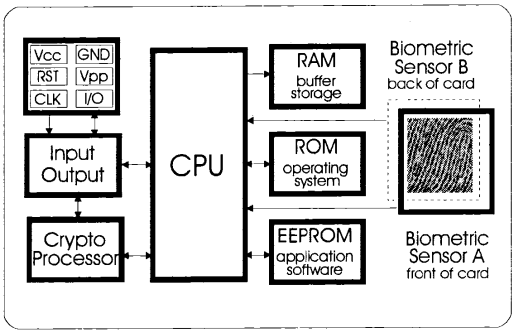


Fig. 3 Dual biometric smart card architecture

In the proposed approach, the identity of the smart card user is verified by using a combination of two non-homogeneous biometric fingerprint sensors. Fig. 3 shows the proposed smart card architecture with embedded dual biometric sensors and a cryptographic processor to speed the encryption and verification process.

Biometric fingerprint Sensor A is based on DC capacitive sensor technology [3]-[5] and biometric fingerprint Sensor B is based on AC electric field sensor technology [6]. Sensor A is embedded on the front of the card and Sensor B is embedded on the back of the card. When a user holds the proposed smart card two fingerprints are simultaneously captured. For example, fingerprint F1 may correspond to the thumbprint and fingerprint F2 may correspond to the lateral print of the user's index finger.

The DC capacitive fingerprint sensing technology of Sensor A uses thousands of tiny capacitor sensor pixels on a silicon chip. The two metal plates of each capacitor pixel are separated by an oxide coating. When a finger is placed on Sensor A, the skin acts as a third plate separated by a dielectric layer whose thickness is determined by the ridges and valleys of the fingerprint. The ridges of the fingerprint F1 create high capacitance because of the close proximity to the sensor; while the valleys of the fingerprint F1 create low capacitance because of increased distance from the sensor surface. The stored charges in the tiny capacitor sensor pixel arrays captures the fingerprint pattern F1.

The AC capacitive fingerprint sensing technology of Sensor B uses an electric field to detect the ridges and valleys of another fingerprint F2 of the same user. When a finger is placed on Sensor B, a very small signal is coupled to the subdermal layer of the skin, generating signals that follow the ridges and valleys of the fingerprint. The sensor matrix receiving these signals based on the ridges and valleys behaves like an array of tiny antennas. This technology is able to penetrate the skin more deeply and extract the fingerprint features F2 even under austere conditions of the finger.

Both sensors A and B are capable of producing images with resolutions greater than 500 dpi as required by the Federal Bureau of Investigation. The ability to capture and process multiple fingerprints simultaneously enhances the reliability of identifying the actual owner of the smart card during its use. The proposed dual biometric sensor smart card architecture makes the card fault-tolerant to sensor failures and resilient to variations in fingerprint quality. The various operating modes of the dual biometric fingerprint sensors are summarized in Table 3.

Table 3 Operation modes of dual biometric sensors

Modes	Dual Sensor Operation Modes
Mode 1	Verification of fingerprint F1 using Sensor A
Mode 2	Verification of fingerprint F2 using Sensor B
Mode 3	Verification of fingerprint F2 using Sensor A
Mode 4	Verification of fingerprint F1 using Sensor B
Mode 5	Verification of fingerprint F1 using Sensor A and fingerprint F2 using Sensor B
Mode 6	Verification of fingerprint F2 using Sensor A and fingerprint F1 using Sensor B

Information captured from fingerprints F1 and F2 can be stored in either the compressed or uncompressed form. Modified fingerprint recognition algorithms can successfully perform identification even with compressed data. Further, if selected characteristics such as the minutiae of fingerprints F1 and F2 are used, the storage requirements will be significantly reduced. Typical file storage requirements range from a few hundred bytes to less than a

few thousand bytes depending on the application and the extracted features. Biometric templates from sensors A and B are stored in a dedicated memory partition. Records must contain information such as date of the record, type of biometric data, length of the record, the biometric data from sensors, and the quality of data for reliable processing and identification. The structure of the records is shown below.

record date
{
stored template date and time for fingerprint F1
stored template date and time for fingerprint F2
new template date and time for fingerprint F1
new template date and time for fingerprint F2
}
biometric sensor type
{
sensor A - fingerprint
sensor B - fingerprint
}
biometric data type
{
raw data for fingerprint F1
raw data for fingerprint F2
selectively processed data for fingerprint F1
selectively processed data for fingerprint F2
fully processed data for fingerprint F1
fully processed data for fingerprint F2
}
record length
{
number of bytes for fingerprint F1
number of bytes for fingerprint F2
}
biometric fingerprint quality
{
set low for fingerprint F1
set low for fingerprint F2
set medium for fingerprint F1
set medium for fingerprint F2
set high for fingerprint F1
set high for fingerprint F2
ignore for fingerprint F1
ignore for fingerprint F2
}
biometric processing algorithm
{
fingerprint F1 {algorithm 1, ..., algorithm n}
fingerprint F2 {algorithm 1, ..., algorithm n}
}
biometric matching results
/* based on modes described in Table 3*/
{
mode 1 {successful, unsuccessful}
mode 2 {successful, unsuccessful}
mode 3 {successful, unsuccessful}
mode 4 {successful, unsuccessful}
mode 5 {successful, unsuccessful}
mode 6 {successful, unsuccessful}
}

IV. Smart Card And User Authentication

The combination of biometric fingerprint quality and the sensor operation modes described in Table 3 provides the card user with enhanced flexibility. In instances where a person's fingers are clogged and not ideal for fingerprinting, the expected fingerprint quality can be preset to low. Mode 5 or Mode 6 allows both sensors to capture fingerprints of different fingers to perform a positive identification with high probability. Using this architecture, the processing algorithm can use either fingerprint F1 or fingerprint F2 in the event any one of the sensors has failed. Such features allow for graceful degradation of the smart card operation without compromising the performance. In the event that both sensors fail, the biometric fingerprint quality is completely ignored and no user verification is performed. The user will still be able to make use of the smart card for emergency purposes and this operation is similar to the smart cards that are commonly available commercially. With the integration of biometric sensors, the modified authentication process is described below.

smart card and owner initiate authentication
begin
{
capture biometric fingerprint data;
compare data with known biometric template;
if a match is detected, proceed with authentication;
card initiates authentication command to reader;
card and reader identify common encryption algorithm;
reader sends a random encrypted number to card;
card uses private key to encode the random number;
card sends the decrypted data back to reader;
reader verifies the random number it generated;
if a match is detected, card and owner identity is validated;
}
end

reader requests card and owner authentication
begin
{
reader sends authentication command to card;
capture biometric fingerprint data;
compare data with known biometric template;
if a match is detected, proceed with authentication;
reader and card identify common encryption algorithm;
card sends a random encrypted number to reader;
reader uses private key to encode the random number;
reader sends the decrypted data back to card;
card verifies the random number it generated;
if a match is detected, reader request is validated;
}
end

When the matching algorithm detects that the biometric fingerprint corresponds to the user of the card, a modified key is generated for encryption. The resulting authentication process that uses the modified key ensures

that the card belongs to the rightful owner. This design requires the smart card to perform sensing, matching, and generation of a biometric-based private key for encryption using internal power. The actual biometric data stored in the card is not shared or transmitted to the external software application during the authentication process.

Authentication using access codes or passwords is simple to implement. However, the proposed architecture uses encryption and authentication algorithms that are based on public and private keys, and requires more memory and computational power. To increase the speed further, a dedicated cryptographic processor that performs encryption using standard algorithms such as DES or RSA 1024 is embedded. The embedded crypto processor in the smart card architecture design accelerates the generation of 512-bit key signatures in a few milliseconds and executes the encryption and decryption algorithms faster than software solutions.

V. Conclusions

In this paper, a novel architecture that uses dual non-homogeneous biometric fingerprint sensors is embedded in the smart card to provide multi-modal operations for increased flexibility, reliability and security. The authentication involves validation of the smart card and positive identification of the user. The smart card design is robust and works reliably even when a sensor fails or when the quality of the fingerprint is poor.

References

[1] C. H. Fancher, "In your pocket: smartcards," *IEEE Spectrum*, Vol.34, No. 2, pp.47-53, Feb. 1997.

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

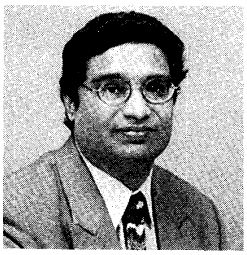
[3] Veridicom, http://www.veridicom.com.

[4] STMicroelectronics, http://us.st.com.

[5] Infineon, http://www.infineon.com.

[6] Authentec, http://www.authentec.com.

Biography



Afzel Noore received the B.S. degree in Electronics and Communications from the University of Madras, India, in 1977; the Master of Science degree in Electrical Engineering from the Indian Institute of Technology, Madras, India in 1980; and the Ph.D. in Electrical Engineering from West Virginia University in 1987.

From 1980 to 1982, he worked as a digital design engineer at Philips India. Dr. Noore is currently the Associate Dean for Academic Affairs in the College of Engineering and Mineral Resources at West Virginia University. He is also an Associate Professor in the Department of Computer Science and Electrical Engineering. His research interests include software engineering, VLSI design, fault-tolerant computing, consumer electronics, biometrics, e-commerce, and wireless applications.