# Research and Design of RFID Security Authentication Protocol Based on Hash Function

ZHANG Feng

Zhejiang Business College, Hangzhou 310053, China
zhangfeng@126.com

*Abstract* — **This paper analyzes the rationality, completeness and security of HSASILC protocol. The results show that HSASILC protocol achieves the original design goals. The design protocol is compared with several typical protocols, and shows several advantages. The experimental environment is built and the protocol is verified. Using simulated RTL benchmarking sign level end design, simulation results show that the protocol is feasible, reasonable, safe and low cost, which lays a solid foundation for the application of the protocol in practice. A security and privacy protection scheme using Hash function bidirectional authentication protocol is proposed. We then use BAN logic to prove the improved protocol. Finally, according to the improved scheme, the process of mutual authentication between reader and tag is simulated in My Eclipse6.0+JDK1.6 environment.**

***Keywords - Hash function; RFID security authentication protocol; hash function; ECC public key cryptosystem; Hash-Chain Technology***

## I. INTRODUCTION

Compared with we are familiar with the Internet, the Internet of things are essentially different. The Internet network more powerful functions, network world are rich, also it is virtual, and we live in the real world or another, in the network world, to perceive the real world is very difficult. However, the birth of the Internet of things, but can truly realize the integration of the real world and the Internet world. RFID technology is a non-contact automatic identification technology, is the perception of contact of things, is the core technology to realize the perception of things, because of low cost and high reliability of its unique advantages and is regarded as one of the most important information technology in twenty-first Century, the most promising. With the continuous development of RFID technology at home and abroad, RFID with its unique advantages has been gradually in various countries and regions of the world increasingly reach into all areas of society, promote the use of the technology and creativity to improve people's life quality[1], improve enterprise efficiency, strengthen the social public security has an important influence. Now, the application of RFID technology more widely with intelligent transportation, health care, retail, manufacturing, logistics warehousing, certificate security, electronic payment, asset tracking management etc.. However, the application of RFID system was originally designed to be completely open, and the electronic label low cost limited computing resources, so most of the RFID system in the development process did not take into account security issues, this is the fundamental reason for the RFID system security risks. If the sensitive information in the label is stolen, or maliciously tampered, it may bring incalculable loss to the logistics field. In addition, an electronic label does not have a reliable security mechanism, there are also easy to proximity reader leak sensitive information, easy to be disturbed and vulnerable to malicious tracking and other security risks. Therefore, in the absence of adequate security trust under the label data security, validity, integrity, availability, authenticity is not guaranteed, this leads to complex security problems for the system operators and users. In the near future, people will also carry a plurality of electronic tags, such as clothes, cash, or even on the key, these can be regarded as a kind of digital fingerprinting allows tracking, which will inevitably bring about privacy issues, to label users therefore solve consumer privacy issues has become a key factor in the promotion of the technology of the. All this shows that the security problem has become an important factor to hinder the further development of the Internet of things based on RFID, if its safety cannot be fully guaranteed, personal information, trade secrets and military secrets so things in the system, are likely to be stolen or not by the method of molecular utilization [2], which will seriously affect the safety and economy military and national security. In short, more complete RFID system solutions should meet confidentiality, integrity, availability, authenticity and privacy and other basic requirements. Because the RFID system provides the back-end server database, and usually assumes that the back-end database computing and storage capacity of strong, specific information label labeling products (such as product name, manufacturer, origin, etc.) can be stored in the back-end database, so the tag without a large amount of data storage and transmission. Typically, the label simply needs to transmit a simple identifier (that is, the label ID), people can use this identifier to access the back-end database to obtain the target object related data and information. However, the fixed identifier is easy to label by illegal tracking, even if the label is encrypted and illegal tracking person does not know the content of the label identifier, still can encrypt information to track the fixed label, it is extremely easy to cause the tag location privacy problem. To solve this problem, there are usually two ways: one is to adopt the mechanism of answering queries based on random numbers, the label in this mechanism ID are generally fixed, each tag in the authentication process to read and write the response is ID and random number series Hash values (such as the Randomized Hash-Lock protocol distributed RFID challenge response authentication protocol) or ID, random number and encryption key function values (such as digital library RFID protocol), each are not the same, the attacker cannot track the malicious tag; two is the label ID dynamic refresh mechanism, database and label each certification process will be dynamic refresh the ID information, to avoid the attacker on the label for tracking and positioning through the fresh keeping of ID tags, such as Hash-Chain protocol, based on hash ID changes Protocol and LCAP protocol. The mechanism for answering queries based on random numbers, its disadvantage is that every authentication occurs when the back-end database to Hash operations or decryption of all ID tags in large databases, the overall consumption of more time, the application is only suitable for small range, for the large database, the mechanism of low efficiency. The label ID dynamic refresh mechanism, its biggest drawback is that the attacker in the backend database and label them a complete data updating of the information communication of the RFID system interference, resulting in data loss between the back-end database and label synchronization, so the mechanism of computing environment is usually not suitable for distributed database. At present, the proposed change label ID mode protocol cannot well solve the problem of data synchronization between database and label after interference. Although the Hash-Chain protocol does not exist the problem of data synchronization, but with the general mechanism of answering queries based on random numbers, each authentication occurs when the back-end database which have a lot of Hash operations, and the agreement is a one-way authentication protocol, the reader can authenticate the legality of the underlying sign, and the tags are not certified the legitimacy of the reader. In addition, the agreement also vulnerable to replay and impersonation attack. Hash function typical application schematic shown in Figure 1, RFID security certification system shown in Figure 2. Therefore, this paper will consider the security requirements and the label cost control problems, Hash-Chain technology design of RFID security authentication protocol based on data synchronization in solving problems at the same time, the lightweight public key encryption technology into RFID system to realize the label and back-end database shared key exchange, in order to reduce the number of back-end database needs Hash operations, improve the efficiency of the RFID system to meet the distributed and large databases use. The security of a system is not absolute but a comparative concept. For the RFID system, there have been many kinds of security mechanisms, but not a security mechanism is absolutely safe, they can only achieve some security functions under specific conditions, itself also has the security problem, still not perfect. Such as the classic Hash-Lock protocol. The agreement through the lock label, to a certain extent, can protect the label data information security. But every time when the certification label for the reader's response is the same false label ID Hash, so the attacker can intercept the information through the corresponding label to determine the identity of the user label, and labels for position tracking. In the security channel transmission key and identity information label phenomenon in the authentication step, this information can easily be attacker interception, the protocol cannot resist replay attack and forgery attack, confidentiality of data information cannot be guaranteed. Randomization followed by the Hash-Lock protocol of Hash-Lock protocol is improved, by introducing a random number for R to read and write response information about tag every time are random cannot be predicted, the protocol can resist position tracking attacks, but for plaintext transmission phenomena in the Hash-Lock without any the improvement is still so problems[3].

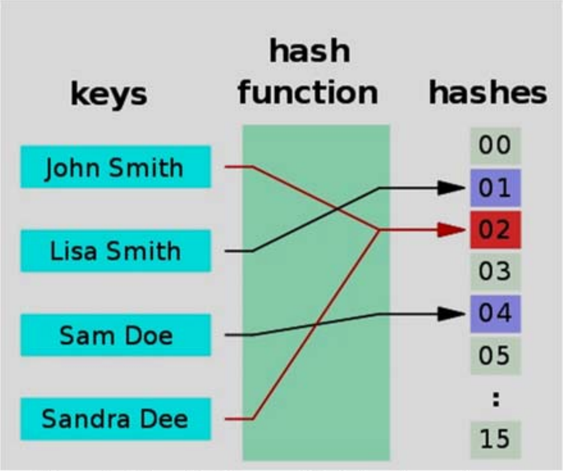

Figure 1. Schematic diagram of Hash function application

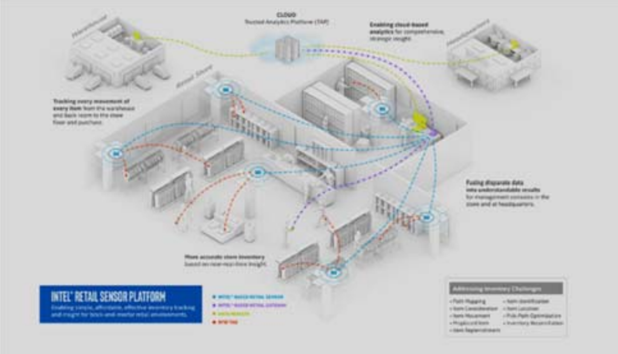
CLOUD
Trusted Analytics Platform (TAP)
INTEL® RETAIL SENSOR PLATFORM

Figure 2. Schematic diagram of RFID security authentication system

In addition, the protocol in each authentication, the server should send all the label information to the reader, the reader and server communication between too large, is not suitable for a large number of label occasions. Some agreement on solving a problem but also introduced another problem, such as the Hash-Chain protocol has a relatively high safety performance, but the computational complexity of the back-end database protocol is relatively large, at the same time, the agreement is likely to be attacked by malicious consumption of resources, vulnerable to DOS. In addition, it is a one-way authentication protocol, that is, the reader can authenticate the identity of the label but the label cannot authenticate the identity of the reader. Concludes that these protocols cannot be used in situations where security requirements are high or resources are limited to low-cost tags. But based on the traditional encryption algorithm RFID authentication protocol, by the label cost, algorithm hardware implementation complexity and related process constraints, only a few into practical application. The design of the existing RFID security authentication protocol is a premise based on the assumption that read and write the communication channel between the device and the back-end server is absolutely safe, but that with the further development of the application of RFID technology is no longer reasonable, such as the emergence of long distance communication and mobility of the reader to request more and more high, the communication between reader and back-end server to wireless communication, assumption no longer holds[4]. In summary, due to the limited resources and computing power in RFID system, the security mechanism design of RFID system is more challenging. In addition, the wireless channel itself has the openness and the complexity of the current network environment, so far there is no safe and efficient RFID security mechanism. How to find a balance between cost and security to design a secure and efficient RFID security authentication protocol becomes a challenging task. Authentication is the first barrier of the system, so the design of a complete and efficient RFID security authentication protocol is very important to solve the safety problems of the RFID system, can even affect the further development of RFID technology.

## II. THEORETICAL BASIS AND BASIC TOOLS

### A. Hash Function

Hash, generally translated as "hash", also transliterated directly as a "hash", is the arbitrary length of the input (also called pre mapping, pre-image), by hash algorithm, transform into a fixed length output, the output is the hash value. This conversion is a contractive mapping, that is, the hash value space is much smaller than the input space, and different input may be hashed into the same output, but cannot only determine the input value from a hash value. Simply put is a function of compressing any length of message to a fixed length message digest. We often see in the eMule log, eMule is the hash file, here is the use of the hash algorithm of the file checksum function, the front has said some of these functions, in fact, and this is a very complex process, in FTP, BT and other software which is the basic principle for the eMule. Is the file block transmission, each piece of this transmission are compared to check, if the error re download, during which the related information written to the met file, until the task is completed, the part file rename, and then use the move command, sends it to the incoming file, then met automatically delete the file, so we sometimes fail to meet the hash file, is refers to the information inside the met and part files, cannot be wrong, In addition to the boot is also sometimes crazy hash, there are two types: one is the first time you use this time to extract all the hash file information, there is a situation in which the last time you shut down illegal, so this time is to check the troubleshooting. Research on the hash algorithm, has been a frontier of information science, especially with the popularity of network technology, its importance is more and more prominent, in fact, every day in the online exchange of information security, we use the key principle in the operating system, which has its shadow, especially for those interested in research the information security of friends, this is a more open information key to the world, it in the hack world there is also a research focus. Because the input message can be finite or infinite set, and the output message is a finite set, and usually the input message length is generally greater than the output message length, therefore, the hash function is often called a compression function. The so-called one-way, which refers to the input message for each given string, can easily calculate the output of the hash value (hash value); a hash value for any given h, to find an input message hash value, the calculated value is equal to h by the input message, in addition to the method of using poor search, in the calculation is not feasible. Certification, also known as the identification. Authentication is often the first fortification of security protection in many application systems, and it is also an important technology to prevent active attacks. Simply put, authentication is a process of verifying a true identity, through which an entity can prove a claim to another entity. Certification can be divided into entity authentication (authentication method is on the real people, process, client, server and system identity authentication and message authentication (message authentication) is the recipient of the message to the target received inspection method whether the message is true). The main purpose of certification is to ensure the authenticity of the sender and the recipient of the message (it is claimed by the entity issued) and integrity of the message (has not been tampered with, insert, delete), but also for the sequential time and verify message (not rearrangement, replay, delay). In short, the source and content of message authentication make the recipient can identify the authenticity of the message, the timing and the destination [5]. This authentication in correspondence between the two sides, does not allow the third party to the above certification. A pure authentication model as shown in figure 3. In this system, the sender of the message through a public channel without interference will send a message to the receiver, the receiver should not only receive the message itself, but also to verify whether the message sender from legal, and whether the message has been tampered with. The attacker not only intercepted and deciphered the encrypted message transmitted in the channel, but also forged the ciphertext to the receiver to deceive. At the same time, may also exist between the sending and receiving of fraud, the need for the sender and receiver authentication. The structure of the Hash function diagram shown in Figure 4.

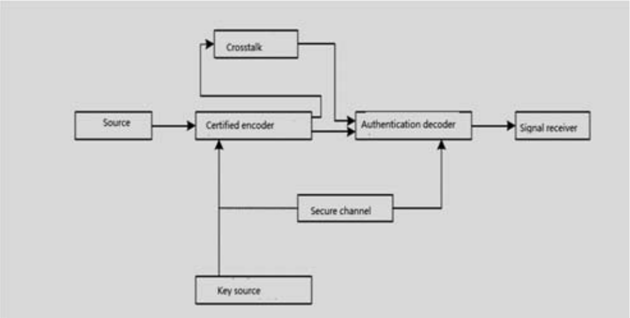

Figure 3. A pure authentication system model diagram

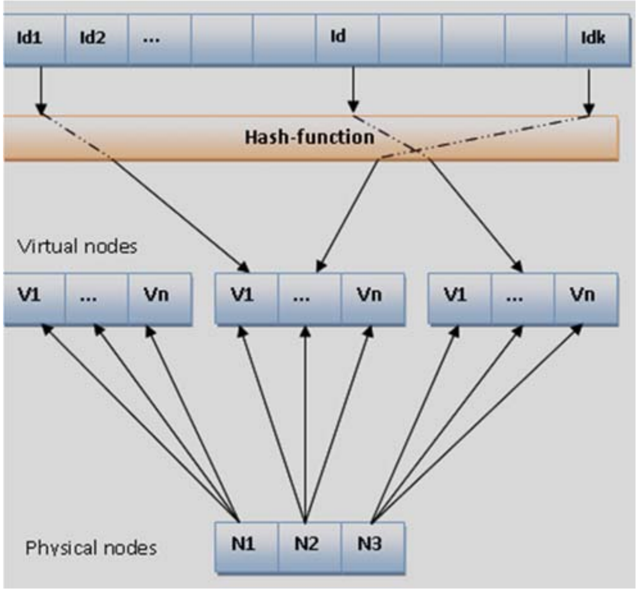

Figure 4. Schematic diagram of Hash function

## B. *RFID Technology*

Radio frequency identification, RFID technology, also known as radio frequency identification, is a kind of communication technology, through radio signals to identify specific targets and to read and write data, between without recognition system and the specific goal of establishing a mechanical or optical contact. RF tag is the physical carrier of product electronic code (EPC), attached to the traceable items, can be circulated globally and identified and read. RFID technology as the key technology to the establishment of the Internet of things "in recent years, people pay attention to. RFID technology originated in the UK, used to identify enemy aircraft in the Second World War began in 1960s of commercial identity. RFID technology is an automatic identification technology, the United States Department of defense regulations after January 1, 2005, all supplies are to use RFID tags; the U.S. Food and Drug Administration (FDA) recommended manufacturers since 2006 by RFID tracking often false drug. Walmart, Metro retail applications RFID technology and a series of actions is to promote the RFID application boom in the world. In 2000, the price of each RFID tag is $1. Many researchers believe that RFID tags are very expensive, only to reduce costs to large-scale applications. 2005, the price of each RFID tag is about 12 cents, and now ultra-high frequency RFID price is about 10 cents. RFID to large-scale applications, on the one hand is to reduce the price of RFID tags, on the other hand, look at the application of RFID can bring value-added services. Statistics show that the EU statistics office, 2010, the EU has led the application of RFID technology application in 3%, distribution of credentials and access control, supply chain and inventory tracking, auto charging, security, production control, asset management. The radio signal is transferred from the label attached to the object by adjusting the electromagnetic field into the radio frequency to automatically identify and track the object. Some of the labels issued from the field in recognition of the recognizer can get energy, do not need batteries; also the label itself has the power, and can emit radio waves (electromagnetic field into radio frequency). The label contains electronic information stored within several meters can be identified. Unlike the bar code, RFID tags do not need to be within the scope of the recognizer's vision or embedded into the tracked object. Many industries use RFID technology. Attach the label to a production vehicle, which is convenient to track the progress of the vehicle on the production line. The warehouse can track where the drug. Radio frequency tags can also be attached to animals and pets to facilitate positive identification of animals and pets (active identification means preventing several livestock use the same identity). Radio frequency identification cards enable employees to enter locked building sections, and radio frequency transponders on cars can also be used to collect toll roads and parking spaces. Conceptually, RFID is similar to the bar code scanning, the bar code technology, it will have a bar code encoding attached to the object and use the special scanning reader using optical signal will be transmitted to the magnetic strip information by scanning the reader; and the RFID is used for the RFID reader and can be attached to the target RFID tag specialized, using frequency signal will be transmitted to the information from the RFID tag RFID reader [6]. The advantages of RFID system is the most important non-contact identification, it can penetrate the snow, fog, ice, paint, dirt and bar code cannot be used in harsh environment to read labels and read fast, in most cases less than 100 milliseconds. The advantages of RFID system active sketch ability are also important. Can be used to process tracking and maintenance tracking interactive business. The main problems restricting the development of RFID system is not compatible with the standard. The main manufacturers of RFID system are provided for system, lead to the different types of frequency and protocol of different applications and different industries, this confusion and separatist situation has restricted the whole RFID industry growth. Many organizations are working to solve this problem, and have made some achievements. Large scale development and wide application of standardization will stimulate the RFID technology. The basic principle of RFID technology is not complex: the label into the field, RF signals received by the reader, by sending the obtained current energy out of the product information stored in the chips (passive tags or passive tags), signals or by active tags send a frequency (Active Tag, active tag or active label), the reader will read and decode the information, sent to the central information system on the data processing. A complete set of RFID system, by the electronic tag reader and transponder is three parts and application software system called the composition, the working principle of the Reader launch a specific frequency radio wave energy is used to drive the circuit, the internal data is sent, the Reader in the order of receiving data for interpretation, application do the corresponding processing program. RFID card reader and electronic label communication and energy sensing methods can be roughly divided into: inductive coupling and backscatter coupling two. The low frequency RFID with the first type, rather than the frequency of most of the second ways. RFID schematic diagram shown in Figure 5.

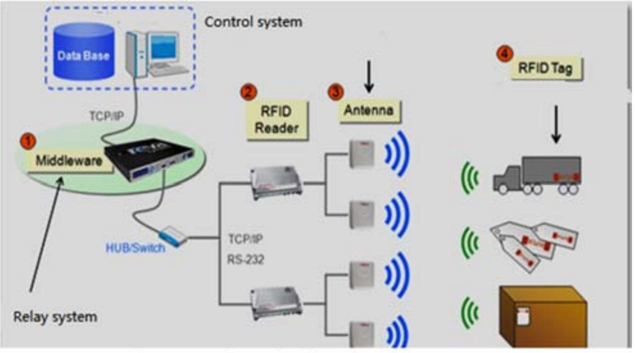

Figure 5. Schematic diagram of RFID system

### C. Typical Application of Hash Function

In cryptography and data security technology, Hash function is an important tool to realize effective, secure and reliable digital signature and authentication. At present, the security field is more and more inseparable from the research of Hash function, and the application of Hash function is more and more inseparable from the field of computational science and its application. (1) the application of digital signature: Hash function is the most likely place in digital signature. If you sign a long file, you can group it and then sign each packet. However, this method is inefficient, especially when using RSA digital signature method, because RSA encryption slower, generally only suitable for encrypting shorter text messages. A better way is to first use the Hash function to act on the entire file and then sign the summary of the Hash function. (2) generation program or document "digital fingerprint", Hash function can be input transform of arbitrary length for the output of fixed length, different input corresponding to different output, therefore, can get hash function transformation program or document based on the value of output, namely "digital fingerprint"[7]. The original "fingerprint" and can be put in a safe place compared to this virus can be found or intruders modify the program or document, use the Hash function to generate the hash value of the data and compare and save the value if they are equal, the data is complete, otherwise, that the data has been tampered with. This is to ensure the integrity of the data, the realization of message authentication, to ensure that the message is not unauthorized illegal modification. In accordance with the desired security requirements, after the Hash function generated fingerprints, even if the original message only changed one bit, the resulting fingerprint will be different. (3) for secure storage passwords: when users log on to a variety of systems need to provide a user name and password to the server, some of the system's user name and password are stored in the form of plaintext on the server. This approach is very dangerous. Because once the attacker can access the server to store user name and password files, you can know the user's password. If the hash value of the password is generated based on the Hash function, and then save the hash value of the user name and password in the system, rather than the password itself, which helps to improve the security of the system. Unix system password management is to use such a security mechanism. When the user login system enter your username and password, Unix system user input password as Hash function of the input, then the output of the Hash function and the stored hash on the machine user password values are compared when the two are equal, indicating the user's password is correct, allowing the user to enter the system otherwise, refused to enter. Currently in information security, the most commonly used hash function has two series: MD (Message Algorithm) series and SHA (Hash Digest) series (Security) series. Typical MD2, MD4, MD5, SHA-1, SHA-256, SHA-384 and SHA-512, they are through the direct construction of complex nonlinear relations to achieve one-way compression requirements. Hash algorithm security password application schematic shown in Figure 6.

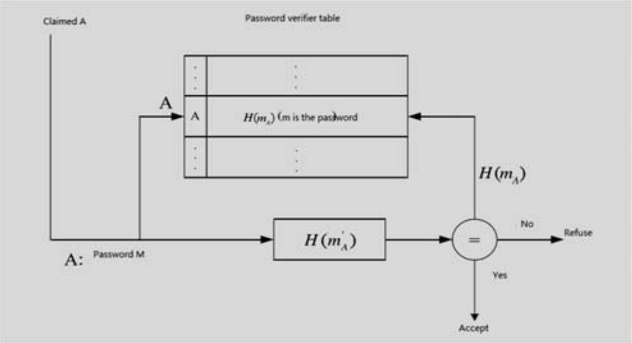

Figure 6. Schematic diagram of Hash algorithm "password" Application

## III. RFID SYSTEM SECURITY ANALYSIS

### A. Contact RFID Networking Technology

The remote control for the end of things, mainly divided into two kinds, one is wired, the other is a wireless, wireless remote control, the main use of RFID technology, it is a kind of automatic identification technology in 1990s began to rise, is an important means for the implementation of the perception of the Internet of things, is perceived contact the Internet of things. As the perceived contact of the Internet of things, RFID system uses radio frequency technology to identify objects in the open system environment. It is an integrated technology which integrates coding, carrier, identification and communication technology. It is through the radio frequency identification signal automatic target recognition and access to relevant data, identify the process without manual intervention, without the need of laser and optical visible, can be read through the external material data, the equivalent of wireless bar code, the operation is very convenient, it can work in all kinds of environment. The most basic RFID system consists of three parts, including tag (Tag), reader (Reader) and antenna (Antenna). As shown in Figure 7. RFID tags have uniquely identified RFID codes attached to objects that need to be identified. Tags can be divided into read-only and read and write two. The RFID reader is a wireless transmitting and receiving antenna device, relative to the label, data processing and storage space are relatively large, it is the most important infrastructure in the RFID system, the general and the backend server connected to the database. An antenna is a device for establishing a wireless communication connection between a label and a read-write device to achieve radio frequency signal space wave storage. The communication between RFID tag and reader is non-contact and wireless, their communication content is easy to leak. In fact, the current wireless communication between RFID system reader and tag is unprotected in most cases, facing huge information and privacy security risks. When RFID is used for personal identification, the attacker can only read electronic encoding from the label, so as to obtain the personal information of users; when RFID is used for item identification; the robbers can use the reader to determine what the target is more. At the same time, some intelligence agents may also be able to obtain useful business secrets by reading a series of tags that lack security mechanisms. Provide a RFID database backend server, and usually assumes that the back-end database computing and storage capacity of strong, specific information label labeling products (such as product name, manufacturer, origin, etc.) can be stored in the back-end database, so no label storage and transmission of large amounts of data information. Typically, the label simply needs to transmit a simple identifier (that is, the label ID), people can use this identifier to access the back-end database to obtain the target object related data and information. However, the fixed identifier is easy to label by illegal tracking, even if the label is encrypted and illegal tracking person does not know the content of the label identifier, still can be fixed by encrypting information to track label. Once the label positioning information exposure means that the label can be tracked for a long time. The attacker can identify the victim's label without contact (remote); master the victim's position information, thereby providing convenient conditions for illegal acts or activities. The lack of security of the electronic tag is very fragile, through technical means some easy, anyone can change or even destroy the useful information on the RFID tag, such as tampering, denial of service attack, replay attack, which will destroy the normal communication system, disrupting the normal operation of the RFID system. Security mechanisms are not good RFID system, very vulnerable to impersonation attacks. In the real communication process, the attacker can obtain sensitive information from the communication data between the tag and the reader, and use it to reconstruct the RFID tag, so as to achieve the purpose of forgery labels. Forged or cloned RFID tags will seriously affect the application of RFID in the field of retail and automatic payment. Physical security mechanism is the mechanism of using physical methods to protect label security, including: Kill instruction mechanism, electromagnetic shielding, blocking tags, active interference and separable tags. These methods are mainly used in some low-cost electronic tags, because these RFID tags have strict cost limits, simple functions, cannot provide complex applications or encryption algorithms to protect privacy [8].

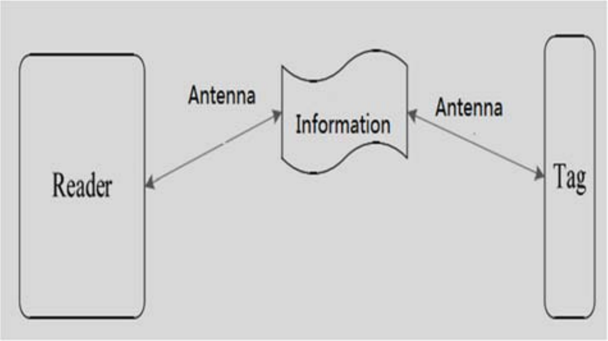

Figure 7. Schematic diagram of RFID system structure

### B. *Analysis of RFID System Security Policy*

Physical security mechanism is the mechanism of using physical methods to protect label security, including: Kill instruction mechanism, electromagnetic shielding, blocking tags, active interference and separable tags. These methods are mainly used in some low-cost electronic tags, because these RFID tags have strict cost limits, simple functions, cannot provide complex applications or encryption algorithms to protect privacy. Kill tags by the standardization organization Auto-ID Center (Automatic Identification Center) proposed, the principle of the program is that consumers remove the label when the goods checkout or even completely kill labels. Once the user implements the "Kill" destroy instruction, all functions of the label will be physically destroyed, and cannot be activated, can perfectly prevent scanning and tracking. Consumers can perform this "Kill" directive after purchasing a product to eliminate labels and eliminate consumer concerns about privacy. However, this method is difficult to verify whether the real implementation of the "Kill" directive, but also limits the further use of RFID tags, such as product after-sales service, waste recycling, etc.. So simple Kill commands are not an effective security policy. From the point of view of electromagnetic field, the radio wave can be shielded by Faraday metal net container composed of conductive material. Users can keep their personal belongings in the shielding bag, to prevent the illegal infringement of reader. However, this requires additional external equipment, use not only caused inconvenience, while increasing the cost, but also, in many fields, such as a safety measure is not feasible, and the clothes on the RFID label cannot use metal mesh shielding container. Stop tag is a special electronic tag proposed by RSA security. It prevents the RFID reader from reading the user's privacy by using a special blocking tag that makes the reader's command read always the same answer data. In addition, by setting a label area, blocking labels can selectively block labels that are set to a privacy state, without affecting the normal work of tags that are set to public status. For example, before the purchase of goods, the label set for the public, businesses the reader can read the tag information; and the goods once sold, the label is set to ensure privacy, tag information cannot be any customer reader to read. However, this method requires an additional blocking tag that makes the cost high and can also cause denial of service attacks, while the label beyond the protected area is not protected. Active interference mechanism can be regarded as another method of screening label [9]. The user can use the label through an additional equipment to broadcast radio signal to stop or destroy things near the reader, the reader near the RF system does not work properly, so as to achieve the purpose of protection of privacy. Obviously, this method also requires an additional external equipment, not only caused inconvenience and increased operating costs, but also may lead to legal problems, because it will give the legal system does not require privacy damage, may also affect other wireless communication. Separable RFID tag is designed by IBM company. Its design principle is that the antenna and chip on the passive label can be easily split. Consumers can shorten the label reading distance by changing the length of the tag antenna. If you use handheld reading devices almost stuck to the label before you can read the information, without the user's permission, reading equipment cannot be remotely concealed access to information. Shorten the label of the antenna itself or can run, so that both the convenience of the goods after service and product return identification, at the same time play a role in the protection of user privacy. However, the manufacturing cost of separable labels is relatively high, not suitable for large-scale use, at the same time; the feasibility of label manufacturing also needs further discussion. Hash-Lock protocol flow diagram shown in Figure 8.

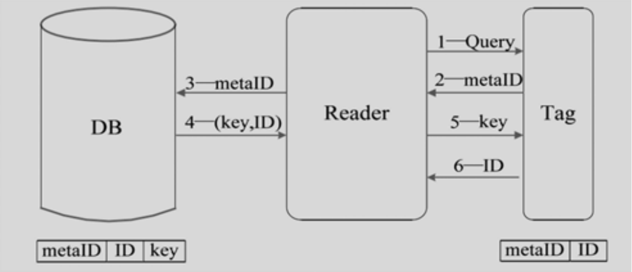

Figure 8. Schematic diagram of Hash-Lock protocol flow

### C. *RFID Authentication Protocol Based on Hash Function and ECC*

A RFID system that can operate normally safely should have the basic features of confidentiality, integrity, authenticity, availability and privacy. This is also the design of the RFID security authentication protocol reference standards. (1) confidentiality of data. In practical application, which contains the RFID tag data are often related to consumers' personal privacy, so to protect the personal privacy of consumers, must design a complete RFID authentication scheme, to ensure that the information contained in the label can only be authorized to read by the reader, and unauthorized reading the reader will not get any confidential information. (2) the integrity of the data. The data transmitted in the insecure communication channel is vulnerable to the malicious tampering and replacement of the attacker. Therefore, the integrity of the data must be tested to ensure the correctness of the data. In the public key cryptosystem, data integrity is realized by digital signature. However, in RFID system, considering the low computational cost and limited storage space, people usually uses message authentication code to test data integrity. In the design of RFID protocols, consider using the Hash algorithm with shared keys, namely the use of the shared key and message to be tested in series with the hash operations Hash value obtained integrity of the received data to test. (3) the availability of data. A reasonable RFID security solution should have such characteristics, design of various security protocols and algorithms should not be too complicated, RFID should fully consider the characteristics of limited resources system computing cost, storage capacity and communication ability. In addition, a variety of service solutions to a secure RFID system provided by authorized users must be able to use, and can effectively prevent the illegal attackers attempted to interrupt the RFID service system of malicious attacks, such as tampering, DOS attack and replay attack. In practical applications, due to the inherent vulnerability of wireless communication, most RFID systems are vulnerable to the attacker's destruction. Therefore, an effective security design scheme should effectively prevent the attacker from malicious consumption of electronic tag resources without restricting the availability of RFID system. (4) the authenticity of the data. In the real communication process, the attacker can obtain sensitive information from the communication data between the tag and the reader, and use it to reconstruct the RFID tag, so as to achieve the purpose of forgery labels. Therefore, the reader to ensure the authenticity of the message, that is, the message from the correct RF tag sent out, you must have an effective authentication of the identity of the electronic tag. (5) the privacy of the user. Because the RFID system provides the back-end server database, and usually assumes that the back-end database computing and storage capacity of strong, specific information label labeling products (such as product name, manufacturer, origin, etc.) can be stored in the back-end database, so the tag without a large amount of data storage and transmission. Under normal circumstances, only need a simple transfer label identifier (i.e. ID tag), people can use this identifier to access the back-end database even if the label is encrypted and illegal tracking person does not know the content of the label identifier [10], still can be fixed by the encryption information to track the tag, which can easily lead to tag location privacy issues. A secure RFID system must be able to solve the label positioning privacy problem, can effectively protect the user's privacy information or the economic interests of the relevant economic entities. In the RFID system, an attacker to reach the ultimate goal is to obtain secret information, RFID tag for the RFID security protocol must have the ability to keep a secret; another is to identify and distinguish the RFID label, in order to confirm its target, namely to achieve effective tracking. Therefore, RFID security protocols must also ensure that tags in the eyes of the attacker is not identifiable and differentiated. Although the privacy and cost of RFID is mutually constrained, but this does not prevent more privacy assurance RFID security protocol is proposed. Moreover, with the development of chip technology, it becomes possible to apply some more complex cryptographic techniques to RFID system. This chapter will construct two RFID security authentication protocols, which are confidentiality, integrity, authenticity, availability and privacy, which are Hash-Chain bidirectional authentication protocol and Hash-ECC hybrid authentication protocol. Digital library RFID protocol schematic shown in Figure 9.

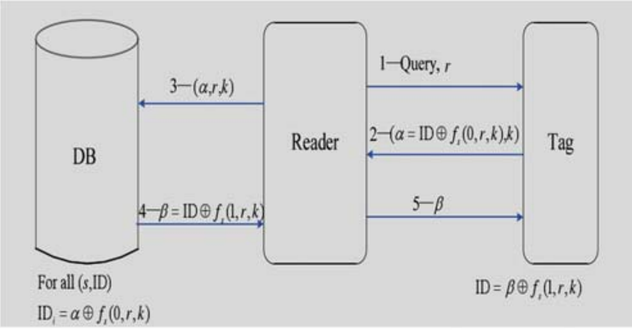
DB
Reader
Tag
1—Query, $r$
$2—(\alpha = ID \oplus f_i(0,r,k),k)$
$3—(\alpha,r,k)$
$4—\beta = ID \oplus f_i(1,r,k)$
$5—\beta$
For all $(s,ID)$
$ID_i = \alpha \oplus f_i(0,r,k)$
$ID = \beta \oplus f_i(1,r,k)$

Figure 9. Schematic diagram of RFID protocol in Digital Library.

## IV. Hash - Chain two-way authentication protocol design

In order to solve the problem of label location privacy, the Hash-Chain protocol introduced in this paper adopts the method of continuous refresh of shared keys. In fact, the backend database and label the shared key to tag identifier (i.e. label ID) role, therefore this method to label ID dynamic refresh mechanism, it does not exist the problem of data synchronization, is after the end of each database in the certification process for a large number of hash operations at the expense of Hash. In view of the existing protocol Hash computation to the back-end database, the label cannot be certified the legitimacy of the reader, the system is vulnerable to replay and impersonation attacks and other shortcomings [11], to make improvements in the following areas in this section of the agreement: (1) interrogator transponder mode by random number to achieve tag to reader legitimacy the authentication, two-way authentication tag and reader. (2) establish a reasonable share key refresh mechanism; consider the label through the reader after the certification of shared key update, to prevent the attacker's malicious consumption of label resources. (3) the problem of data synchronization is solved by introducing proofreading key, and to some extent, the operation load of back-end database is reduced and the execution efficiency of RFID system is improved. Compared with the Hash-Chain protocol, update the shared key tag Hash-Chain mutual authentication protocol proposed in this section has better control mechanism, the label only in the shared key $S_j$ to read and write the legitimacy of the authenticator through will update their and the back-end database, which can effectively prevent the attacker to tag malicious resources consumption. Moreover, by using the introduction of proofreading the key, in solving the problem of data synchronization at the same time, also greatly reduced on each label Hash operations (the back-end database in the Hash-Chain protocol to m times, among them, 1⩽ m⩽ M, M is the largest chain length; the preset in the Hash-Chain protocol in the most for the 2 time), to a certain extent, improve the efficiency of the implementation of the protocol. In view of the above Hash-Chain mutual authentication protocol proposed in large database in the back-end database load calculation of relatively large limitations, this section considers the ECC public key cryptosystem is embedded into the RFID system, to achieve the exchange of keys in the backend database and tag, back-end database Hash is to reduce the number of hash operations. Below, will be based on the Hash function and ECC proposed another RFID mutual authentication protocol -- Hash-ECC hybrid authentication protocol based on data synchronization to solve the problem of the backend database and label on the RFID, to further improve the efficiency of the system, to meet in large databases. Compared with the Hash-Chain protocol described above, Hash-ECC hybrid authentication protocol will ECC public key cryptosystem is embedded into the RFID system, using ECC public key cryptosystem on the shared key $T_j$ encrypted before transmission, to realize the exchange of keys in the backend database and tag, and then query for all the data items in the database, to find after the data, as long as a Hash operation to implement the reader on the label certification, reached a substantial reduction in the back-end database Hash the number of hash operations[12], so the application of Hash-ECC hybrid authentication protocol can be applied to large databases. Certification schematic shown in Figure 10.

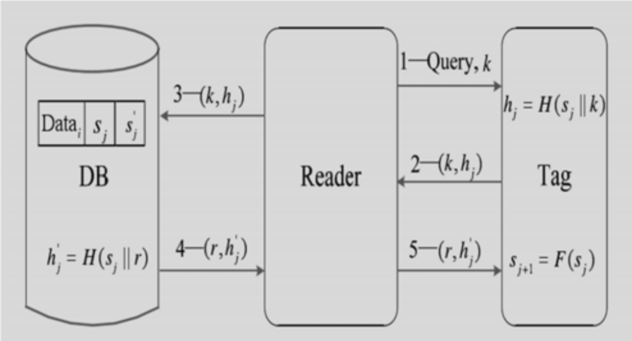

Figure 10. Schematic diagram of protocol structure.

## V. Conclusion

RFID technology is a non-contact automatic identification technology, as a wireless version of the bar code, it has many bar codedoesnt have waterproof, antimagnetic, high temperature resistance, anti-pollution, reading distance, long service life, the label data can be encrypted, it has larger data storage capacity and can be reused. However, communication between reader and tag is exposed in the open environment without a safety guarantee in, in the absence of adequate security trust under the label data security, validity, integrity, availability, authenticity cannot be guaranteed, which will bring the complexity of the security and privacy issues for the system operators and users, so to ensure the safety and security of the tag information user's personal privacy, we must establish a perfect RFID system solutions. At first, physical security mechanisms based on physical methods were adopted, including Kill instruction mechanism, electromagnetic shielding, blocking tag, active interference and separable tags. These methods are mainly used in some low-cost electronic tags, because these RFID tags have strict cost limits, simple functions, cannot provide complex applications or encryption algorithms to protect privacy. The security mechanisms based on physical methods have big defects; people have proposed a lot of cryptographic security mechanisms based on modern cryptography, that is, RFID authentication protocol. The existing Hash-Lock protocol and Randomized Hash-Lock protocol, Hash-Chain protocol, based on Hash changes of ID protocol and LCAP protocol in some aspects of security risks exist. Although distributed RFID challenge response protocol, RFID protocol, digital library has so far found no obvious security vulnerabilities exist, but each time authentication occurs when the back-end database which have a lot of Hash operations, the system efficiency is low, especially in large databases, the more obvious defects. Therefore, to reduce the number of back-end database requires Hash operations, improve the execution efficiency of RFID system is the main direction of research on RFID security authentication protocol. This paper designed two basic features of confidentiality, integrity, authenticity, availability and privacy RFID security authentication protocol, use the Hash function, discrete logarithm, and elliptic curve cryptosystem, El Gamal cryptography, from the function, safety, efficiency and cost of the 4 aspects of the design. The agreement is discussed. Among them, the first Hash-Chain mutual authentication protocol, the protocol of innovation is introduced through the use of proofreading key, solve the backend database and tag communication after disturbance data synchronization problem; second Hash-ECC hybrid authentication protocol, the ECC public key cryptosystem is embedded into the RFID system, to realize the sharing of the session key exchange database and tag, and then query for all the data items in the database, find the matching data by a Hash operation to implement the reader standard signed certification, reduce the number of times the back-end database need Hash operations. On the basis of solving the problem of data synchronization between back-end database and tag, the execution efficiency of RFID system is further improved to satisfy the use of large database.

## ACKNOWLEDGMENTS

Zhejiang province education department project: Research of electronic information protection system based on mobile Internet (Y201635571).

## REFERENCES

[1] Zhu Hongyan, Xie Xiaoyao, Wu Jingchun. Research and design of RFID security authentication protocol based on Hash function. Journal of Chongqing University of Science and Technology: Natural Science Edition, 2016, 18 (4): 113-115.

[2] Gong Jing, Deng Yuanqing, Shi, et al. Study on RFID security authentication protocol based on Hash function. 2014, micro electronics and computer, 31 (9): 135-137.

[3] Zhu Hongyan, Xie Xiaoyao, Wu Jingchun. Improvement of RFID security authentication protocol based on Hash function. Journal of Yangtze University (self SCIENCE EDITION), 2016, 13 (39-43.): (in Chinese).

[4] Wang Mingfei, Wei Yong, sun ting. The lightweight RFID security authentication protocol based on Hash function and arrangement. Xiangtan University Journal of natural science, 2016, 38 (1): 115-119.

[5] Zheng Ying, Ouyang Dantong, He Lili, et al. Hash function against the loss of synchronization of RFID security authentication protocol based on. Journal of Jilin University, 2015, 53 (3): 499-504.

[6] Gong Haiyu, Li Fei,. Lightweight RFID bidirectional authentication protocol based on Hash function. Journal of Sichuan University of Science and Engineering (self SCIENCE EDITION), 2015, 28 (45-49.): (in Chinese).

[7] Xie Jinbiao, ou Yuyi, Ling Jie. A two-way authentication protocol based on RFID Hash function improved. Journal of Guangdong University of Technology, 2014 (3): 62-66.

[8] The court, Xu Yang, Qi Yincheng, etc. RFID mutual authentication protocol and asymmetric key cipher based on Hash function. Journal, 2014, 1 (5): 456-464.

[9] Wang Xuyu, King Fengxuan, Wang Yuqing. An improved Hash function based on RFID authentication protocol. Journal of Shandong University: Science Edition, 2014, 49 (9): 154-159.

[10] Ding Jie, Wang Zezhong. RFID identity authentication protocol based on hash function. Electronic product world, 2016 (1): 30-32.

[11] Zhou Zhicheng. An improved RFID authentication protocol based on Hash function. Wireless Interconnect Technology, 2016 (5): 68-69.

[12] Taoyuan, Zhou Ma Yupeng, joy, etc. mobile mutual authentication protocol based on Hash function. Computer application, 2016, 36 (3): 657-660.

.