ENHANCING PRIVACY PROTECTION SCHEME IN RFID ENABLED BANKNOTE

A.Punitha[1], J.Madhusudhan[2], M.Ganesan[3], P.Karthikeyan[4], Dr.V. Prasanna Venkatesan[5]

[1,2,3,4]Department of Computer Science and Engineering, Sri Manakula Vinayagar Engineering
Pondicherry University, Madagadipet
[1]punithaneetchan@gmail.com
[2]contactmadhu@gmail.
[5]Department of Banking Technology, Pondicherry University, Pondicherry
[5]prasanna_v@yahoo.com

ABSTRACT

Nowadays, money is one of the familiar talks worldwide, and also money is inseparable among the people in tradition. But money suffers from lack of security through money laundering, counterfeits, privacy protection and speediness in currency counts. Thus, to have these securities in money an application of RFID is a banknote attached a tag to determine the authenticity of money and to stop counterfeits. We propose RFID banknote protection scheme by using the optical and the electrical contacts. RFID- enabled notes can be tracked by the legal law agency and verified by the merchant. Effective issues on RFID- enabled notes towards privacy are discussed and new approach is proposed.

Keywords : RFID, Banknote, Privacy Protection, Money.

I. INTRODUCTION

Radio Frequency Identification (RFID), an automatic identification method, typically consists of radio-tag, the reader and backend database system. A tag is a small object attached to a product, animal, or person, and it responds to radio queries from a reader which communicates with the backend system. RFID had attracted much attention in various applications. For example, Wal-Mart using RFID for inventory control and supply chain management is a popular business application now, and it is also the most powerful conductor in RFID development.

In the high technology world of the 21st century, traditional currencies seem out of place. We live in a world that is connected globally; we buy high technology gadgets that are designed in California, manufactured in China and we get our customer support from India. We work in a digital economy that is weightless, borderless, virtual and efficient [1]. Many of us work, shop and socialize in the virtual world of the internet. Yet, we still live in a world driven by cold hard cash.

Cash is inefficient and insufficient for the modern world [2]. In a world where so many business processes have been reengineered, automated and streamlined our handling of cash is still largely a manual endeavor. Handing cash takes time and costs money. Businesses have to count cash then they have to make entries into their computer system.

Then their cash is deposited in the bank where the bank has to go through the same process. Machines can be used to count money but in many places counting is still done by hand. All of this counting and accounting is inefficient. Then there is the matter of security [3].

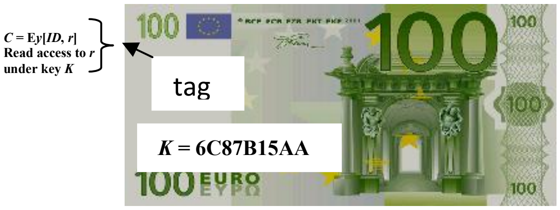

Fig 1. RFID tagged money

The main objective of a RFID-enabled banknote system is to determine the authenticity of money and stops counterfeits, stops money laundering by the new privacy protection sheme and issues on this approach are discussed.

At first, the European Central Bank proclaims that they consider adopting the RFID tag to protect Euro banknotes [4]. Also, Japanese government plans to embed RFID chipsets into their 10,000 Yen notes [5].At Financial Cryptography 2009, Juels and Pappu [6] firstly proposed a practical RFID banknote protection scheme (RBPS) which a note can be tracked by the legal law agency and verified by the merchant. Meantime, an unauthorized attacker cannot scan the notes for tracking if one has no physical contact with the notes.

However, some effective attacks on this Juels and Pappu RBPS severely compromising the privacy of the banknotes' bearers were shown in [7].

II. THE JUELS AND PAPPU RBPS

Except the banknote bearers, there are three parties in theJuels-Pappu RBPS: the central bank, the law enforcement agency (LEA) and the merchant. A central bank issues the banknotes and has a key pair (SKB, PKB) for the signing function Sign(.). LEA is a department of the central bank with the authority to track the notes through EPC network[9 , 10] and aims at tracking the suspected banknotes and arresting forgers. LEA is the only one agency to track the banknote legally, and has a private/public key pair (SKL, PKL) for the encryption function Enc(.).

A merchant scans banknotes when receiving them in a trading, and checks whether banknotes are fake money or not. When finding a forgery, he has the responsibility to notify LEA. The Juels-Pappu RBPS used the radio tag to prevent the banknote from counterfeiting, and simultaneously allowed LEAs to track the banknotes. However, a major concern of a banknote bearer is the privacy. He does not want to be tracked by a unauthorized reader without physical contacting this banknote.

So, Juels and Pappu used two data sources on a banknote to achieve this privacy. One is the optical data printed on banknote, e.g., PDF417 2D bar code [8], which can be physically scanned by a bar code reader and the other is the electronic data stored in a radio tag with the keyed-reading and keyed-writing commands. Figure 1 shows two data sources (the optical data and the RFID data) on a banknote. There are two access-keys DM= h(E) and DL in our RBPS.

An access-key DM (same to an access-key D) in the Juels-Pappu RBPS, is used for a merchant, while a key DL is a global key for LEA. A central bank can create different DL for the different banknotes and deliver this global key to LEAs with the authority to track the notes through EPC network [5]. If the central bank distributes the DL to every LEA, the banknotes can be tracked by any LEA like the Juels-Pappu RBPS.

The tag's size with more memory cells increases and is not suitable on a banknote. This approach trades one more command for saving one memory cell. In the approach, only added one extra memory cell, the ε-cell is keyed-readable with a key DM or DL, and unwritable. Other two memory cells, the γ-cell and the δ-cell, and the optical data are same to the Juels-Pappu RBPS. Moreover, three commands "(γ)+(ε)→(γ); R(ε)→(ε); (γ)+(ε)→(γ)" are performed by a tag when the γ-cell is queried. Also, a command "(γ)+(ε)→(γ)" is performed by the tag after that the γ-cell is keyed-written. The optical and RFID data of this approach are illustrated in Table I.

A. Banknote Creation

B creates banknotes, determines which L tracks which banknote, and delivers the global tracking key DL to LEAs through EPC network

(C-1) B uses a secret key to sign the serial number and the Denomination (Si||deni) and then prints Si and the signature Σi= Sign (SKB,Si || deni) on a banknote

(C-2) B selects two random numbers, r1 and r2, and stores them in the δ-cell and ε-cell, respectively.

(C-3)B computes Ci = Enc (PKL, Σ ||Si, r1)+ r2 and stores in the γ-cell.

(C-5) B sets the reading/writing capabilities of memory cells as follows: the γ-cell is universally-readable and keyed writable with a key DM; the δ-cell is keyed readable/ keyed-writable with a key DM; the ε-cell is keyed-readable with a key DM (or DL) and un-writable.

TABLE I : OPTICAL AND RFID DATA ON THE BANKNOTE

<table>
<tr><td colspan="3">RFID</td></tr>
<tr><td>Cell γ universally readable/keyedwritable</td><td>Cell δ keyed-readable/keyedwritable</td><td>Cell ε keyed-readable/unwritable</td></tr>
<tr><td>$Ci = Enc(PK_{L,}\Sigma \| Si, r_1) + r_2$</td><td>$r1$</td><td>$r2$</td></tr>
<tr><td colspan="3">Optical</td></tr>
<tr><td>S</td><td colspan="2">$\Sigma i = Sign\ (SK_B, S \| den_i)$</td></tr>
</table>

B. Banknote Verification

M verifies banknotes while receiving from a consumer

(V-1) M scans the optical region and obtains Si and Σi, and then computes a access-key DM=h(Σi).

(V-2) 1. M transmits a read query to tag for reading the δ-cell and ε-cell.

2. Tag challenges M by sending a nonce.

3. M computes h (DM || nonce) and responds to tag.

4. Tag verifies h (DM || nonce. After successful verification, a tag sends r1 and r2 to M.

(V-3**)** M reads Ci from the γ-cell.

(V-4) M uses r1 and r2 to verify C =? Enc (PKL,

Σi || Si, r1) + r2.

(V-5) After reading the γ-cell, the following commands will start by a tag: $(\gamma)+(\varepsilon)\rightarrow(\gamma)$; $R(\varepsilon)\rightarrow(\varepsilon)$; $(\gamma)+(\varepsilon)\rightarrow(\gamma)$.

The operation is described as follows: a tag firstly XORs the random number r2 with the value of γ-cell and stores the result Enc (PKL, Σi || Si, r1) into the γ-cell. Then, randomizes the r2 in the ε-cell to r′2 , and do the command $(\gamma)+(\varepsilon)\rightarrow(\gamma)$ again. Finally, the γ-cell has (Enc(PKL, Σi || Si, r1) + r′2).

C .Banknote Anonymization

M re-encrypts the ciphertext after verification

(A-1) M randomly chooses 1 r′ and keyed-writes it into the δ-cell.

(A-2) M computes Ci= Enc (PKL, Σi □ Si, r1) and keyed-writes it into the γ-cell.

(A-3) After writing the γ-cell, a command (γ) + (ε) → (γ) is started by a tag, i.e., the value of ε-cell (r′2) is XOR-ed with the value of γ-cell and stored back into the γ-cell. Finally, the γ-cell has Enc (PKL, Σi|| Si, r1) + r′2.

D. Banknote Tracking

L tracks a banknote without the optical contacting

(T-1) 1. L transmits a read query to tag for reading the ε-cell.

2. Tag challenges L by sending a nonce.

3. L computes h (DL || nonce) and responds to tag.

4. Tag verifies h (DL ||nonce), and sends r2 to L after successful verification.

(T-2) L reads Ci from the γ-cell.

(T-3) L uses r2 to recover Enc(PKL, Σi □ Si, r1) from Ci+r2.

(T-4) Decrypts Enc(PKL, Σi □ Si, r1)to get(Σ ||

Si) .

(T-5) L verifies the signature(Si || den) =? Veri(

PKB,Σi) and obtains a serial number Si for

tracking.

(T-6) After reading the γ-cell, a command (γ) + (ε)→(γ) is started by a tag.

E. Vulnerabilities

Determining the vulnerabilities in the scheme for addressing privacy issues such as pick pocketing, data recovery, cipher text tracking, access-key tracking, cookies of service, sleeping and dead banknotes in proposing system.

1) Cryptographic weakness: The Fujisaki: Okamoto scheme has been applied to ElGamal encryption in an insecure way, enabling the data recovery attack. This in turn enables the aggressive variant of the ciphertext tracking attack.

2) Static response between re-encryptions: In particular the ciphertext tracking attack has been enabled by the static response from the tag when reading the γ memory cell.

3) Static access key: The static access key that is used to read the δ meory cell and to write to both memory cells allows it to be stored in a database for later use or allows an eavesdropper to query the tag afterwards.

4) Lack of on-tag input validation: Because the tag doesn't validate any information that is written to either memory cells, it is open to the denial of service attack.

III. THE PROPOSED RBPS

In the new protection scheme, going to have three contents in the RFID tag such as serial number, denomination and signature. This information is going to be encrypted in the tag memory by using to El Gamal encryption in a secure way. There are two memory are used in RFID Tag such as γ cell and δ cell. Table II shows two data sources (the optical data and the RFID data) on a banknote. Used two data sources on a banknote to achieve this security, one is the optical data printed on banknote, which can be physically scanned by a reader and the other is the electronic data stored in a radio tag with the keyed reading and keyed writing commands. Notation of the serial number, the denomination and the signature of a banknote are S, den and the fig. private/public key pair (SKL, PKL) for the law enforcement agency (LEA). Private/public key pair (SKM, PKM) for the Merchant. It includes the following modules of this new protection scheme, such as Creation, Verification, Anonymization and Tracking, are described step by step. Addressing the privacy issues on this protection scheme such as

1) Pick pocketing

2) Data recovery

3) Cipher text tracking

4) Access- key tracking

5) Cookies threat

6) Denial of service

7) Sleeping and dead banknotes

A. Banknote Creation

B creates banknotes, determines which L tracks which banknote, and delivers the global tracking key DL to LEAs through EPC network

1. B uses a secret key to sign the serial number and the Denomination (Si||deni) and then prints Si and the signature Σi= Sign (SKB ,Si || deni) ◌ Sign (SKB ,Si || fig)on a banknote.

2. B selects two random numbers, r1 , and stores them in the δ-cell respectively. B computes C=((Enc(PKL,Σ||Si,r1)◌(Enc(PKB,Σ||fig,r1) ◌ r1) and stores in the γ-cell.

3. B sets the reading/writing capabilities of memory cells as follows: the γ-cell is un-readable and keyed writable with a key DM(or DL),the δ-cell is keyed readable/ keyed-writable with a key DM(or DL).

B. Banknote Verification

M verifies banknotes while receiving from a consumer

1. M scans the optical region and obtains Si, Σi, and fig then computes a access-key DM=h(Σi).

2. M transmits a read query to tag for reading the δ-cell and γ -cell.

3. Tag challenges M by sending a nonce.

4. M computes h (DM || nonce) and responds to tag.

5. Tag verifies h (DM||nonce. After successful verification, a tag sends r1 to M.

6. M reads Ci from the γ-cell.

7. M uses r1 to verify C =? ((Enc(PKL,Σ||Si,r1)◌(Enc(PKB,Σ||fig,r1) ◌ r1)

8. After reading the γ-cell, the following three commands will start by a tag: (γ)+(δ)→(γ); R(δ)→(δ); (γ)+(δ)→(γ). The operation is described as follows: a tag firstly XORs the random number r1 with the value of γ-cell and stores the result Enc (PKL, Σi ||Si, r1) into the γ-cell. Then, randomizes the r1 in the δ-cell to r′1 , and do the command(γ)+(δ)→(γ) again. Finally, the-γ-cell has((Enc(PKL,Σ||Si,r1)◌(Enc(PKB,Σ||fig,r1) ◌ r’1).

C .Banknote Anonymization

M re-encrypts the ciphertext after verification

1. M randomly chooses r′1 and keyed-writes it into the δ-cell.

2. Mcomputes C=((Enc(PKL,Σ||Si,r1)◌(Enc(PKB,Σ||fig,r1) ◌ r1) and keyed-writes it

   into the γ-cell.

3. After writing the γ-cell, a command (γ) + (δ) → (γ) is started by a tag, i.e., the value of δ -cell (r′1) is XOR-ed with the value of γ-cell and stored back into the γ-cell. Finally, the γ-cell has ((Enc(PKL,Σ||Si,r1)◌(Enc(PKB,Σ||fig,r1) ◌ r’1).

TABLE II : OPTICAL AND RFID DATA ON THE BANKNOTE

RFID Electrical contact	
γ cell	δ cell
C=((Enc(PKL, Σ||Si,r1)◌(Enc (PKB,Σ||fig,r1) ◌r1)	r1
Optical contact	
S, fig	Σ=Sign(SKB,S||den)◌ Sign(SKL,S||fig)

D. Banknote Tracking

L tracks a banknote without the optical contacting

1. L transmits a read query to tag for reading the δ -cell.

2. Tag verifies h (DL ||nonce), and sends r1 to L after successful verification.

3. L reads Ci from the γ-cell.

4. L uses r1 to recover

((Enc(PKL,Σ||Si,r1)◌(Enc(PKB,Σ||fig,r1) ◌ r1from Ci

5. L verifies the signature(S ||den||fig) =? Veri(PKB,Σi,fig) and obtains a serial number Si for tracking.
6. After reading the γ-cell, a command (γ) + (δ) → (γ) is started by a tag. As the step (V-5), the cipher text will be changed, so that can avoid the cipher text tracking.

E. Cryptographic Analysis

Encryption and signature schemes can be chosen among the existing secure schemes. However they should bring security without involving high overhead. Juels and Pappu suggest to use an El Gamal-based encryption scheme using elliptic curves. Let G denote an elliptic-curve-based group with prime order q and let P be a generator of G. Let $SKL = x\ E\ R\ Zq$ be the law enforcement agency private key and $PKL = Y = xP$ the corresponding public key. A message $m\ E= \{0, 1\}^n$ where n is reasonable sized, is encrypted with the El Gamal scheme under the random number r as follows: Enc($PKL; m; r$) = ($m + rY, rP$), Since El Gamal encryption scheme is not secure against adaptive chosen ciphertext attacks, Juels and Pappu suggest to use the secure integration method due to Fujisaki and Okamoto , the message m is then encrypted as follows: Enc¤($PKL\ m\ r$) = (Enc($PKL; r,h1(r||m)),h2(r)$ ◌ m) where $h1$ and $h2$ are two hash functions from $\{o,1\}^*$ *to* $\{o,1\}^n$.

F. Security Analysis

Our scheme ensures the privacy of the banknotes' bearers against the data recovery attack, the access-key tracking, the cookies threat, the cipher text tracking, and the denial of service attack. However, a dishonest merchant and the privacy issue that a backward channel can be eavesdropped by an attacker are beyond the scope of the privacy for our RBPS. The argumentation that an attacker cannot intercept a backward radio channel from a tag to a reader is reasonable due to the following rationales. Generally, there are two eavesdropping ranges of RFID protocols- the reader-to-tag eavesdropping range (i.e. a forward range), and the tag-to reader

Eavesdropping range (i.e. a backward range). In a forward range, since a reader transmits information to a tag with a higher power than a tag, so adversaries could easily eavesdrop with the information sent by a reader to a tag, can claim that an attacker can intercept a forward channel for an access-key. However, in a backward range, since a passive tag on banknote has a shorter communication range. Also, a tag has a short transmission time than a reader (note: a reader usually broadcasts radio signal as long as necessary to bring sufficient power to a tag and wait its response).

A tag just sends the numbers $r1$ and $r2$ in an extremely short time. As a result, if adversaries tend to eavesdrop the information sent by a tag, they need a reader staying near the tag and scanning all time. So, it is almost impossible to illegally steal $r1$ and $r2$ while the note's bearer is not aware of an adversary.

The attacks, exclusive the ciphertext tracking, are attributed to the disclosure of the access-keys *DM* and *DL*. Hence, we first describe why an attacker cannot steal *DM* and *DL*. An attacker does not physically contact the banknote, so he cannot retrieve the Σ. to compute $DM=h(\Sigma)$. Also, an attacker cannot intercept the EPC network to get a *DL* because a secure VPN network should be established between all LEAs and a central bank. Moreover, we use the challenge-response strategy and so that an attacker only has a *nonce* and $H(DM||nonce)$ (or $H(DL||nonce)$) but he cannot recover the *DM* (or *DL*).

The goal of the re-encryptions is to prevent banknotes tracking, as we mentioned. If an attacker does not have optical contact with a given banknote, then he should not be able to track it in the long-term. Actually, when a tag owns a unique access-key and responds if and only if the key sent by the reader is the valid one, this key can be used to track the tag. On may think that the tag could thwart such an attack by replying with some garbage when the access-key is wrong, instead of remaining silent. Unfortunately, sending static garbage opens a new way to perform tracking attacks, and requiring the tag to be able to generate random garbage is not yet realistic due to the low capability of such devices.

The pick pocketing attack and making the banknote sleeping and dead. These two attacks are caused by the native property of a RFID tag but not the RBPS itself, and usually are overcome by a hardware solution.

A clever way to abuse the tag is to put the cookie only in the δ -cell: since the value *r* stored in this cell is a random number, it can be used to store some information. Obviously, the *γ* -cell value will have to be re-encrypted with the new random number. This kind of cookie will be untraceable and will stay available until the next re-encryption.

When a merchant finds a discrepancy on a banknote, he cannot accept the payment and should warn the law enforcement agency. This could however be used to harm banknote bearers: all that is required is to input incorrect data into either δ and γ, by means of having encryption by using both merchant and the LEA, cant access to the optical data but also cant able to perform the first step of the attack because of the involvement of the public key of both merchant and the LEA.

G. RFID Challenges

One of the biggest problems concerns cross tag reading. When passive tags are employed the RFID reader emits a signal which then turns the tag on causing it to broadcast its signal. The RFID reader can cause several tags to broadcast at once. For some applications that may be desirable but for most it presents a real problem. Technical solutions will have to be designed that prevent that problem from occurring.

Technical standards are another challenge that should be addressed in advance of implementing r-money solutions. Since economic crime is increasingly a transnational phenomenon, the solution has to be a multinational effort. For that reason, international agreement for the technical standards of the RFIDs embedded in money is desirable. The national standards of the UK may be presented on one tag and the standards and requirements of the European Union on another. Also, each tag would likely employ different encryption protocols.

RFIDs are vulnerable to physical abuse. At the moment there is nothing to prevent people from breaking the RFIDs. Such acts would make it necessary to replace bank notes – an expensive undertaking. Even if laws were created that made the destruction of RFIDs in money illegal they would have little impact on a crime that is carried out in private.

H. CONCLUSION

The main aspects of banknote protection and described the Juels and Pappu scheme, which is based on both Optical and Radio Frequency Identification systems. We show that two parties can benefit directly from the use of tags in the banknotes: the central bank and the law enforcement agency, both profiting from this system by enforcing banknote tracking and anti-counterfeiting, stop money laundering, improved speed of the process. RFID tags embedded in bank notes have the potential to provide law enforcement agencies with another tool to detect, prevent and solve crimes.

RFID tags embedded in bank notes would provide a greater degree of traceability of money. At the same time, r-money would provide businesses with improved internal controls over cash. Eventually, they may provide a greater degree of efficiency in their handling of money. This paper has addressed some issues surrounding r-money from the perspective of the information systems discipline. The real issues surrounding r money are not associated with having RFID tags embedded in bank notes. The tags just allow computer information systems to be able to sense objects.

The real issues are associated with the information systems that support r-money. Furthermore, some described issues are beyond the scope of the banknote protection and we think that our contribution should be taken into account in future designs of RFID privacy protection schemes.

ACKNOWLEDGMENT

I would like to thank my guide Mr.J.Madhusudhanan, Assistant Professor, Department of Computer Science and Engineering, for providing him valuable guidance and suggestions for my project “Enhancing privacy protection scheme in RFID enabled banknotes”. I thank him for the continuous encouragement and the interest shown on me to bring out my project work at this stage and also for providing the freedom that i needed and wanted.

REFERENCE

[1]. Sharma, S.K. (2005) *‘Socio-economic impacts and influences of e-commerce in a digital economy’*, in Kehal, H.S. and Singh, V.P. (Eds.): Digital Economy: Impacts, Influences and Challenges, Idea Group Publishing, Melbourne.

[2] Gemmell, P.S. (1997*) ‘Traceable e-cash’*, Ieee Spectrum, Vol. 34, pp.35–37.

[3] Int. J. Business Governance and Ethics, ‘*Curbing economic crime with RFID enabled currency’*Vol. 5, Nos. 1/2, 2010.

[4] J. Yoshida, *“Euro Bank Notes to Embed RFID Chips by 2005,”* available at: http:// www.eetimes.com/story/OEG20011219S0016.

[5] M. Roberti, *“The Money-Trail - RFID journal,”* available at: http://www. rfidjournal.com/article/articleview/523/ 1/2/.

[6] A. Juels, and R. Pappu,*’Enhancing Privacy and Security in RFID-Enabled Banknotes’*2009 IEEE International Symposium on Parallel and Distributed Processing with Applications.

[7] G. Avoine, “*Privacy Issues in RFID Banknote Protection Schemes,”* The 6th International Conference on Smart Card Research and Advanced Applications, pp. 33-48, 2004.

[8] A. Juels*, “RFID Security and Privacy: A Research Survey,”* IEEE Journal on Selected Areas in Communications vol. 24, pp. 381-394, 2006.

[9] *“EPCglobal: The EPCglobal Network: Overview of Design, Benefits and Security,”* available at: http://www.epcglobalinc.org.

[10] K.S. Leong, and ML., Ng, “*A Simple EPC Enterprise Model,”* Auto- ID Labs Workshop Zurich 2004, available at http://www.m-lab.ch.

[11] B. Fabian, O. Günther, *"Security Challenges of the EPCglobal Network," Communications of the ACM*, 52(7), pp. 121-125, 2009.

[12] Yu-Yi Chen, Jun-Chao Lu, Shin-I Chen, Jinn-Ke Jan*" A Low-cost RFID Authentication Protocol with Location Privacy Protection"* 2009 Fifth International Conference on Information Assurance and Security .

[13] Li, Y.Z., Cho, Y.B., Um, N.K., and Lee, S.H. (2006): *"Security and Privacy on Authentication Protocol for Low-cost RFID"*. 2006 International Conference on Computational Intelligence and Security. 2:3-6.

[14] B. Nath, F. Reynolds, and R. Want, *"RFID Technology and Applications,"* IEEE Pervasive Computing, vol. 5, no. 1, 2006, pp. 22-24.

[15] Rushi Vyas, Student Member, IEEE, Vasileios Lakafosis, Student Member, IEEE, Amin Rida, Student Member, IEEE, Napol Chaisilwattana, Scott Travis, Jonathan Pan, and Manos M. Tentzeris, Senior Member, IEEE, *"Paper-Based RFID-Enabled Wireless Platforms for Sensing Applications"*

[16] Yung-Chin Chen, Wei-Lin Wang, Min-Shiang Hwang Asia University, Asia University, National Chung Hsing University,*" RFID Authentication Protocol for Anti-Counterfeiting and Privacy Protection"*

[17] L. Yang and M. M. Tentzeris, *"Design and characterization of novel paper-based inkjet-printed RFID and microwave structures for telecommunication and sensing applications,"* in *IEEE MTT-S Int. Microw. Symp. Dig.*, Jun. 2007, pp. 1633–1636.

[18] Gan Yong, He Lei, Li Na-na, Zhang Tao School of Computer and Communication Engineering Zhengzhou University of Light Industry Zhengzhou, China ,*"An Improved Forward Secure RFID Privacy Protection Scheme"* 2010 2nd International Asia Conference on Informatics in Control, Automation and Robotics

[19] sung kook park, younghee lee, ji yeon cho, seo hyoung han and bong gyou lee graduate school of information, yonsei university 134 shinchondong, seoul 120-749, korea, *"The roles of rfid in ubiquitous computing"*, iadis international conference wireless applications and computing 2008.

[20] Xiaoyun Chen, Youli Su, Hui Xiong, Yukai Yao, Guohua Liu, Min Yue School of Information Science & Engineering, Lanzhou University, PRC (730000) Lanzhou, China*, " An Improved Authentication Approach to Enhance Security and Privacy in RFID System"*, 2010 Second International Conference on Intelligent Human-Machine Systems and Cybernetics