# SECURED RFID MUTUAL AUTHENTICATION SCHEME FOR MIFARE SYSTEMS

Kuo-Tsang Huang and Jung-Hui Chiu

Department of Electrical Engineering, Chang Gung University, Tao-Yuan, Taiwan
d9221006@gmail.com, jhchiu@mail.cgu.edu.tw

## *ABSTRACT*

*This research study and analyse the various attacks RFID card on Mifare's disadvantage and safety concerns crux of the problem. The key recovery attack method depends on a plaintext-ciphertext pair on the existing relationship, as well as the secret parameters of the pseudo random number for use of the timing inappropriate. We proposed a scheme to improve the mechanisms for authentication, no additional secret parameters into the standard, solely by readers and tags communication between the timing of the change of use of the secret parameters. This mechanism can make plaintext-ciphertext pair of the derivation relationship does not exist and be used in the Mifare-like of the RFID products. Attackers don't have the possibility to obtain the key stream, thus making available to obtain the secret key of the attack ineffective. Besides, we also proposed an enhanced authentication for ubiquitous computing. The present invention is to achieve RFID for improvement mutual authentication and protects against skimming attacks. The invention uses streamcipher technologies can strengthen the implementation of ISO 9798-2 security authentication mechanism, such as the defence has been publicly Mifare Classic from the various attacks. Our proposed authentication protocol can be used to solve the secret key recovery security problems of RFID systems.*

## *KEYWORDS*

*RFID, Mutual Authentication, Ubiquitous, Low-Resource*

## 1. INTRODUCTION

RFID (radio frequency identification) systems, there are two major components of basic elements: Tag (transponder), attached to objects to mark the uniqueness of the component; card reader (interrogator), the system on which the read-write tag devices. Tag is a system of user-side device operation, which provides storage field, with identity authentication, data access to provide application functionality. Sophisticated card structure, have more memory space, providing more powerful encryption and decryption functionality module, of course, will cost more expensive.

Tag is a system of user-side device operation, which provides storage field, with identity authentication, data access to provide application functionality. Sophisticated card structure, have more memory space, providing more powerful encryption and decryption functionality module, of course, will cost more expensive.

A typical deployment of an RFID system involves three types of legitimate entities, namely tags, readers and back-end servers. The tags are attached to, or embedded in, objects to be identified. They consist of a transponder and an RF coupling element. The coupling element has an antenna coil to capture RF power, clock pulses and data from the RFID reader. The readers typically contain a transceiver, a control unit, and a coupling element, to interrogate tags. They

implement a radio interface to the tags and also a high level interface to a backend server that processes captured data. The back-servers are trusted entities that maintain a database containing the information needed to identify tags, including their identification numbers. Since the integrity of an RFID system is entirely dependent on the proper behaviour of the server, it is assumed that the server is physically secure and not attackable. It is certainly legitimate to consider privacy mechanisms that reduce the trust on the back-end server; for instance, to mitigate the ability of the server to collect user-behaviour information.

A variety of RFID applications in daily life have been quite a lot, such as building access control, take the bus rapid transit, mobile micro-payment, borrow library books and logistics supply chain management. This technology enhances the security of these applications of RFID, and it should enhance the additional value of products and competitiveness. This proposed technology can be applied using RFID products in many applications of the techniques, for example: transportation systems, access control systems, logistics, supply chain systems and mobile payment system.

In this paper, however, we shall not investigate such privacy attacks. These have been discussed extensively elsewhere. Here we shall consider the servers to be entirely trusted. The verify part, devices need an identification system because both parties unknown whether the other party as legitimate members of. Identity verification devices have two major techniques. The one-way hash identification is the most commonly used one-way authentication. The mutual authentication is over the challenge-response authentication mechanism to achieve. Low-cost RFID tags are already being used for supply chain management and are a promising new technology that can be used to support the security of wireless ubiquitous applications. RFID tags may be components of larger ubiquitous systems, and many RFID authentication protocols are executed in arbitrary composition with other secure protocols. RFID protocols are not used in isolation, but concurrently, possibly involving other ubiquitous applications (e.g., Sensors, meats, etc.).

## 2. RELATED WORKS

Radio Frequency Identification is the product of limited resources with a low-cost, slight computing power and a few memory capacity attributes. Therefore it is a good design to take stream ciphers to achieve its authentication mechanism and encryption algorithms without too many resources.

For example, Mifare Classic RFID uses a stream cipher to archive encryption authentication. However cryptographic algorithms used for the system is weak, even if the identity authentication mechanism is the use of international standard methods. If this identity authentication mechanism parameter design is not ideal, the whole system designed is still unsafe.

Identity authentication mechanism is currently accepted standard practice “Challenge-Response Authentication”, to respond to questioning the identity authentication mechanism. For example, B is the challenger to authenticate the identity for responser A, the mechanism requires: B is to make sure A has only know the common secret parameters K. The identification process is, first, B produces the random number *r* when questioning the value of Challenge sent to A. A to receive the *r* and calculates Response S with the both sides secret parameters generated by the cryptographic value K of response, back to the B. B receives a response values, with their common to both of the secret parameters of K by comparing the results of cryptographic operations, if the same can be sure the other has only the A and B have the secret parameters, which the other does as A.

## 2.1. ISO 9798-2 [1]

The currently operate identity authentication mechanism by symmetric encryption for the international standard ISO 9798-2, the one-way identity authentication mechanism, as shown below, set B to identify whether the other side A or not; B generate random value rB when the cross-examination to give the other side A; Then A using the common secret key **K** and random number on the receipt of rB to generate an encrypted identifier may EK (rB, B*) as a response value back to the B. In EK (rB, B*) the "*" indicates the identifier for the option B is an option, "," that order with or concatenation means. B receives a response value is obtained if the correct decryption rB and B* with correct K, can be recognized the other has a K, the other for the A. Namely B of A for questioning actions by authenticated responding.

1. A← B: rB

2. A→ B: EK(rB, B*)

An RFID protocol requires at least two passes for (one-way) tag authentication: a challenge from the server and a response from the tag. If the tag initiates the protocol then we need at least three passes for secure tag authentication. For a minimalist approach one should aim for two passes. O-TRAP is an RFID one-way authentication protocol that was proposed in [2]. Each tag stores two values: a pre-shared, private, long-term key k_tag, and a volatile identifying pseudonym r_tag which is updated each time the tag is challenged. The server has a database in which it stores for each tag the pair of values (r_tag, k_tag) indexed by r_tag. The reader selects a random string r_sys and broadcasts it to all tags in their range. r_sys would be used to authenticate all tags and be used to update which's pseudorandom value r_tag in the RFID system. The cost for both tag and server is just one application of a pseudo-random function (PRFs). O-TRAP shows that such level of security is achievable at a low cost.

## 2.2. Mifare Standard [3]

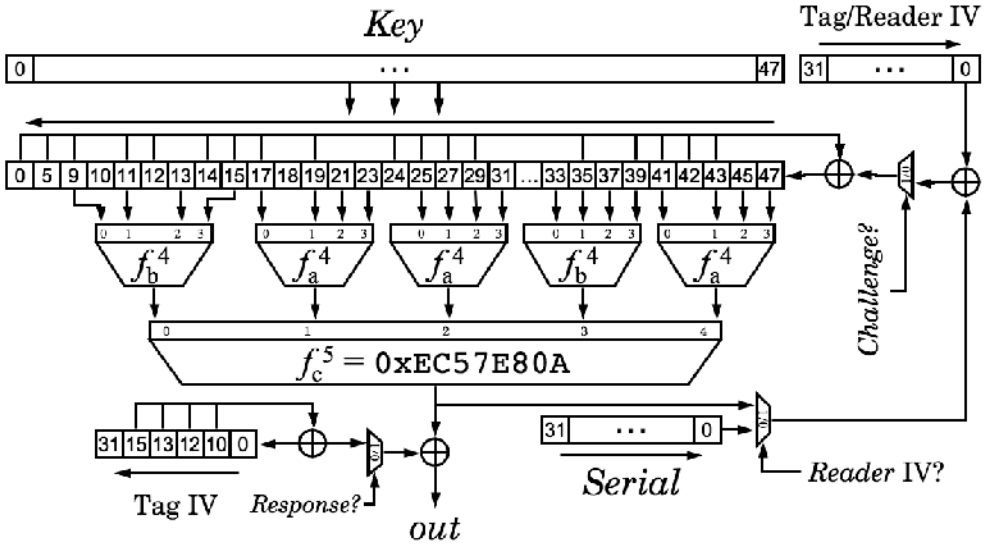


Figure 1. CRYPTO–1 Cipher [3]

Mifare Tag used in cryptography CRYPTO-1[4] is streaming the password system (stream cipher), a linear feedback shift register (LFSR) based streaming cryptography. The reverse engineering analysis, the streaming cipher for Mifare Tag is simple, fast encryption speed, but because the 48bit key length is shorter, can not provide enough security strength. CRYPTO-1 in 48bit the LFSR state values produced by the nonlinear filter function 1 bit keystream output. LFSR state values, only 20 bits of the odd location of the bit will enter the nonlinear filter function (fa, fb, fc) conducted operations. Somewhat short of the 48-bit key value is the Mifare weakness in high-computing environment is relatively easy to brute force attack.

Mifare system in the security part of the authentication protocol is the use of ISO three pass authentication process, based on challenge-response of the ISO9798-2 standards-based, two-way identity can be achieved identification, to the effect of mutual authentication. Step 1: Reader sends an authentication request to tag. Step 2: Tag choose a challenge nonce, which notes nT, returns nT to Reader. Step 3: Reader choosing a challenge nonce, which notes nR, and computing an answer, which notes aR, then send nR and aR to tag. Step 4, Tag calculated response value aT, and aT pass Reader, the end of the authentication process.

We use the notations summarized in Table 1 to describe protocols throughout the remainder of this paper. The following diagram represents an RFID authentication process in which the parameters for the description of Figure 2 appeared in the definition:

Table 1. Notations

| Notation | Description |
|---|---|
| Tag | RF tag, or transponder. |
| Reader | RF tag reader, or transceiver. |
| K | Cryptographic key, shared between Tag and Reader. |
| Uid | The Unique ID of Mifare Tag is a unique identification number of Tag, shared between Tag and Reader. |
| nT | The authentication challenge sending from Mifare Tag. |
| ks1,ks2,ks3 | ks1,ks2,ks3,…are keystreams used to encrypt and decrypt, generated from the PRNG of CRYPTO–1. The rear number is the number of rounds. Each round time is 32-bit shift time duration. |
| { } | Brace means that informations had been encrypted. |
| {nR} | The authentication challenge sending from Mifare Reader. |
| {ackR} | The authentication response sending from Mifare Reader. |
| {ackT} | The authentication response sending from Mifare Tag. |
| $prng^{x}( )$ | A pseudo random number generator based on LFSR architecture, superscript x is the number of rounds. Each round time is 32-bit shift time duration. Brackets for the LFSR initial state, which is commonly, know as the seed value. |

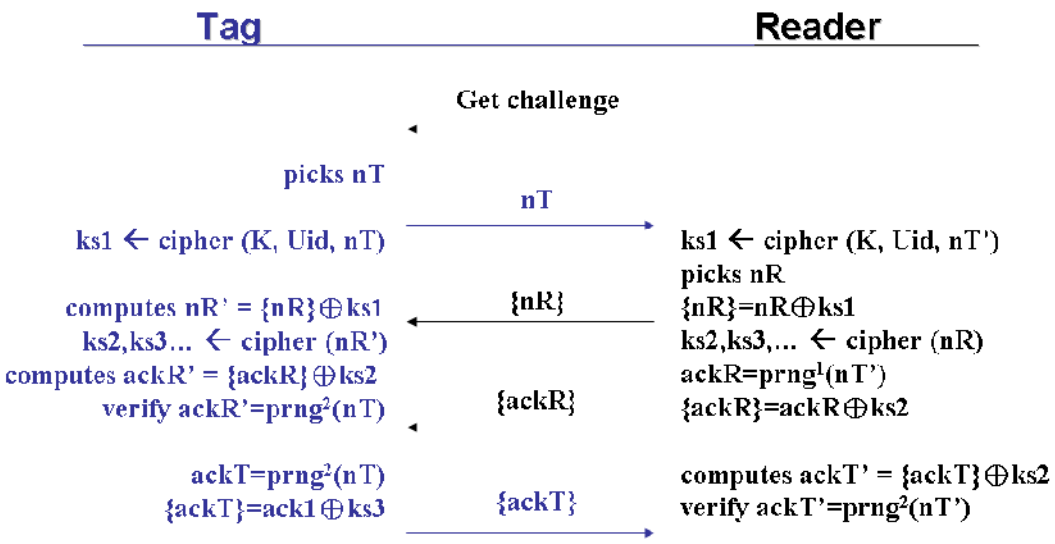


Figure 2. Mifare mutual authentication scheme

## 3. EXISTING MIFARE ATTACKS AND THE CRITICAL WEAKNESSES

The ability to create clones of tags can be used as a means to overcome counterfeit protection (e.g., in passports). The ability to create clones of tags can be used as a preparatory step in a theft scheme. Again, it exposes corporations to new vulnerabilities if RFIDs are used to automate verification steps to streamline security procedures.

Identity and authentication mechanisms are key technologies in many of the security and privacy RFID applications. Most RFID devices achieve the key distribution through authentication mechanisms. Once the authentication mechanisms are compromised, or information leaks vulnerabilities enough to be cracked, the security of data protection almost nonexistent. One example was Mifare card hack. Mifare card was the most widely used contactless smart cards currently. Mifare cards have been revealed, there are some security flaws. In October 2007, the hacker group after another released the messages of Mifare card security concerns. The research [5] by way of reverse engineering for the dismantling of the logical circuit discovered the internal Mifare chipencryption module structure. The research [6] claimed that the ready ability to forge Mifare card. This chapter discussion Mifare weakness and help to improve the program.

### 3.1. Existing Mifare attacks recently

There are some side-channel attacks and timing attacks, both types are physical attacks that target the protocol layer interface. In the international conference Usenix2008, "Reverse-Engineering a Cryptographic RFID Tag" use the techniques field of computer science, physical attack, circuit implementation, authentication protocols analysis, reverse analysis of the chip structure. This stage of the secret key recovery attacks was the use of rainbow table technique. In the Chaos Communication Camp 2007 conference, "Practical RFID Attacks" introduced the sniffer tools for Mifare card, OpenPCD and OpenPICC at Aug. 10, 2007. Then "A Practical Attack on the MIFARE Classic" published in 2008, sniffer tool changed to use ProxmarkIII. The paper introduced keystreams recovery attacks, include keystream recovery, keystream mapping and authentication replay. At this stage, only for the repeatability of the keystream to

be used, not to crack the encryption key [5][7]. Henryk Plötz wrote his doctor thesis in German finalization at Aug. 2008. Mifare attacks against them had classified the existing discussion. At this time of key recovery, still in use legitimate card reader for on-line brute force attack. In the trial stage, the thesis discussed the authentications of 2^48 times. This is very typical of the time-memory trade-off equipment; and to explore the random number generator's cycle length is too narrow to capture. The value of information can be used repeatedly; keystream recovery approach is the same as "A Practical Attack on the MIFARE Classic"[7] The most valuable parts of this study is that their team delivered the software to simulate the operation of opensource agreement, Philips / NXP Mifare Crypto-1 implementation v1.0 by Karsten Nohl, Henryk Plötz, Sean O'Neil. The open source C language program code was almost for the following key recovery attack to achieve the reference to the study.

"Anatomy of a Subway Hack" [9] in 2008, MIT students to practice for the Boston subway attack, and show tickets for illegal value-added means of magnetic stripe. [8] point out about Mifare cards the random number generator the narrow length, the filter function of the framework law of a segmentation feature. Although they did not reach the realization of dense Mifare breaking. But a substantial disclosure by the media had begun to cause public panic, nontechnical background issues of concern and attention."Dismantling MIFARE Classic"[5] and the Security & Privacy 2009 Best Paper "Wirelessly Pickpocketing a Mifare Classic Card"[8] can be regarded as key recovery of the real discussion and possible implementation. The use of legal tag for off-line brute force attack costs about as big as a 0.6ms/time ~ 1500times/sec. time. Concludes these papers can be summarized in the following two points: (1) calculated under the somewhat short of the safety of 48-bit key value, high-computing environment in a relatively easy to brute force, could not resist off-line brute force attacks; (2) inappropriate The error handling mechanism for an attacker provides additional information to judge for the hacker attacks using error handling and then simplify the verification steps violent attacks.

The papers [5][6][7][8][9] introduced keystreams recovery attacks, include keystream recovery, keystream mapping, authentication replay and key recovery. The above researches are existing Mifare attacks recently and these have included the critical weaknesses of the Mifare system under attacks. This chapter does not discuss weakness but do improve the program. For details on such issues, and more generally on standards for RFID systems, the reader is referred to the Mifare, ISO 14443a standard and above researches about attacks.

### 3.2. The critical weaknesses of Mifare system under attacks

Symmetrical secret agreement by the challenge response based on the encryption technology, defined in ISO/IEC 9798-2 standard [1]. One-way authentication as follows: There are two partners A and B have the same private key. B sends a random number rB to A. A encrypted this random number rB using pre-shared key K and sent it back to B. B prove results and can be verified A status legal or illegal. The mutual authentication protocol is similar work. B sends a random number Rb to A. A encryption shared key K and self-generated random number Ra, and sends it to B. B decrypts the message, you can prove that if Rb and get the right pull. B change the sequence of random numbers encrypted with K it for the A: and B demonstrate the results of the authentication [10].

Control 3-pass authentication, the operation of the process Mifare Tag sending Uid is equivalent to sending the pre-operation steps to initialize. When Tag sends a random number nT, the equivalent of challenge1 gave Mifare Reader. Mifare Reader uses the random number nT for the second round as seed derivative, that is aR. aR as response1 back to the Mifare Tag. Mifare Tag

verifies received response1 to authenticate Mifare Reader. This is a one-way authentication from Tag to Reader.

Mifare Reader get {nR} to the Mifare Tag, as challenge2. If Mifare Tag can decrypt the ciphertext {nR}, get nR, Mifare Tag encrypted using the random number seed nT for the third round of derivatives with secret parameter nR, denoted as aT, as response2 back to the Mifare Reader. Mifare Reader will verify this response2 to authenticate Mifare Tag. Reader completed the one-way on the Tag authentication; thus complete the mutual authentication.

Malicious could have access to keystream opportunity to the communication process in authentication. As described below: Malicious people can figure out $prng^2(nT)$ depend on nT and public *prng( )* function. Therefore people can calculate the ks2. It can calculate the $prng^3(nT)$ to obtain ks3, and so on. On the other hand, suddenly removed the Mifare card during communicating in the authentication process, the reader will be heard a suspension of halt command. Halt command and ks3 for the XOR operation, the halt instruction formats have been standardized in ISO14443 standard. Therefore, a malicious person can get through the calculation of some ks3 information. Malicious people can restore the capacity used in the authentication of ks1, ks2, some or all of the ks3.

An attacker only obtained in the following communication channel relevant information, close to the Mifare secret key hack : (1) Uid : the Unique ID of Mifare Tag. (2) nT : the authentication challenge sending from Mifare Tag. (3) {nR} : the authentication challenge sending from Mifare Reader. (4) {aR} : the authentication response sending from Mifare Reader. (5) {aT} : the authentication response sending from Mifare Tag.

Authentication mechanism based on the original standard protocol Tag sent Reader authentication stage of the response $suc^2(nT)\oplus$ks2, as long as the use of retrieval to obtain the plaintext *nT*, after $prng^2(nT)$ of the operation, you can get ks2. With the same operations, it is available of ks3. If an attacker can legally between Tag and Reader to retrieve the authentication of a successful communication, then the attacker can specify the relationship between ciphertext on, informed ks2, ks3. With ks2, ks3 to be anti back to verify the introduction of state; back to the introduction of the target state, can roll back to the initial KEY, Mifare system is used by 48-bit secret key.

The authentication mechanism between Mifare Classic RFID Tag and Mifare RFID Reader identity, as shown below, is the use of international standard ISO9798-2 mutual authentication mechanism, but the small magnitude of the improvement. The RFID anti-collision process has been completed before identity authentication. The reader already has the tag ID (uid). Start the identity authentication process, electronic tags should produce a random number of nonce nT when questioning the value of Challenge to give the reader; Then, the common key K, uid⊕nT and nR, the random number of readers have, concatenation to send the keystream generated from LFSR. The LFSR by the (K, uid⊕nT) generated keystream ks1, and then generate the keystream ks2 with nR. With ks1 encryption nR, nT derivative, $suc^2(nT)$, with the number of encryption ks2, must respond to the value, nR⊕ks1 and $suc^2(nT)\oplus$ks2, back to the electronic tags. Tags receive a response value, the use of (K, uid⊕nT) generated decryption keystream ks1 was nR, nR even then have ks2 decryption sequence was $suc^2(nT)$; electronic tag authentication confirmation $suc^2(nT)$ to confirm the identity of the reader. If accurate, electronic tags and then

produced on the keystream ks3 XOR *suc²(nT)* derived *suc³(nT)* encryption, authentication back to the reader to complete the mutual authentication process.

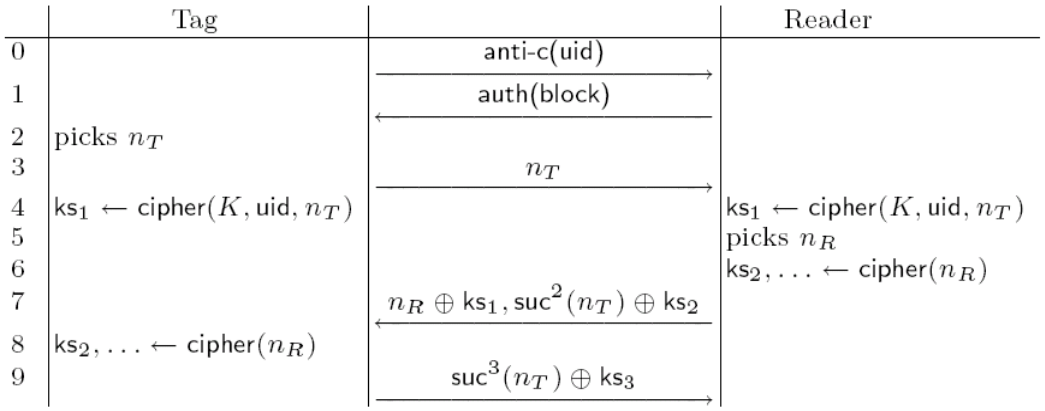


Figure 3. Parameters for CRYPTO–1 Cipher [8]

From the above, we can see Mifare Classic RFID system is not directly on the random number nT encryption, but will not open after the first nT through *suc²( )* operation before the encryption. Message *suc²(nT)*⊕ks2 cannot be directly derived by keystream ks2, should be more secure. But *suc²( )* as a linear function, and has been discovered through reverse engineering analysis, so *suc²( )* has been known. It can be deduced, this is the crack point of Mifare Classic system.

## 4. PROPOSED SECURED RFID MUTUAL AUTHENTICATION SCHEME

In this section we briefly describe Mifare-like authentication protocol. The protocol has two improvement benefits and is illustrated in Figure 5. Two implementations are considered, one using a Timestamp, the other the delay effect. One is the the defence for existence of relations between plain-ciphertext pairs, and the other one is the defence for an inappropriate use opportunity of nR (, the improper use of time). Both have a small footprint and low-cost characteristics, well within Mifare constraints for tags with read-write capability. We conclude by discussing the need for a modular security approach with RFID technology that will support off-the-shelf applications, and the need for making RFID technology resistant to side-channel attacks.

### 4.1. The main defences

For such improvements of those disadvantages, we proposed following idea of the complete program. There are two defences.

#### 4.1.1. The defence for existence of relations between plain-ciphertext pairs

The parameters used for verification which was only by the express delivery of nT for the derivatives as a random number seed is indeed a dangerous way! Mifare system clear view of the existence of the lack of plain-ciphertext pairs, we proposed defence mechanism with considerations of hidden explicit. We act as the random challenge encrypted. The attacker gets out keystream based on the fail. The following description of the practice:

Refer to Figure 2, Mifare authentication protocol, we first explain that the keystream generated ks0 by cipher(K,Uid) which used to encrypt the plaintext challenge nT. Taking into account the

value of K is given, Uid for the fixed value, the type arising out of ks0 constant. There will be security concerns. People can eliminate the value of ks0. Because the attacker encrypts the challenge made by the two mutually exclusive or operation. So we will timestamp features into key generation parameters, in order to confuse the key characteristics of streaming ks0 value.

Control 3-pass authentication process steps, Mifare Reader do the initial process sending time stamp TS to disrupt ks0, which we used to encrypt the previous plaintext message, random number nT, here. When Tag sends encrypted random number nT, denoted as {nT}, it is the equivalent of challenge1 gave Mifare Reader. Mifare Reader receives and decrypts it, use this decrypted random number nT for the second round seed derivatives, denoted as aR. Then reader encrypted aR as response1, denoted as {aR}, back to the Mifare Tag. Mifare Tag verifies this response1 to authenticate Mifare Reader. This is a one-way authentication from Tag to Reader.

Mifare Reader get {nR} to the Mifare Tag, as challenge2. If Mifare Tag can decrypt the ciphertext {nR}, get nR, Mifare Tag encrypted using the random number seed nT for the third round of derivatives with secret parameter nR, denoted as aT, as response2 back to the Mifare Reader. Mifare Reader will verify this response2 to authenticate Mifare Tag. Reader completed the one-way on the Tag authentication; thus complete the mutual authentication.

This scheme which changes the timing of the use of cipher encryption parameters will be encrypted previous plaintext random number and then send {nT}. The verify basis nT derivatives were protected. Even if scheme procedures are public, plain-ciphertext pairs would not exist.

### 4.1.2. The defence for inappropriate use opportunity of nR

Agreement on the standard operation of the authentication mechanism, if attackers can retrieve the identification of a successful communication between Tag and Reader, then they can get information ks2 and ks3, depend on (a.) the relationship of plain-ciphertext pairs. With informed ks2 and ks3, attackers can verify and reverse back to the possible cipher internal secret states. Correct target states can be released. Although there is a secret parameter nR used to encrypt transmissions to prevent successful rollback, but the designers did not consider of the detailed bit-operation sequence characteristics. Therefore attacks who can take advantage of (b.) the existing timing lack of nR improper usage, through the attack sequence of circuit techniques to obtain disclosure of information operations nR. Attackers can still roll back to the initial secret KEY.

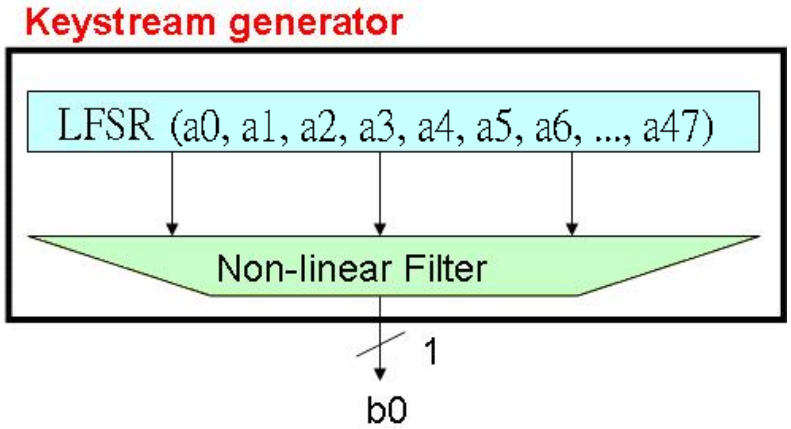

Figure 4. CRYPTO–1 LFSR-based keystream generator

Firstly, simplify the CRYPTO-1 LFSR-besed keystream generator of Figure 4, which shows the internal structure of Mifare. The 48-bit LFSR by the non-linear filter generate a keystream bit at each time slot. Each time slot delivery time shift sequence is corresponding to each plaintext input bit, each parameter bit of states, each keystream bit, each ciphertext bit from plaintext bit by bit XOR keystream and each internal state bit. Here the internal states referred to is that the above keystream generator LFSR states, size of 48-bit. Like sliding window LFSR slide on the way in the internal states bit transitive forward.

According to sequential characteristics of the circuit operation, the time slot shift easily pushed export delivery nR message leakage, when the Tag receives each nR bit immediately use the next bit encryption parameters. The sequential circuit operation although explore the diversity of the Reader ks, but also makes the information secret parameters too concentrated. We could let the parameter nR with a delay to the next unit of time, which is the next round. After 32 clocks, then it is equivalent to the operation of the parallel word units. The recovery of nR will be complex and difficult to achieve. The the time cost of ks pushed back operation pay is 9.44μs * 32 = 0.3 ms.

## 4.2. The Improvement Mifare-like Protection Scheme

For improvements of the two disadvantages, we proposed following idea of the complete program. Mifare Tag sending timestamp TS, equivalent to the Initial steps for the preliminary work, involved the generated keystream ks1 and ks2 which used to encrypt in the following steps. The purpose of TS parameter is used to disrupt the fixed cycle characteristics of keystream generating in the initial cold boot. Reader then sends encrypted random number nR using ks1, denoted as {nR}. Tag sends encrypted random number nT using ks2, denoted as {nT}. At this stage each of the two parties throws challenges to each other. And then while taking advantage of nR and nT used to encrypt the following steps involved in generating the keystreams ks3 and ks4. If both sides can decrypt getting solutions, each with the other party's secret, from another point of view, it is equivalent to key exchange (key agreement) of secret parameters of the operating mechanism.

Mifare Reader nT for the use of random number seed derivatives of the first round, which is ackR, ks3 encrypted by a {ackR}, as response1 back to the Mifare Tag. Mifare Tag verify this response1 to authenticate Mifare Reader, completed Tag to Reader's authentication. Mifare Tag encrypted nT seed the random number for the derivatives of the second round using nR and nT, which is ackT, encrypted by ks4 a {ackT}, as response2 back to the Mifare Reader. Mifare Reader then verifies this response2 to authenticate Mifare Tag, Reader completed a one-way on the Tag authentication. This completes the mutual-way authentication.

The program changes the timing of the use of cipher encryption parameters. Even though Mifare architecture was exposed, plain-cipher text pairs would not exist. The complete concept of the security scheme is nT based on a random number of unknown and uncertain characteristics, as well as the secret parameters of the pseudo random numbers using timed operation.

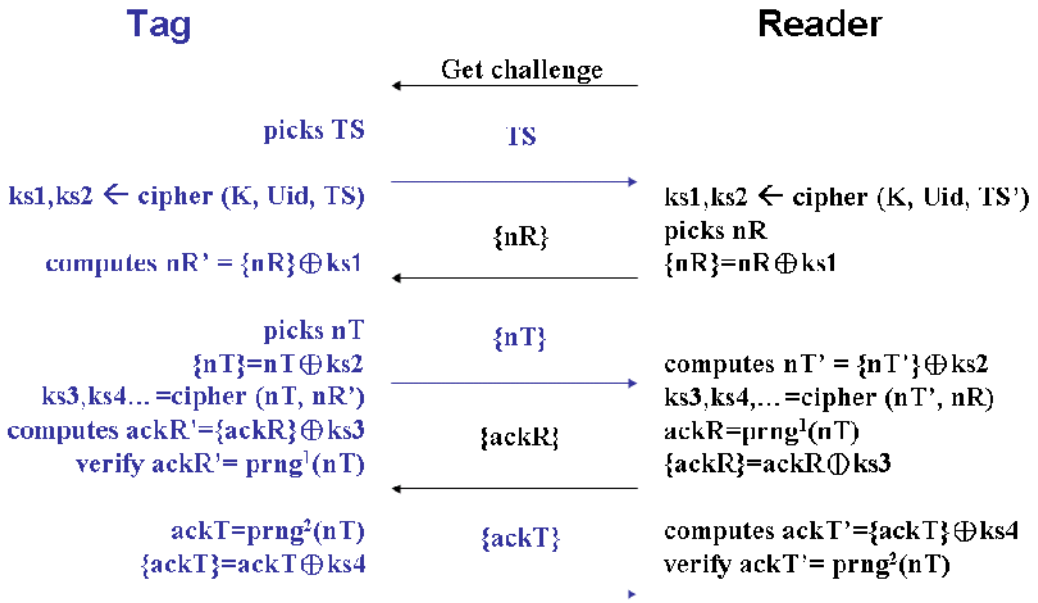


Figure 5. The Proposed Mifare-like Enhanced Authentication Scheme

Declared for the current density of the attack broke Mifare, which can be divided into online and offline attacks against the two major categories. Online attacks using wireless transmission, to eavesdropping (sniffing), collecting the normal transmission between tag and reader as identification information, to extract the data required to achieve key crack, counterfeiting identity, ... such purposes. Off-line attack is based on non-legitimate reader equipment, that repeat the verification Mifare tag to get a specific response in order to make the necessary compared with trial and error to achieve the purpose of cracking the key.

Between tags and readers based authentication protocol that can be exploited by malicious people use public transport message to get the keystreams. Repeatedly used to obtain the key stream operations to be open on the encryption mechanism CRYPTO - 1 reverse authentication, then the state of LFSR can be obtained. Besides, people just need to eavesdrop or malicious the communication information between Mifare card and the reader to be collected, it can be crack to find the available keystream between tags and readers. It would be able to fake legitimate after the Mifare card reader for reading, writing and copying and other activities.

We produce timestamp features into key generation parameters. The timestamp operation of this mechanism need not be protected, just as not to disrupt the fixed keystream characteristics with the purpose of valuation. Originally used to be as plaintext and cleartext pairs on the attack nT, caused by the keystream ks2 encryption, so no direct access to the known association specified characteristics of the known ciphertext. Current [5][6] against failure.

After the amendment protection strategy nR, the attacker can not easily get the nR from plaintext-ciphertest pairs. That can not be easily pushed back to the 48-bit secret key. That is the attacker trying to crack the ciphertext on the relationship between nT clear whether there is or not feasible under violent attack, the attacker even more difficult to calculate 2^32 complexity of the trial and error levels. Such [5][6][7][8] against failure.

## 5. PROPOSED SECURED RFID MUTUAL AUTHENTICATION SCHEME IN UBIQUITOUS

After the protection scheme design, we proposed a general case Secured RFID Mutual Authentication Scheme Based on Fast Stream Cipher.

International standard ISO9798-2 two-way (mutual) identity authentication mechanism, as shown below, in addition to B of A for questioning actions by authenticated response (step 1 and step 2) outside, A is also for cross-examination of the B response to actions by authenticated (step 2 and step 3).

1. A← B: rB

2. A→ B: EK(rA, rB, B*)

3. A← B: EK(rA, rB)

If the Challenge-Response Authentication of the cryptographic operations is the use of streaming encryption algorithms, the encryption key stream flow (keystream) K[n] is can be easily derived, and let the identity authentication mechanism more extra security concerns. For example, if the ISO 9798-2 identity authentication mechanism using streaming encryption, then the one-way authentication, and EK(rB, B) = K1[n] ⊕ (rB, B)[n]; mutual authentication, and EK(rA, rB, B) = K2[n] ⊕ (rA, rB, B)[n]. Therefore the attacker from the code to the rB and B of the ID, can be introduced (rB, B) corresponding to the keystream block K1[n] or K2[n]. This phenomenon of the use of strong secure stream cipher strength is still not a big problem, but weaker on the use of secure stream cipher strength of the limited resources of devices such as RFID, the attacker could launch by the flow of key K[n], then A and B for further derived the common secret parameters, stream cipher key KAB, so the identity authentication mechanism which is triggered to crack the big problem.

Here we provide a method for verifying identity, which can improve the functional deficiency for verifying host. When a second host receives a challenge value transferred from a first host, the second host obtains a secret identify value through an operating function according to the challenge value and a secret parameter. And the second host generates a response value by encrypting the secret identify value, and sends the response value to the first host, such that the first host verifies the identity of the second host according to the response value. Similarly, the second host could verify the identity of the first host. In the present invention, because the secret parameter and the public operating function are used in coordination, plaintext-ciphertext pairs can’t be calculated from the challenge value and the response value under the unknown secret parameter. Accordingly, the known plaintext attack will be prevented.

### 5.1. Way to implement this technology

The mechanisms of the technology for streaming encryption algorithms using the limited resources of devices such as RFID, the Challenge-Response authentication mechanisms defensible streamcipher keystream is easily derived, so that limited resources can more layer of protection to guard against known plaintext attacks. The mechanism techniques to one-way authentication between A and B, for example, the following shows:

1. A← B: rB1

2. A→ B: EK(rB2, B*)

The design of the technology is the challenge value C and response R with the C=rB1, R=K1⊕ rB2, rB1≠rB2, and rB1 and rB2 do not derive the relationship between each other. This resolve the challenge-response by streaming encryption algorithms respond to the authentication mechanism secret key projections of the shortcomings of current easily.

**5.2. Four embodiments to implement this technology**

In order to achieve value C and response value R satisfy the conditions of the technology, there are several embodiments:

(A) rB1 for the A and B there are the pre-shared secret parameters of the operation K on rB results, rB2 for the random number:

For example, rB =f(K, rB), rB is random; rB2=rB; A and B have a pre-shared secret parameter K. A receipt rB1 can be calculated $rB=f^{-1}(K, rB1)$, where f() as a function of inverse function of the cryptographic operations. Therefore, Challenge-Response authentication mechanism can be

1. A← B: f(K, rB)

2. A→ B: EK(rB, B*)

(B) rB2 for the A and B the operation of K on the rB results, and rB1 for the random number:

For example, rB1=rB; rB2=f(K,rB), rB is random; A and B have a pre-secret secret parameter K. A receipt rB can be calculated rB2=f(K,rB), where f() for the cryptographic operations functions. Therefore, the authentication mechanism can respond to

1. A← B: rB

2. A→ B: EK(f(K, rB), B*)

(C) rB1 order with time stamp T and pre-shared secret K of the operation result of rB, and even rB2 is the order of T and rB:

For example, rB1=T,f(K, rB), rB is random; rB2=rB; A and B have a pre-shared secret parameter K. A receipt rB1 cut out T, f(K, rB), can be calculated $rB=f^{-1}(K, f(K, rB))$. Therefore, the authentication mechanism can respond to

1. A← B: T, f(K, rB)

2. A→ B: EK(T, rB, B*)

(D) rB2 order with time stamp T and pre-shared secret K of the operation result of rB, and rB1 sequence with T and rB:

For example, rB1=T,rB; rB2=T,f(K,rB), rB is random; A and B have a pre-shared secret parameter K. A received T,rB can be calculated rB2=T,f(K,rB), where f() for the cryptographic operations functions. Therefore, the authentication mechanism can respond to

1. A← B: T, rB

2. A→ B: EK(T, f(K, rB) B*)

## 6. CONCLUSIONS

In recent RFID systems, it is still possible to get both reader and tag messages in one capture. To analyse unknown RFID protocols it is very convenient to get a full trace of the transaction [12][13][14][15]. This feature was of great use to retrieve the keystream from one authentication session to construct the optimized table attack exploiting linear combinations.

We introduce security mechanisms appropriate to defeat RFID authentication attacks, and show how a recently proposed RFID authentication protocol uses them to achieve security. This technique does not have to import any additional secret parameters. Solely by readers and electronic tags read and write the secret parameters of the use of time between changes without any new pre-shared secret parameters. People can make plaintext-ciphertext derivation relationship does not exist, to achieve improved security identification. The secret of having an additional parameter in the standard, just reading and writing machine and the electronic tag through the secret parameters of the use of time between changes, no new pre-share the secret parameters, you can make plaintext, ciphertext Derivation of relationship does not exist, to achieve improved security identification. It provides low-resource hardware implementation of a common solution for multi-mode. It is proper to ubiquitous computing devices such as a sensor mote or an RFID tag.

## REFERENCES


[1] International Organization for Standardization. ISO/IEC 9798-2: Information Technology - Security techniques — Entity Authentication Mechanisms Part 2: Entity authentication us-ing symmetric techniques. ISO/IEC, 1993

[2] M. Burmester, T. van Le, and B. de Medeiros, (2006) “Provably secure ubiquitous systems: Universally composable RFID authentication protocols,” *Proc. of the 2nd IEEE/CreateNet International Conference on Security and Privacy in Communication Networks (SECURECOMM 2006)*, pp.1–9.

[3] Philips Semiconductors, Mifare Standard Card IC MF1 IC S50 Functional Specification, July 1998 / May 2001

[4] CRYPTO–1 Cipher [Online].Available: http://en.wikipedia.org/wiki/MIFARE

[5] Flavio D. Garcia, Gerhard de Koning Gans, Ruben Muijrers, Peter van Rossum, Roel Verdult, Ronny Wichers Schreur, and Bart Jacobs, (2008) “Dismantling MIFARE Classic,” SpringerVerlag *Lecture Notes in Computer Science (LNCS)*, Vol. 5283, pp.97–114.

[6] Karsten Nohl and Henryk Pl¨otz. Mifare, (2007) “Little Security, Despite Obscurity,” Presentation on the 24th Congress of the Chaos Computer Club in Berlin.

[7] Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia, (2008) “A practical attack on the MIFARE Classic,” *Proc. of the 8th Smart Card Research and Advanced Applica-tion Workshop (CARDIS 2008), LNCS*, Vol. 5189, pp.267–282.

[8] Flavio D. Garcia, Peter van Rossum, Roel Verdult and Ronny Wichers Schreur, (2009) "Wirelessly Pickpocketing a Mifare Classic Card," *Proc. of 30th IEEE Symposium on Security and Privacy (S&P 2009)*, pp.3–15.

[9] R. Ryan, Z. Anderson and A. Chiesa. Anatomy of a Subway Hack [Online].Available: http://web.mit.edu/zacka/www/subway/

[10] Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer, (2004) " Strong authentication for RFID systems using the AES algorithm," SpringerVerlag *Proc. of the Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004), Lecture Notes in Computer Science (LNCS),* Vol. 3156, pp. 357–370.

[11] Flavio D. Garcia, Gerhard de Koning Gans, and Roel Verdult, (2012) "Tutorial: Proxmark, the swiss army knife for RFID security research," Technical report, Radboud University Nijmegen.

[12] Benedikt Driessen, Ralf Hund, Carsten Willems, Carsten Paar, and Thorsten Holz, (2012) "Don't trust satellite phones: A security analysis of two satphone standards," *Proc. 33rd IEEE Symposium on Security and Privacy (S&P 2012)*, pp.128–142.

[13] Flavio D. Garcia, Gerhard de Koning Gans, Roel Verdult, and Milosch Meriac, (2012) "Dismantling iClass and iClass Elite," SpringerVerlag *Proc. 17th European Symposium on Research in Computer Security (ESORICS 2012)*, Lecture Notes in Computer Science.

[14] Arjan Blom, Gerhard de Koning Gans, Erik Poll, Joeri de Ruiter, and Roel Verdult, (2012) "Designed to fail: A USB-connected reader for online banking," SpringerVerlag *Proc. 17th Nordic Conference on Secure IT Systems (NordSec 2012)*, Lecture Notes in Computer Science.

[15] Josep Balasch, Benedikt Gierlichs, Roel Verdult, Lejla Batina, and Ingrid Verbauwhede, (2012) "Power analysis of Atmel CryptoMemory - recovering keys from secure EEPROMs," SpringerVerlag *Proc. 12th Cryptographers' Track at the RSA Conference (CT-RSA2012), Lecture Notes in Computer Science (LNCS)*, Vol. 7178, pp.19–34.

[16] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone (1996). *Handbook of Applied Cryptography*. CRC Press. ISBN 0-8493-8523-7.

**Authors**

**Mr. Kuo-Tsang Huang** received B.Sc. from Chung Hua University in 2001 and M.Sc. from Aletheia University in 2003. He is currently studying for the Ph.D. degree in Department of Electrical Engineering of Chang Gung University, Taiwan. He is a member of the International Collaboration for Advancing Security Technology (iCAST). His research interests include wireless network, information security, cryptography, computer architecture issues and technology.

**Dr. Jung-Hui Chiu** received B.S.E.E. from Tatung University in 1971, M.S.E.E. in signal processing and Ph.D. in communication from National Taiwan University in 1973 and 1986 respectively. From 1975 to 1981, he was a research staff with Chunghwa Telecom Labs where he was involved in the research of fiber communications and the microwave systems. During 1981–1986, he was an institutor for the Electronic Department, National Taiwan University of Science and Technology, and was associate professor from 1986 to 2003. He is currently an associate professor in the Department of Electrical Engineering of Chang Gung University, Taiwan. He is a member of IEEE Communications Society, the Chinese Cryptology and Information Security Association (CCISA), and the International Collaboration for Advancing Security Technology (iCAST). His research interests include digital communication systems, wireless communication systems, information security, RFID, hardware security, smart card, and cryptography.