A Secure Privacy and Authentication Protocol for Passive RFID Tags

Chia-Hui Wei

National Central Library, Taiwan, R.O.C.,
Taipei, Taiwan, ROC
E-mail: d938321@oz.nthu.edu.tw

Min-Shiang Hwang*

Department of Computer Science & Information Engineering,
Asia University,
500, Lioufeng Rd., Wufeng, Taichung 41354, Taiwan
Department of Medical Research, China Medical University
Hospital,
China Medical University,
No.91, Hsueh-Shih Road, Taichung 40402, Taiwan
E-mail: mshwang@asia.edu.tw
*Corresponding author

Augustin Yeh-Hao Chin

Department of Computer Science, National Tsing Hua University
101, Section 2, Kuang Fu Road, Hsinchu 300, Taiwan, R.O.C.
E-mail: yhchin@cs.nthu.edu.tw

Abstract: A privacy and authentication protocol (PAP) requires a tag to perform four simple operations in mobile communications: Comparing two numbers used to execute a hash function, storing and retrieving a number in users' memory banks, and flipping a bit. In this paper, we will propose an improved PAP which is well-secured and efficient in a small amount of computations, and is also capable of dealing with both privacy and authentication.

Keywords: Authentication; Mobile communication; Privacy; RFID; Security.

Biographical notes: Chia-Hui Wei received the M.S. degree in Information Management from Chaoyang University of Technology and Ph.D. degree in Computer Science from National Tsing Hua University, Taiwan. Currently, she is serving in National Central Library, Taiwan. Her current research interests include RFID security, information security, and mobile communications.

Min-Shiang Hwang received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, ROC, in 1980; the M.S. in Industrial Engineering from National Tsing Hua

University, Taiwan, in 1988; and the Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician 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 chairman of the Graduate Institute of Networking and Communications, CYUT, during 2002-2003. He obtained the 1997, 1998, 1999, 2000, and 2001 Outstanding Research Award of National Science Council of the Republic of China. He is currently a professor of the department of Management Information System, National Chung Hsing University, Taiwan, ROC. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr. Hwang had published over 200 articles on the above research fields in international journals.

Augustin Yeh-hao Chin reveived the the Ph.D. degree from University Texas at Austin. Currently, he is a professor with the Department of Computer Science from the National Tsing Hua University, Hsinchu County, Taiwan. His current research interests include database systems, algorithm design, system programming, and software engineering.

1 Introduction

Radio Frequency Identification (RFID) tag is a small electronic component, which is easy to be embedded in different products (Chen et al., (2007); Wei et al., (2011); Qian et al., (2016)). Furthermore, the RFID tag can be read by radio wave within several meters without having direct contact or using the line of sight scanning. The RFID systems are convenient due to its fast speed in identifying an object; therefore it became more and more popular in many industries, such as supply chain management, e-passports, and credit cards (Hunter, (2005); Liu et al., (2015); Musa et al., (2015); Naveed et al., (2012); Wei et al., (2011, 2006)). Although RFID systems have many benefits as described above, these functions could result in many security and privacy problems (Hwang et al., (2009); Juels, (2006); Khedr, (2014)). Such problems could occur when the cloning of tags replaying attack, disclosure of private information, and fake authentication have taken place (Cui, (2016); Wei et al., (2012)).

Many researchers have proposed various solutions in the last few years (Chikouche et al., (2015); Kang et al., (2008); Liu et al., (2009); Peris-Lopez et al., (2009); Sun et al., (2008); Tajima, (2007); Zhang et al., (2008)). Recently, one of the researches called "Privacy and Authentication Protocol (PAP)" is proposed (Liu et al., (2009)); it is applied in supply chain management. The PAP is the procedure of an authentication protocol for making an inventory of products in a store, checking the sold products, and dealing with the product returning services. The PAP can resist replayed attack and mutual authentication. Unfortunately, we have found out that the PAP protocol cannot resist private information leakage and tag cloning. In fact, private information leakage attack can disclose the secret data on tag, and the attacker could easily clone the tag so that the reader cannot authenticate the genuine tag.

For example, one of the researchers named Chris Paget used inexpensive off-the-shelf components to build a mobile platform that can clone a large number of the unique electronic identifiers used in US passport cards and next generation driver licenses (Goodin, (2009); Zhou et al., (2015)). Cloning and impersonating RFID tags could be financially lucrative for hackers or malicious employees in all applications. Therefore, tag cloning and private information leakage attack are considered the serious security obstacles for strengthening RFID systems. In this paper, we will present the leak in the PAP protocol. More precisely, we will analyze the security weaknesses of PAP protocol and fix them while preserving the privacy and authentication feature. We have proposed a new PAP protocol which not only prevents replayed attack and mutual authentication, but also resists tag cloning and private information leakage.

The remainder of this paper is organized as following. In Section 2 we will review the PAP protocol. Section 3 has the analysis of the vulnerabilities of the PAP protocol. Section 4 contains a countermeasure and security analysis. Finally, the concluding remarks and future work are represented in Section 5. Table 1 shows the notations used throughout the paper.

Table 1 Notations and indexing terms

id	A static identification.
K	A secret key.
Privacy bit	Setting 0 indicates the tag has non-privacy while 1 indicates the tag has privacy.
$name$	The name of the tag (ex. item of product).
n_t	The tag generates its own random nonce.
n_r	The reader generates its own random nonce.
T_i	The i-th timestamp.
id_A	A counterfeit tag.

2 Review of the PAP

The PAP involves three entities: tags, readers, and a back-end database. PAP recognizes the reader and the server as one entity and shares a secure channel. On the other hand, the other channel between the reader and the tag is considered insecure. In PAP, each tag and database need to store a record consisting of these four values: (1) the tag initialized with a static identification id, (2) a secret key k shared by both the reader and the tag, (3) the product type with a generic name, and (4) a privacy bit set to 0 or 1, which indicates whether the tag is in non-privacy or privacy. The PAP also includes the following four situations: in-store, checkout, out-store, and return protocols. The in-store protocol focuses on the inventory, and the reader queries a tag located within a store; therefore, Liu et al. assumed all of the readers in a store are authorized, and the tag's privacy bit is preset to 0. The checkout protocol is used to query a tag and to authenticate each other during a checkout procedure. After the tag has left the store, the off-store protocol is adopted to query the tag within home. The return protocol is used to cope with the returning of an item from where it was sold. The steps of the in-store protocol in PAP are described in Figure 1.

Step 1: The reader sends query to the tag.

Step 2: The tag generates a random nonce n_t, and then sends itself a static identification id and sends n_t to the reader.

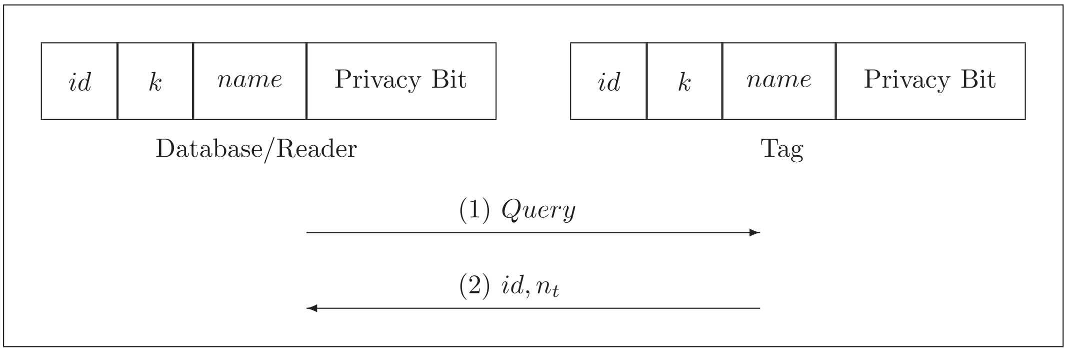

Figure 1 The in-store protocol in PAP.

The steps of the checkout protocol in PAP are represented in Figure 2. The first 2 steps are identical as in the in-store protocol. Other steps are listed as follows.

Step 3: The reader searches the secret key k by id, and then computes $H_1 = h(n_t, k)$. After that, the reader generates a random nonce n_r and sends (H_1, n_r) to the tag.

Step 4: The tag verifies whether H_1 is successful. If it recognizes the secret key k, then the tag would compute $H_2 = h(n_r, k)$, which will be sent to the reader. Then the reader checks H_2. The authentication will be finished if the check is successful. Otherwise, it would fail.

The steps of off-store and return protocols in PAP are similar to that of the in-store and checkout protocols, respectively. The only difference is that the tag sends

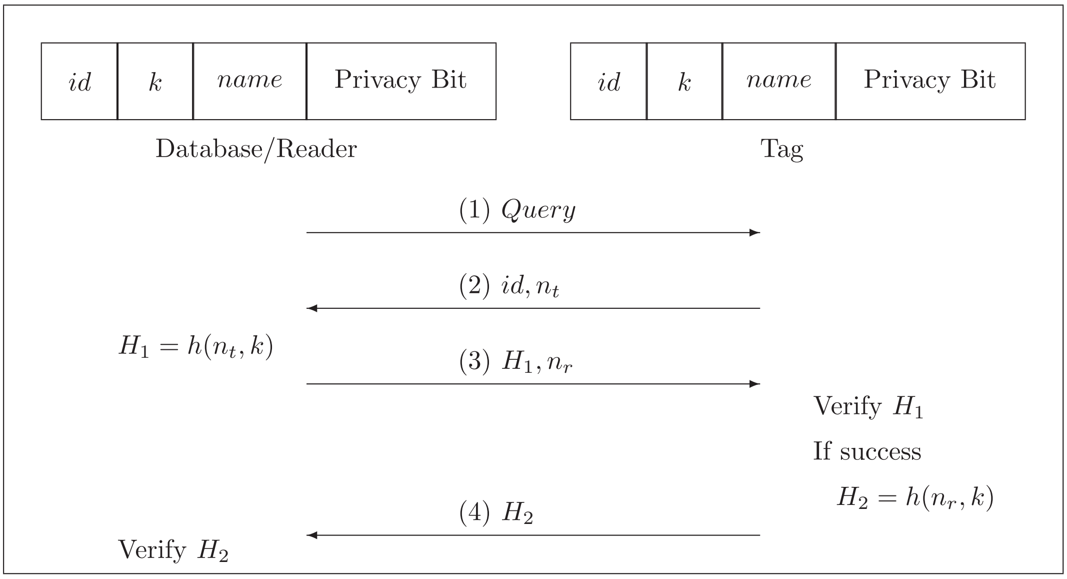

Figure 2 The checkout protocol in PAP.

id to the reader in the in-store and checkout protocols, while the tag sends *name* to the reader in out-store and return protocols in PAP. The more description was in (Liu et al., (2009)).

3 Vulnerabilities of the PAP Protocol

The PAP protocol is used to automatically identifying, categorizing, locating and tracking the products. The PAP assumes that ”PAP is an established level of security that does not allow unauthorized RFID readers within a scanning range of these tags”; however, this assumption is actually not practical. Since the business spies or malicious employees could surreptitiously listen to the entire communication message through radio waves, therefore, the process is easy to be sniffed or eavesdropped. One important condition for a secured RFID system is that even if the attacker is able to observe all interactions between the reader and the tag, the attacker still could not obtain useful messages to track or fake. In PAP, the business spies or malicious employees can clone the tag that has a low price, and then attach this replica to the valuable product in order to cheat the reader.

In this section, we will demonstrate how to clone the tag and expose the private information in PAP. One prerequisite is that the attacker must be able to eavesdrop on the communication message between the tag and the reader.

Attacker 1 (Tag Cloning): Although PAP assumes that only legitimate readers can query the tag, the PAP does not prevent the malicious employees from cloning the tag. Since the communication message (id, n_t) is not encrypted in Step 2 in in-store protocol, business spies or malicious employees can collect communication messages and then duplicate the tag to transmit counterfeit message (id, n_t) in order to cheat the reader in in-store protocol. This situation allows the reader to believe that the tag is still in the list of inventory; however, in fact, the tag is a fake one. Such scenario is considered as a successful attack in tag cloning. The attacker performs actions in the following steps as shown in Figure 3.

Step 1: A normal communication session takes place. The attacker is able to sniff out the message *id*.

Step 2: When the communication message of in-store protocol reaches Step 2, the attacker then eavesdrops the message *id* sent by the tag.

At the end of Step 2, the counterfeit id_A is generated. The id_A and the n_t are used in the next session when the reader queries the tag.

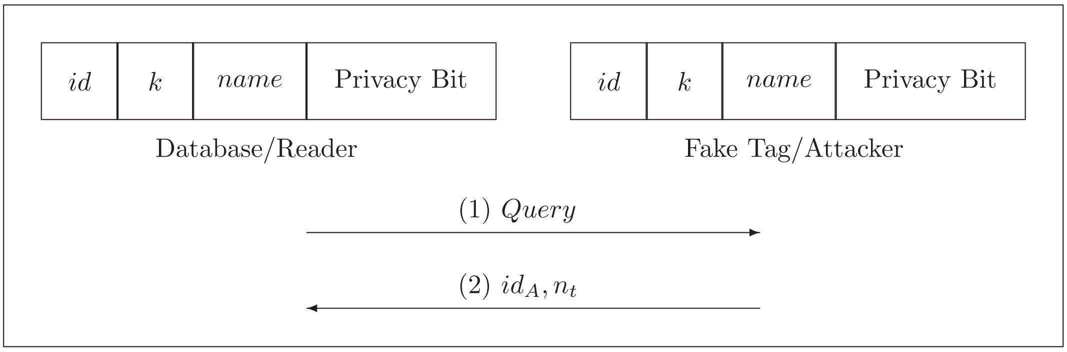

Figure 3 Attacker 1 in PAP.

Attacker 2 (Exposed Privacy Information): After he/she bought a product and went out of a store at off-store protocol, an arbitrarily reader is able to get close to the tag and then get the generic name of the product by off-store protocol, which would result in an information leakage. In fact, the business spy is capable to know what a customer have bought in this supermarket or what item sells best. The detailed steps are shown in Figure 3. Note that the messages are not encrypted to protect privacy.

4 Countermeasure and Security analysis

As stated in Section 3, the PAP protocol would be vulnerable to attacks including tag cloning and privacy information leakage. In this section, we will show that PAP's improved protocol can resist these attacks. The key weakness behind this protocol is that the communication messages are sent between the tag and the reader by radio wave, which does not give the corresponding encryption.

In order to mend the PAP protocol, we will reuse one of the previously implemented primitives, or more precisely, the primitive in hash function and the timestamp. There are established levels of security when a tag is in different location, namely in-store protocol, checkout protocol, off-store protocol, and return protocol. The former two protocols occur when the tag is inside a store. The later two protocols occur when the tag is in the checkout counter and when it goes out of the store. The purpose of the in-store protocol is to have the ability to query a tag located within a store and then make an inventory. Each tag has id_i which is the i-th static identification id, the product item name, and a secret key k and i-th timestamp T_i. Each tag and the reader keep $(id_i, k, name)$. To resist the possible replayed attacks, the timestamp is attached, which means that we can analyze the possible attacks later. The querying process consists of two steps as shown in Figure 4.

Step 1: Initially, the reader generates a timestamp T_i and sends it to query the tag. The tag then uses the reader's timestamp T_i and the tag's k to compute $M_1 = h(k, T_i)$.

Step 2: The tag responds with its (id_i, M_1) to the reader. The reader first checks whether the timestamp is in the time interval or not. If the timestamp is legitimate, it would go on to the next step; otherwise, the query fails. The reader will generate fresh timestamps if they query again. After successfully checking the timestamps, the reader computes M_1 depending on the id_i and k found in the database, and then the tag is written in the list of inventory if the reader has been successfully checked.

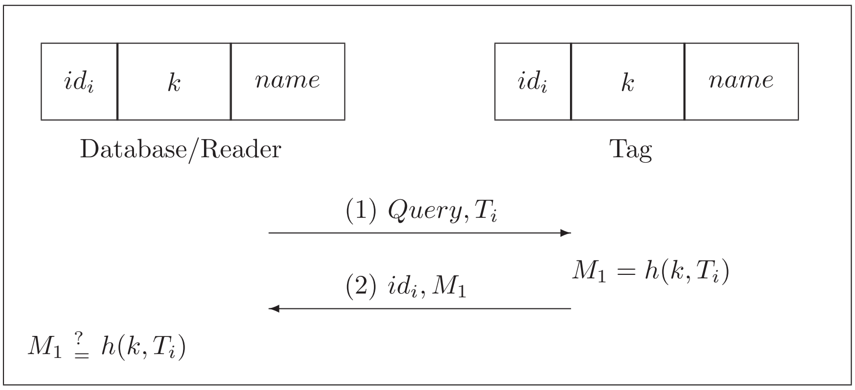

Figure 4 The in-store protocol in the proposed PAP.

The purpose of checkout protocol is not only querying a tag, but also authenticating both the reader and the tag by connecting to a back-end database to check the product's selling procedure. The checkout protocol consists of four steps in Figure 5; note the first two steps are identical as in the in-store protocol.

Step 1: Initially, the reader generates an i-th timestamp T_i and sends it to query the tag. The tag uses the reader's timestamp T_i and the tag's k to compute $M_1 = h(k, T_i)$.

Step 2: The tag responds with its (id_i, M_1) to the reader. The reader first checks whether the timestamp is within time interval or not. If timestamp is legitimate, it would go on to the next step; otherwise, the query fails. The reader will generate fresh timestamps if they query again. After successfully checking the timestamps, the reader computes M_1 depending on the id_i and k found in the database. If the reader verifies that the tag $M_1 = h(k, T_i)$ is successful, the reader would generates a next timestamp T_{i+1} and then compute $M_2 = h(name, T_{i+1})$.

Step 3: The reader generates a timestamp and sends the (M_2, T_{i+1}) message to the tag, and then the tag verifies the value of M_2. If the verification is successful, it would compute the value M_3.

Step 4: The tag sends M_3 to the reader. Upon receiving M_3, the reader uses its local values to verify M_3.

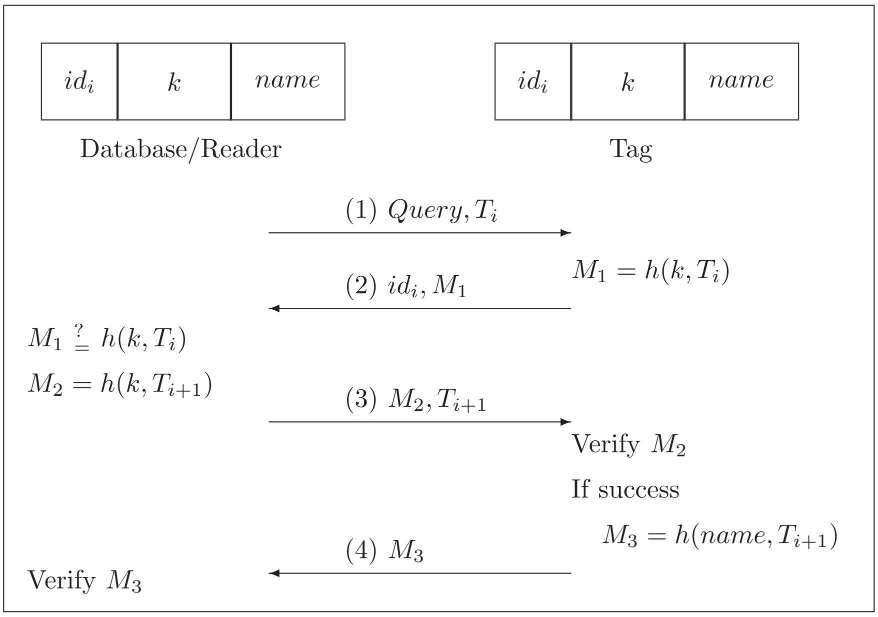

Figure 5 The checkout protocol or return protocol in the proposed PAP.

The off-store protocol and return protocol are adopted when the tag leaves the store. The goal of off-store protocol is to query a tag if you have a smart machine. For example, a smart refrigerator can soon know exactly what food it contains through the tag, what you've already eaten today, and what food will be ran out of. These smart refrigerators can query the tag by off-store protocols, which are convenient to us if it could recognize the state of the food inside them. The off-store protocol consists of two steps as shown in Figure 6.

Step 1: Initially, the reader generates an i-th timestamp T_i and sends it to query the tag. The tag uses the reader's timestamp T_i and the tag's name to compute $M_1 = h(name, T_i)$.

Step 2: The tag responds with its (id_i, M_1) to database/reader. The reader first checks whether the timestamp is within time interval or not. If timestamp is legitimate, it would go on to the next step; otherwise, the query fails. The reader will generate fresh timestamps if they query again. After successfully checking the timestamp, the reader computes M_1 depending on the id_i and the name found in the database. Next, the tag will be written in a smart machine if the reader has been checked successfully.

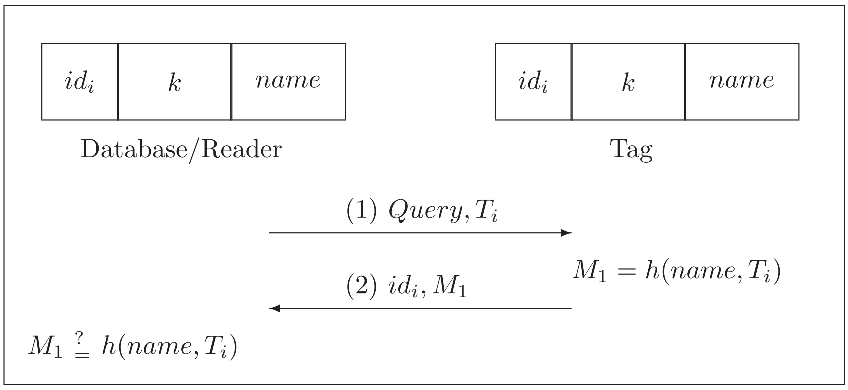

Figure 6 The out-store protocol in the proposed PAP.

The return protocol will not be frequently used if after-care service seldom happens. Most stores have after-care services, meaning they are willing to alter an exchange or refund on those unsatisfactory goods, since they need to maintain the market by raising customers' satisfaction, or more importantly, their loyalty to the store. In other words, a customer can return or exchange the goods back to the store. The store needs to verify whether or not the good was sold from there, so, the mutual authentication becomes important. We have assumed that the steps of the return protocol are the same as the ones in the checkout protocol.

The detailed steps of our proposed protocol are described in the last paragraph. In our proposed protocol, the reader not only could successfully resist the tag cloning, but also could successfully establish a mutual authentication with the tag. Next, we will analyze our scheme in different types of attacks. We first give it a brief description for each attack, and then we will analyze the security of the proposed protocol by examining the required properties and the possible attacks as follows:

1. Resistance to replayed attack. The attacker repeats or delays the same message when valid data are transmitted. The adversary tries to intercept

the data and retransmit them, and then cheat or spoof either the reader or the tag in order to obtain the access data. In our proposed protocol, the attacker may replay the response M_1 from a tag and M_2 from a reader. However, the attacker will replay the invalid value because the timestamp T_i is limited in certain time interval from the reader or the tag, while the new timestamps are generated in each session. Therefore, the attacker could not obtain the access data even if they replay the message either from the reader or the tag.

2. Tag cloning. The attacker eavesdrops the message from the tag, and then clones the tag by writing all the obtained data into other tags since the tags are usually attached to the product within open environments, such as supermarkets, hospitals, schools, and other public places. In our proposed protocol, although the attacker could eavesdrop id_i, M_1 and M_3 from the tag, the attacker could not clone the tags because the messages M_1 and M_3 are well-constructed by a hash function. Thus, tag cloning is infeasible if an attacker attempts to certify the fake message M_1 or M_3. In addition, the attacker would find it difficult to understand the disclosed message such as M_1, M_2, and M_3, which are protected by integrated timestamp T_i and a hash function. In fact, the timestamp is a value that is being continuously changed in each session. Therefore, the attacker could not clone the tag from the past communication messages.

3. Resistance to disclosed information. The attacker can know what items the consumer has bought from the store or what books the consumer have borrowed from the library by eavesdropping. The computation of M_1 includes the hash value and timestamp T_i in off-store protocol. Therefore, the name is well-protected by a hash function.

4. Mutual authentication and data integrity. The tag must prove its identity to a reader, and the reader must prove its identity to the tag, before transmitting the message. In our proposed protocol, the tag and the reader authenticate each other because only the genuine reader has the value $h(id_i)$ to generate the value M_2; only the genuine authentic tag has the secret value k to generate consistency value, and to verify the success among them followed by generating the response M_3. Therefore, only the authentic reader and the authentic tag have the ability to generate the required values.

The performance is evaluated in our proposed protocol in terms of security, computational cost, communication cost, and storage requirement. First, we compared the strength of security with PAP protocol that is described in Section 3; we analyzed the attacks for PAP protocol, which is vulnerable to tag cloning and private information leakage in the four-scenario protocol. Note that the message is in plaintext, which is easy to a clone tag and then to cheat the reader. Since the communication message (id_i, n_t) is not encrypted, those business spies or malicious employees could get the message (id_i, n_t) and then duplicate the tag. The compared security list of PAP protocol and our proposed protocol are shown in Tables 2 and 3. We have proven that our proposed protocol is more secure than PAP protocol, because the timestamp is combined with the hash function at four scenarios.

Second, the computational cost for our proposed protocol involves only that the timestamp is considered, which has a low-cost and can be effectively generated. The computation of our proposed protocol for Tag is 1 hash at in-store and off-store protocols, and 2 hashes at checkout and return protocol, while the PAP has 1 hash at checkout protocol and none at other two protocols. The computation of our proposed protocol for Reader contains 1 hash at in-store protocol and off-store protocol, 3 hashes at checkout and return protocol, while the PAP has 2 hashes at checkout and return protocols, and none at other two protocols. The Reader and Tag computations of PAP are lower than our proposed protocol, because our proposed protocol is encrypted in each message before transmitting the message. The traffic cost of our proposed protocol and PAP are equal, two values $16bits$, between the tag and the reader. The operation types of our proposed protocol are hash function and timestamp; the PAP is hash function and privacy bit. The total steps of our proposed and PAP protocol are equal, which are 3 steps. They are shown in Table 4. In short, although the tag computation and reader computation of ours are higher than PAP, our proposed protocol is proven to be more secure than PAP at Tables 2 and 3.

Finally, we examined the storage requirements of our proposed protocol; it is required to store three values, id_i, k, and *name*, with total $24bits$. The PAP is needed to store four values id_i, k, *name*, and *private bit*, with total $32bits$. In summary, our proposed protocol requires a less number of memory sizes than that of PAP protocol.

Table 2 The security characters for different in-store and out-store protocols.

	In-store & Out-store Protocols of PAP	In-store & Out-store Protocols of the Proposed PAP
Tag Cloning	No	Yes
Information Leakage	No	Yes
Resistance to Replay Attack	Yes	Yes

5 Conclusions

In this paper, we have analyzed the security of the PAP protocol. We have shown that an attacker can clone the tag and disclose the tag's information by eavesdropping. Thus, PAP protocol cannot enhance the security of RFID systems under a passive attack. We also have proposed a new privacy and authentication protocol. The proposed PAP improves the security, reduces computational cost, ensures tag cloning resistance, and further prevents the privacy information disclosure problem. Further, we have reduced one unit of the memory size on the tag so it only needs to store (id_i, k, T_i). The proposed PAP would be both secure

Table 3 The security characters for different checkout and return protocols.

	Checkout & Return Protocols of PAP	Checkout & Return Protocols of the Proposed PAP
Tag Cloning	No	Yes
Information Leakage	No	Yes
Resistance to Replay Attack	Yes	Yes
Mutual Authentication	Yes	Yes

Table 4 The performance comparisons for different protocol.

	Tag Computation	Reader Computation	Traffic	Total Steps	Operation Types	Memory Size
In-store & Out-store Protocol of PAP	none	none	16 *bits*	2 *steps*	none	32 *bits*
Checkout & Return Protocol of PAP	1 *hash*	1 *hash*	16 *bits*	4 *steps*	hash, private bit	32 *bits*
In-store & Out-store Protocol of Our Proposed	1 *hash*	1 *hash*	16 *bits*	2 *steps*	hash, timestamp	24 *bits*
Checkout & Return Protocol of Our Proposed	2 *hashes*	3 *hashes*	16 *bits*	4 *steps*	hash, timestamp	24 *bits*

and efficient in supply chain management, therefore making it very attractive to low-cost RFID systems.

References

Chen, J.L., Chen, M.C., Chen, C.W., and Chang, Y.C. (2007) 'Architecture design and performance evaluation of RFID object tracking systems,' *Computer Communications*, vol. 30, no. 9, pp. 2070–2086.

Chikouche, N., Cherif, F., Cayrel, P.L., Benmohammed, M. (2015) 'Improved RFID Authentication Protocol Based on Randomized McEliece Cryptosystem,' *International Journal of Network Security*, vol. 17, No. 4, pp. 413–422.

Cui, P.Y. (2016) 'An Improved Ownership Transfer and Mutual Authentication for Lightweight RFID Protocols,' *International Journal of Network Security*, vol. 18, No. 6, pp. 1173–1179.

Goodin, D. (2009) 'Passport RFIDs cloned wholesale by 250 eBay auction spree,' *http://www.theregister.co.uk/2009/02/02/low_cost_rfid_cloner/*.

Hunter, P. (2005) 'London terrorist attacks heat up identity card debate and highlight uncertainties over their efficacy,' *Computer Fraud & Security*, vol. 2005, no. 7, pp. 4–5.

Hwang, M.S., Wei, C.H. and Lee, C.Y. (2009) 'Privacy and security requirements for RFID applications', *Journal of Computers*, Vol. 20, No. 3, pp. 55–60.

Juels, A. (2006) 'RFID security and privacy: A research survey,' *IEEE Journal on Selected Areas in Communication*, vol. 24, no. 2, pp. 381–394.

Kang, S.Y., Lee, D.G., and Lee, I.Y. (2008) 'A study on secure RFID mutual authentication scheme in pervasive computing environment,' *Computer Communications*, vol. 31, no. 18, pp. 4248–4254.

Khedr, T. (2014) 'On the security of moessners and khans authentication scheme for passive EPCglobal C1G2 RFID tags,' *International Journal of Network Security*, vol. 16, no. 4, pp. 369–375.

Liu, A. X., and Bailey, L.A. (2009) 'PAP: A privacy and authentication protocol for passive RFID tags,' *Computer Communications*, vol. 32, no. 7, pp. 1194–1199.

Liu, Y., Yang, Y., Wei, J., Wang, X. (2015) 'An examination on RFID innovation diffusions in Chinese public intelligent transportation services,' *International Journal of Mobile Communications*, vol. 13, no. 5, pp. 549–566.

Musa, A., Khan, H.U., AlShare, K.A. (2015) 'Factors influence consumers' adoption of mobile payment devices in Qatar,' *International Journal of Mobile Communications*, vol. 13, no. 6, pp. 670–689.

Naveed, M., Habib, W., Masud, U., Ullah, U., and Ahmad, G. (2012) 'Reliable and low cost RFID based authentication system for large scale deployment,' *International Journal of Network Security*, vol. 14, no. 3, pp. 173–179.

Peris-Lopez, P., Li, T., Hernandez-Castro, J.C., and Tapiador, J.M.E. (2009) 'Practical attacks on a mutual authentication scheme under the EPC class-1 generation-2 standard,' *Computer Communications*, vol. 32, no. 7, pp. 1185–1193.

Qian, Q., Jia, Y.L., Zhang, R. (2016) 'A Lightweight RFID Security Protocol Based on Elliptic Curve Crytography,' *International Journal of Network Security*, vol. 18, no. 2, pp. 354–361.

Sun, B., Xiao, Y., Li, C.C., Chen, H.H., and Yang, T.A. (2008) 'Security co-existence of wireless sensor networks and RFID for pervasive computing,' *Computer Communications*, vol. 31, no. 18, pp. 4294–4303.

Tajima, M. (2007) 'Strategic value of RFID in supply chain management,' *Journal of Purchasing and Supply Management*, vol. 13, no. 4, pp. 261–273.

Wei, C.H., Hwang, M.S., and Chin, A.Y.H. (2011) 'An authentication protocol for low-cost RFID tags,' *International Journal of Mobile Communications*, vol. 9, no. 2, pp. 208–223.

Wei, C.H., Hwang, M.S., and Chin, A.Y.H. (2011) 'A mutual authentication protocol for RFID,' *IEEE IT Professional*, vol. 13, no. 2, pp. 20–24.

Wei, C.H., Hwang, M.S. and Chin, A.Y.H. (2012) 'An improved authentication protocol for mobile agent device in RFID,' *International Journal of Mobile Communications*, vol. 10, no. 5, pp. 508–520, 2012.

Wei, J., Liu, L.C., Koong, K.S. (2006) 'An onion ring framework for developing and assessing mobile commerce security,' *International Journal of Mobile Communications*, vol. 4, no. 2, pp. 128–142.

Zhang, X., and King, B. (2008) 'Security requirements for RFID computing systems,' *International Journal of Network Security*, vol. 6, pp. 214–226.

Zhou, P., Xu, Z., Li, Y., Wang, F., Zhang, L. (2015) 'Research on identity authentication management in mobile commerce based on ECC and dynamic fingerprint key,' *International Journal of Mobile Communications*, vol. 13, no. 5, pp. 535–548.