APPLICATION OF PUF-ENABLED RFID TAGS IN ELECTRONIC BANKING

Saeed Mehmandoust[1] and Reza Ebrahimi Atani[1, 2]

[1]Department of Information Technology, The University of Guilan,
Anzali International Branch, Anzali, Iran
saeedmehmandoust@gmail.com

[2]Department of Computer Engineering, The University of Guilan, Rasht, Iran
rebrahimi@guilan.ac.ir

ABSTRACT

Radio Frequency Identification (RFID) tags have a variety of applications in e-banking. For effective utilization of the technology, this should be reinforced toward security holes and attacks. One of the common attacks on RFID systems is RFID tags cloning. In this paper we review cloning attacks in e-banking. We propose solutions based on physical unclonable functions (PUF) and provide a suitable security protocol for tag authentication in off-line environments.

KEYWORDS

RFID, eBanking, physical Security, Cloning Attacks, PUF, Authentication, Network Protocols.

1. INTRODUCTION

Emerging e-banking capabilities such as automation, optimization of internal processes, access control to resources, costs reduction, increasing competitiveness and customer relationship management has encouraged many reputational financial organizations [1]. One of the proposed technologies in e-banking is the application of RFID. RFID is an electronic tagging technology, which can provide a digital identity for an object. This technology uses radio frequencies to exchange data between a tag attached to an object and a reader. RFID tags can be active or inactive. Passive tags are inexpensive, low range and with no internal power supply. Active tags are more expensive, with higher range and internal power supply. Data storage can typically range between 32 to 256 bits in passive tags and several mega bytes in active ones.

RFID technology applications in e-banking can improve customer relationship management; prevent counterfeiting, financial document management, electronic payments using contactless cards and access control to resources. So RFID has important effects in e-banking applications. Many of the banks are analyzing or implementing solutions in order to use RFID for managing relationship with their special customers. The idea is to equip customers with a unique means for example, a RFID card. This way the bank can identify its client upon her arrival to bank environment so the type of facilities can be determined. RFID tags can be embedded in banknotes with high value in order to encrypt their security data against counterfeiting. In addition, loss of bank documents can cause large economic losses to banks. Using RFID for tracking and managing sensitive bank documents is of great interest. In this way an RFID tag is placed on document. So management and control on documents will prevent bank frauds.

RFID impact in electronic payments is enormous. Proximity cards are electronic devices which can propose easier access to electronic payment systems. RFID technology can be used to

DOI : 10.5121/ijcsit.2011.3214

establish wireless communication between the card and reader. The range of contactless cards is usually so that the user can perform transactions without removing the card from her purse. It also facilitated the operation and leads to physical security of payment cards. There are important applications of RFID access control technology in e-banking. Access control is used to control employee's access to resources, ranging from physical to information systems. Considering the potential of RFID in various banking affairs, this technology can be one of the most suitable tools for the development of e-banking. Despite the great advantages, specific RFID vulnerabilities blocks the widely use in critical e-banking applications.

One of the sever attacks in e-banking RFID systems cloning is duplication of security features such that they are consider authentic during authentication. In RFID tag case, cloning is defined as the simulation of the original tag's behaviour physically or virtually. In such attacks, reader cannot distinguish authentic tag from the imposter one and may prove the authenticity of the tags falsely. Tag cloning can severely threaten anti-counterfeiting solutions in e-banking systems and therefore should be taken into consideration during the e-banking RFID solutions.

Physical unclonable function (PUF) is a function that is integrated in a physical device and is easy to evaluate and make but hard to predict the behaviour and therefore duplication. PUFs help to implement challenge-response authentication protocols. When a PUF structure is stimulated using a challenge, it reacts unpredictably and gives a specific corresponding response. The uniqueness of responses in comparison with other chips in the same family and even the same manufacturing parameters is due to randomness in production phase which is unavoidable. PUFs are subjected to environmental variations such as temperature, supply voltage and , which can affect their performance. Therefore, rather than just being random, the real power of a PUF is its ability to be different between devices, but simultaneously to be the same under different environmental conditions.

Using RFID-tags for anti-counterfeiting purposes and cloning problem of RFID tags has been discussed in [4]. It proposes an efficient protocol for authenticating these tags. Generally it focuses on online authentication of RFID-tags. It means that the reader shares a secret key with the RFID-tag. Considering large deployment of RFID tags, there are many situations we need offline authentication where there is no valid reader available. In [9], RFID tags suitable for cloning attacks are discussed. Based on an Integrated PUF (I-PUF) a PUF-Certificate-Identity Based identification scheme was uses. This scheme makes offline authentication possible. Then implementation of the Schnorr identification scheme was investigated. This protocol is only secure against passive attacks but it is very efficient. The PUF architecture in [9] is based on coating intrinsic PUFs. Using this type of PUF, there is a need to change the production line of RFID tags. This increases the cost of tag productions. One important necessity in application of RFID in large-scale banking systems is to implement low cost tags. There were some attempts for hardware implementation of public key cryptography on RFID tags or other low-power application platforms such as sensor nodes in sensor networks. While RSA is not a feasible solution for RFID tags [18] showed the possibility of ECC implementation on RFID tags which meet the constraints imposed by limited resources. Authors in [20] has proposed a low-power ECC processor.

Our solution is based on silicon arbiter PUFs while other architectures in the literature are generally based on optical or coating ones. We suggest offline authentication in banking applications which needs ECC as public key cryptography to be executed on the RFID tag. This article seeks to provide a structure to deal with risks resulting from RFID tag cloning in e-banking. For this purpose, first a general classification of RFID attacks presented and cloning as one of the major attacks in RFID is described. Solutions to deal with cloning attacks are presented and unclonable functions as unclonable physical solutions will be discussed. In the

second part we examine various layers of RFID system, and related attacks will be examined. The third part discusses about attacks on RFID tags cloning and introduces some solutions to tackle with the problem. Section 4 describes PUFs and addresses the validity of a protocol to determine the overall RFID system based on this solution. Section 5 is based on hardware architecture for an unclonable RFID tag using cryptography, and finally paper concludes in section 6.

2. ANALYZING ATTACKS ON RFID

RFID networks have been implemented in many banking applications and no doubt soon this field will be developed further. RFID tags are comprised of small chip and an antenna that can pass data from objects to a reader using electromagnetic waves. In addition to general applications, including collecting tolls in highways, tracking animal species and applications in smart houses and cars, RFID networks has penetrated in financial services. A typical application is in euro banknotes. This initiative by the Central Bank of Europe is to prevent fraud and money laundering [3]. Despite the high potential of RFID in automated financial systems, banking systems have many inherent points of vulnerabilities which stop widespread use of the technology. RFID systems exposed to a wide range of malicious attacks from passive eavesdropping to active intervention. For example, since RFID tags can be read without permission access, their digital content can be available to hackers.

Dividing RFID network to distinctive layers helps us to identify and review different attacks more effectively. Different layers of RFID system can be seen in [2]. RFID networks include physical layer components such as physical interfaces, radio frequency signals and RFID tags. Network layer determines the way to transfer data between components of RFID network. Application layer consists of components which link between users and network. Strategic layer express trade secrets, business sensitive information and development policies related to organization which provides RFID services in a competitive business environment.

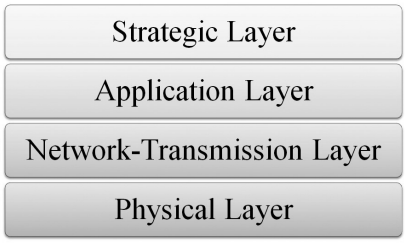

Figure 1- Different layers of RFID system

There are some attacks on physical layer which affect radio signals, tags or readers. In this layer, attacks take advantage of wireless structure network and weak security schemes. The network-transmission layer RFID attacks target communication protocols such as ISO 159693/1443. Network-transmission layer attacks are divided to tag, reader and protocol attacks. Tag attacks are comprised of cloning and spoofing of a fake tag. Reader attacks are impersonation and eavesdropping. The application layer attacks are unauthorized tag reading and modification. The middleware attacks are injecting malicious codes into the system. Ultimately, in strategic layer hackers uses security holes due to business organizations ignorance to proper security policies, development programs and user information privacy. These attacks can occur in form of spying for commercial competitors. shows a general classification of attacks in different layers [2].

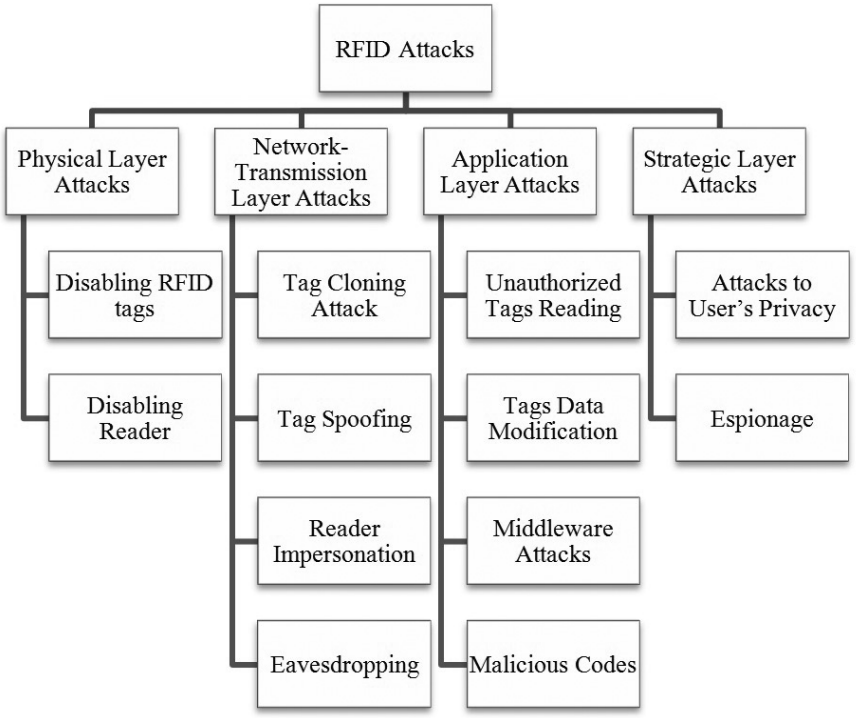

Figure 2. RFID Layer Attacks

3. RFID TAG CLONING ATTACKS

Most important feature of RFID tags that is their identity which makes them unique, is exposed to malicious attacks. Practically RFID tag cloning does not need high cost techniques. In the case that RFID tag has no security facility, cloning is solely an attempt to digital tag rubbery. However, if tags have additional security features, the attacker had to do more complex operations to copy the tag identity. A cloned tag deceives a reader to accept it as a legitimate one. The amount of required operations for a successful strike is related to security features in the RFID tag. Other form of tag cloning is non-physical spoofing of an RFID tag. In this way the attacker, forge a real RFID tag using advanced simulation tools. This requires full access to communication channels, knowledge of authentication protocols and password compromise [3].

Challenge/response authentication protocols are very useful to tackle with tag cloning. There are various methods to establish challenge/response protocols. One solution is deploying PIN for access control and authentication [4]. These methods are generally based on online systems while many e-banking applications require off-line authentication. In off-line authentication there is no need for encryption keys to go outside the tag and the mechanism is completely done inside. Using asymmetric encryption schemes in off-line authentication, overall network security will be improved.

One solution to create challenge/response mechanisms is PUF. PUF essence is that being easily created, but not reproducible. PUF uses randomness in its production process. This randomness can be produced by different physical features and by different ways. In the next chapter we will discuss different aspects of PUF in more detail.

4. PHYSICAL UNCLONABLE FUNCTIONS AS AN ANTI-CLONING SOLUTION

PUFs are physical systems which map a set of inputs (challenges) to a set of outputs (responses). The mapping is such that only the system owner can quickly get the correct responses and calculating output within a reasonable time by another person is very hard [6].

As previously discussed, an important application of RFID tags in e-banking is to prevent forgery. This requires RFID tags to be unclonable, as well as they provide identity to objects [5]. For systems with limited computing resources and high information storage such as RFID tags, even implementing encryption algorithms is not so simple [7]. However, research shows that for RFID tags with issues like security and cost, PUFs can be deployed to create unique identity to prevent cloning [8].

PUF can be implemented using different physical techniques. For instance optical PUF uses speckle pattern of a laser beam shines on the material. Coating PUF uses random capacitance due to production to generate a unique identity. Some models of PUFs use the intrinsic properties of silicon based integrated circuits. Most important types of silicon PUFs use logic gate delays. The uniqueness is originated from random changes in the silicon chips manufacturing process, which leads to large differences in gate response time. Research so far shows the use of intrinsic PUF is the most successful method to create a safe and secure chip. Security techniques that use silicon PUFs have many benefits compared to other techniques. Among them we can address great resistance against reverse engineering techniques, covert channel resistance and a higher response rate [6]. Therefore, in this paper we will focus on intrinsic silicon PUFs. We use silicon PUFs to design components of an authentication protocol for unclonable RFID tags.

4.1Design of a PUF-enabled tag

In this section, considering e-banking circumstances as an assumption we discus about the proper type of the PUF to be used in such applications. These assumptions will form a basis for proposed authentication protocol. Three conditions for the appropriate PUF are as follows:

1 - PUF should indistinguishably be linked to the RFID chip. This means that any attempt to removal of PUF will lead to the overall loss of the chip.

2 – Attacking the of communication channel between the chip and the PUF is impossible.

3 - PUF response is not available to the attacker.

Given these assumptions, we can conclude that the proper type of PUF is coating PUF or intrinsic one [9]. Unlike non-intrinsic PUFs, like coating or optical ones, intrinsic PUFs make use of the random characteristics of the chip in the manufacturing process. Using this type of PUF, there is no need to change the production line and much lower hardware overhead is needed. One major requirement in application of RFID in large-scale banking systems is to implement low cost tags. On the other hand, low cost RFID tags lead to severe limitations of processing resources. A low-cost RFID tag has only 1000 to 4000 gates [10]. Efforts have been done to come up with limited resources on RFID tags in order to achieve low-cost PUF solutions. We will discuss about the advantages and disadvantages of different types of intrinsic PUF-enabled RFID tags.

The main three types of intrinsic PUFs are Arbiter PUFs, Ring Oscillator PUFs, and SRAM PUFs. The idea is based on the physical structure of SRAM cells. The advantage is that these

methods can be implemented using RFID tags SRAM memory and they require no additional hardware to be implemented [11].

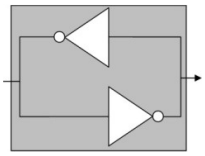

Figure 3. SRAM PUF

SRAM PUFs are based on the fluctuations of the silicon components occur during production as a source of randomness. A SRAM cell is a common type of memory which made up of two cross-coupled logic inverters (Figure 3). It is clear that this circuit has two stable states and by going to each it will store one logic bit. In the system startup, SRAM cells are located in random manner. Determining this state is very difficult for each chip. In silicon production processes such as CMOS, a manufacturer tries that two inverters similarly be implemented. This will improve power consumption and speed of the memory cell. However in reality due to changes in the process of manufacturing, there are very small differences in physical properties of the two inverters. In fact the mismatch of cells defines SRAM startup value between zero and one. However, random thermal noise at the time of startup can change these values. It can be concluded that each SRAM cell is a fingerprint of the chip. Having a SRAM memory on the chip it can be considered that a memory address is a specific set of challenges and SRAM cell startup state is a set of responses.

Silicon PUFs use random changes in the gate delays occur during chip manufacturing. So silicon PUFs are based on the gate delay from an input to output path. Delay PUFs use the differences between time delays of the two path to generate unique responses [6]. Structures based on delay use an element called arbiter in order to convert this time difference to a logic bit. An arbiter is a sequential element with two inputs and one output. An arbiter output will be one if the first input signal reaches to its cut off point faster. Otherwise the arbiter output will be zero. Two Symmetric digital delay lines are created on a chip and are stimulated simultaneously. Random deviations due to each part of the circuit, cause little difference in the time of response in each path. Finally by putting an arbiter we can detect which line is faster.

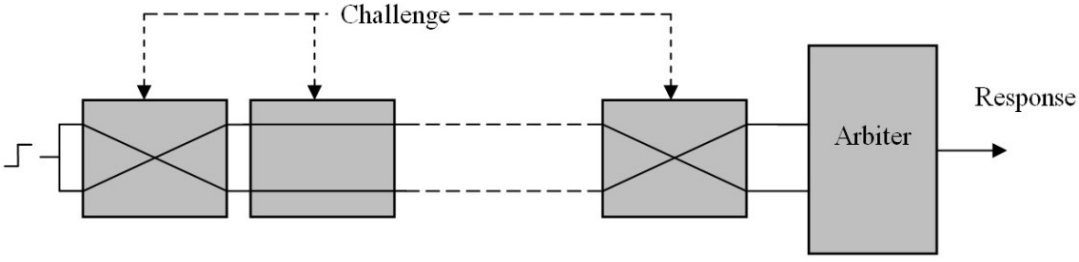

Figure 4. Arbiter PUF architecture

As shown in Figure 4 two symmetric delay lines can be made by putting multiple logical switches sequentially. Each of these switches can map input directly or cross depending to the output. Using n number of components, 2^n different directions can be selected by an n-bit vector. Since every possible arrangement could make a different delay, the role of a query vector is like a challenge to the PUF. Another type of delay PUF can be in form of a ring oscillator. Like arbiter PUF, ring oscillator PUF uses inherent randomness in a digital circuit

delay. However, instead of direct measurement of delay, PUF converts a path delay into a ring oscillator using a reversed feedback to the input (Figure 5).

An edge detector gate, every time a rising edge occurs generates a pulse. Counting the number of pulses can be used to calculate oscillator frequency. Due to random variations in gate delays, the number of pulses measured by a specific chip is unique. Number of pulses, is considered as ring oscillator PUF response. One way to implement ring oscillator is using two rings. In this case a challenge is two pairs of the oscillator pulse that are selected. Counter value is compared and a bit based on the response which is higher value. This structure has advantages like greater stability against environmental conditions.

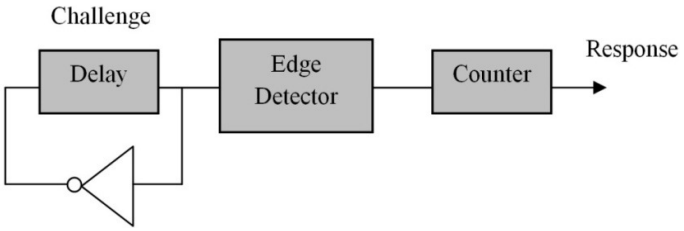

Figure 5. Ring Oscillator

We will review methods based on silicon arbiter PUF and study the use of such PUF in RFID tag architecture. This solution is much cheaper and more reliable to implement tags which are reasonably safe. It seems that in applications that require the use of low-cost tags with severe limitation of resources on tags, this kind of PUFs has economic justification. In addition, the SRAM PUF is highly prone to fluctuations due to environment conditions so they require more complex techniques to deal with this problem.

4.2 Implementing the tag PUF RFID:

A typical block diagram of a RFID tag can be seen in Figure 6. A RFID tag circuit is divided into three main parts: RF (Radio Frequency) interface, memory and logic circuits. RF interface is comprised of antenna interface, modulator, oscillator and clock pulse. Memory circuits include volatile, non-volatile, read-only and read – write memories [10]. Class 1 tags have read-only memory, while the class 2 tags have some amount of EEPROM [12]. Logic circuits control the tag performance as well as read and write access to tag.

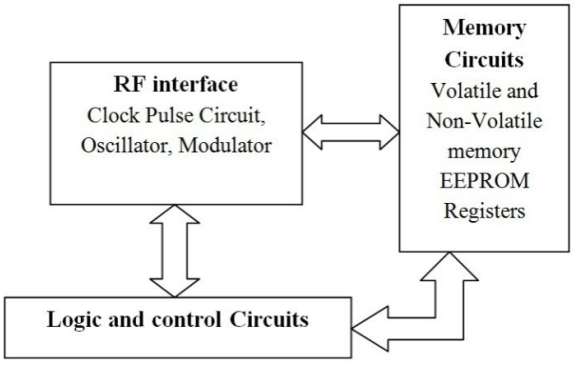

Figure 6. Components of RFID Architecture

Idea of using PUF in an RFID tag is shown in [13].Variety of solutions has been used to extract keys from inexpensive tags. This is possible due to the possibility of long-term and secure key storing on RFID tags. Figure 7 shows a model of RFID tag with a PUF circuit and its relationship with other components of the tag. This model is comprised of an arbiter PUF for implementing challenge/response protocol.

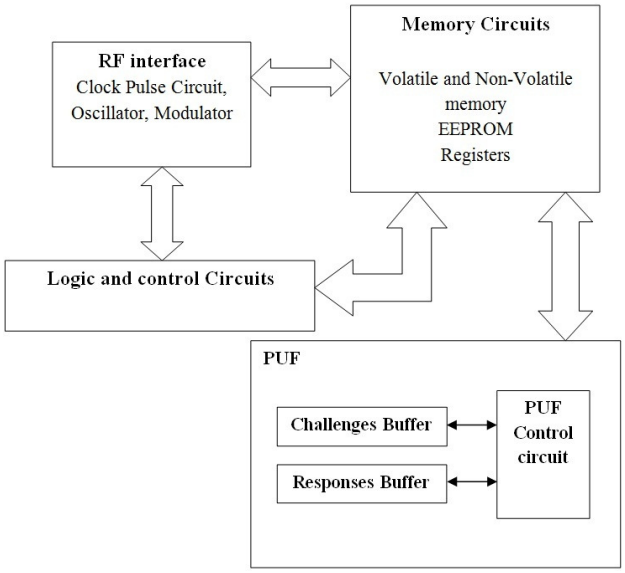

Figure 7. PUF-enabled RFID tag

4.3 Authentication Protocol

In this section, we will give an overview of the authentication protocol which can check the validity of a product based on PUF-enabled RFID tag. Two main stages of the authentication protocol are enrolment and verification. In enrolment stage several fingerprints are calculated from PUF using a number of challenges and corresponding responses. At this stage, auxiliary data for the verification phase is extracted. Challenges, fingerprints and auxiliary data, is signed a unique signature of the issuer. In verification stage, the reader challenges the tag using a set of challenges on the tag. Then using the signed fingerprint on the tag, the authenticity of the data on the card will be verified.

To clone a tag, attacker must place correct fingerprints from existing challenges. Having a set of challenges and associated fingerprints, a fake PUF would not be able to generate valid fingerprints. One possible method of attack can be designed using a forged PUF through unauthorized access to enrolment information like challenges, fingerprints and auxiliary data. However due to lack of attacker access to issuer secret key he cannot produce a valid signature on responses and make correct fingerprints [9].

We proposed the use of PUF-based architecture for off-line RFID e-banking applications. An important component of this architecture is to use cryptographic techniques for secure authentication. Cryptography in form of digital signature prevents manipulation and forgery of fingerprints on the tag. As previously discussed a RFID tag contains the object identity information. During enrollment, using issuer's secret key some fingerprints of PUF are placed on tag's non-volatile memory. During verification the reader is provided with a valid public key associated with the issuer private key to verify digital signatures.

In enrollment phase, PUF is challenged using a set C and the response set X is measured. Then the key S and the auxiliary data W is calculated by G (X, W) = S. The pair (G, W) is a key extraction function from noisy data. According to [15], the G function can be used under some conditions to extract a private key k from the PUF.

Quadruplet (IDPUF, C, W and S) is stored on the tag. In verification phase the identity of the tag will be send to the reader. Reader in role of a verifier randomly selects a set of challenges and questions the PUF using the correspondent auxiliary data. Response X^t form PUF is measured. The key S^t is calculated by $S^t = G(X^t, W)$ for authentication protocol. For the production of unclonable tags we can take advantage of silicon delay PUFs to create private keys. As previously discussed in order to create a private key in each authentication session the required auxiliary data W is extracted from PUF responses using a key extraction algorithm.

An identification scheme based on identity certification is used for off-line tag authentication. This scheme is defined according to [14]. Consider $SI = (K_g, P, V)$ is a standard identification scheme. K_g is a key generation algorithm and P and V are protocols which tags and reader run in the role of a prover and verifier respectively. $SS = (SK_g, Sign, V_f)$ is a standard signature scheme. SK_g is a key generation algorithm, $Sign$ is a signing algorithm and V_f is the reader verification algorithm. The identity based identification scheme is made up of SI, SS and the identity I in the form of $cert - IBI = (MK_g, UK_g, P, V)$. During enrollment the tag issuer uses SK_g as the master key generation algorithm MK_g. This means that the master key m_{sk} is for signature generation and m_{pk} is for signature verification. The user key generation algorithm is UK_g. For each RFID tag with the identity I, the issuer generates a private-public key pair (p_k, s_k) using K_g. The issuer runs the following protocol in order to authenticate the tag [14].

1. It challenges tag's PUF with a challenge set C and measure the response set X.

2. Having X and issuer private key s_k the auxiliary data W is calculated using $s_k = G(X, W)$.

3. The auxiliary data W and the certificate $Cert \leftarrow (p_k, Sign(m_{sk}, p_k||I)$ are written into the tag EEPROM.

During authentication, the tag in the role of a prover runs the following protocol together with a reader.

1. The tag runs the protocol P. In this protocol, the tag challenges its embedded PUF using C and gets the Y response. The private key $s_k \leftarrow G(Y(c), w)$ is calculated. Protocol P of the SI scheme is initiated using s_k.

2. The verifier uses (m_{pk}, I) for verification algorithm. The verifier obtains the certificate as a firs message from the tag. It verifies the certificate by running $V_{\mathrm{f}}(\mathrm{m}_{\mathrm{pk}}, p_k||I, Sign(m_{sk}, p_k||I))$.

3. If the certificate is not valid the protocol will halted. Otherwise V is initialized by p_k. If V is valid the verifier accepts tag's identity.

5. HARDWARE ARCHITECTURE OF PUF-ENABLED RFID TAGS USING CRYPTOGRAPHY

Efficient cryptographic algorithms are needed to minimize the hardware requirements of discussed authentication protocol on RFID tags. Different types of symmetric and asymmetric cryptography techniques can be used. For example, in [17] implementation of AES algorithm is shown on RFID tags. However symmetric cryptography techniques limit the authentication to online form. This requires the presence of the tag and the main issuer simultaneously. While the use of asymmetric cryptographic techniques allows offline authentication of a RFID tag which is very probable in e-banking situations.

The fundamental problem in performing public key cryptography is the severe restrictions on the hardware resources of RFID tags. Many efforts have been done to improve public-key encryption algorithms on RFID tags. In [18] feasibility of public key encryption based on RFID tags using elliptic curve cryptography (ECC) is shown. This section reviews algorithms for the identification scheme based on identity and propose hardware architecture requirements.

According to [14] a suitable SI scheme is one which is robust against the active, inactive and concurrent attacks. If only the resistance to passive attacks is considered Schnorr identification scheme can be used. In Schnorr scheme a tag will prove its identity to a reader in role of a verifier, using an ECC algorithm [16]. Elliptic curve encryption algorithm includes several components such as adders, multiplication and division on integer numbers. Modular division is the most time consuming operation in ECC [19]. So many suggestions for optimizing ECC operations for RFID tags have been presented [20]. Figure 8 shows architecture of a PUF-based RFID tag with an ECC processor for secure authentication.

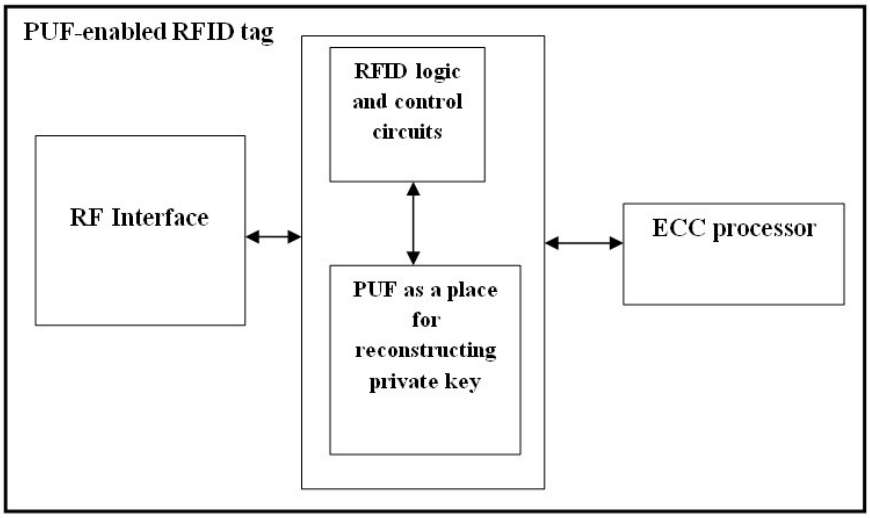

Figure 8. ECC based PUF-enabled RFID tag architecture

6. CONCLUSION

In this article we analyzed cloning attacks on RFID tags and possible solutions to deal with it. A probable solution for e-banking applications is embedding PUFs on RFID tags in order to provide anti-counterfeiting. This paper discussed proper protocols for PUF-enabled tags authentication. As indicated, public key encryption methods are needed for tag authentication and secure application of RFID tags. Elliptic curve algorithm proposed as a solution.

However RFID tags are typically very limited in processing resources needed for ECC. Hence the need for ECC processor hardware design considering resource limitations like power consumption, hardware area and operation speed is necessary. Since now, studies have examined ECC cryptography for tags without PUF structure. In some other studies the solutions are mainly based on non-intrinsic PUFs. Considering the advantages introduced for silicon intrinsic PUFs, in subsequent studies we will try to optimize ECC based PUF-enabled RFID tags regarding the restrictions exist on conventional tags.

REFERENCES

[1] P. Gupta, A. Joseph, (2006) "Using Radio Frequency Identification in Cash Management", HSBC's Guide to Cash and Treasury Management in Asia Pacific.

[2] A. Mitrokotsa, M. R. Rieback, A. S. Tanenbaum, (2009) "Classifying RFID attacks and defenses", Inf. Sys. Front, Springer, Published online 29 July 2009.

[3] C. Poirier and D. McCollum, RFID Strategic, (2006) "Implementation and ROI: a Practical Roadmap to Success", Florida: J. ROSS Publishing, 2006.

[4] A. Juels, (2005) "Strenthening EPC Tag against Cloning",ACM Workshop on Wireless Security (WiSe), M.Jakobsson and R. Poovendran (Ed.), pp.67-76.

[5] S. A. Weis A. Juels, (2005) " Authenticating pervasive devices with human protocols", In V. Shoup, editor, Advances in Cryptology: Proceedings of CRYPTO 2005, volume 3621 of Lecture Notes in Computer Science, pages 293–308. Springer-Verlag.

[6] M. Majzoobi, F. Koushanfar, and M. Potkonjak, (2009) "Techniques for design and implementation of secure reconfigurable PUFs", ACM Transactions on Reconfigurable Technology and Systems (TRETS), 2(1).

[7] G. E. Suh and S. Devadas, (2007) "Physical unclonable functions for device authentication and secret key generation". ACM, In Design Automation Conference, pages 9–14.

[8] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, T. Khandelwal, (2008) "Design and Implementation of PUF-Based "Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications", In: IEEE International Conference on RFID 2008, 58–64.

[9] P. Tuyls, L. Batina, (2006) "RFID-tags for Anti-Counterfeiting", In D. Pointcheval, editor, Topics in Cryptology - CT-RSA 2006, Lecture Notes in Computer Science, San Jose, USA, February 13-17 2006. Springer Verlag.

[10] D.C. Ranasinghe, D. Lim, P.H. Cole, S. Devadas, (2007) "A low cost solution to authentication in passive RFID systems", Networked RFID Systems and Lightweight Cryptography Raising Barriers to Product Counterfeiting. Springer.

[11] D. E. Holcomb, W. P. Burleson, K. Fu, (2007) "Initial SRAM state as a fingerprint and source of true random numbers for RFID tags", RFIDSec.

[12] P. Cole and D. Ranasinghe, (2008) "Networked RFID Systems ,and Lightweight Cryptography — Raising Barriers,to Product Counterfeiting. Springer.

[13] D. Ranasinghe, D. Engels, P. Cole, (2004) "Security and Privacy: Modest Proposals for Low-Cost RFID Systems", Proc. Auto-ID Labs Research Workshop, Zurich, Switzerland.

[14] M. Bellare, C. Namprempre, G. Neven, (2004) "Security proofs for identity-based identication and signature schemes". Proceedings of Eurocrypt 2004, volume 3027 of Lecture Notes in Computer Science, pages 268-286.

[15] J.P. Linnartz and P. Tuyls, (2003) "New shielding functions to enhance privacy and prevent misuse of biometric templates". In J. Kittler and M. Nixon, editors, Proc. of the 3rd Conference on Audio and Video Based Person Authentication, volume 2688 of Lecture Notes in Computer Science, pages 238-250.

[16] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, I. Verbauwhede, (2006) "An elliptic curve processor suitable for RFID-tags". Cryptology ePrint Archive, Report 2006/227.

[17] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, (2004) "Strong authentication for RFID systems using the AES algorithm". In M. Joye and J.-J. Quisquater, editors, Cryptographic Hardware and Embedded Systems (CHES), Springer-Verlag, LNCS, Vol. 3156, pages 357-370.

[18] J. Wolkerstorfer, (2005), "Scaling ECC Hardware to a Minimum. In ECRYPT workshop – "Cryptographic Advances in Secure Hardware" - CRASH 2005.

[19] D. Hankerson, A. J. Menezes, and S. Vanstone, (2004), "Guide to Elliptic Curve Cryptography. Springer-Verlag New York Inc., New York, USA.

[20] H.R. Ahmadi, A. Afzali-Kusha, (2009) Low-Power Low-Energy Prime-Field ECC Processor Based on Montgomery Modular Inverse Algorithm, IEEE,Digital System Design, Architectures, Methods and Tools.

Authors

Saeed Mehmandoust was born in 1984. He received his B.S degree in Electrical Engineering at the University of Guilan, Iran. He is currently pursuing a M.Sc degree from the University of Guilan (Anzali International Branch) in the field of Information Technology (e_Commerce). His interests include Coprocessor design for fingerprint authentication and E-commerce security.

Reza Ebrahimi Atani was born in 1980. He received the B.S. degree in electrical engineering from the University of Guilan in 2002 and the M.Sc and PhD degrees in electronics from Iran University of Science and Technology in 2004 and 2010 respectively. Since 2010, he is an assistant professor in Computer Engineering Department at the University of Guilan. His current research interests include stream cipher design and cryptanalysis, cryptographic hardware and embedded system (CHES), side channel attacks (Power and fault attacks), and design of VLSI circuits.