FUJITSU FRAM
Smart Card Security

Specifications are subject to change without notice. For further information please contact each office.
What is FRAM?

FRAM is a type of memory that uses a ferroelectric film as the dielectric of a capacitor to store data. Ferroelectric films electrically polarize and reverse polarity, depending on the direction in which the electric field is applied. The storage function takes advantage of this characteristic. The adoption of ferroelectrics for the memory cells allows FRAM to maintain nonvolatile data characteristics, as well as high speed and high write frequency, thus combining the best features of both RAM and ROM. Furthermore, ferroelectrics enable low-voltage read and write operations, making this an ideal memory for mobile devices, which demand low power consumption.
The Need for Security

As smart cards continue to evolve as part of the societal infrastructure, it is essential to establish fundamental technologies that will allow us to maintain security and ensure peace of mind. As the range of information and functions associated with smart cards increases, security measures to prevent unauthorized access or modification of data will become issues of higher concern than ever before. Realizing this objective will require ensuring security that makes the most of LSI manufacturing technologies, as well as of design and software technologies. In addition, it will also be necessary to manage design and other data in such a way as to ensure that such data will be neither stolen nor otherwise revealed. With respect to FRAM Smart Card IC for multi-application, Fujitsu has taken the following security measures:

Security in Design and Manufacturing

(a) Scramble wiring, planarization of the oxide layers, and multi-layer wiring + (conf.)*

In terms of design technology, we have implemented scramble wiring, making it extremely difficult to trace a circuit through observation of the surface of the LSI. In addition, in terms of manufacturing technology, the oxide layers have been planarized and multi-layer wiring + (conf.)* used, making it impossible to determine interconnect of wiring from the surface of the LSI.

Thanks to the aforementioned measures, it would be impossible to trace the circuit should the LSI surface be exposed. Moreover, even for parties with the know-how and equipment required to strip off each layer of the semiconductor circuit, tracing would still be extremely difficult.

*Confidential information may be disclosed to customers who have signed a non-disclosure agreement with us.

(b) Removal of the measurement pad

When a wafer is cut into chips in the manufacturing process, pads for measurements can be removed (patented by Fujitsu 40001-35597). As the measurement pad, in the form of a card, is removed, should one be able to expose the LSI from the card, there would be no terminal to detect signal input/output, rendering it impossible to analyze the LSI's internal operations.

Following is an overview of the security measures we have taken with respect to FRAM (memory for storage of data within FRAM Smart Card IC).

(a) Physical Security Measures

To prevent unauthorized analysis of FRAM, a metal cover can be applied over the FRAM-cell area, so that the FRAM cell may not be directly observed. This means that, should the LSI surface be exposed and the surface of the chip observed, one would nonetheless be unable to see into the FRAM cell.

If one were able to expose the FRAM area and observe it with a metalurgical or scanning electron microscope, one would still be unable to read the pattern of the FRAM cell.

(b) Functional security measures

To combat any attempts to stop the supply of power while accessing FRAM to arbitrarily destroy FRAM data, a protective circuit has been implemented. In addition, the FRAM area is divided into small blocks in which a read-and-write-protection function can be set on a block-by-block basis. Thus, should there be any attempts to gain access to such protected blocks, the system will immediately be brought to a halt. Additionally, signals sent by the IC are encrypted, greatly increasing the difficulty of data analysis, even if detection were possible.

Memory Access (FRAM-Cell Tamper Resistance)
(a) Design Environment Control
- Area Control
  Measures are adopted to restrict entry to the design work area by implementing a system whereby only authorized personnel will be able to unlock the door.
- Design-Information Control
  With regard to protected design information (i.e., electronic data), the system is designed to permit only authorized personnel to access those information.
  - Mutual authentication between the card and the terminal:
    - Restrictions can be implemented so that verification may be executed only when internal or external authentication is completed.
  - Secure messaging
    - The communication code between the card and the terminal is encrypted so that it can neither be concealed nor altered.
- Personnel Control
  Educational/training programs to improve designer awareness of security issues have been implemented.

(b) MASK & Reticle Control
- Area Control
  Measures are adopted to restrict entry to the MASK & Reticle work area by implementing a system whereby only authorized personnel will be able to unlock the door.
- Information Control
  - Measures are adopted to restrict access to the design work area, with only authorized personnel able to unlock the door.
  - Mutual authentication between the card and the terminal:
    - Restrictions can be implemented so that verification may be executed only when internal or external authentication is completed.
  - Secure messaging
    - The communication code between the card and the terminal is encrypted so that it can neither be concealed nor altered.
- Personnel Control
  Educational/training programs to improve designer awareness of security issues have been implemented.

(c) Security Policy

(d) FRAM Sector Protection
  A hardware mechanism allows division of the FRAM area into sectors, in which read/write-protected functions can be set on sector by sector. In the event of any attempt that violates this setup, an exceptional cut-in would occur, which is linked to software.
  - PIN authentication function: to identify the controller
  - Manage the state of the card’s life cycle
    - The execution can be restricted according to card status (card on hold/card complete/application on hold).
  - Mutual authentication between the card and the terminal:
    - Restrictions can be implemented so that verification may be executed only when internal or external authentication is completed.
  - Secure messaging
    - The communication code between the card and the terminal is encrypted so that it can neither be concealed nor altered.
  - Implementation of encryption functionality
    - For security, basic encryption processing functionalities are implemented. A cryttoprocessor is used to increase processing speed.
  - Private key algorithms:
    1) DES encryption/decryption
    2) TripleDES encryption/decryption
    3) RSA encryption/decryption
    4) Elliptic curve encryption/decryption
    5) Signature generation
    6) Signature authentication

(e) Disposal
  Final wafer or package products and other associated materials are to be shredded within the premises under the immediate oversight of those assigned this duty.