IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Blocking RFID Tag for Preventing Credit Card Fraud

[1]Sampreet Kumbhar, [2]Paresh Sawant, [3]Ravindra Ghugare

[1]Student, [2]Student, [3]Guide

[1]Computer Engineering Department,

[1]Bharti Vidyapeeth College of Engineering, Navi Mumbai, India

Abstract: RFID-enabled credit cards are widely deployed in the United States and other countries, but their is no public study that has thoroughly analyzed their mechanisms that provide both security and privacy. By using samples from a variety of RFID-enabled credit cards, our study has observed that (1) the cardholder's name and often credit card number and expiration are leaked in plaintext to unauthenticated readers, (2) our homemade device costing around Rs. 10000 effectively clones one type of skimmed cards thus providing a proof-of-concept implementation for the RF replay attack, (3) information revealed by the RFID transmission cross contaminates the security of both RFID and non-RFID payment contexts, and (4) RFID-enabled credit cards are susceptible in various degrees to a range of cutomary attacks such as skimming and relaying.

***Keywords*— RFID, credit cards, contactless, vulnerabilities**

I. INTRODUCTION

An increasing number of credit cards now contain a tiny wireless computer chip and antenna based on RFID (Radio Frequency Identifier) and contactless smart-card technology. RFID-enabled credit cards permit contactless payments that are fast, easy, often more reliable than magstripe transactions, and require only physical proximity (rather than contact) between the credit card and the reader. An estimated 20 million RFID credit cards and 150,000 vendor readers are already deployed in the U.S. According to Visa USA, "This has been the fastest acceptance of new payment technology in the history of the industry."

The conveniences of RFID credit cards also lead to new risks for security and privacy. Traditional credit cards require visual access or direct physical contact for retrieving information such as the cardholder's name and the credit-card number. By contrast RFID credit cards make these and other sensitive pieces of data available using a small radio transponder that is energized and interrogated by a reader.

Experimental Results: Although RFID-enabled credit cards are widely reported to use sophisticated cryptography, our experiments found several surprising vulnerabilities in every system we examined. We collected two commercial readers from two independent manufacturers and approximately 20 RFID-enabled credit cards issued in the last year from three major payment associations and several issuing banks in the U.S. We were unable to locate public documentation on the proprietary commands used by RFID-enabled credit cards. Thus, we reverse engineered the protocols and constructed inexpensive devices that emulate both credit cards and readers. The experiments indicate that all the cards are susceptible to live relay attacks, all the cards are susceptible to disclosure of personal information, and many of the cards are susceptible to various types of replay attacks. In addition, we successfully completed a proof-of-concept cross-contamination attack.

1.1 Background

Scale of Current Deployment: Several large chain stores in the U.S. have deployed many thousands of RFID readers for credit cards: CVS Pharmacies (all 5,300 locations), McDonald's (12,000 of 13,700 locations), the Regal Entertainment Group of movie theaters, and several other large vendors. Reports estimate that 20 to 55 million RFID-enabled credit cards are in circulation, which is 5% to 14% of all credit cards. In addition to traditional payment contexts, RFID-enabled credit cards are becoming accepted in other contexts such as public transportation. The New York City subway recently started a trial of 30 stations accepting an estimated 100,000 RFID-enabled credit cards. A participant in this trial uses her credit card as a transit ticket as well as a credit card in place of the traditional magstripe-based dedicated subway tickets.

Integration of RF Technology into Existing Credit-Card Infrastructure: In a typical deployment, an RFID-enabled credit card reader is attached to a traditional cash register. Each reader continually polls for cards by broadcasting a radio signal, to which RFID enabled credit cards can respond. The RFID payment cards that we examined seem to have been designed specifically for easy integration into the existing payment-authorization infrastructure. For instance, even though no magnetic stripes are read during an RF transaction, the RFID credit card readers that we examined reformat received RFID data into "Track 1 Data" and "Track 2 Data" before passing it along to point-of-sale terminals. In other words, data is presented to the charge-processing network in the

same format regardless of whether the credit-card reader received the information from an RF transaction, or a traditional swipe of a magnetic strip.

Our work focuses on the first step in a long chain of system interactions: card presentation. When considering the potential impact of the vulnerabilities we have observed in RFID card presentation, one must take into account the expertise credit card issuers have gained in detecting fraudulent transactions by tracking patterns of behavior. While detecting fraud is an effective defense against many types of financial risk, it does not *prevent* invasion of privacy. Our study considers vulnerabilities to privacy that today's anti-fraud methods do not prevent.

Communications Protocol Used by RFID Credit Cards: All of the credit cards we tested use a communications protocol specified by the International Organization for Standardization in a series of documents titled ISO 14443-1 through 14443-4 [22]. Our experiments indicate that the cards use the B version of this protocol, with an additional proprietary communications layer carried over ISO layer 4.

2 Related Work

RFID-enabled credit cards share many of the challenges and approaches for security and privacy as other RFID-based authentication and identification systems.

RFID Authentication and Cloning: Many types of RFID tags merely emit static identifiers, making them easy to clone. These tags are sometimes used in inappropriate contexts such as building access control. Westhues has demonstrated a simple, inexpensive device that can skim many types of cards at a distance—even through walls—and then simulate the. If unclonability is a security assumption, then this is a security break.

More sophisticated tags do not emit static data, but use cryptography to emit different data during different transactions. For example, the Texas Instruments Digital Signal Transponder (DST) is present in the ExxonMobil Speedpass, and is also part of a common theft deterrent system for automobiles. These systems have been shown to be vulnerable because of faulty cryptography. To contrast with the RFID credit cards we have examined: the DST uses cryptography to increase the difficulty of cloning, but does not carry personally identifying information, e.g., the name of its owner.

Read Ranges: Industry claims around the security of RFID devices often hinge on their short read ranges. Some cautionary notes are in order, however: RFID tags do not have a single, definitive read range. While the *nominal* read range of an RFID tag may be quite short, a non-standard reader or large antenna can increase the range at which an attacker can skim an RFID tag. The credit cards we examined are ISO 14443-B cards with a nominal range of 4 to 5 centimeters. Skimming ranges of over 20cm have been demonstrated for cards of this type and ranges of up to 50cm are hypothesized in the literature.

Furthermore, while skimming requires that a reader power the targeted tag, an attacker performing passive eavesdropping on a session between a legitimate reader and RFID tag can potentially harvest tag data at a considerably longer range. Claims have surfaced of tests where e-passports, which rely on the same ISO standard as credit cards, were read at a distance of 30 feet and detected at a distance of 20 meters.

Our study makes no claims about the read ranges of RFID-enabled credit cards beyond the observation that characterization of these ranges is not straightforward and constitutes an important open research question.

3 Methodology and Experiments

The following sections highlight our methodology for testing security of RFID-enabled credit cards against eavesdropping, skimming, and replay. A more detailed version is available in our technical report.

Eavesdropping Experiments: In our eavesdropping experiments we observed transactions between readers and cards with an oscilloscope attached to an antenna. Examination of data thus obtained demonstrated the efficacy of this simple attack, since the full cardholder name and card expiration date were present in cleartext in all transactions. A majority of cards examined transmitted credit card number in cleartext, while a minority broadcast a separate (but static) credit card number apparently reserved for wireless transactions. Section 4 provides further details.

Skimming Experiments: In our most simple skimming experiment we took a commercial RFID credit card reader and presented it with each of our experimental cards, obtaining in each case ISO 7813 (magstripe style) data. Since this is the exact data that is normally transmitted by a POS terminal to a charge processing network, this most naive of skimming attacks is sufficient for perpetration of certain kinds of financial fraud.

We programmed an RFID reader not intended for credit card use to emulate an RFID credit card reader. Eavesdropping on transactions between our credit card reader emulator and real RFID credit cards demonstrated that all of the RFID credit cards we tested responded to our emulator exactly as they respond to a commercial RFID credit card reader. This strongly suggests that cards do not use any secure mechanism to authenticate an authorized RFID reader before releasing sensitive information.

Replay Experiments: Our credit card emulator is a microprocessor-controlled device with a simple radio permitting broadcast of arbitrary bytes over the ISO 14443-B transport layer.

Fig.1 Our Assembled Credit Card Emulator

We programmed our credit card emulator to expect the RFID credit card reader commands that we captured during eavesdropping experiments, and to transmit replies captured from real RFID credit cards during a skimming attack performed with the reader emulator described above. In our experiments commercial readers were unable to distinguish between our emulated card and the real card upon which it was based.

Since the output from the card emulator is identical to that of the real card from which it was skimmed, a simple replay attack using this device would succeed. As noted above, many pieces of data go into an overall transaction approval decision including sophisticated risk-based fraud detection mechanisms on the back end. For this reason, a valuable future research direction would include field tests in which a credit card emulator is used to perform a purchase in a retail location rather than a laboratory.

4 Analysis and Results

To protect the identity of our cards, we label the cards A, B, C, and D based on semantic equivalence classes determined by observing behavior between cards and readers. Table 1 summarizes some of the vulnerabilities of three classes of cards.

Table 1. A summary of susceptibility to various attacks for the three semantic types of cards (A, B, C) from three payment associations (1, 2, 3). *Because the cards have no shielding or notion of time, all the cards are susceptible to relay. **This attack is proven in the field, but is limited to certain merchants. ***This card admits unrestricted replay for the readers we tested, while the others induce a race condition

Card Type	Payment Association	Privacy Invasion	Relay Attack	Cross-Contamination	Replay Attack
A	1	Yes	Yes	Limited	Yes
B	2	Yes	Yes	Limited	Limited
C	3	Yes	Yes	Limited	Limited

4.1 Observations of RFID-enabled Credit Card Protocols

This section explores some of the RFID credit card protocols that are in current deployment. The analysis is based on the ISO 7813 (magstripe format) data output by the serial port of RFID credit card readers when presented with different types of credit cards. Where pertinent, our analysis compares this serial output with the raw RF data from the same transactions as captured by our eavesdropping apparatus.

In keeping with a philosophy of ethical attacks research, we have redacted several pieces of information from the following subsections in part because of a desire to prevent criminal misuse of our findings. Cardholder name and card number have been concealed. Additionally, we have obscured the number of digits in the card number in order to obscure which observations correlate with the products of specific payment associations and issuing banks.

Card A Protocol: When presented (RF transaction) with any sample of a card of type A, our reader outputs serial data identical to the data contained on the magstripe of the same credit card. When presented with the same card, the output is always the same: in the serial output there is no evidence of a counter, one-time-password, or any other mechanism for prevention of replay attacks.

```
Bxxxxxx6531xxxxxx^DOE/JANE^0906101000000000000000000000000000858000000
xxxxxx6531xxxxxx=09061010000085800000
```

Fig. 2. Serial output from a commercial reader after an RF transaction with a card of type A

Card B Protocol: The sample card B output in Figure 3 demonstrates the presence of a counter, determined to be such because of monotonic incrementation with successive transactions. Additionally, we observe three digits that change with each transaction in no pattern that we have identified. Because of the relatively high entropy of these three digits, we consider it likely that they are the output of some cryptographic algorithm that takes the transaction counter as an input. If this is the case, then the algorithm must also take a card-specific value like a cryptographic key as an input since we observe that different cards with the same counter value produce different codes. We speculate that these data may serve as a stand-in for the traditional CVC.

```
Bxxxxxx1079xxxxxx^DOE/JANE^0901101100000000000100000000000
xxxxxx1079xxxxxx=090110110000016 00221
Bxxxxxx1079xxxxxx^DOE/JANE^0901101100000000000100000000000
xxxxxx1079xxxxxx=090110110000074 00231
```

Fig. 3. Sample of reader serial output after RF transaction with a card from issuer B. In this sample we see a three digit code (shown in bold italic font), and a four digit counter (shown underlined).

Card C Protocol: Card C's protocol differs from Card B's in a few crucial details:

1. its unique transaction codes are eight digits instead of three
2. its transaction counter, now located in the Cardholder Name field, displays only three digits instead of four
3. rather than sending the embossed card number over the air, it uses a fixed pseudonym

```
Bxxxxxx2892xxxxxx^DOE/JANE          017^10011010 10691958
xxxxxx2892xxxxxx=10011010 10691958 01700
Bxxxxxx2892xxxxxx^DOE/JANE          018^10011010 40146036
xxxxxx2892xxxxxx=10011010 40146036 01800
```

Fig. 4. Sample output from a card of type C. Transaction codes are shown in bold italic font, transaction counter is shown underlined.

4.2 Analysis of RFID-enabled Credit Card Protocols

The following sections analyze the susceptibility of the card types to replay, relay, cross-contamination, and privacy/tracking attacks. Our analysis considers only the protection mechanisms of the cards and readers, not the security of the charge processing network (e.g., fraud detection algorithms).

Replay Attacks: Replay attacks come in several flavors depending on what data are communicated from the credit card all the way to the back end charge processing network.

1. Unrestricted replay: A card that always reports the same data need be scanned only once. After that, the attacker can replay the captured data at will, and the processing network cannot detect any difference between a replay and successive transactions with a real card. Since we observed the serial output from real POS readers to always be static with respect to cards of type A, we conclude that cards of this type are susceptible to this attack.

2. Replay with race condition: A card that uses a transaction counter and rolling code poses more of a challenge if the back end processing network stores and checks counter values. In such a case, once transaction *n* has been accepted by the network, transactions numbered less than *n* should be declined if presented. However, if an adversary skims a transaction from a card, then replays that transaction to the network before the legitimate user has a chance to use their card, then the charge-processing network should accept the adversary's transactions, and actually decline the legitimate ones. Although the attacker is faced with a counter synchronization problem, such challenges are far easier to defeat than the cryptographic problems on which we prefer to base our security whenever possible.

3. Counter rollover: If a transaction counter is the only changing input to a code, then the number of possible codes is limited by the maximum possible transaction counter value. There are then two cases; in one the counter is permitted to roll over, repeating from the beginning, thus also repeating the codes from the beginning. In the other case the card refuses to engage in additional transactions after the counter is exhausted.

   In the first case, an adversary that enjoys sufficient time in proximity to a card can build a database of all possible counter values and their corresponding codes, and therefore can mimic all possible behavior of the target card. Cards of type B are susceptible to this attack.

   In the second case, denial-of-service can be perpetrated against the card if the attacker has sufficient time in proximity to exhaust the counter by repeated skimming. Our experiments determined that cards of type C exhibit this behavior.

Relay Attack: Even in the case of a hypothetical card we have not examined that combines a challenge-response protocol with a transaction counter, the relay attack may still succeed. In an example relay attack, the adversary consists of a *mole* and a *proxy* that perform a purchase at an innocent user's expense. The mole possesses a clandestine credit card *reader emulator* with a (non-RFID) radio link to the proxy's clandestine credit *card emulator*. The mole sits down or stands next to the user, and the mole's device rapidly discovers the user's credit card. The proxy receiving this relayed signal approaches the POS terminal and initiates a purchase. The proxy presents his credit card emulator to the POS terminal. The emulator receives commands from the POS terminal and relays them to the mole's device, which transmits the commands to the user's credit card. The responses from the user's card are likewise relayed through the mole's device and are broadcast from the proxy's emulator to the POS terminal. The purchase should succeed, and the cost will be charged to the user. Observe that even with application-layer challenge-response or transaction-counter protocols, this attack will still succeed, as protocol messages will simply be relayed between the card and reader.

Cross-contamination Attack: To analyze the feasibility of a cross-contamination attack, we took a credit card of type A, placed it in a sealed envelope, and performed a "Johnny Carson attack" by reading the card through the envelope using our custom programmed TI s4100 reader.

We combined the data thus obtained with address and telephone information looked up in the telephone directory given the cardholder name transmitted through the envelope (for postal mail, the attacker already knows the cardholder address!). Using only this information we placed an online purchase for electronic parts from one of our major research-parts suppliers. Our purchase was successful, and we conclude that the cross-contamination attack is effective for cards of type A and merchants that do not require a CVC.

Privacy Invasion and Tracking: Our eavesdropping transcripts show that personally-identifying information is broadcast in cleartext by every RFID-enabled credit card we have examined.

This must be considered a privacy vulnerability in that automated, full identification of a person carrying an RFID credit card is easily demonstrated in the lab, and should be feasible in the field. This vulnerability is exacerbated by an adversary who could use the full identity disclosure of the RFID credit card to build up a database of associated pseudonyms based on other RFID tags with longer read range that a user may commonly carry.

In addition, the transaction counter found in some of the cards could be exploited by a vendor: by storing the transaction counter, a retailer could tell how often the card was used to purchase goods from others. Heavy card-users might be targeted for specific advertising, for instance.

5 Countermeasures

In addition to fraud detection to limit financial risk, several other countermeasures could significantly reduce risk of fraud and invasion of privacy.

Shielding and Blocking: One countermeasure to some cases of skimming and relay attacks is to ensure that credit cards are unreadable when not in use. A Faraday cage is a physical cover that assumes the form of a metal sheet or mesh that is opaque to certain radio waves. Consumers can today purchase Faraday cages in the form of wallets and slip-cases to shield their RFID-enabled cards against unwanted scanning. Note that this countermeasure offers no protection when the card is in use, since a card must be removed from a shielded wallet before an RF purchase can be made. However, credit card companies ought to at least ship cards through the mail enclosed in a Faraday cage to obviate the dangers of the Johnny Carson attack.

A slightly more sophisticated approach to preventing attack against dormant RFID devices is to disrupt ambient RFID communication. Blocker tags and the RFID Guardian are two examples of devices that can selectively disrupt RFID communications to offer tag owners improved access control.

Signaling Cardholder Intent: As an alternative approach to protection, the credit cards themselves could be modified to activate only after indication of user intent. A simple push-button would serve this purpose, but more sophisticated sensors might serve the same purpose, such as light sensors that render cards inactive in the dark, heat sensors that detect the proximity of the human hand, motion sensors that detect a telltale "tap-and-go" trajectory, etc. Ultimately, credit-card functionality will see incorporation into higher-powered consumer devices, such as NFC-ready mobile phones, and will benefit from the security protections of these host devices, such as biometric sensors and increased computational capacity.

Better Cryptography: Contactless smart cards capable of robust cryptography have long been available. These techniques have already been applied to payment cards in the EMV standards, detailed in Section 6. If personally identifiable data can only be decrypted by authorized readers, then the danger of many of the privacy-invasion attacks discussed in the paper are obviated. Anecdotal accounts suggest payment associations are moving to improve the on-chip cryptographic features of these cards, including challenge-response protocols to further frustrate replay attacks.

6 Discussion

As time goes on and technology costs decrease, we can expect issuers to provide more effective cryptographic protocols. Well-established methods to thwart these attacks already exist and issuers may in fact already be implementing these defenses. But even today, in most cases a financially motivated attacker has easier avenues to exploit than RF based attacks in order to perpetrate financial fraud. For instance, simple cloning of cards is often not sufficient to commit fraud. There are many back-end fraud-detection measures in place to help thwart fraudulent use of card information. Nevertheless, privacy vulnerabilities should be addressed wherever they are found; privacy invasion may lead to financial fraud, but preventing financial fraud is not the only reason to protect privacy.

Comparison with Other Types of Fraud: It is hard to directly compare the security of traditional magstripe cards and RFID-enabled cards. RFID-enabled cards are only more secure than their traditional counterparts against *certain kinds* of attacks. For example, some traditional card reading mechanisms, such as taking a physical carbon copy of the face of the card, leave a physical image of the card in the hands of a possibly adversarial merchant or clerk. In fact, the use of a magstripe generally means handing one's card to a clerk who may have nefarious intent. By contrast, an RFID transaction leaves behind no physical carbon copy; in fact, the card never leaves the cardholder's hands. Certainly, the effort required to obtain an RF copy of the transaction is greater in this case.

Additionally, some RFID-enabled cards include a unique code for each transaction replacing the static data in a magstripe. This mechanism protects against some kinds of attacks, but creates opportunities for new types of attacks that cannot be easily addressed by traditional fraud control (such as cardholder tracking attacks).

Perhaps the most important difference between RFID-enabled cards and traditional cards is the difference in cardholder control. Whereas a traditional magstripe reveals one's name and card number only when the artifact is physically handed to a merchant, an RFID enabled card is in some sense "always on." The card can be scanned and privacy can be compromised remotely and without the knowledge or consent of the cardholder.

Comparison with Other Electronic Cards: The relationship between the cards we examined and the EMV series of standards is unclear. Certainly, in Europe, EMV techniques like the UK's "Chip and PIN" are seeing wide deployment and analysis. But based on our observations, the protocols used by the U.S. contactless cards do not appear in the EMV standards.

It is not clear to us why the U.S. payment associations have chosen to develop new protocols, with significant vulnerabilities, rather than use the more secure protocols that are already deployed in Europe. We can surmise that this choice was motivated by the prevalence of online readers in the U.S. (some of the expense of supporting the EMV standards has to do with support for offline operation) and a focus on contactless operation (whereas most of Europe's cards are contact based).

Policy and Regulation: Several state legislatures have recently considered bills on RFID. For instance, Gov. Schwarzenegger recently vetoed California's SB 768, which would have required interim protections for RFID cards, especially cards carrying personally identifiable information, and a process for figuring out long-term protections. The information made available by the cards, including name and card number are called personally identifiable information (PII) in the parlance of that bill. If signed into law, ID cards issued by the state government carrying PII would have been required to implement mutual authentication and encryption to release the data. While credit cards are not state ID cards, as time goes on we can expect more RFID-related legislation like SB 768 to be introduced. Indeed, U.S. Senator Charles Schumer recently announced his intent to increase federal regulation of RFID-enabled credit cards.

Beyond regulation, it is an important open problem how best to offer incentives to all custodians of personal data to take adequate precautions. The core of the financial industry is risk management. However, we have yet to find a satisfying definition of privacy for the equation of risk management. How do we quantify user privacy when different users place different values on privacy? In hard figures, how does this value affect the bottom line of businesses that are custodians of personal-data?

7 Conclusion

Despite the millions of RFID-enabled payment cards already in circulation, and the large investment required for their manufacture, personalization, and distribution, all the cards we examined are susceptible to privacy invasion and relay attacks. Some cards may be skimmed once and replayed at will, while others pose a modest additional synchronization burden to the attacker. After reverse engineering the secret protocols between RFID-enabled credit cards and readers, we were able to build a device capable of mounting several advanced replay attacks under laboratory conditions. While absolute security and privacy in a contactless-card form factor may be impossible to achieve, we hope that next-generation RFID-enabled payment systems will protect against the vulnerabilities that our study identifies.

Acknowledgement

I sincerely express my deep sense of gratitude to my Guide Prof. Ravindra Ghugare and Co-coordinator Madhuri Ghuge for their valuable guidance, continuous encouragement and support whenever required.

I would like to give sincere thanks to our honourable Principal Dr. Sandhya Jadhav and Head of Department of Computer Engineering Dr. D.R. Ingle for valuable guidance, encouragement and timely help given to me throughout the course of this work.

Last but not least I would like to thanks to all staff member of Bharati Vidyapeeth College of Engineering (Computer Engineering Department) for their valuable guidance and suggestions to brighten me.

References

[1] L. Castro, S.F. Wamba, "An Inside Look at RFID technology", Journal of Technology Management & Innovation, Vol.2, Issue 1, pp.1-14, 2007.
[2] A. Sharma, D. Thomas, "Looking Backwards to Look Ahead: Lessons from Barcode Adoption for RFID Adoption and Implementation", Journal of Information Systems Applied Research (JISAR), Vol. 7, Issue 4, pp. 1-13, 2014.
[3] K. Ahsan, H. Shah, P. Kingston "RFID Applications: An Introductory and Exploratory Study", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 1, pp. 1-7, 2010.
[4] W. Zhang, D. Li, "Research on barcode Image Binarization in Barcode Positioning", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 5, pp. 1-5, 2012.
[5] M. Kaur, M. Sandhu, N. Mohan, P.S. Sandhu, "RFID Technology Principles Advantages Limitations & Its Applications", International Journal of Computer and Electrical Engineering, Vol. 3, No. 1, pp. 1-7, 2011.
[6] S. Jamal, A. Omer, A.S. Qureshi, "Cloud Computing Solution and Services for RFID Based Supply Chain Management", Advances in Internet of Things, Vol. 3 No. 4, pp. 1-7, 2013.

[7] T.S. Heydt-Benjamin, D.V. Bailey, K. Fu, A. Juels, T.O. Hare. "Financial Cryptography and Data Security", IFCA/Springer-Verlag Berlin Heidelberg, USA, pp.2-14 2007.
[8] J. Westhues "Hacking the prox card", Springer, USA, pp.291-300. (2005)
[9] A. Juels, "RFID Security and Privacy: A Research Survey", IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, pp. 1-14, 2006.
[10] B. Preneel, "Cryptographic HASH Functions: An Overview", In the Proceedings of the 6th International Computer Security and Virus Conference (ICSVC), Belgium, pp.1-9, 1993.