Research of RFID Certification Security Protocol based on Hash Function and DES Algorithm

Xu bin, ZHANG li-hui, and TAN Xiao-pin
Jianghan University Physics and Information Engineering Institute, Hubei, China
Email: xubinls@163.com

Abstract—RFID has been more and more attention and application by people, but the existence of security and privacy problems worthy of attention is concern. The certification process analysis of several typical security protocols is based on existing RFID authentication protocol. It proposed an improved bidirectional authentication algorithm. The use of one-way HASH function can solve the security problem of RFID. The protocol has anti-replay, impedance analysis, forgery, and tracking performance, and is suitable for the distributed system. With the development of computer and Internet is widely used in various industries, interaction of high-speed information transfer process. The problem of information security is concern. The paper produce and use all kinds of algorithms based on hash function firstly. Then as information on a solid safety lock, MD5, SHA-1 file verification, encryption, digital signature, PKI building has security full of all kinds of information. Finally, it can effectively prevent the attack, ensuring the authenticity of the information not to be modified or leaks.

Index Terms—RFID, Security Protocol, Hash Function, Rabin Algorithm

I. INTRODUCTION

RFID security technology refers to the label with limited hardware resources to achieve security mechanism, effective and practical with certain strength. The security mechanism of RFID is used mainly include physical method and security routing protocol based on password mechanism. Among them, the physical methods include kill tag and Faraday cage and Active jamming and Blocker tag to prevent labels. Compared with physical method and security protocol is based on password mechanism more attention. Security protocol is the communication between both sides of the identity authentication, data encryption, digital signature and other functions using the password mechanism [1]. Should the cost from the security requirement, system factors in the practical application of RFID, consider the protocol complexity, using the RFID security protocol is suitable.

RFID security protocol at present can be divided into: security protocol, Hash security protocol based on symmetric functions based on cryptography and security protocol asymmetric cryptography mechanism [2]. The security of security protocols based on Hash function is constructed based on one-way Hash function [3]. Secure security protocol based on symmetric cipher mechanism generally used DES, AES encryption method to protect RFID [4]. Security protocol based on asymmetric cryptography using elliptic curve cryptography (ECC) mechanism and McElieic password mechanism [5].

The proposed security protocol is based on Hash function of Hash-Lock protocol, chain protocol, Chains protocol, Triggered Hash. But these protocols have many security vulnerabilities or flaws, but also in areas where improvement is needed in the implementation of efficiency, tag protocol cost [6]. Elliptic curve cryptography is an excellent asymmetric cryptography. Its security is the elliptic curve discrete logarithm problem (EDLP) which based on the very high safety. But the traditional security protocol based on elliptic curve is not applicable to RFID system. Therefore need to take full account of the actual situation of the RFID system. They are proposed for RFID system security protocol based on elliptic curve cryptography [7]. In addition, it also made certain progress in the study of elliptic curve cryptography processor for RFID tag chip. All this shows that the elliptic curve cryptography mechanism will play an important role in the protection of RFID system [8].

Aiming at the security and privacy problems in RFID technology are studied deeply. It based on the analysis of the existing literature relevant to the algorithm of security protocols, and related to the improved. In the RFID algorithm, proposed an improved binary tree algorithm.

In the RFID algorithm, proposed an improved binary tree algorithm. In the RFID security protocol, it proposed the improvement based on the RFID security protocol of Hash function and Rabin algorithm.

II. RFID COMMUNICATION SYSTEM

This part briefly introduces the basic structure of RFID system, communication model and basic security requirements. The RFID system is generally composed of three parts: RFID tag (Tagore transponder), RFID card reader (reader or transceiver) and the back-end database (server).

The RFID tag is composed of wireless communication for the coupling coil circuit and computing, data storage logic gate circuit. It can be divided into active and passive tag two in accordance with the tag energy source. Active tags are powered by a fringe on the label of the battery. It has a far distance of data transmission. Passive tags by
coil coupling energy are data transmission distance, low
cost, permanent life cycle etc.

The reader by the wireless transceiver module, antenna,
control module and interface circuit, has the ability to
read, write tag. When a query commands and receives the
returned tag information, the reader will send information
to the back-end database. The back-end database is the
database system can run on any hardware platform.
Usually it has data analysis and storage capabilities,
contains the entire data information card.

RFID system generally consists of electronic label
(Tag), reading and writing (Read - er) and the back-end
Database (Database) of three parts, as shown in figure 1.
Electronic tag is the carrier of goods identification, it
consists of antenna, rf circuit, memory and the
composition of digital circuit. Electronic tag compared
with the traditional bar code technology's biggest
advantage is that the data can be repeatedly wiped, thus
can realize reuse. Is read/write device with a wireless
transmitting and receiving antenna devices, used to read
labels carry information in the label and write data. Back-
end database stored in the tag and to read and write all the
information, through the realization of mutual
communication and reading and writing of the entire
RFID system operation management.

Figure 1. RFID System organization

The ISO/IEC 18000 standard defines the
communication model of RFID, a total of 3 layers:
application layer, communication layer and physical layer.
For solving the most directly related to the application
and content, including authentication, identification and
representation, the application layer data processing logic.
Under normal circumstances is the application layer
protocol RFID protocol. The definition of the RFID read
and write are a means of communication between reader
and tag. Anti-collision protocols belong to this layer,
mainly to solve the multiple tags at the same time and a
reader communication conflict.

Defines the air interface physics, including the
problem of frequency, the physical carrier, data coding,
time-sharing. RFID technique does not contact, not
visible, signal broadcast features brought huge space to
the attacker. In addition, RFID equipment (mainly tags)
the requirement of low cost makes them with very limited
computing resources. Generally speaking, low cost RFID
tags contain 5000~10000 gate circuit, can be used for
security mechanism is the 400~4000 gate. All of these
features and limitations are put forward special
requirements for design of the security mechanism of
RFID system. Therefore the design of safety, high
efficiency and low cost RFID protocol has become a new
subject with challenge.

RFID Tag has some limitations, such as limited
computing ability, limited storage space (storage space in
the RFID tag is extremely limited, the cheapest Tag only
64~128bit ROM, which can only contain a unique
identifier). The appearance is very small. The power
supply is limited. All of these features and limitations of
the security mechanism of RFID system design poses
special requirements, also enables designers to select
password mechanism has many restrictions.

In RFID system, reverse channel and forward channel
are wireless channel occupancy. It can be said to be
exposed. So it is easy to receive the malicious attack and
destruction. The security problems are faced by a RFID
system.

After the attacker fake reader response to record label,
with the response to respond to legitimate reader makes
the legitimate reader still think that the true label is still
an attacker. But in fact the label has changed. Generally
speaking, the main way to solve the problem of
counterfeit attack is to perform authentication and data
encryption.

The effective signal by an attacker to intercept the read
and write are communication between the device and the
label. After an attack on the system of retransmission and
the effective signal is RFID system. To solve the replay
attack problems requires a response mechanism,
mechanism of timing and counting are often used to resist
re-transmission attack.

Two kinds of attack is different from the front tracking
is a threat to human security problem. The attacker
through the response information is track label. Therefore,
a RFID system should satisfy: indiscernibility and
forward security (forward security). Indiscernibility is
included in the ID Anonymous (anonymity) is a concept,
means a issued by a label information with other label
information can not be resolved, which is unrelated to ID.
Forward security is that if an attacker gets the label
previously issued information so the attacker, using the
previously obtained information can not determine the
label. Generally speaking, the random characteristic and
the random number Hash function is used to solve this
kind of problems.

Resynchronization refers to the label and the backstage
database stored information inconsistency leads to a
threat of tag failure. The reader has read and write two
operation on the label, RFID applications in the reality.
The write operation is the main content of the label ID.
The attacker to write operations (such as ID) strike and
bring to synchronization problems. Eavesdropping
(eavesdropping) in between reader and tags are wireless
communication. The attacker can to read written
communication between effective signal and label, which
act to strengthen the attack. Such as retransmission or
counterfeit attack; session hijacking (session
hijacking/interception) of the attack is the man in the
middle attack (man-in-the-middle attack) is a concrete
expression of the main threat to form. It brings is the
application layer to the synchronization problem. So can
resist the impersonation attack, replay attack, tracking and synchronization and other security threats are commonly used as an evaluation of application layer security index.

With the wide application of RFID technology, researchers have recognized its security problems. Researchers are trying to find a more effective, more economical to solve the problem of system security. There have been many RFID security protocol is presented, the following brief introduction of its. The Hash-Lock protocol is RFID security protocol proposed by Sarma et al. Label the initial is locked. The label storage value and metaID, replace the real one, metaID=Hash (key); key key, back-end database to store each label metaID, ID. The deal initially solved the privacy preserving access control, but the metaID remained unchanged. But also by no security channel to transmit to clear the way, vulnerable to the replay attack and spoof attack, does not have the indiscernibility, attackers easily on the label tracking. Randomized Hash-Lock protocol is an improved form of Hash-Lock protocol. Label in Hash function, also embedded in a pseudo-random number generator, back-end database stores all of the ID tags.

The protocol uses the random number to solve the location privacy problem label. But the label has integrated the pseudo random number generator, difficult to achieve in low cost and limited computing power of the case. At the same time the label still fail to respond to the retransmission and spoof attack. In addition, the traffic volume back-end database and the card reader is larger, the reader needs to find out the corresponding tag identification from all the ID logo, increase the read operation card reader. Therefore, it is still not practical.

The use of two different Hash function is Hash chain protocol. Dynamic constantly in the process of authentication refresh tag can be authentication using ID. The agreement because of the dynamic tag ID update mechanism, it has strong resistance to guess the impedance analysis. However, one of its important vulnerability lies in his strong security is only one-way authentication. That is to say, tag cannot effectively distinguish authenticity if the attacker masquerades as a legitimate reader. At the same time, computation of database is very large: if there is an N label, is the backstage database to N search, 2N Hash calculations, and N comparisons. So the protocol is not suitable for large amounts of label. Finally, the dynamic updating system and system synchronization attacks and affect the normal certification process.

III. THE RFID SYSTEM COMPOSITION AND PROTOCOL ANALYSIS

In the EPCglobal Class 1 Generation 2 in the agreement, read and write the selection is using Inventory. Access the three basic operations management TAB groups. At the same time label according to the operation of the reader is Ready and arbitration response, confirmed. Open and protection, killing seven state, as shown in figure 3.

There is several security problems in the EPC agreement from the tag to read the information transmitted in plaintext. It wills easily into the surrounding the attacker leak information saved in the tags. Speaking, reading and writing in the label they have been used to write a handle an RN and data to be written or after delivery. So that to avoid the plaintext transfer, but the attacker can easily intercept as imperative sentence handle an RN. And analyze the information to be written to the tag, or even pretend to be legitimate, speaking, reading and writing to label any tampering with the data.

RFID security mechanism research is based on the research of the password techniques. It has put forward a variety of security protocols. Such as Hash - Lock protocol, randomized Hash - Lock protocol, distributed RFID asked a response authentication protocol, etc. Some of these methods to make up for RFID protocol security vulnerabilities, to a certain extent, improve the system security. But there are still significant security vulnerabilities. In Hash - Lock protocol there are label ID in plaintext transfer, the attacker can easily get the fake ID, and easy for tracking label.
To solve above problems, the read-write device and label of mutual authentication mechanism, joined the read and write device in the process of system certification certification for label, prevent illegal read/write device by attacking label information or unauthorized read/write device tracking label. Joined the cipher text information in the tabs at the same time, through the digital signature technology to protect the secret information in the label is not illegal to read. Label and the mutual authentication between reading and writing process as shown in figure 4.

In the process of the above certification that is Encrypt as encryption function. There are many good encryption algorithms such as ECC, RSA and AES, etc. But these algorithms resource overhead is too big, not suitable for low-cost RFID tags in the circuit. And DES algorithm is designed for the realization of hardware circuit, the encryption speed, and good security; from produce to now still have a wide range of applications. This system USES an improved DES algorithm, is suitable for the RFID system. Legibility of labels certification process is as follows:

1. to read and write device after certification by tag ID (Ti) is encrypted, and the cipher text Encrypt (RN), Ti) transfer to, speaking, reading and writing.
2. after the read/write device receives the request signal returns a random number RN label.
3. labels will receive a random number with its own ID (Ti) is encrypted, and the cipher text Encrypt (RN), Ti) transfer to, speaking, reading and writing.
4. to read and write the cipher text with an RN, get Ti*, and back to the back-end database.
5. the back-end database to find whether there is the tag ID, if there is a prove that the legal label, label for return confirmation (ACK).
6. to read and write on label after confirm the label for legal label to read and write access or the whole certification process is complete.

DES algorithm is the core of a wheel function, clear data after the initial replacement for 16 times round function of the operation. Finally through an inverse initial permutation get output result. In each round function used in the key Ki is the initial key after replacement. So each round key is different 64 b expressly for input is divided into two parts of the same length, Li, Ri. Then output to the next round of the 64 b data as follows:

\[
L_{i+1} = R_i
R_{i+1} = L_i \oplus P(S(E(R_i) \oplus K_i))
\]

where E means extending the right half of the 32 b data of 48 b, with the key or after 8 S box, each box S receive 6 b input, to produce the output of 4 b. And then through a permutation matrix P, and left again after xor the right half of the data for the next round of function.

Since the S box in the entire algorithm occupies a large area and power consumption, so in this paper the original algorithm to improve the S box, using a single S box instead of the original eight will be extended to 48 b is divided into eight pieces. Through a multi-channel selector in turn by the S box, and then synthesize results into a 32 b number input permutation matrix P (as shown in figure 5). Thus greatly reduce the circuit size, at the same time; due to the decrease of the size the circuit also reduces power consumption, more suitable for RFID tags.

The proposed RFID security system can prevent a variety of means of attack, the mutual authentication mechanism and comparison security of DES algorithm, improved the security of the system.

1. It prevents an attacker eavesdropping. Generally, speaking, reading and writing and channel using wired connection between the back-end databases. It can be considered to be a secure channel, and read/write device channel between tags can be an attacker hacked object. Not safe design, there is no clear transmission channel, so the eavesdropper cannot get useful information.
2. It mutual authentication mechanism to prevent the unauthorized read/write device was carried out on the label, speaking, reading and writing, but also to prevent forgery of label information is read.
3. It prevent replay attack, the attacker intercepts information because every time a request first sends a random number. The attacker even if intercepted, speaking, reading and writing and label data cannot effectively attack in the process of transmission.
4. It adopted based on DES encryption function. The attacker is difficult from the transmission of cipher text data in useful information. Deficiency of the algorithm are the key length is short, but is the structure of the algorithm itself without any defects, crack the algorithm comes with a price and take a long time, so still has a broad application. System for the security requirement is very high considering the longer key, or a variation of DES algorithm (triple DES algorithm).

IV. PROTOCOL ANALYSIS

In this agreement, all private messages are a one-way Hash function encryption through, attackers and listener unable to decrypt the received information from the original data. In the improved protocol, for each encryption operation, add a random number. So the last transmitted messages are random. The addition of R allows the attacker cannot predict and control, so even if the attacker to record the next communication data. Validation cannot playback of the data obtained by either party both sides of communication.
The complexity of the algorithm, the label with a total of 2 times Hash operations in the verification process, 2 XOR operation; the reader need to generate a random number calculation, the backstage database the need for 2 Hash operation. In the algorithm space, tags and database are required to store IDi, MI and Ki of three groups of data.

Table marked the safety performance in the comparison protocol and other protocols. Where X represents not safe and V said security.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Resistance to tracking</td>
<td>X</td>
<td>V</td>
<td>V</td>
<td>V</td>
</tr>
<tr>
<td>Forward security</td>
<td>X</td>
<td>V</td>
<td>V</td>
<td>V</td>
</tr>
<tr>
<td>Replay attack</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>V</td>
</tr>
<tr>
<td>Spoofing attacks</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>V</td>
</tr>
<tr>
<td>Traffic analysis</td>
<td>X</td>
<td>X</td>
<td>V</td>
<td>V</td>
</tr>
<tr>
<td>Distributed environment</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
</tr>
</tbody>
</table>

The table below is a comparison of efficiency, which H said Hash operation, R said the random number generation calculation. In addition, randomness also let the communication data did not follow the law, effectively preventing the data analysis attack. In the two authentication on both sides, with two pairing parameters to verify identity, and used to verify the parameters after Hash one-way encryption, which only had hold the correct parameters to be verified, the attacker cannot forge identity.

<table>
<thead>
<tr>
<th>Protocol name</th>
<th>Calculation amount</th>
<th>Storage space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash-Lock</td>
<td>1H</td>
<td>---</td>
</tr>
<tr>
<td>Random Hash-Lock</td>
<td>1H, 1R</td>
<td>(ΣID/2)H</td>
</tr>
<tr>
<td>Hash chain</td>
<td>2H</td>
<td>---</td>
</tr>
<tr>
<td>Protocol</td>
<td>2H</td>
<td>1R</td>
</tr>
</tbody>
</table>

Miller-Rabin is a very easy and widely used simple algorithm, it Gary part of the Miller imaging method based on Rabin development, Michael. In fact, this is a simplified version of NIST is recommended in DSS recommendation algorithm. More and more people call it the test. Because the Miller-Rabin test does not necessarily is the prime, non prime by testing the probability is 1/4. Using Fermat’s little theorem, for a given integer n, we can design a primarily testing algorithm. Through the calculation of d=2^x (n-1) mod n to determine the integer n primarily. When the D is not equal to 1, n is certainly not the prime; when D is equal to 1, n is very likely to be the prime. But there are also a number of n such that 2^x (n-1) = 1 (MOD n). For example, the minimum number of meet this condition is n=341. In order to improve the accuracy of the test, random selection of the integer 1 Fermat’s little theorem is a necessary condition for primarily testing we can. Integer satisfying Fermat’s little theorem condition is not all prime numbers n. Some number satisfies Fermat’s little theorem conditions. These and the number are called Carmichael number, the first 3 Carmichael number is 5611015729. The Carmichael number is very small. Integer in the range of 1~10000000 only 255 Carmichael number. Use the following two detection theorem can be on the top of the primarily testing algorithm for further improvement, in order to avoid the Carmichael numbers as primes. The two detection theorem if P is a prime number, 0<x<p. Then the equation x^2 = 1 (mod p) solution for x=1, ..., p-1.

The following talk about specific steps of the algorithm, N, is we want to test data:

1. to calculate m, J, makes the n-1=m*2^j, where m is a positive odd number, j is a nonnegative integer.
2. a randomly selected B, 2<=b<=n.
3. Calculation of b^m mod n.
4. if v==1, through testing, return.
5. i=1.
6. if v==n-1, through testing, return.
7. if v==ej, non prime, end.
8. v=v^2 mod n, i=i+1.
9. circular to Step 5.
Finally, a test run results of course not satisfied, running several random testing. So we misjudge probability becomes (1/4) 1/loop), also often go through a small primes showed some screening to improve efficiency.

Hash, generally translated as "hash", also have a direct transliteration is "hash". is of arbitrary length of the input (also called pre mapping, pre-image), through the hash algorithm, transform into output of fixed length, the output is the hash value. This conversion is a contraction mapping. That is, the hash value space is typically much smaller than the input space; different input might hash to the same output. But could not only determine the input value from a hash value. Simple said is a kind of squeezing a message of arbitrary length to a fixed length of the message digest function. HASH is mainly used for the encryption algorithm in the field of information security. He took some of the different length of the information into a sprawling 128 bit code, called the Hash value.

The Hash function is a one-way function special, generally can be divided into two categories: the Hash function without the key and the keyed Hash function. The former contains only one input parameter (message). The latter contains two parameters, the message and the key. The Hash function should have the following properties:

(1) \( H \) can be used for any size of data packets.
(2) \( H \) produce the output length.
(3) For any given \( x \), \( H(x) \) easy to calculate, for software and hardware implementation.
(4) For any given message digest \( y \), looking for \( x \) the calculation \( y = H(x) \) is not feasible.
(5) For any given message \( x \), find \( x' \), that \( x' \neq x \), \( H(x) = H(x') \) in the calculation is not feasible.
(6) The search for arbitrary \( (x, x') \), the calculation \( H(x) = H(x') \) is not feasible.

A chaotic system has the following properties: sensitivity to initial conditions and parameters, scattered and distribution and periodicity. The iterative process of chaotic system is unidirectional. In addition, the network composed of chaotic system not only has the chaotic properties, but also can generate more complex chaotic sequence and partially overcome finite precision problem.

Hash function used in this paper is shown in Figure 2. First of all, will have any length (in bytes) of the message \( P \) is padded with 0, the message length of 4 (bytes) multiples. Then the sequence after filling is divided into different packets \( P_1, P_2, P_3, \ldots, P_n \), each packet length is 4 bytes. The Hash value of the steps is shown as follows:

1. Arbitrarily select initial vector is \( x_0, x_1, x_2, x_3 \), the initial vector to secrecy.
2. Each symbol information can transferred into their corresponding ASCII code. Then through a linear transformation of the ASCII code value is converted into \((0, 1)\) a decimal interval number. Namely, perform the following operation for each message packet \( P_i \) (\( r = 0, 1, 2, \ldots \)) as follows:

\[
P_i = (P_i + 0.8) / 256, \quad i = 0, 1, 2, 3
\]

Then the message packet and the initial vector is mixed according to the following formula:

\[
x_0 \leftarrow (P_i + x_i) \mod 1, \quad i = 0, 1, 2, 3
\]

3. Iterate the piecewise Logistic map. For convenient description, we put the \((i, j)\) is a mapping \( L_{i,j}(x_i) \). Among them as follows:

\[
x_0 = x_j, \quad \mu = [(x_j + x_{i(1,1)}) \mod 1]*0.4 + 3.6.
\]

The output \( L_{i,j}(x_i) \) is \( x_{i(1,1)} \). If \( P_i \) is the last block, \( x_i \) will output feedback \( x_{i(1,1)} \) to give \( x_i \), and go to step 2. The cipher block chain (CBC) all encrypted packet mode makes use of output depends on the initial conditions, the current and previous, this also makes the chaotic system has better scattered and distribution characteristics.

4. Extract the corresponding bits to form the final Hash value.

At the completion of all cipher block after extraction of 32 bits, each output \( x_i \), and recorded as \( h_i (i = 0, 1, 2, 3) \). The final Hash value is \( h = (h_0, h_1, h_2, h_3) \).

Protocol description is as follows:

1. The reader sends a query request at the same time, generate a random number \( R \), and the query request sent.
2. The label \( H (mi+R) \) ki calculation, and send the result to the reader.
3. The reader forward the results to the database, according to the Ki in the database query, such as a query to a ki’=ki, then read out the corresponding M and Di’, and calculate the H (MI’ +R). If the results of H and (mi+R) the same, the label through the verification, because he has the right metalD and key. Otherwise the label is illegal.
4. The database H (IDi’ +R) is calculated and sent to the reader, the reader will be forwarded to the label.
5. The label from the storage read out their own IDi, and the same calculation of H (IDi+R), if H (IDi+R) =H (IDi’ +R), the reader / background database is legitimate, certification is complete. Otherwise the reader is illegal.

The two basic elements of confusion and diffusion of encryption algorithm, this is no exception to the Hash function. If the Hash expression results in binary form, each bit can only be 0 or 1. Therefore, the ideal confusion effect should be when the initial conditions, control parameter or message itself have any slight change of probability of each bit is 50%. Typically, people use the following parameters for statistical analysis.

1. The minimum bit value change:
\[
B_{min} = \min(B_1, B_2, \ldots, B_N)
\]
2. The maximum bit change value:
\[
B_{max} = \max(B_1, B_2, \ldots, B_N)
\]
3. The average bit change value:
\[
B = \frac{1}{N} \sum_{i=1}^{N} B_i
\]
4. The average bit rate:
\[
P = (B / 128) \times 100\%
\]
5. Variance bit variation:
\[ \Delta B = \frac{1}{N-1} \sum_{i=1}^{N} (B_i - \bar{B})^2 \]

(6) The rate of change of mean variance:

\[ \Delta P = \frac{1}{N-1} \sum_{i=1}^{N} (B_i / 128 - P)^2 \times 100\% \]

Among them, \( N \) is the number of experiments, \( B_i \) is a bit change the \( i \) experimental value.

Each experiment the change value 1 bits of the plaintext message, calculating the corresponding Hash function value. Value table III gives the Hash function corresponding to different statistical number value change statistics.

**TABLE III. STATISTICS ANALYSIS OF THE HASH FUNCTION ALGORITHM**

<table>
<thead>
<tr>
<th>( N )</th>
<th>( B_{\max} )</th>
<th>( B_{\min} )</th>
<th>( \bar{B} )</th>
<th>( P(%) )</th>
<th>( \Delta B )</th>
<th>( \Delta P(%) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>256</td>
<td>47</td>
<td>45</td>
<td>63.70</td>
<td>49.77</td>
<td>5.57</td>
<td>4.35</td>
</tr>
<tr>
<td>512</td>
<td>46</td>
<td>82</td>
<td>63.90</td>
<td>49.93</td>
<td>5.74</td>
<td>4.48</td>
</tr>
<tr>
<td>1024</td>
<td>45</td>
<td>82</td>
<td>63.91</td>
<td>49.93</td>
<td>5.62</td>
<td>4.39</td>
</tr>
<tr>
<td>2048</td>
<td>45</td>
<td>82</td>
<td>63.82</td>
<td>49.86</td>
<td>5.59</td>
<td>4.37</td>
</tr>
</tbody>
</table>

We can see small change of plaintext message sequence algorithm corresponds to 1 bit from table 1, the average bit Hash function to calculate the value change value is very close to 64, the average change probability is close to 50%, the effect is ideal. This allows an attacker cans not forge or some known plaintext message out other. In addition, two variance changes are small, illustrate the confusion and diffusion properties of the algorithm to the plaintext message is relatively stable. The experimental results show that, the huge change message any small change will cause the Hash to the Hash function, this is due to the high sensitivity to initial value. This property to resist differential attack plays an important role in.

This design mainly aimed to reduce the chip area, in the original DES encryption algorithm based on improved, with Synopsys company tool DesignCompiler improved the performance of the system is analyzed, comprehensive using the Stoic library 0. 18 mu m process, performance comparisons are shown in table 4.

**TABLE IV. DES ALGORITHM PERFORMANCE ANALYSIS**

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>AREA</th>
<th>POWER</th>
<th>DYNAMIC</th>
<th>STATIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES</td>
<td>26468</td>
<td>1.844 mW</td>
<td>1.047 µ W</td>
<td></td>
</tr>
<tr>
<td>Improved DES</td>
<td>20284</td>
<td>2.215 mW</td>
<td>886.1 nW</td>
<td></td>
</tr>
</tbody>
</table>

Here, we need to make some description of the algorithm. First of all, the reason why each packet length divided into 4 byte is because most of the computer is 32 bits, so convenient for computer processing. Of course, if the 64 computer can be divided into 8 byte packet length, but the network structure of the algorithm is to adjust for 32 chaotic maps. Secondly, because the Hash structure 128 in some cases which do not conform to safety needs, so it can be selected according to requirements in Hash results from 256 or more Hash results, in order to enhance its security. Finally, each wheel algorithm to update the initial values \( x_i \) and parameters \( \mu \), this is to ensure that the Hash sequence has better confusion and dispersion characteristics. In order to prevent the differential analysis attack or statistics, if you simply just to update \( x_i \), then the Hash value change is not obvious results. That is to say the confusion and dispersion effect is poor, which affects the security of the algorithm.

**VI. CONCLUSIONS**

The method in the safety, reliability, robustness is relative to the existing protocols have different degrees of improvement and perfection. At the same time, a small amount of computing, storage demand is not large, high efficiency, very suitable for RFID system with low cost, and can be used in distributed database system scale. It has high practical value. Hash algorithm has long been in a large number of applications in computer science, computer security; network security has outstanding contribution, along with the development of modern cryptography. One-way hash function has become an important structure of the module in the field of information security. We have the reason to study the design theory and method of application.

Security problem restricts the development and application of RFID technology in the analysis of the EPCglobal the security issues of the agreement and the existing loopholes in security protocols. And it proposes a security mechanism of reading and writing, which effectively prevents the variety of attacks, and combining the DES encryption algorithm to further improve the security of system and data. The improved DES algorithm has the characteristics of small size, low power consumption, more suitable for RFID tag circuit.

**REFERENCES**


**Xu Bin**, born in 1970, male, People in Hubei province of China, graduated from Huazhong University Hankou campus, computer application major. Worked at Jianghan University, lecturer, his main research direction is computer application technology.

**Zhang Lihui**, born in 1963, male, worked at Jianghan University, his main research direction is Theory and experiment in physics teaching.

**Tan Xiaoping**, born in 1957, male, worked at Jianghan University, his main research direction is physics experiment teaching.