Journal of Software Engineering

ISSN 1819-4311

Academic
Journals Inc.

www.academicjournals.com

OPEN ACCESS Journal of Software Engineering

ISSN 1819-4311
DOI: 10.3923/jse.2016.263.271

Research Article
An ECC-based Tree-structure RFID Grouping-proof Protocol

Kang Hong-Yan

Department of Computer and Information Engineering, Institute of Embedded Systems and Internet of Things, Heze University, Heze, China

Abstract

In this study an Elliptic Curves Cryptography (ECC)-based tree-structure radio frequency identification (RFID) grouping-proof protocol is proposed to overcome low efficiency and vulnerability to various security threats of existing RFID grouping-proof protocols. Security performance is improved because of the design of the key structure, authentication approaches and procedures for the ECC-based tree-structure RFID grouping-proof protocol. During protocol interaction, grouping-proof efficiency is improved by introducing the tag-reader mutual authentication mechanism to reduce interaction with unauthentic RFID readers and tag computing workload and to complete proof information acquisition with less computation. There are a detailed description and a security analysis of the protocol in this study. As analysis results show, the protocol meets security and privacy requirements. Compared with existing grouping-proof protocols, the proposed protocol is of high efficiency and availability as it brings enhanced security and performance with less computational complexity.

Key words: RFID, ECC, grouping-proof, mutual authentication, tree-structure

Received: March 17, 2016 Accepted: May 06, 2016 Published: June 15, 2016

Citation: Kang Hong-Yan, 2016. An ECC-based tree-structure RFID grouping-proof protocol. J. Software Eng., 10: 263-271.

Corresponding Author: Kang Hong-Yan, Department of Computer and Information Engineering, Institute of Embedded Systems and Internet of Things, Heze University, Heze, China

Competing Interest: The author has declared that no competing interest exists.

Data Availability: All relevant data are within the paper and its supporting information files.

INTRODUCTION

The internet of things realizes intelligent identification, positioning, tracking, monitoring and management by connecting objects to the internet in conventional protocols via information sensing equipment such as RFID technology, infra-red sensors, Global Positioning System (GPS) and laser scanners to communicate and exchange information. The RFID as one of the most important technologies at the sensing layer of the internet of things, realizes the sensing of end objects in the internet of things. It has been widely applied in such domains as identity authentication, traffic control, automatic identification of human and objects, warehouse management and supply chain management. The RFID has significantly improved efficiency and cut Total Cost of Ownership (TCO).

In actual application, end objects in the internet of things are often with obvious grouping attributes, i.e., two or more tags must be present simultaneously. Otherwise, authentication fails. For instance, all commodities connected to the internet of things in a large supermarket assert that they belong to the same supermarket in order to ensure security. Other examples are boarding pass, passport and baggage belonging to the same person at an airport and a set medical instruments exclusive for a specific operation in a hospital. The grouping attribute requires the capability to process group communication of RFID security protocols to be designed.

The RFID yoking proof was firstly proposed by Juels (2004). He called it the yoking-proof protocol (Juels, 2004). The protocol is used to prove that two tags are scanned and present simultaneously. Saito and Sakurai (2005) however, indicated that the protocol could not resist replay attack and an attacker could hoke up valid grouping proofs from several authentication sessions. Therefore, improved the protocol by introducing the timestamp mechanism and proposed an improved grouping-proof protocol. Piramuthu (2006) found that the improved protocol was still flawed to resist replay attack. To overcome the flaw, a new random number based grouping-proof protocol was proposed. The new protocol failed to resolve such security threats as privacy disclosure, forward security and DOP attack, though it had a higher security level. Burmester *et al.* (2008) insisted that it was not secure enough to ensure only tag co-existence. They proposed three group authentication protocols based on shared group keys, among with the third one was anonymous and forward secure.

Hermans and Peeters (2013) proposed the security model based on RFID grouping proofs. Peris-Lopez *et al.* (2011) had security analysis of previous grouping-proof protocols. Ma *et al.* (2012) and Ham *et al.* (2015) proposed that there should be a tag with certain computing power in each group. Nevertheless, the former could not ensure tag anonymity and the latter was vulnerable to DOS attack.

According to data acquisition approaches, current grouping-proof protocols are divided into two categories: link grouping proof protocols (Lo and Yeh, 2010; Kang, 2013) and broadcasting grouping proof protocols (Zhang and Xu, 2011; Duc *et al.*, 2010). Correlation is adopted in the first category. A tag is correlated to other tags at the DLL or in other ways. Firstly the reader initiates a yoking proof generation request when yoking proofs are to be generated. The first tag passes the result to the next correlated tag through certain computations after it receives the request. The last tag passes the computational result to the reader and then the reader generates a yoking proof. In the second category, the reader broadcasts a request and then each calculates a response message and sends it to the reader. The reader generates yoking proofs according to tag response messages. As the analysis reveals, tags must firstly be correlated in a specific way in the first category of grouping-proof protocols. In addition, the generation of yoking proofs depends on one by one message delivery between tags. In this category of protocols, the input to tag$_i$ depends on the previous i-1 tags, i.e., tag$_i$ can be processed only when the previous i-1 tags have been processed. Apparently, authentication efficiency will be influenced when there are a large quantity of tags. Besides, the protocols are of a poor scalability. The second category can facilitate the generation of yoking proofs for a large quantity of tags and is thus, more efficient than the first category.

Study of grouping-proof protocols are mainly based on hash and random functions, shared secret and pseudo-random functions or symmetric cryptographic algorithms. Research using public-key cryptography (especially ECC) is still unpopular. It may bring such problems as security and privacy preservation. The industry has the impression that public-key cryptography is not suitable for low-cost and weak computing power RFID tags. Actually, it is not the case. As Lee *et al.* (2008) proposes, ECC is suitable for RFID system design. An ECC-based processor for RFID tags is designed in the literature. The ECC gradually draws attention of the industry thanks to its advantages such as short keys, less computation and quick computation at the same security level. Batina *et al.* (2010) first proposed the ECC-based privacy-preserving RFID grouping-proof protocol but the scheme had the timeout problem. Batina *et al.* (2012) proposed a privacy preserving multi-players grouping-proof protocol, which is exclusively dependent on the use of ECC. Moreover, Lv *et al.* (2011) indicated that it could not resist tracking attack and an improved protocol was proposed to solve this issue. Ko *et al.* (2011) later found the protocol (Lv *et al.*, 2011) has impracticability on the basis of public-key cryptography and then proposed an enhanced protocol to satisfy the functionalities and resist tracking attack. Lin and Zhang (2012) proposed a protocol to improve the efficiency of Batina *et al.* (2010) resolving the timeout problem in the generation of grouping-proofs. This study proposes an ECC-based tree-structure RFID grouping-proof protocol and provides security proof and privacy analysis of the scheme.

MATERIALS AND METHODS

Generation approaches of broadcasting yoking proofs and link yoking proofs are different. In the link approach, tags are already linked, i.e., authenticated. In the broadcasting approach, tags are, however, not linked and have to be authenticated.

In the process of a grouping proof, both a tag group and the identity validity of individual tags are to be proved. Only grouping proofs provided by valid tags will be accepted. In the process of a grouping proof, the privacy security of both individual tags and their group as a whole must be considered. Processing complexity of both individual tags and their tag group as whole must be considered to improve group authentication efficiency. The following design criteria, therefore, must be highlighted in the design of a grouping-proof protocol besides requirements for common RFID system authentication protocols.

Data confidentiality: A yoking-proof protocol is to maintain the confidentiality of sensitive messages as messages are exchanged in insecure wireless channels in RFID systems.

Tag anonymity: An attacker cannot distinguish or trace a tag with exchange messages between the reader and the tag. Neither can the attacker acquire sensitive information of the tag, such as ID identifier or key.

Reader anonymity: An attacker cannot acquire sensitive information of a reader with exchange messages between the reader and tags or between the reader and the verifier.

Unforgeability of grouping proofs: An attacker cannot forge a yoking proof, i.e., no valid yoking proof will be generated if the attacker passes himself off as a tag, adds a tag or reduces a tag.

In the tree-structure-based protocol, a tag group has both group information and tag information. In this model, tag information represents individual information to distinguish each tag with its unique ID identifier. Group information of a tag, which characterizes its obvious group feature can reduce interaction with unauthentic RFID readers in protocol interaction to reduce computing load of a tag and to enhance protocol security. This protocol consists of four phases: System initialization, reader authorization, reader-tag mutual authentication, grouping-proof generation and grouping-proof verification. In the system initialization phase, the communication key between the server, the reader and tags is set; in the authorization phase, the verifier authorizes the reader to generate grouping proofs; in the grouping-proof generation phase, the reader generates grouping proofs according to tag information and in the grouping-proof verification phase, the verifier verifies the validity of grouping proofs.

The difficulty in elliptic curve discrete logarithms is the basis for the security of ECC. It can be described as below. The given ECC group in finite field Fp is as follows:

$$E\ (F_p) = \{(x, y)|\in F_p\times F_p,\ y = x^3+ax+b,\ a,\ b\in F_p\}\cup\{0\} \qquad (1)$$

Point P = (x, y)'s order is n. And n is a big prime number. Thus:

- With integer a given, it is easy to calculate point Q = aP
- With point Q given, it is rather difficult to calculate integer x and make xP = Q

Select a secure elliptic curve E_p in finite field F (p). The P is a base point on the curve. Additive group G is the set of all points on the elliptic curve. The #E represents the order of E_p. Prime number q is the greatest prime factor of #E. Symbols used in this study are as in Table 1 and 2.

The Y is the public key of the verifier and is stored in tags and the reader, x_{group} is the private key of the group of

Table 1: Tag information

Index	T_{group} (0) (j)	T_{group} (1) (j)	T_{group} (m-1) (j)
0	Y	Y	Y
1	x_{group0}	x_{group1}	$x_{group\ m-1}$
2	$ID_{0,j}$	$ID_{1,j}$	$ID_{m-1,j}$
3	$x_{0,j}$	$x_{1,j}$	$x_{m-1,j}$

Table 2: Reader information

Index	R_{group} (0)	R_{group} (1)	R_{group} (m-1)
0	Y	Y	Y
1	rID_0	rID_1	rID_{m-1}
2	k_0	k_1	k_{m-1}

tag $T_{g,j}$. And $x_{g,j}$ is the identity private key of the tag. The $ID_{g,j}$ is the identifier of the jth tag in group g. Reader R_k has its unique ID identifier rID_k with random number k_g as its private key.

System initialization: The backend server selects a random number $y \in Z_l$ as its private key and calculates the public key Y (= yP). For tag $T_{g,j}$, select random number x_{group}, $x_{g,j} \in Z_l$ as its private key. The x_{group} is the private key of the group of tag $T_{g,j}$ and its public key is $X_{group} = x_{group}P$. The $x_{g,j}$ is its identity private key and its public key is $X_{g,j} = x_{g,j}P$. For reader R_g, select random number k_g as its private key. Its public key is $K_g = k_gP$. Calculate $X_{g,j} = x_{g,j}P$ and make it the identifier $ID_{g,j}$ of the jth tag in group g. Then store {$ID_{g,j}$, X_{group}, y} and other relevant information in the database and store {x_{group}, $x_{g,j}$, Y, P} in the tag.

Assume that each reader R_k has its unique ID identifier rID_k. For reader R_k, select random number k_g as its private key. Its public key is $K_g = k_gP$. Figure 1 for the reader and tag initialization process.

Reader authorization: It is to apply for reading authorization for the tag group from the verifier V to generate grouping proofs when the reader reads tag group $X_{G,i}$ for the first time. When the first tag $T_{g,1}$ in a tag group is in the reading range of the reader, the reader generates random number e and sends the number to it. After receiving the random number, tag $T_{g,1}$ selects random number r and calculate $T_0 = rP$, $T_1 = rK_g$ and $s = \dot{r}(T_1)+x_g+er$ and returns (T_1, s) to the reader R_k. The reader calculates $X_{group} = (sP\text{-}\dot{r}\ (k_gT_0)\ P\text{-}eT_0)$, i.e., the public key for the tag group to generate grouping proofs (Hermans *et al.*, 2014). The reader generates random number r, calculates T_0, T_1 and sends it to the verifier V. The verifier calculates $X'_{group} = T_1\text{-}yT_0$ and searches the registry database to identify if there is $X_{group} = X'_{group}$. If there is $X_{group} = X'_{group}$, the verifier generates random number $v \in Z_l$ and sends V = vP to the reader. It also stores (rID_k, X_{group}, v) in the authorization database. Otherwise, abort the protocol and return failure information. Figure 2 for the reader authorization process.

Reader-tag mutual authentication: After reader authorization is successful, the reader selects random number $r_j \in Z_l$, calculates $T_1 = r_jP$ and sends T_1, r_j to tag $T_{g,j}$.

After receiving T_1, r_j the tag selects a random number $h_j \in Z_l$, calculates $T_2 - h_jP$ and $T_3 = T_1+(r_jx_g+h_j)K_g$ and sends T_2, T_3 to the reader.

After receiving T_2, T_3 the reader calculates $(k_g^{-1}(T_3 - T_1) - T_2)r_j^{-1}\ ? = X_{group}$ using its private key k_g. If the

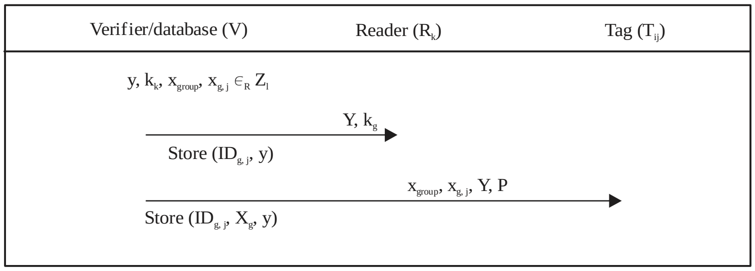
Verifier/database (V)
Reader (R_k)
Tag (T_{ij})
$y, k_k, x_{group}, x_{g,j} \in_R Z_l$
Y, k_g
Store ($ID_{g,j}$, y)
x_{group}, $x_{g,j}$, Y, P
Store ($ID_{g,j}$, X_g, y)

Fig. 1: System initialization

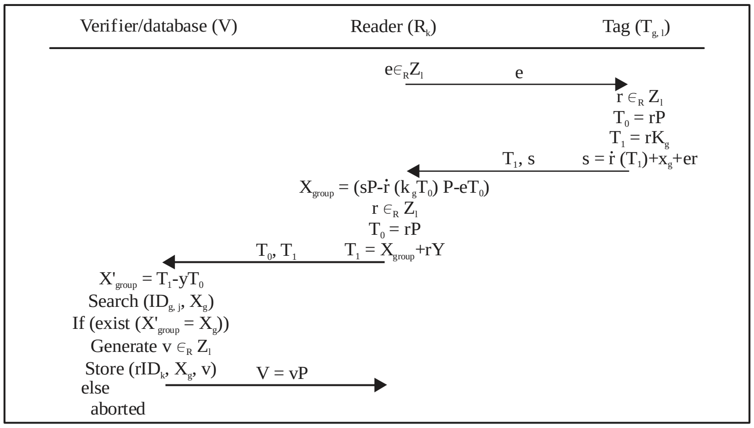

Fig. 2: Reader authorization

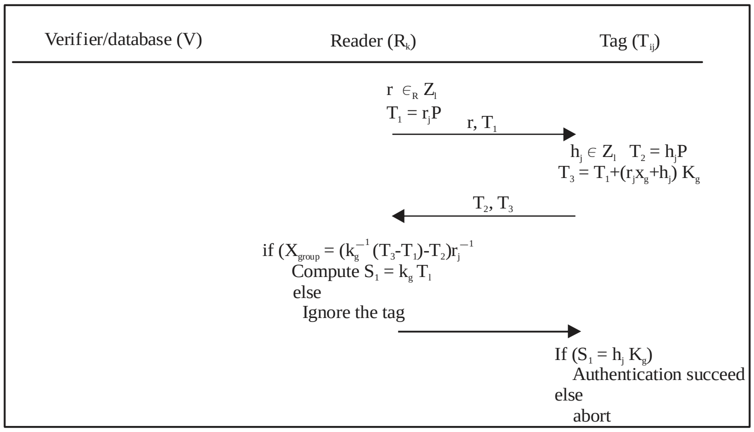

Fig. 3: Reader-tag mutual authentication

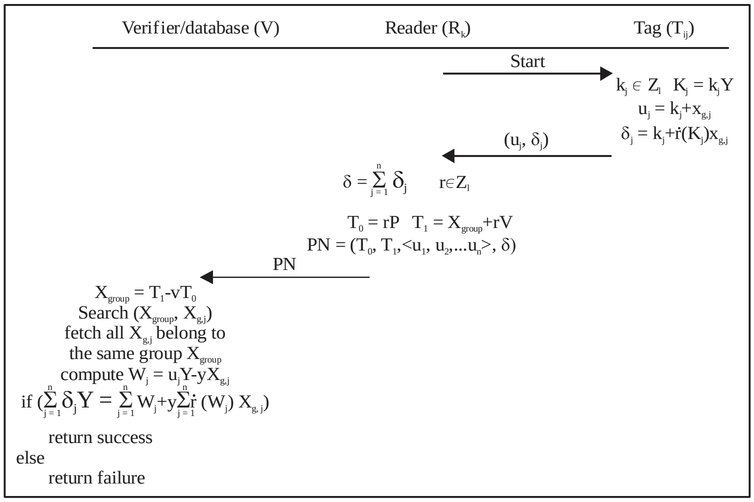
Verifier/database (V)
Reader (R_k)
Tag (T_{ij})
Start
$k_j \in Z_l$ $K_j = k_jY$
$u_j = k_j+x_{g,j}$
$\delta_j = k_j+\dot{r}(K_j)x_{g,j}$
(u_j, δ_j)
$\delta = \sum_{j=1}^{n} \delta_j$
$r \in Z_l$
$T_0 = rP$ $T_1 = X_{group}+rV$
$PN = (T_0, T_1,<u_1, u_2,...u_n>, \delta)$
PN
$X_{group} = T_1-vT_0$
Search (X_{group}, $X_{g,j}$)
fetch all $X_{g,j}$ belong to
the same group X_{group}
compute $W_j = u_jY-yX_{g,j}$
if ($\sum_{j=1}^{n} \delta_jY = \sum_{j=1}^{n} W_j+y\sum_{j=1}^{n}\dot{r} (W_j) X_{g,j}$)
return success
else
return failure

Fig. 4: Generation and verification process of grouping proof

equation holds, authentication succeeds, i.e., the tag belongs to the group. Otherwise, authentication fails. If authentication succeeds, the reader calculates $S_1 = k_gT_1$ and sends it to the tag. The tag then calculates h_jK_g and compares it to S_1. If they are equal, the tag finds the reader valid. Otherwise, authentication fails. The reader-tag mutual authentication process is shown in the Fig. 3.

Generation and verification of grouping proofs: After reader-tag mutual authentication is completed, the reader sends the start command to the tag. After receiving the command from the reader, tag $T_{g, j}$ selects random number $k_j \in Z_l$, calculates $K_j = k_jY$, $u_j = k_j+x_{g, j}$ and $\delta_j = k_j+\dot{r}(K_j\ x_{g, j})$ and sends sub-proof (u_j, δ_j) to the reader.

After receiving the nth (u_j, δ_j) the reader calculates $\delta = \sum_{j=1}^{n} \delta_j$. Then reader R_k selects random number r and calculates $T_0 = rP$ and $T_1 = X_{group}+rV$. In addition, the reader sends $PN = (T_0, T_1, <u_1, u_2,..., u_n>, \delta)$ as grouping proof to the verifier V. The verifier V then calculates $X_{group} = T_1\text{-}vT_0$, searches the registry database (X_{group}, $X_{g, j}$), fetches all tags $X_{g, j}$ in tag group X_{group} and calculates $W_j = u_jY\text{-}yX_{g, j}$. If the equation:

$$\sum_{j=1}^{n} \delta_j Y = \sum_{j=1}^{n} W_j + y\sum_{j=1}^{n} \dot{r}(W_j)X_{g,\,j}$$

holds, authentication succeeds. Otherwise, return failure information. The generation and verification process of grouping proof is shown in the Fig. 4.

RESULTS

The following security analysis on the protocol is made in accordance with the objective to be achieved by the grouping-protocol proposed by the study:

Correctness analysis

Theorem 1: The grouping-proof scheme proposed in this paper is correct.

Proof: Assume that grouping proofs are calculated in the previously mentioned process, then the grouping-proof generation and verification process is as below:

- Calculating the group of the tag:

The tag calculates $T_0 = r\,P$, $T_1 = r\,K_g$ and $s = \dot{r}(T_1)+x_g+er$ and returns (T_1, s) to reader R_k. The reader calculates:

$$\begin{aligned} & sP - \dot{r}(k_g T_0)P - eT_0 \\ & = (\dot{r}(T_1) + x_g + er)P - \dot{r}(k_g rP)P - erP \\ & = \dot{r}(rK_g)P + x_g P + erP - \dot{r}(rK_g)P - erp \\ & = X_{group} \end{aligned} \tag{2}$$

The reader collects all members belonging to group $X_{G,\,j}$ and generates grouping proofs.

- Verification:

$$\begin{aligned} W_j &= u_j Y - yX_{g,\,j} \\ &= (k_j + x_{g,\,j})Y - yX_{g,\,j} \\ &= k_j Y \end{aligned} \tag{3}$$

$$\begin{aligned} \sum_{j=1}^{n} \delta_j Y &= \sum_{j=1}^{n} W_j + y\sum_{j=1}^{n} \dot{r}(W_j)X_{g,\,j} \\ &= \sum_{j=1}^{n} (k_j + \dot{r}(K_j)x_{g,\,j})Y \\ &= \sum_{j=1}^{n} k_j Y + \sum_{j=1}^{n} \dot{r}(K_j)x_{g,\,j}Y \\ &= \sum_{j=1}^{n} W_j + y\sum_{j=1}^{n} \dot{r}(W_j)X_{g,\,j} \end{aligned} \tag{4}$$

According to the computational Diffie-Hellman (CDH) assumption, $k_jY = yK_i$ and $yX_{g,j}Y$. To calculate their values, k_j, y and $x_{g,\,j}$ must be given. These three values are however, respectively stored in the reader, the verifier and the tag. It is impossible for an attacker to influence them. This protocol is thus, correct.

Security: Zhang and Xu (2011) proposes the five security requirements for a grouping-proof RFID protocol in the internet of things, i.e., strong privacy preservation, untraceability, reader anonymity, tag anonymity and authorization. Security of the proposed protocol is analyzed in these five aspects below.

Strong privacy preserving: Only an authorized reader can read the coexistence proof of a tag group. An attacker cannot acquire any reader or tag identity information even if all messages are maliciously captured in all interactions. During protocol generation, only a reader authorized by the backend server can generate grouping proofs. In addition, there is reader-tag mutual authentication.

For a tag, privacy information transmitted during authentication is mainly group private key and identity private key (x_{group}, $x_{g,j}$). In transmission, both group private key and identity private key are blinded by $s = \dot{r}(T_1)+x_g+er$, $T_3 = T_1+(r_{ij}\,x_g+h_j)K_g$, $u_j = k_j+x_{g,\,j}$ and $\delta_j = k_j+\dot{r}(K_j)\,x_{g,\,j}$. In addition, r_j, k_j will be updated after each authentication process. An attacker, therefore cannot acquire any privacy information of a tag through private key.

For a tag group, an attacker cannot acquire privacy information of it if he fails to acquire the group private key and identity private key of a tag. In grouping-proof information (<u_1, u_2,..., u_n>, δ), both $u_j = k_j+x_{g,j}$ and:

$$\sum_{j=1}^{n} \delta_j = \sum_{j=1}^{n} (k_j + \dot{r}(K_j)x_{g,\,j})$$

contains random numbers. In the entire interaction process, an attacker, therefore can neither acquire reader or tag identity information nor distinguish what in the captured information represents reader or tag identity information.

Untraceability: An attacker cannot judge the relation between two grouping proofs PN_1 and PN_2 through a captured grouping proof set, i.e., can neither identify if the generators of two grouping proofs belong to the same group nor determine if the generators of two grouping proofs include the same member.

Though he may acquire multiple grouping proofs, the attacker cannot identify if the generators of two random grouping proofs are identical because the parameters r, k_j, r_j, h_j etc., used in each grouping-proof generation process are generated by readers and tags independently. There is no common law for grouping proofs to trace tags. Tag groups are therefore, untraceable.

Reader anonymity: Reader anonymity means that any attacker cannot acquire reader identity information. In interaction, information sent from tags to the reader and from the reader to the tag is encrypted with the public key. An attacker cannot acquire identity information related to the reader if he fails to acquire the private key. The attacker, therefore cannot acquire reader identity.

Tag anonymity: Tag anonymity means that any attacker cannot acquire the identity information of tag $T_{group,j}$. A random number r, k_j, r_j, h_j is selected to blind and encrypt the interaction information in both the reader-tag mutual authentication and grouping-proof generation processes. An attacker cannot acquire tag identity according to tag response information as r, k_j, r_j, h_j will be updated in each authentication process.

Authorization: A security issue often neglected in the generation of broadcasting yoking proofs is reader-tag mutual authentication. In this protocol, the reader and the tags in the same group have mutual authentication after the verifier V authorizes the reader. An attacker cannot forge a yoking proof, i.e., no valid yoking proof will be generated if the attacker passes himself off as a tag, adds a tag or reduces a tag.

An attacker may let a tag outside the group participate and complete grouping proof through forgery or reply attacks. Reply attack will not succeed as different random numbers are introduced in protocol interaction and all sessions are mutually independent. This is because it is impossible for the attacker to know the group private key and identity private key of the current valid tag or to acquire the authorization private key v. Then the verifier V cannot calculate $X_{group} = T_1\text{-}vT_0$ and $W_j = u_jY\text{-}yX_{g,j}$ and cannot verify if:

$$\sum_{j=1}^{n}\delta_j Y\ ?= \sum_{j=1}^{n} W_j + y\sum_{j=1}^{n}\dot{r}(W_j)X_{g,\,j}$$

holds. Authentication, therefore, fails. The protocol is therefore, resistant to impersonation attack.

DISCUSSION

So, after analyzing the existing ECC-based grouping-proof protocols, the article proposed a new ECC-based tree-structure grouping-proof protocol and analyzed its privacy and security. According to the above mentioned security analysis of the proposed protocol, Table 3 compares the proposed grouping-proof protocol to those proposed in the references in terms of the following aspects: Reply attack, parallel method, tracking attack, impersonation attack and authorization. As the comparison shows, the protocol proposed in this study basically meets the design requirements and is thus, secure to a certain extent.

In Table 3, all the schemes are designed for the grouping-proof application. The scheme proposed by Batina *et al.* (2012) was exclusively dependent on the use of ECC. Moreover, Lv *et al.* (2011) indicated that it could not resist tracking attack and an improved protocol was proposed to solve this issue. But the enhanced protocol was shown by Ko *et al.* (2011) to be impractical for use in public-key cryptography and then proposed an enhanced protocol to satisfy the functionalities and resist tracking attack. Although, the protocol proposed is more efficient than Batina *et al.* (2012), it cannot resist the modified tracking attack. Ko *et al.* (2014) proposed a new protocol to avoid the defects of protocol (Lin and Zhang, 2012) such as impersonation attack and tracking attack. However, our proposed protocol can resist those attacks.

Later, some literatures Hermans and Peeters (2012) and Guo *et al.* (2014) have also proved that there are security and privacy problems for the above protocols and corresponding improvement measures have been proposed. Although the public key system based, especially ECC-based grouping-proof protocols have been proposed and modified constantly, there are still insufficiencies. In Table 3, all the schemes in the references are designed with serial method and the grouping-proof we proposed is designed with broadcasting method. The proofs in the parallel method are more efficient than that in the serial method.

Table 3: Comparisons of ECC-based grouping-proof protocol

	Reply attack	Parallel method	Tracking attack	Impersonation attack	Authorization
Batina *et al.* (2012)	×	×	×	×	×
Lv *et al.* (2011)	√	×	×	×	×
Ko *et al.* (2011)	√	×	×	×	×
Lin and Zhang (2012)	√	×	×	×	×
Ko *et al.* (2014)	√	×	√	√	×
Hermans and Peeters (2012)	√	×	√	√	×
Guo *et al.* (2014)	√	×	√	√	×
Proposed	√	√	√	√	√

Table 3 depicts that our scheme has the highest security than others and it illustrates that our protocol can secure against all the RFID attacks, which was mentioned above.

CONCLUSION

There are soaring demands for tag grouping proofs RFID application constantly grows. An ECC-based tree-structure RFID grouping-proof protocol is proposed based on parallel multi-signature in this study. The protocol features such security advantages as strong privacy preservation, untraceability, reader anonymity, tag anonymity and authorization. It also prevents forgery attack because of the introduction of the reader-tag mutual authentication mechanism and tag computing workload is reduced in interaction. Security analysis of the proposed grouping-proof protocol is presented in this paper with a comparison between the protocol and existing counterparts. Compared with previous schemes, grouping-proof generation efficiency of this scheme has been significantly improved. It is of high availability to effectively generate grouping proofs in the scenario of a large tag quantity.

ACKNOWLEDGMENTS

This study is supported by scientific research project of Heze university (No. XY12KJ09) and the science and technology project of the Shandong province universities (No. J14LN21).

REFERENCES

Batina, L., Y.K. Lee, S. Seys, D. Singelee and I. Verbauwhede, 2010. Privacy-Preserving ECC-Based Grouping Proofs for RFID. In: Information Security, Burmester, M., G. Tsudik, S. Magliveras and I. Ilic (Eds.). Springer, New York, ISBN: 9783642181788, pp: 159-165.

Batina, L., Y.K. Lee, S. Seys, D. Singelee and I. Verbauwhede, 2012. Extending ECC-based RFID authentication protocols to privacy-preserving multi-party grouping proofs. Personal Ubiquitous Comput., 16: 323-335.

Burmester, M., B. de Medeiros and R. Motta, 2008. Provably Secure Grouping-Proofs for RFID Tags. In: Smart Card Research and Advanced Applications, Grimaud, G. and F.X. Standaert (Eds.). Springer-Verlag, Berlin, Heidelberg, ISBN: 978-3-540-85892-8, pp: 176-190.

Duc, D.N., D.M. Konidala, H. Lee and K. Kim, 2010. A survey on RFID security and provably secure grouping-proof protocols. Int. J. Internet Technol. Secured Trans., 2: 222-249.

Guo, C., Z.J. Zhang, L.H. Zhu, Y.A. Tan and Y. Zhen, 2014. A novel secure group RFID authentication protocol. J. China Univ. Posts Telecommun., 21: 94-103.

Ham, H., I. Kim and J. Song, 2015. An efficient offline grouping proof protocol using multiple types of tags. Proceedings of the 9th International Conference on Ubiquitous Information Management and Communication, January 8-10, 2015, Bali, Indonesia, pp: 1-8.

Hermans, J. and R. Peeters, 2012. Private yoking proofs: Attacks, models and new provable constructions. Proceedings of the 8th International Workshop on Radio Frequency Identification. Security and Privacy Issues, July 2-3, 2012, Nijmegen, The Netherlands, pp: 96-108.

Hermans, J. and R. Peeters, 2013. Private Yoking Proofs: Attacks, Models and New Provable Constructions. In: Radio Frequency Identification. Security and Privacy Issues, Hoepman, J.H. and I. Verbauwhede (Eds.). Springer, Berlin, Heidelberg, ISBN: 978-3-642-36139-5, pp: 96-108.

Hermans, J., R. Peeters and B. Preneel, 2014. Proper RFID privacy: Model and protocols. IEEE Trans. Mobile Comput., 13: 2888-2902.

Juels, A., 2004. Yoking-proofs for RFID tags. Proceedings of the 2nd IEEE Annual Conference on Pervasive Computing and Communications Workshops, March 14-17, 2004, Washington, DC., USA., pp: 138-143.

Kang, H.Y., 2013. Analysis and improvement of grouping-proof Protocol for RFID based on ECC. Comput. Eng., 39: 153-156.

Ko, W.T., S.Y. Chiou, E.H. Lu and H.K.C. Chang, 2011. An improvement of privacy-preserving ECC-based grouping proof for RFID. Proceedings of the Cross Strait Quad-Regional Radio Science and Wireless Technology Conference, Volume 2, July 26-30, 2011, Harbin, pp: 1062-1064.

Ko, W.T., S.Y. Chiou, E.H. Lu and H.K.C. Chang, 2014. Modifying the ECC-based grouping-proof RFID system to increase inpatient medication safety. J. Med. Syst., Vol. 38. 10.1007/s10916-014-0066-5

Lee, Y.K., L. Batina, K. Sakiyama and I. Verbauwhede, 2008. Elliptic-curve-based security processor for RFID. IEEE Trans. Comput., 57: 1514-1527.

Lin, Q. and F. Zhang, 2012. ECC-based grouping-proof RFID for inpatient medication safety. J. Med. Syst., 36: 3527-3531.

Lo, N.W. and K.H. Yeh, 2010. Anonymous coexistence proofs for RFID tags. J. Inform. Sci. Eng., 26: 1213-1230.

Lv, C., H. Li, J. Ma, B. Niu and H. Jiang, 2011. Security analysis of a privacy-preserving ecc-based grouping-proof protocol. J. Convergence Inform. Technol., 6: 113-119.

Ma, C., J. Lin, Y. Wang and M. Shang, 2012. Offline RFID grouping proofs with trusted timestamps. Proceedings of the IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, June 25-27, 2012, Liverpool, United Kingdom, pp: 674-681.

Peris-Lopez, P., A. Orfila, J.C. Hernandez-Castro and J.C.A. van der Lubbe, 2011. Flaws on RFID grouping-proofs. Guidelines for future sound protocols. J. Network Comput. Applic., 34: 833-845.

Piramuthu, S., 2006. On existence proofs for multiple RFID tags. Proceedings of the IEEE International Conference on Pervasive Services, June 26-29, 2006, Lyon, France, pp: 317-320.

Saito, J. and K. Sakurai, 2005. Grouping proof for RFID tags. Proceedings of the IEEE International Conference on Advanced Information Networking and Applications, March 28-30, 2005, Taiwan, China, pp: 621-624.

Zhang, Z. and Q.L. Xu, 2011. Universal composable grouping-proof protocol for RFID tags in the internet of things. Chinese J. Comput., 34: 1188-1194.