INFORMATICA, 2016, Vol. 27, No. 4, 723–732


DOI: http://dx.doi.org/10.15388/Informatica.2016.108

# An Authentication Protocol for Lightweight NFC Mobile Sensors Payment

Tung-Huang FENG[1], Min-Shiang HWANG[1,2]*, Liang-Wei SYU[1]

[1]*Department of Computer Science and Information Engineering, Asia University*
*No. 500, Lioufeng Raod, Wufeng Shiang, Taichung, Taiwan*
[2]*Department of Medical Research, China Medical University Hospital*
*China Medical University, Taiwan*
*e-mail: mshwang@asia.edu.tw*

Received: September 2015; accepted: April 2016

**Abstract.** Following the White Paper HCE that Google released in August 2014, it was expected that NFC mobile phone payment would cause a wave of security discussion. After all, Android HCE will allow anyone to develop his own payment service on the Android platform to get rid of restriction from telecommunications, financial industries, or third party trust centers. On this security mechanism observation period, we propose a lightweight authentication protocol on NFC mobile sensors payment. Through introducing this security agreement, it not only allows individuals to have privacy protected, but also can prevent malicious attackers from the track, which will make legitimate Tags verified, while effectively preventing an illegal Tag from being forged as an authenticated Tag. Therefore, constructing full security mechanisms will benefit to the development of mobile NFC payment.

**Key words:** near field communication, sensing payment, user identification.

## 1. Introduction

In recent years, RFID (Radio Frequency Identification) is used widely, so RFID technology has become an important technology for the future development of the global industry (Lau *et al.*, 2010; Lehlou, 2009; Ngai *et al.*, 2007; Wen, 2010). RFID possesses no impact on environment, overwritability, non-contact sensor, unique traceability and other characteristics. Advantages and ease of use of RFID are better compared with traditional barcodes. Therefore, it should bring the bright prospects of RFID industry (Cui, 2016).

NFC (Near Field Communication) is a membership of RFID (Saparkhojayev *et al.*, 2014; Want, 2011), and also uses the 13.56 MHz HF of RFID frequency bands. The main difference between them is that NFC is two-way communication, single scan and communication only within 10 centimeters. Thus the use of RFID can solve the largest threat facing eavesdropping (Chikouche *et al.*, 2015; Qian *et al.*, 2016). Also, thanks to the advances of the hand held communication, everyone has at least one smart phone in one's lifetime, and NFC phones use Host Card Emulation (HCE) technology modelled as a Tag

*Corresponding author.

placed in the personal cell phone owned by the consumer without increasing a trace of weight so that owning the card is no longer a burden. Therefore, consumers no longer worry about the increase of consumer cards, and are no longer afraid to apply for a new card. Then they could accept a variety of membership cards recommended by a store. Because of the analog Tag convenience, all stores not only can launch their own exclusive member benefits Tag to their memberships, but also can change its discount program in response to consumer trends at any time. Also it is worth mentioning that the change in the personal thick wallet can be loaded into individual handsets to help consumption. It is estimated that these modern consumer habits will make become a history people carrying a wallet. It will be replaced with a type of electronic wallet with a NFC mobile phone.

Therefore, we can conclude that the importance degree of holders to keep this Tag of a new mobile phone carrier is much larger than a thin RFID Tag card (Wei *et al.*, 2011). For the risk degree suffered from loss of property, a NFC Tag is less risky than a RFID card. Therefore, NFC is more suitable for mobile payments when compared to RFID. Thus, in view of the advantages of NFC payment, there are more and more mobile phone manufacturers willing to launch NFC built-in mobile phone market, and they attempt to join the waves of mobile payment; it will completely change the face of human intelligence life.

The NFC payment mode seems to have a simple operation, but ecologically it's a really complex type of payment (Chi *et al.*, 2015; Ling *et al.*, 2017). It involves the sectors including a mobile phone manufacturers, telecom operators, carriers, financiers, service providers, shops and trust services. If you want to achieve the prosperity, absolutely, it requires an open environment that provides a development platform and allows anyone to develop his own payment service on the platform, where all development can be expected. Fortunately, Android platform has been taking the lead in this trend, and published HCE (Host Card Emulation) white paper in August 2014 (Smart Card Alliance, 2014), so the ecological parties add another Host option outside SIM Card, Security Element (SE), and Trusted Service Manager (TSM) security Mode fiduciary services (Pannifer *et al.*, 2014). It intends to get rid of the shackles of payments in the ecosystem, and create a consumer paradise of the pay action.

As Google HCE white paper claimed, someone still has a lot of doubts about HCE security. To arrange features in NFC mobile phones in pairs to communicate with the parties without handshake so as to have immediate interoperability, and to develop the habits of consumer transactions, it is difficult for consumers to make consumption as same as the RFID Tag card directly connected to Reader on cash register system POS (Point of Sale) terminals for completion of the transaction. In this context, traditional cryptography has some limitations either in symmetric encryption or asymmetric encryption. Therefore, it demands for a lightweight mobile sensors NFC payment authentication protocol to cope with the habits of consumer transactions. That is what this article is seeking to solve.

Payment constituent elements of NFC mobile sensors are similar to those of RFID. They include three types: a simulation Tag in consumer phone, the store POS cash register system combined with a Reader, Back-end Database, etc. (Cao and Shen, 2009; Chen *et al.*, 2011; Zhang and King, 2008). It operates on the reader by a non-contact and short-range way, reads the Tag information, and then transmits it via reader back to the database access.

Since it is by short distance and non-contact reading way, it is very important to confirm the legitimate reader. In addition, when NFC Tag is placed in the phone, it indirectly uses the phone itself to track, locate and identify, which will be harmful to individual privacy concerns. Therefore, NFC mobile sensors payment authentication protocol must overcome these security and privacy issues to really realize available security mechanisms.

The following sections of this article are organized as follows: Section 2 describes related research more suitable for NFC mobile sensors payment authentication. Section 3 proposes the authentication mechanism in this paper. Section 4 describes security threat. Section 5 analyses the safety of this article's authentication mechanism. Section 6 analyses the performance; and finally a conclusion is proposed about the contribution of the research results.

## 2. Related Research

Many scholars have proposed Tag systems with security in order to solve security and privacy issues on Tag in the past. In recent years, scholars establish Tag security based on a hash function. Tag has some limitations to use a conventional encryption technology due to limited storage and computing. Therefore, it would be more appropriate to perform a simple arithmetic, such as the hash functions. Especially, in case of NFC payment induction, it is unlikely for a RFID card to be placed on reader waiting for transaction ends. Usually after induction, a user's cell phone will be readily withdrawn, and therefore it needs a faster authentication protocol to meet consumer's habits. Lee recommended low-cost Tag authentication protocol (Lee *et al.*, 2005) using only two one-way hash function operations, which is very efficient. The safety mechanism proposed by Lee is shown in the following:

**Step 1:** Reader sends Request to give Random Number $N_R$ to Tag.
**Step 2:** Tag just takes the left half of the ID, then conveys to Reader after calculating $hL(ID||N_R)$ and $h(ID)$.
**Step 3:** Reader sends this message forwards to Back-end Database.
**Step 4:** Back-end Database verifies the legality of Tag; if successfully validated, compute $hR(ID||N_R)$ and then transfer to Reader.
**Step 5:** After Reader receives messages from Back-end Database, it sends them to Tag.
**Step 6:** When Tag receives the message transferred by Reader, and successfully verifies $hR(ID||N_R)$, it processes transactions with Reader later.

Since Lee's method generates a new Random Number each time, it is possible to effectively prevent Spoofing Attack; however, scholars (Kim *et al.*, 2008; Piramuthu, 2007; Syamsuddin *et al.*, 2008) stated that this method can't resist Traceability Attack.

Additionally, Song and Mitchell (2008) proposed a low-cost Tag authentication protocol. Its performance is better than Lee's (2008), but Rizomiliotis *et al*. proved Song-Mitchell protocols are insecure (Rizomiliotis *et al.*, 2009), because they are subject to simultaneous attacks between Tag and Reader which is forged as legitimate reader. Therefore, Rizomiliotis *et al*. continued inheriting performance advantages of Song–Mitchell's

Table 1
Notation.

| | | | |
|---|---|---|---|
| $h$ | One-way hash function | $i$ | Reader numbers |
| $hL$ | The hash value of the left half number | $j$ | Tag numbers |
| $ID_R$ | Reader identification code | $l$ | Bit length |
| $ID_T$ | Tag identification code | $\|\|$ | Concatenation operation |
| $N_R$ | Random value of Reader end | $\gg$ | Shift right operation |
| $N_T$ | Random value of Tag end | $\leftarrow$ | Replace operation |
| $N*'$ | New random value | $\oplus$ | XOR exclusive operand |

protocol to improve and claim that their protocol is better than Song–Mitchell's. The biggest advantage of these two protocols is that they can store a value only in Tag and save Tag storage space. However regarding these two protocols, it is assumed that the channel is safe between the Reader and Tag. In fact, the more reasonable assumption should be that there is an insecure channel between the Reader and Tag. Yeo *et al.* (2009) proposed an assumption close to the similar relative facts. Different from Song and Mitchell (2008) and Rizomiliotis *et al.* (2009), Yeo *et al*.'s study is based on Mobile Agent Tag environment. The protocol requires an additional mobile agent authentication design, while Song–Mitchell and Rizomiliotis *et al*'s. protocols don't require it. This paper continues to improve the advantage of protocol in Song–Mitchell and Rizomiliotis *et al.*, and design a lightweight security protocol for low-cost NFC mobile sensors payment under unsafe circumstances.

## 3. Research Methods

In the following, the lightweight protocol method about NFC mobile sensors payment authentication was proposed. This proposal continues the spirit of SM Lee's simple security mechanism and improves the protocol proposed by Song–Mitchell and Rizomiliotis, and then considers the environment used in practical mobile payment. To save the storage costs of Cloud Database, Reader and Tag simply store ID and Nonce random value as identification code and verification code. These can reach mutual authentication between Reader-Tag, Back-end Database-Reader and Back-end Database-Tag. Therefore, we called it a lightweight security mechanism. The mechanism used the hash and MAC methods, and in Synchronization, it used updated technology to exert transaction verification capabilities so as to achieve the characteristics of Tag security needs. For a clearer explanation of the protocol, Table 1 lists symbols of associated instructions.

The environment set up for the protocol contains only mobile Tag and Reader beep induction phase to use NFC channel, and the others are assumed to be in an insecure channel. The security mechanisms are distinguished by setting and authentication. The following describes the whole process of the protocol as follows.

### 3.1. *Initial Stage*

Back-end database manages all the stores' Reader that participates in the pay operation, and consumers' Tag to pay with NFC mobile sensors. After the participants are regis-

tered, the managers give exclusive identification codes to stores' Reader and consumers' Tag, which are $ID_R$ and $ID_T$, respectively, and then handed over to their respectively stored $(ID_R, N_R)$ and $(ID_T, N_T)$ to prepare for a certification phase. After each successful transaction, the verification code $N_R$ and $N_T$ of each party will be updated as $N'_R$ and $N'_T$. $ID_R$ and $ID_T$ operated by shift operation are updated by XOR operation with original $N_R$ and $N_T$ and used as their next transaction for identification codes and authentication codes.

Because this mechanism maintains the synchronization based verification, in case of an occurrence of sync state, it needs to re-apply this back to the setting stage.

### 3.2. *Certification Phase*

Through the authentication phase, stores' Reader and consumers' Tag are the public authentication entry trusted by back-end managers. Therefore, in this stage, transaction parties, besides the exchange of information between them, must pass the relevant certification information with back-end databases to complete the certification so as to achieve the purpose of the security of transactions. The contents of each step are described in the following:

**Step 1:** After the store Reader induces the consumer Tag, Reader generates new $N'_R$ and performs the hash processing of Reader's $N'_R$; and the left part of $M_R = hL(N'_R)$ is then sent as a message of the Tag end. Messages sent to Back-end database include identification code $ID_R$ of the current Reader, and hashed $h(ID_R||N_R)$ and $N_R \oplus N'_R$ sent, which wait for a response of authentication information.

**Step 2:** After consumers' Tag is successfully connected with the stores' Reader, new $N'_T$ generated by Tag performs the hash process, and then $M_T = hL(N'_T)$ of the left parts is used as a message transmitted to the Reader-end. In addition, identification code $ID_T$ of the current Tag is hashed to get $h(ID_T||N_T)$ and $N_T \oplus N'_T$, which are sent out to await the response of authentication information.

**Step 3:** After the Back-end database receives Reader messages in the 1st step, the first $ID_R$ received by a hash operator is compared with the index value in the database to quickly search $h(ID_R)$ to find the relative $(N_R)_i$; then it receives $ID_R$ and finds $(N_R)_i$ hash together to verify $h(ID_R||N_R)$ transmitted from Reader. If it's successful, it means that stores are involved in the transaction. If not successfully verified, it means it's a non-legal Reader; therefore it discards this information and returns the message of authentication failure so that the transaction will not be established. To the message received from Step 2, Back-end database also performs the same procedure on Reader as described above to check $h(ID_T||N_T)$; if it's successful, it means the $j$ consumer is involved in the transaction. The consumer authentication is completed in this transaction.

Therefore, when the consumers' $(N_T)_j$ and the stores' $(N_R)_i$ are confirmed, Back-end database will get $N'_T$ and $N'_R$ which are solved from consumers' Tag $N_T \oplus N'_T$ and stores' Reader $N_R \oplus N'_R$, which are sent back to Tag and Reader for inverse certification. Thus, the stores' Reader will receive $M'_T = hL(N'_T)$ and $h(N'_R)$.

**Step 4:** On the other hand, Back-end Database will also return $M'_R = hL(N'_R)$ and $h(N'_T)$ to the consumer Tag for final confirmation before trade transaction.

**Step 5:** Store's Reader compares the information $M_T$ transferred by Tag-end at the 2nd step with the information $M'_T$ transferred by Back-end databases. At some time, it also verifies if $h(N'_R)$ matches the hash values of its own $N'_R$. If they are consistent, then it achieves certification. Because only $N_T$ and $N_R$ stored in Back-end Database can solve $N'_T$ and $N'_R$, therefore, after successful authentication, it can carry out the transaction. And it updates $N_R$ as $N'_R$ after transaction, and operates $(N'_R \gg \frac{1}{4}) \oplus N_R$ to update the original $ID_R$ used for next transaction.

**Step 6:** Checked and compared with consumers' Tag-end, Reader end in the 1st step sends information $M_R$ with its own $h(N'_T)$, a message $M'_R$, and $h(N'_T)$ transferred by Back-end database. If it's successful, the transaction may be conducted. And after transaction, it updates $N_T$ as $N'_T$, and operates $(N'_T \gg \frac{l}{4}) \oplus N_T$ to update the original $ID_T$.

Back-end database records the transaction content based on the results from transactions after it confirms the completion of transaction. At the same time, use the same procedures on the 5th and the 6th steps to carry $\gg$ displacement and $\oplus$ *XOR* operation to update both sides of the transaction $h(ID_R)$, $h(ID_T)$ and original $N_R$ and $N_T$. Thus it completes the certification of all of the transactions on tripartite party.

## 4. Security Threat

Tag security protocol simultaneously considers the privacy and security for an authentication protocol, and its relation threats are outlined as follows.

### 4.1. *Privacy*

- Tag tracing: as long as the attacker accesses Tag's $ID_T$, whether it is a legitimate or illegitimate reader, through the collection and analysis, he can easily grasp Tag user's purchases' whereabouts, and even shopping list, so that users are in the disturbed mental state that will reduce the user's willingness to pay using induction.
- Individual data privacy: usually induction payment system will store personal privacy information, so interested parties can make use of known Tag $ID_T$ to pass through Back-end database authentication and to check out the sensitive personal information of all Tag users, exposing their privacy.

### 4.2. *Security*

- Tag cloning: hackers can get all the information which is intercepted from the legitimate Tag after the copy-forgery to confuse a new Tag. Tag cloning usually occurs when the card is lost or stolen in the RFID consumer environment, and the owner can't easily be detected. While in the NFC mobile sensors payment environment, the amount and frequency of the usage of mobile phones are greater than RFID, phone holders are alerted about how to reduce the risk of Tag cloning. And the user takes immediate report of loss and closes card measures in the event.

- Eavesdropping: this is the biggest source of threat on RFID. NFC's communication distance is only 10 cm short, and the eavesdropping threat would not be so wide like RFID. However, the environment of induction payment depends on the wireless communications, so there still exists a crisis of eavesdropping by interested parties.
- Replay attack: the attacker intercepts Tag's $ID_T$ and re-transmits it to the certification unit or counter party to obtain a legitimate access and cause financial loss of the original user.
- Denial of service: an attacker transfers large amounts of information to the authentication unit to attempt to paralyse the system operation so that there is no time to deal with normal trading.
- Forward security: after the attacker gets Tag's $ID_T$, it can track the related transaction information to know the holders' trends.

## 5. Security Analysis

This section explains each of lightweight NFC mobile sensors payment mechanism proposed in this study in response to the above-mentioned types of security threat analysis.

- Tag tracing: after the transaction is completed in security mechanism, the transaction parties immediately update the identification number $h(ID_R)$, $h(ID_T)$. Therefore, even if the attacker intercepts plain $ID_R$ and $ID_T$, it's still no security concern because his identity is not being tracked.
- Individual data privacy: when an attacker obtains $ID_R$ and $ID_T$, due to the certification of the update mechanism, any old information or estimate information is unable to pass authentication of Back-end database; therefore, it is able to protect a resource security.
- Tag cloning: induction payment uses the phone to simulate a Tag technology and the features of micro-payment; when Tag cloning occurs, the holder can carry out remedial measures in the shortest possible time. Therefore, it can reduce insurance losses to a minimum.
- Eavesdropping: at induction moment, NFC only has 10 cm in the short-range communications. And Reader can only transact to communicate with a single simulation Tag within a cell phone. In this case, an attacker still can't eavesdrop on the communication information between Reader and Tag in today's technology. Although the attacker could eavesdrop on wireless communication information under other trading environment, he still can't pass mutual authentication on this mechanism, thus failing.
- Denial of service: the mutual transaction of Reader and Tag will generate a new random value $N'_R$ and $N'_T$ and update to confirm the current validity of each transaction. And the Back-end database can be very easily compared with simple $h(ID_R)$ and $h(ID_T)$ index method. It disposes an illegal authenticator for the first time; therefore, it will not allow the system to be shut down and continue conducting other normal transactions.
- Forward security: as Tag tracing instructions, the security mechanism immediately updates the $ID_R$ and $ID_T$ identification code and verification code $N_R$ and $N_T$; you

Table 2
Authentication Protocol comparison of performance.

| Items | Song–Mitchell approach | Proposed approach |
|---|---|---|
| 1. Server authentication | Yes | Yes |
| 2. Reader authentication | No | Yes |
| 3. Tag authentication | Yes | Yes |
| 4. Decode to search | Yes | No |
| 5. Update operations | $1h, 3\oplus, 2 \gg$ | $1\oplus, 1 \gg$ |
| 6. Store memory | 5 variables | 4 variables |

will never have the same $ID_R$, $ID_T$, $ID_T$, $N_T$ appear. Even if an attacker wants to track Tag trends, he will fail. Based on the above safety analysis results, it is proved that the NFC mobile sensors payment mechanism can effectively solve the problem of privacy invasion and insecurity. It's a really practical security mechanism.

## 6. Performance Analysis

Based on low-cost NFC mobile sensors payment and considerations of unsafe circumstances, Table 2 shows the proposed authentication protocol performance compared with Song–Mitchell's scheme.

This authentication protocol aims to improve Song–Mitchell approach and is applied to the mobile-payment environment. Hence, it includes the Reader Authentication function. Table 2 shows the efficiency of the performance from Item 4 to Item 6, and this protocol can be better than Song–Mitchell approach due to smaller computation cost, smaller memory space and faster search speed. On the basis of the protocol facing undefendable DOS attacks, this method could effectively reduce the damage and enhance transaction security.

## 7. Conclusions

Google I/O General Assembly held in May 2015, Arstechnica, foreign media noted that to fight market against Apple Pay, Google released new initiatives payment API, called Android Pay. Companies can easily add this API to their payment service operations introduced to consumers. In fact, Google's HCE (Host Card Emulation) technology allows third-party Android App to use a NFC chip on the phone to make a payment, which achieves the dream that anyone can develop payment services on the Android platform.

The proposed lightweight NFC mobile sensors payment security certification is the solution matching HCE tide. The advantage of this authentication mechanism is that it makes it possible to effectively solve the problems of insecurity and worries of invasion of privacy. Under this simple security mechanism with Google's HCE, the store can even be of single use; as long as consumers have NFC phones and Internet connections, without any other players to join the relevant ecological payments, it can also establish a comprehensive induction payment process, so as to touch the hearts of consumers, extend levels of interoperability, and reach consumers's paradise.

**Acknowledgements.** The study was funded by the Ministry of Science number: 103-2815-C-486-046-E, Research Project Funding Grants.

## References

Cao, T., Shen, P. (2009). Cryptanalysis of two RFID authentication protocols. *International Journal Network Security*, 9, 95–100.

Chen, C.L., Lai, Y.L., Chen, C.C., Deng, Y.Y., Hwang, Y.C. (2011). RFID ownership transfer authorization systems conforming EPC global class-1 generation-2 standards. *International Journal Network Security*, 13, 41–48.

Chi, Y.L., Chen, C.H., Lin, I.C., Hwang, M.S. (2015). The secure transaction protocol in NFC card emulation mode. *International Journal Network Security*, 17, 431–438.

Chikouche, C., Cherif, F., Cayrel, P.L., Benmohammed, M. (2015). Improved RFID authentication protocol based on randomized McEliece cryptosystem. *International Journal Network Security*, 17, 413–422.

Cui, P.Y. (2016). An improved ownership transfer and mutual authentication for lightweight RFID protocols. *International Journal Network Security*, 18, 1173–1179.

Kim, S., Lim, J., Han, J., Oh, H. (2008). Efficent RFID search protocols using counter. *IEICE Transactions Communications*, 91-B, 3552–3559.

Lau, P.Y., Yung, K.K., Yung, E.K.N. (2010). A low-cost printed cp patch antenna for RFID smart bookshelf in library. *IEEE Transactions on Industrial Electronics*, 57, 1583–1589.

Lee, S.M., Hwang, Y.J., Lee, D.H., Lim, J.I. (2005). Efficient authentication for low-cost RFID systems. *Lecture Notes in Computer Science*, 3480, 619–627.

Lehlou, N. (2009). An online RFID laboratory learning environment. *IEEE Transactions on Learning Technologies*, 2, 295–303.

Lim, J., Oh, H., Kim, S. (2008). A new hash-based RFID mutual authentication protocol providing enhanced user privacy protection. *Lecture Notes in Computer Science*, 4991, 278–289.

Ling, J., Wang, Y., Chen, W. (2017). An improved privacy protection security protocol based on NFC. *International Journal Network Security*, 19, 39–46.

Ngai, E.W.T., Cheng, T.C.E., Au, S., Lai, K.H. (2007). Mobile commerce integrated with RFID technology in a container depot. *Decision Support Systems*, 43, 62–76.

Pannifer, S., Clark, D., Birch, D. (2014). HCE and SIM secure element: it's not black and white. *Consult Hyperion, Securing Tomorrow's Transaction*. http://www.chyp.com/wp-content/uploads/2015/01/HCE-and-SIM-Secure-Element.pdf.

Piramuthu, S. (2007). Protocols for RFID tag/reader authentication. *Decision Support Systems*, 43, 897–914.

Qian, Q., Jia, Y.L., Zhang, R. (2016). A lightweight RFID security protocol based on elliptic curve crytography. *International Journal Network Security*, 18, 354–361.

Rizomiliotis, P., Rekleitis, E., Gritzalis, S. (2009). Security analysis of the Song–Mitchell authentication protocol for low-cost RFID tags. *IEEE Communications Letters*, 13, 274–276.

Saparkhojayev, N., Dauitbayeva, A., Nurtayev, A., Baimenshina, G. (2014). NFC-enabled access control and management system. In: *International Conference on Web and Open Access to Learning*. doi:10.1109/ICWOAL.2014.7009188.

Smart Card Alliance (2014). Host Card Emulation (HCE) 101. *A Smart Card Alliance Mobile & NFC Council White Paper*, Publication number: MNFCC-14002.

Song, B., Mitchell, C.J. (2008). RFID authentication protocol for low-cost tags. In: *Proceedings of the First ACM Conference on Wireless Network Security*, pp. 140–147.

Syamsuddin, I., Dillon, T., Chang, E., Han, S. (2008). A survey of RFID authentication protocols based on hash-chain method. In: *Proceedings of the Third International Conference on Convergence and Hybrid Information Technology*, pp. 559–564.

Want, R. (2011). Near field communication. *IEEE Pervasive Computing*, 10, 4–7.

Wei, C.H., Hwang, M.S., Chin, A.Y.H. (2011). An authentication protocol for low-cost RFID tags. *International Journal Mobile Communications*, 9, 208–225.

Wen, W. (2010). An intelligent traffic management expert system with RFID technology. *Expert Systems with Applications*, 37, 3024–3035.

Yeo, S.S., Kim, S.C., Kim, S.K. (2009). Protecting your privacy with a mobile agent device in RFID environment. *Wireless Personal Communications*, 51, 165–178.
Zhang, X., King, B. (2008). Security requirements for RFID computing systems. *International Journal Network Security*, 6, 214–226.

**T.-H. Feng** received his MS in Information Management from Chao-Yang University of Technology, Taichung, Taiwan, ROC, in 2002. He is currently pursuing the PhD degree from Computer Science Information Engineering Department of Asia University, Wufeng, Taiwan. His research interests include information security, cloud computing, networked control system and Sensor Networks.

**M.-S. Hwang** received the PhD in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. Dr. Hwang passed the National Higher Examination in the field of Electronic Engineering, in 1988. He also passed the National Telecommunication Special Examination in the field of Information Engineering, qualified as advanced technician of the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a chairman of the Department of Information Management, Chaoyang University of Technology (CYUT), Taiwan, during 1999–2002. He was a professor and a Chairman of the Department of Management Information Systems, NCHU, during 2003–2009. He was also a visiting professor in the University of California (UC), Riverside and UC, Davis (USA) during 2009–2010. He was a distinguished professor of the Department of Management Information Systems, NCHU, during 2007–2011. He obtained the 1997, 1998, 1999, 2000, and 2001 Excellent Research Award of National Science Council (Taiwan). Dr. Hwang was a dean of College of Computer Science, Asia University (AU), Taichung, Taiwan. He is currently a chair professor in the Department of Computer Science and Information Engineering, AU. Dr. Hwang has published over 200 articles on the above research fields in international journals.

**L.-W. Syu** received his BS in Computer Science and Information Engineering from Asia University, Taichung, Taiwan, ROC, in 2016. His research interests include RFID, cloud computing and network security.

## Mokėjimų NFC tipo mobiliaisiais įrenginiais pagerintas autentifikavimo protokolas

Tung-Huang FENG, Min-Shiang HWANG, Liang-Wei SYU

Straipsnyje nagrinėjamas mokėjimų NFC (Near Field Communication) tipo mobiliaisiais įrenginiais pagerintas autentifikavimo protokolas, analizuojamas šio protokolo saugumas, atlikta jo kokybės analizė. Protokolas garantuoja vartotojo privatumą ir yra atsparus piktavališkoms ryšio kanalo atakoms. Pasiūlytas saugumo užtikrinimo metodas padės atlikti saugius mokėjimus NFC tipo mobiliaisiais įrenginiais.