A New Design for Smart Card Security System Based on PUF Technology

Elham Kordetoodeshki and Sattar Mirzakuchaki

***Abstract*—IP protection in smart cards is the most important aspect in the production process. Various solutions based on the idea of bit stream encryption have been proposed. In this paper SRAMPUF technology is used to obtain an acceptable security level in smart cards. At first, the strategy of SRAMPUF for producing physical unreachable code is used. Then the output of SRAMPUF is combined with customer's password to generate a unique and highly secure code. This is based on a powerful encrypting method. At last the result of this process is sent to data-center for comparison with a predefined database and authentication purposes.**

***Index Terms*—Challenge-response pair, IP arbiter, smart cards security, SRAM PUF.**

I. Introduction

Decades ago, the first generation of smart cards was introduced. And because of the vast variety of their applications, they have been developed very fast.

One of the most important aspects in smart card technology is the security aspect and therefore many encrypting methods for IP protection in smart cards have been proposed.

IP used on SRAM FPGAs is vulnerable to external attacks and the configuration bit stream can be easily copied and used on a similar off-the-shelf chip. Various methods relying on battery backed [1] or flash based [2] key storage on chip [3] were proposed to encrypt the bit stream stored in external non-volatile memory but because of problems for the field deployment they are not very widespread.

In the non-volatile memories, secret key is present in the memory and therefore they are vulnerable to invasive attacks. This problem can be solved by temper sensing circuitry with continuous battery power with an associated higher price.

The idea of using physical unclonable functions was proposed by Pappue in 2001 and later the possibility of its implementation on the silicon without requiring separate manufacturing process lead to significant increase in its usage.

Physical Unclonable Functions (PUFs) [4], [5] with characteristics of their unique circuit are innovative primitives to drive secret keys from complex physical characteristics of integrated circuits rather than storing them in digital memory. For example, random delay characteristics of transistors and wires can be used to generate a volatile secret key. In addition, an invasive attacker requires mounting an attack while the IC is running and using the secret key, and therefore during the invasive process, the attacker with very high probability will destroy the PUF. These issues make PUF very resistive to invasive attacks.

Simpson and Schaumont [6] proposed a new approach based on PUF that allows binding of a particular IP to a particular chip.

In [7], the authors use start up values of SRAM memories to introduce PUFs for chips. An SRAM cell is arranged as two cross coupled inverter circuits and two access switches which retain the stored value using positive feedback. Once the SRAM is turned on, due to the function of an inverter one of the floating outputs is driven positively within the loop and SRAM is forced to go to a logic 1 or 0. Which state is taken on is dependent on the characteristics of transistors making up each cell [8].

This is a practical construction of a PUF on the chip and in this paper based on this characteristic of SRAM PUF, a new method for encryption of the smart cards is proposed. In Section II we explain SRAM PUF structure and use it to produce unique a secret key. Section III describes novel smart card systems and their operation for information coding. Section IV discusses authentication and cryptographic key generation and section V concludes the paper.

II. SRAM PUF Review Stage

The structure of this kind of memory is based on a bi-stable latch which will retain its value as long as the circuit is powered and consists of 6 CMOS transistors as shown in Fig. 1.

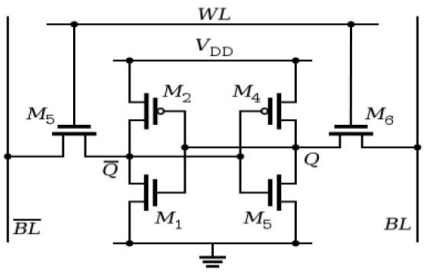

Fig. 1. 6T Cell SRAM.

Two transistors which labeled as 'M5' and 'M6' in the Fig. 1 are known as access transistors since they control the access to the storage cell during write and read process.

A. Ease of Use

In order to read or write to the cell, the word line labeled as 'WL' needs to be enabled to connect the two access

Manuscript received October 17, 2012; revised March 8, 2013.

Elham Kordetoodeshki is with the Department of Electrical and Computer Engineering, Islamic Azad University, Science and Research Branch, Tehran, Iran (e-mail: eli_007_k@yahoo.com).

Sattar mirzakuchaki is with the Department of Engineering, Iran University of Science & Technology, Tehran, Iran (e-mail: M_kuchaki@iust.ac.ir).

transistors to the bit lines, 'BL' and 'BLC'. The presence of two access lines leads to reduction in noise [7].

Some of uncontrollable factors in the manufacturing process such as dopant concentration, variations in oxide capacitor (Cox) lead to variations in the relative threshold voltages V_t of the transistors and cause each cell to tend toward logic zero or a logic one. Equation (1) shows the relation between these parameters and V_t .

$$V_{t\text{-}mos} = 2\phi_b + \frac{Q_b}{c_{ox}}, \phi_b = \frac{KT}{q} Ln(\frac{N_A}{n_i}) \quad (1)$$

where in (1) $Q_b = \sqrt{2\varepsilon_{si} q N_A 2\phi_b}$

All of these parameters cause an unpredictable behaviour of transistors and various threshold voltages. To verify threshold voltage variation effect on the output of transistors in 0.18 nm technology, we simulated it by Hspice using level49 typical model. The regulated threshold voltage change is about ±37.5%. Such a circuit is a simple latch built using two cross-coupled inverters. Notice that such cross-coupled circuits have an unstable operation point (to store the bit value). The circuit can be driven easily from one unstable state to another state due to slight differences in the parameters of transistors as shown in Fig. 2.

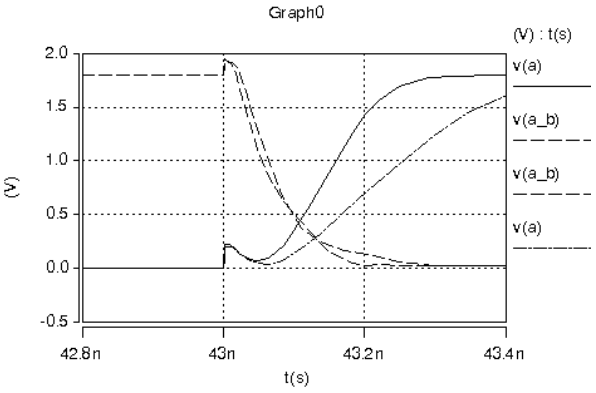

Fig. 2. Diagram variation with threshold voltage variation.

We use this fact to build a PUF where the circuit is initially at the unstable operation point and left to attain one of the two stable points without any external excitation.

III. Smart Card System

The smart card system consists of 4 main parts. 1-smart card 2-card reader system 3-translating system between card reader system and data base 4-data base.

Each part has its own Security importance and therefore the security of all parts must be considered all together and the commercial aspect is important too. Because of high security level of PUF systems and the ease of their implementation they have been used.

In the next part implementation of PUF technology for reaching a secure system for producing Smart Cards has been explained.

A. Security System with PUF Technology

As it is well-demonstrated, in this design only one PUF circuit is used. Because PUF circuits are unique, we feed some random numbers to the circuit input and save these numbers and related outputs to existing database as the result of this circuit.

This procedure is done for all PUF circuits. In other words, for each produced circuit, some random numbers are given to the circuit input and circuit output results accompanied by the input are recorded in the reserved part of the data base for that specific circuit(like A).

Finally we have a database which consists of some random numbers and the results of applying them to the PUF circuits. After delivering these cards to the users, for user authentication, one of those random numbers is sent to the card reader machine.

This random number is given to the embedded PUF circuit in the card as an input and related output which is a unique code is returned to the main centre. In order to recognize the identity of Card, the system compares this code with those stored in the database.

After finding identical code, the identity of that card is approved. This procedure is executed for all produced circuits. Fig. 3 shows the system structure.

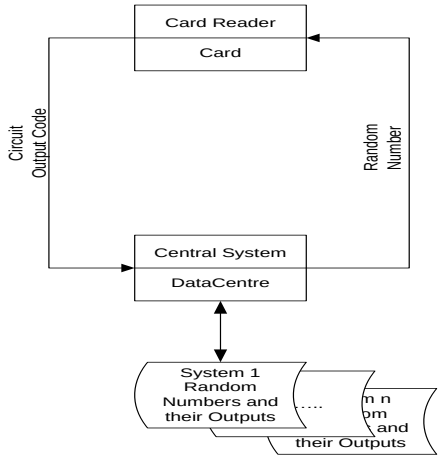

Fig. 3. Proposed smart card system.

In following sections, the method of producing the code and the type of the circuits, will be discussed.

IV. Cryptographic Key Generation and Authentication

The SRAM memory is being used for information saving. In this part we explain the usage of SRAMPUF for generation of a unique code without saving any data in the circuit which in turn leads to increasing system's security.

In fact, instead of using data for generating secret key, structural features of the SRAM cells are used. As mentioned in part one, every SRAM PUF circuit has unique and especial physical characteristics and thus their response to the same input can be different.

The aim is creating a unique code as an output of the circuit.

A. Key Generation

For generating such a unique code, a 16 word memory cell is used. Let's suppose that the structure of the memory cells is such as shown in Fig. 4.

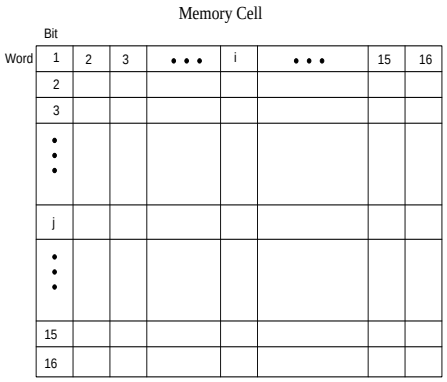

Fig. 4. A 16 word memory cell.

Each memory cell is an SRAMPUF circuit which goes to one or zero state depending on the input pulses and physical conditions. It means that when a pulse is applied to these cells, the recorded results can be different, either a logic one or zero.

Finally, we have a set of cells, while their values can be different. Each memory comprises 16 words. Therefore there are $16\times16=256$ memory cells with 0 or 1 value. Since each memory cell can take on two different states (0 or 1) independently, each of them can lead to a new word.

Finally the total possible and different values that can be assigned to these memory cells equals to 2256.

Since environmental factors like temperature or humidity can influence the SRAMPUF circuit values, for discarding these effects we test the hardware output 16 times and record related results. At last, the average of these values is calculated and a one bit code will be produced.

In other words, the average of those 16 bits is calculated to produce one bit. Equation (2) demonstrates the method of calculation:

$$B=\frac{(\sum_{i=1}^{16}M_i)}{16} \tag{2}$$

In the above equation, B is the average bit; (i) demonstrate the number of turning on and off the hardware.

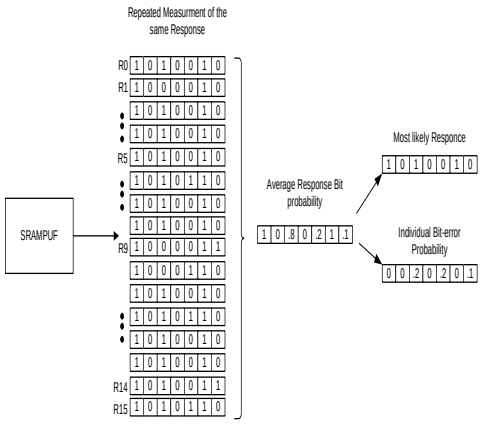

Fig. 5. A 16 word memory cell.

The output result might be a non-integer number between 0 and 1, so the produced average is rounded to the nearest integer 0 or 1. (Fig. 5) Now there are 256 bits which can be either 0 or 1, and therefore a code is produced which is 256 bits long.

Since the inputs of the circuit are 128 bits long; these 256 bits must be reduced to 128 bits. There are various approaches to do this. In this paper, XOR algorithm is used. Two bits are applied to an XOR gate and outputs of each two adjacent bits are used to generate the final secret key as shown in Fig. 6.

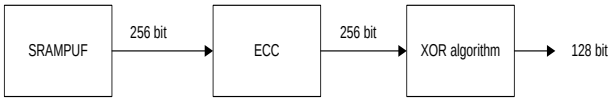

Fig. 6. 256 bits reduced to 128 bits.

B. User Authentication Process

So far, we have a unique code containing 128 bits which can be used for recognizing and determining card identity. There is an especial secret code for each user that is used for authentication. The authentication process is as follows: first the card reader gets an input pin from the user. This input pin consists of 4 digits which can be converted to a 16 bit binary number. But these 16 bits should be extended to 128 bits. This procedure is performed internally by the card with a specific manner. The algorithm used is as shown in Fig. 7.

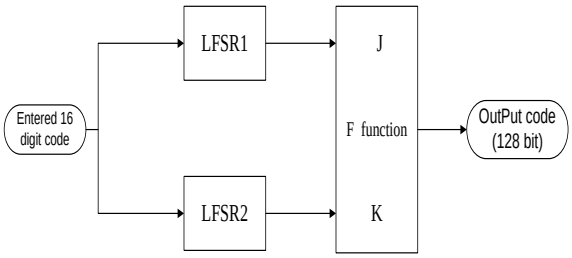

Fig. 7. The block diagram of a nonlinear composer function.

In this algorithm, two LFSR functions are used and 16 bits are given to each of them. These 16 bits are the exact input pin which the user has memorized. The function of each of these LFSRs differs from the other one and their outputs go to a nonlinear composer function. This action is done during 8 clock pulses and in each clock pulse 16 binary digits are produced. Therefore there are $8\times16=128$ digits and 128 bits are produced. In the next step, for generating the final 128-bit code, the AES algorithm is used which is shown in Fig. 8.

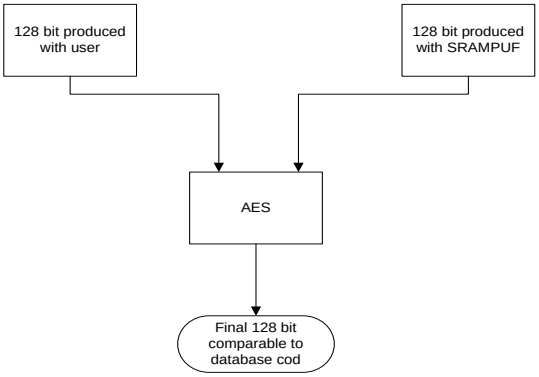

Fig. 8. The block diagram of encryption.

One of the inputs in Fig. 8 contains 128 bits produced by a nonlinear composer function and from user's cryptic code and the other one is a 128-bit input produced by SRAMPUF. The output of this algorithm consists of 128 bits which is known as

final cryptic code and has a high security.

This procedure is executed one time in the database before delivering the card to the user and the results are stored there as described before. Finally the card is delivered to the user and every time the card is used, the produced code is sent to the database and compared with corresponding code which is stored there. The identity of user will be approved in case of a true correspondence.

V. Conclusion

In the presented method, because of using SRAMPUF technology, the memory is volatile against invasive attacks and therefore makes it very hard for an outsider to obtain the key. There are few random numbers reserved in database and for each one there is a related response of PUF circuit that allows central system to send different numbers for different card authentication demands from card reader.

This feature leads to more security in translating system comparing to one with a single key allocated to each user. If attacker can find related code from translating system, this key cannot be true for all future authentication. These benefits are the most important superiority of proposed method comparing to conservative methods. For more efficiency, one may use a cryptographic method prior to 128 digit code generation in SRAMPUF which leads to higher security. Noise margin for sub-threshold SRAMPUF is another aspect of circuit that can be examined in a future work.

References

[1] R. Krueger. (July 8, 2004). *Using High Security Features in Virtex-II Series FPGAs.Xapp766 (v1.0), Xilinx*. [Online]. Available: http://www.xilinx.com/bvdocs/appnotes/xapp766.pdf

[2] Using the design security feature in stratix ii and stratix ii gx devices. *ALTERA. Application Note 341, v2.0*. (February 2007). [Online]. Available: http://www.altera.com/literature/an/an341.pdf

[3] Xilinx, *Security Solutions Using Spartan-3 Generation FPGAs*, Xilinx, San Jose, 2008.

[4] B. Gassend, D. Clarke, M. V. Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. the Computer and Communication Security Conf.*, November 2002.

[5] J.-W. Lee, D. Lim, B. Gassend, G. E. Suh, M. V. Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits with identification and authentication applications," in *Proc. the IEEE VLSI Circuits Symposium*, June 2004.

[6] E. Simpson and P. Schaumont, "Offline hardware/software authentication for reconfigurable platforms," in *Cryptographic Hardware and Embedded Systems-CHES 2006*, L. Goubin and M. Matsui, Eds. Springer, October 2006, vol. 4249 of *LNCS*, pp. 311–323.

[7] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *Cryptographic Hardware and Embedded Systems-CHES 2007*, P. Paillier and I. Verbauwhede, Eds. Springer, 10-13 September, 2007, vol. 4727 of *LNCS*, pp. 63–80.

[8] D. E. Holcomb, W. P. Burleson, and F. Kevin, "Initial SRAM state as a fingerprint and source of true random numbers for FID tags," in *Proc. the Conf. on RFID Security*, July 2007.

Elham Kordetoodeshki received the B.S. in Electrical Engineering from the University of Azad University of Iran in 2000, and the M.S. in Electrical Engineering from the University of Azad University, Science and Research Branch, Tehran, Iran in 2006. Her current research interests include characterization of semiconductor devices and design of VLSI circuits.

Sattar Mirzakuchaki received the B.S. in Electrical Engineering from the University of Mississippi in 1989, and he received his M.S. and Ph.D. in Electrical Engineering from the University of Missouri-Columbia, in 1991 and 1996, respectively. He has been a faculty member of the College of Electrical Engineering at the Iran University of Science and Technology, Tehran since 1996. His current research interests include characterization of semiconductor devices and design of VLSI circuits. Mirzakuchaki is a member of IEEE and IET (formerly IEE) and a chartered engineer.