

Security Design of Smart Cards and Secure Devices with Embedded FRAM

Current memories implement various security functions such as parameter storage/updating, high-speed processing of cryptographic algorithms, firewalls between applications, and anti-tampering measures. This article presents the FRAM applications in cipher and security system development employing FRAM.

Introduction

In recent years, various services such as music and video image delivery and electronic data sales in which communication and electronic commerce are conducted openly over the network have come to be a part of IT that is expected to make our lives more efficient. The fundamental technology that must be established is the security services using encryption techniques effectively and efficiently. It is essential that the media connected to the relevant network system be capable of handling the relevant security requirement at any stage in which they are connected.

FUJITSU applies FRAM in the design and development of IC cards and security devices that incorporate security functions. FRAM is a nonvolatile memory with four primary features: high-speed writing, low power consumption,

unlimited rewriting times, and byte rewrite permission. Devices adopting FRAM memories have progressed from a simple nonvolatile memory that stores a key to a functional application that accelerates encryption algorithms. This article introduces examples of FRAM application in cipher systems and also presents an approach on encryption and security systems using FRAM^{*1~4}.

Cipher Classification and Algorithms

Encryption algorithms are largely divided into common key ciphers and public key ciphers. Common key ciphers are also called secret key ciphers; the common key is used as

Figure 1 Encryption/Decoding (Secret Key Cryptography)

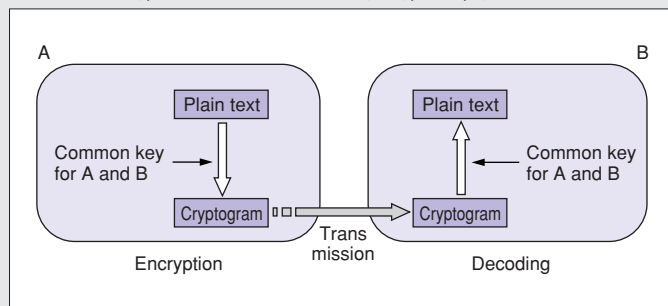
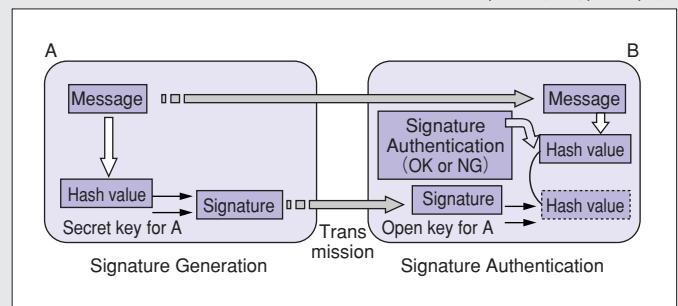


Figure 2 Signature Generation/Signature Confirmation (Open Key Cryptography)



the key for both encryption and decoding (**Fig.1**). These types of ciphers have a long history—the DES (Data Encryption Standard) was stipulated by the US Department of Commerce, National Institute of Standards & Technology in 1977 and is today's world standard for data encryption. At present, triple DES is more commonly used since single DES with a 64-bit key length does not assure sufficient security. Since Rijndael has been designated as the algorithm for the AES (Advanced Encryption Standard), which is the DES's successor, it is expected that applications will shift to AES.

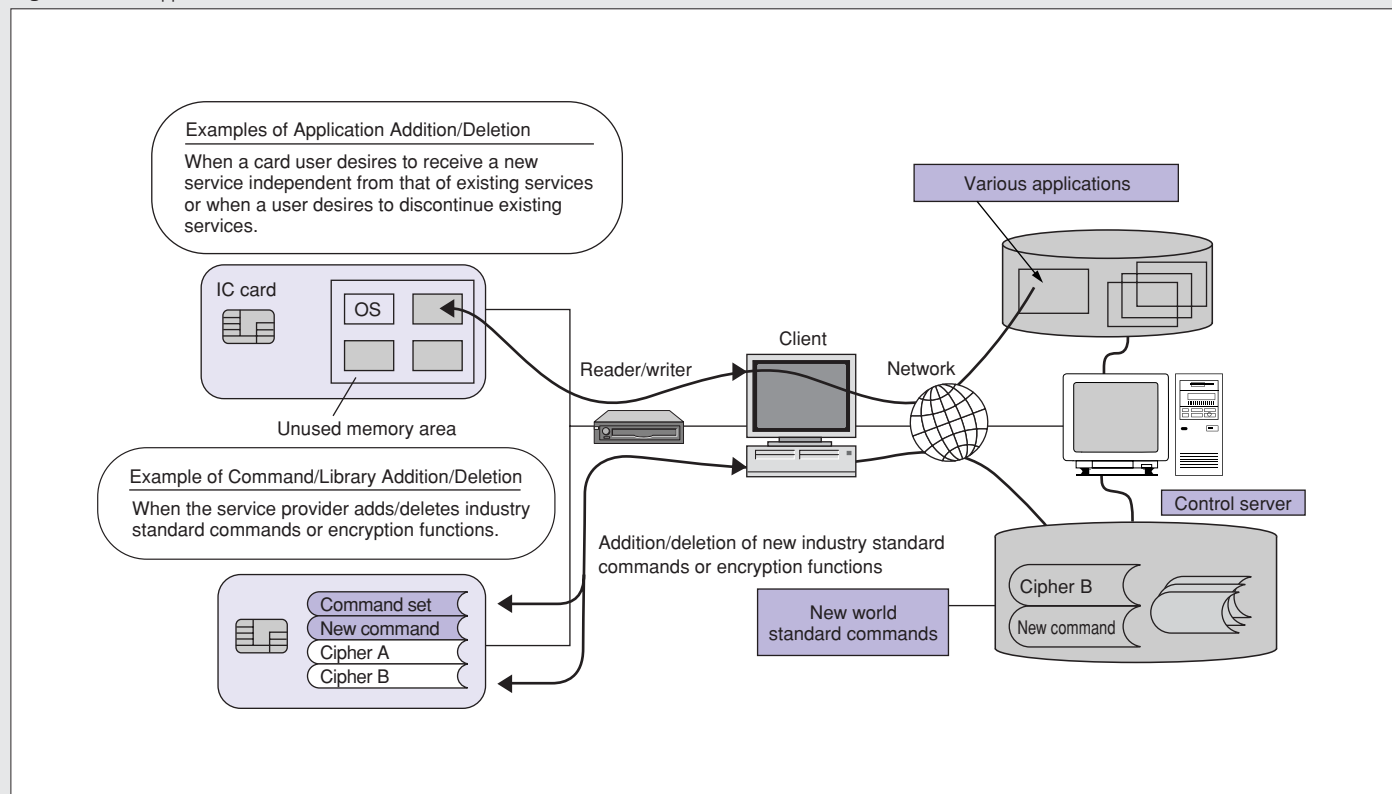
Public key ciphers use different keys for encryption and decoding. To perform encrypted communication, the sender holds the public key and the receiver holds the private key (decoding key). Because large calculations are required to derive the private key from the public key, its design effectively prevents this. With public key encryption, encrypted communication is possible without sharing the

private key between the sender and the receiver as long as the receiver's public key is known. Thus, it is considered suitable for use in communication with an indefinite number of receivers. It was popularized primarily as an encryption suited to digital signatures; RSA encryption and elliptic curve cryptography are typical examples of this group.

Fig.2 presents the relationship between signature generation and signature confirmation.

Although a 1,024-bit key length is used in RSA encryption for safety, the elliptic curve cryptography (ECC) method has a comparatively short 160-bit key length with the same level of safety and is thus expected to become more popular in the future. FUJITSU adopts characteristic 2 finite fields, which has good safety and allows for mounting in a small circuit scale, especially for IC card and security device purposes.

Figure 3 Multi-Application Smartcard Functions



Security Problems in Memories

The memory functions demanded in encryption security systems are classified as follows:

Parameter storage and updating

In recent operation services using the Internet, the end user's reception of a new service that is independent of the existing service or discontinuation of an existing service is implemented by erasing/reloading application software using high-speed communication. In such cases, ciphers, parameters, and keys must be correctly used at each operation site. This is expected to be an essential requirement in SIM cards, which will be mounted in IC cards and mobile phones of the future. Parameter management and change is also an important requirement in IC cards with limited resources.

Speedup in mounting

Mounting of the encryption process, which is a de facto standard of common key encryption and public key

encryption, fixes the necessary amount of algorithm calculation since the key length and parameter size cannot be restricted. Hence, a software method in which the software description is written in the processor language (assembler language) in order to reduce the number of cycles for the execution program and also a method in which the hard macro development of the operation process section is provided in order to improve the speed of both the hard macro and the software are adopted for speedup in general. The most effective method is to develop the hard macro for everything if the chip size is sufficient. However, this is not feasible in environments where resources are limited such as IC cards. Therefore, a method in which a calculated table is stored in the memory in advance and allows the results to be scanned and obtained by searching this table and to reduce the mounting by the operator may be used in some cases. The table in this case is generated on a nonvolatile memory. Considering that changes will be made for each application, it is important that a memory with high-speed writing ability be selected.

Firewall

When multi-applications are required, a means of control is necessary to prevent reference/change from one application to the storage area (program or data) of a different application. It is essential to utilize mounting that enables area separation using the hardware by mounting a virtual machine (VM) and preventing execution of the application without the intervention of the OS (Fig.3).

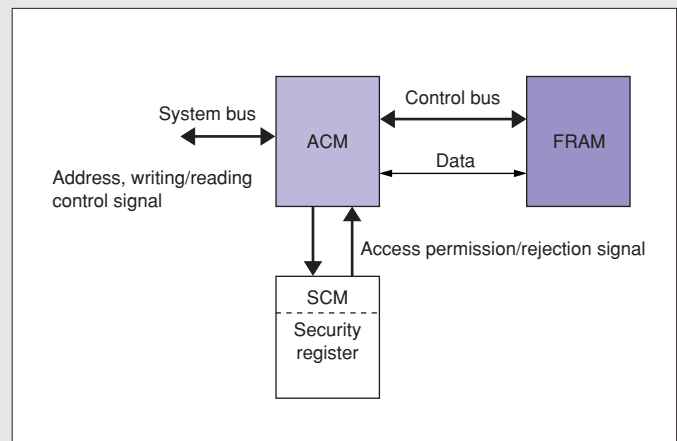
Table 1 Property Comparison among EEPROM, Flash Memory, and FRAM

	EEPROM	Flash Memory	FRAM
Memory type	Nonvolatile/10 years	Nonvolatile/10 years	Nonvolatile/10 years
Unit of data rewriting	Byte	Sector	Byte
Read-out cycle	200ns	100ns	100ns
Writing cycle	10ms	1s or larger	100ns
Times of rewriting	100 thousand times	100 thousand times	10 billion times
Internal writing voltage	14V	14V	3V

Table 2 Comparison of Security Function Properties

	EEPROM	Flash Memory	FRAM
Key/parameter storage	○	○	○
Key/parameter modification ease	×	○	○
Speedup in mounting	×	×	○
Firewall	○	○	○
Anti-tampering structure	Record existent	Record nonexistent	Record existent

Figure 4 Security Structure with FRAM Control



■ **Anti-tampering functions**

Anti-tampering measures are used to ensure security against malicious attacks. Techniques to deal with attacks can be classified from the viewpoints of circuit, method, and process. Attacks can be classified as invasive attacks or noninvasive attacks. The former type performs peeking/operations on circuits by directly accessing the IC surface to invade or destroy the anti-tampering properties of the card. Processes such as chemical solution treatments, micro-probing, converging ion beams, electron beams, layout reconstructions, etc. are used for this. The latter type is carried out without direct involvement of the IC itself. Means of invalidating the effectiveness of security keys have been developed by identifying and abusing weaknesses in software protocols/encryption algorithms. This is carried out by analyzing supply current fluctuations and leak current signals to access protected data (current analysis method) or by operating the device under some external stress to induce malfunction (glitch attack). These attacks may be executed with relatively simple facilities and a short period of analysis time. Therefore, functions that are capable of dealing with such attacks are essential in memories.

Table 3 Cipher Processing Rate and Code Size (at 13.56MHz)

Code size	Code size	Processing rate	
ECC (Characteristic 2 finite fields)	11K bytes	Signature generation*4	49.88ms
		Signature confirmation*4	129.82ms
RSA	7K bytes*3	Signature generation*5*6	210.8ms
		Signature confirmation*5*7	147.2ms
DES*1	—	Single DES ECB (hard macro)	43.39Mbps
		Single DES ECB	1.046Mbps
		Triple DES CBC	465kbps
AES*2	—	Round processing (key length 128-bit)	18.46Mbps
		Round processing (key length 192-bit)	15.50Mbps
		Round processing (key length 256-bit)	13.35Mbps

* 1: With each single DES ECB mode, software processing with the use of a hard macro is implemented.
 * 2: Hard macro only * 3: Size with exponentiation excess operation only
 * 4: Key length 163-bit * 5: Key length 1,024-bit
 * 6: CRT method used * 7: Public index e=65537

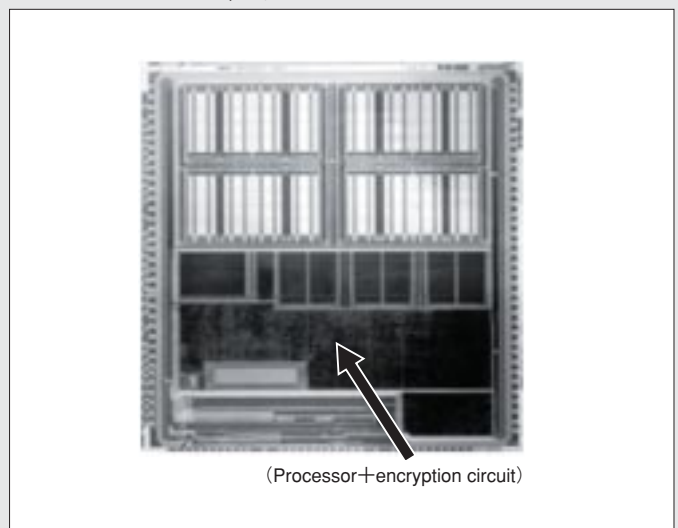
■ **Mounting of Security Structure Using FRAM**

■ **Comparison between FRAM and other nonvolatile memories**

Table 1 presents a comparison of the properties of EEPROM, flash memory, and FRAM, all of which are available as nonvolatile memories. FRAM has been significantly improved over the conventional nonvolatile memory, EEPROM, and in the present context it has 100 thousand writing cycles and rewriting times.

Table 2 provides a comparison of security function properties. Comparing the security problems, EEPROM is more difficult to modify in terms of control regarding writing cycles and rewriting times although it allows byte accessing. Its high-speed mounting characteristics are also poor. Generally, flash memories are weak in terms of writing time, although it is not difficult to establish firewalls since they adopt sector rewriting. In addition, there is an unknown quantity of anti-tampering mechanisms. FRAM can be considered as an optimal memory due to its ease of parameter modification, application downloading advantages, and speedup in mounting with its writing cycles being 100,000-fold or more faster than other memories as well as its improved times of rewriting.

Figure 5 MB94R202 Chip Layout



■ Security structure seen in IC cards

Fig.4 depicts the security structure of FRAM control. The smartcards “MB94R202/R211”, which address multi-applications, adopt this structure as a protective measure against noninvasive attacks. In addition to FRAM access control, this product is capable of dividing FRAM sectors and setting up the read/write protect for each sector according to the security register setup. It is also mounted with a mechanism that generates an exceptional interrupt signal on the system bus using an access permission/rejection signal to notify the processor if access that violates this setting occurs. Furthermore, the system is notified when voltage drops are detected and data assurance during FRAM access is also provided.

Fig.5 depicts a layout intended to protect against invasive attacks in a photograph of an IC chip for the smartcard, “MB94R202”. As shown in the figure, the layout is scrambled by wiring the processor core section, logic controller, and encryption macro resource in a mixture. It is impossible to determine the wiring connections by observing the LSI surface.

Moreover, the actual processing techniques, which involve flattening the wiring interlayer films, multilayer wiring, dummy wiring, and metal cover films, make it difficult to observe the wiring connection among surfaces or with the patterns on the next lower layer.

The FRAM macrostructure also has the physical address allocation that is free from the processor’s logical address. Since even data with a continuous length of 32-bit on the logical address physically exists in a scattered form, it is almost impossible to search for the locations and read by individual bit using any invasive method.

■ Encryption speed performance for cards

Table 3 presents the processing speed and code size for each developed encryption algorithm.

The common key ciphers DES and AES have been developed entirely by hard macro. For DES, the processing speed slows with triple DES. This is because one hard macro is called three times and for this software processing time is required. However, AES, which will be commonly used in the future, is as fast as 13.35Mbps, since up to a 256-bit length has been achieved using the hard macro.

As shown in **Fig.6**, using elliptic curve cryptography, which is a public key cipher (characteristic 2 finite fields),

the section that performs the scalar multiplication is expanded in a table on FRAM to be searched to enable speedup. Calculation of the table is performed and set up only once in advance based on the parameters provided by the operation site. In addition, the code size by the FR30 processor for signature generation and authentication has been addressed with 11Kbytes. Since the RSA cipher involves prime number calculation, it contains a special 32-bit residue operator. This enables high-speed processing of 147.2ms for signature authentication.

■ Future Development

It is expected that IT development will continue to advance in the future and that encryption and security will become essential fundamental technologies for the social infrastructure. In particular, IC cards are expected to be significantly improved in terms of convenience by expanding OSs that support multi-applications. Nevertheless, it is also feared that new attacks may be developed, as in the problem of PC viruses. Thus, FUJITSU will continue to proactively approach new security problems to provide IC cards and security devices mounted with safe, high-speed, and highly reliable FRAM. *

Reference

- *1: T. Kato et al.: IC cards that address both security and service improvements, FUJITSU, Vol.52, No.6, p.525-530 (2001).
- *2: FUJITSU: FRAM smartcard security, FUJITSU, 2001.
- *3: N. Torii et al.: Elliptic curve encryption, FUJITSU, Vol.50, No.4, p.197-201 (1999).
- *4: E. Okamoto: Introduction to encryption logic, Kyoritsu Shuppan, 1993.

Figure 6 Scalar Multiplication of Fixed Points Using Tables

Stores in FRAM the table in which multiples of the fixed point P have been calculated in advance.
 KP is calculated by giving the scalar coefficient K from a high order.
 KP calculation is performed by combining addition and doubling while using the values on the table efficiently.
 A point with high calculation frequency is selected as the fixed point.

●Example of scalar multiplication calculation

1.A = $(2^{11}P + 2^7P + 2^3P)$
 2.A = A + A
 3.A = A + $(2^{10}P + 2^6P + 2^2P)$
 4.A = A + A
 5.A = A + $(2^9P + 2^5P + 2P)$
 . . .

●Example of a table

FRAM area
P
2P
2P + P
. . .
$2^9P + 2^5P + 2P$
. . .
$2^{10}P + 2^6P + 2^2P$
. . .
$2^{11}P + 2^7P + 2^3P$
. . .
$2^{11}P + 2^{10}P + . . . + 2P + P$