International Journal of Control and Automation
Vol. 9, No. 7 (2016), pp.343-352
http//dx.doi.org/10.14257/ijca.2016.9.7.32

Analysis and Improvement of ECC-based Grouping-proof Protocol for RFID

Kang Hong-yan[1,2]

[1]*Department of Computer and Information Engineering, Heze University, Heze 274015, Shandong, China*
[2]*Institute of Embedded Systems and Internet of Things, Heze University, Heze 274015, Shandong, China*
khyky@sina.com

Abstract

RFID grouping-proof protocols draw high attention as RFID technology is being widely applied. This paper proposes an improved ECC-based grouping-proof protocol on the basis of studying the grouping-proof protocol proposed by Batina et al. to solve the problems of existing grouping-proof protocols, such as low grouping-proof efficiency and being vulnerable to impersonation attacks, tracking attacks, and other security threats. First of all, this paper proved that the protocol by Batina et al. is vulnerable to impersonation attacks and tracking attacks. Secondly, the proposed improved grouping-proof protocol was described and analyzed. Malicious query of tags has been prevented because a new function of reader verification by tags is added to the existing protocols. Finally, the security performance of the proposed protocol was proved and a comparison with the protocols proposed in the references was made. As the theoretical analysis and comparison reveal, the scheme, with a significantly enhanced security and performance compared with similar schemes, meets the requirements for security and privacy.

Keywords: *Grouping-proof Protocol; Elliptic Curve Cryptography; impersonation attack; tracking attack; RFID*

1. Introduction

Compared to bar codes, RFID technology is advantaged in many aspects such as non-contact, affordable price, flexible deployment, easy-to-manage as well as availability in identifying moving objects, *etc*, which enable RFID technology to gradually develop into one of the most popular technologies among automatic identification technologies. RFID technology is widely applied to many fields such as supply chain management, automatic identification of persons or objects, warehouse management and identity recognition [1,2,3], thereby improving working efficiency remarkably while reducing the overall costs. As RFID technology develops rapidly, identification and authentication of multi-tag increasingly gain people's attention and are widely applied to fields such as logistics, supply chain management and medicine distribution [4]. RFID reader automatically collects a group of tag data through radio frequency signals and processes the data, identifies and verifies multiple tags simultaneously in a short period of time to indicate that these multiple tags are present at the same time, thus achieving the efficient and transparent management of a group of tags and providing proof that two or more tags are scanned at the same time by the same reader in its communication range. The identification of group tags and the authentication problems which exist at the same time are called as the grouping-proof of tags. In this application, it is not enough to only guarantee the security of single object. Moreover, whether multiple objects exist at the same time in one group should be verified, thus to guarantee the completeness and

ISSN: 2005-4297 IJCA

security of these objects, such as drugs under the same prescription which the doctors issue for patients; the whole set of medical apparatus and instruments which the hospital aims at certain specified operations; the boarding check, passport and luggage which belong to the same person in the airport [5,6,7]. Such group application characteristic of RFID technology requires that authentication protocol must have the capability to process, access and verify multiple tags at the same time.

2. Related Work

In 2004, using the ideas of mutual signature between two tags, Juels et al. [8] brought up the scheme for the first time to prove that two tags existed at the same time, which the authors called yoking-proof, indicating that two tags were scanned simultaneously. The introduction of this protocol raised the interests of many experts and scholars, and triggered heated debates and researches, which made improvements on this protocol one after another. Saito et al. [9] later proved that Juels's scheme was easy to suffer replay attack and improved yoking-proof, added timestamps as well as expanded from two tags to multiple tags. However, Piramuthu [10] proved that Saito's scheme did not fully solve the problems of replay attack. Bolotnyy et al. [11] brought up a new group-proof protocol and solved privacy problems related to the protocol. The new protocol was called anonymous group-proof protocol, in which each of the tags had the capability to compute Hash functions with secret keys. The main shortcomings of this protocol were that the verifier's computation complexity reached $O(n^2)$. Later, Peris Lopez et al. [12] made improvements on this scheme, which made the complexity of verification process reduced to $O(n)$. Concerning the authentication problems of tag group, Burmester et al. [13] put forward a secure model based on universally composable model, which was, however, easy to suffer impersonation attack from multiple parties. Lien et al. [14] put forward a group-proof protocol irrelevant to response orders of tags and improved the efficiency of tag group-proof protocol. However, Lien's grouping-proof protocol would leak the identification of tags, thus invading the privacy of tags. Later, Batina et al. [15] put forward yoking-proof based on public key cryptosystem. The security of Batina's protocol was established on the basis of Schnorr identity recognition protocol. However, the attackers could also fake the proof that T_a and T_b existed at the same time.

Vaudenay [16] pointed out that it was necessary to introduce public key cryptographic algorithm into RFID authentication protocol in order to provide strong privacy protection in the aspect of the leakage of tags' identity information. Lee et al. [17] and Hein et al. [18] put forward the possibility to introduce public key cryptogram, especially elliptic curve cryptosystem (ECC), into RFID protocol. Batina et al. [19] put forward RFID grouping-proof protocol at the earliest which had privacy protection based on ECC. But Lv et al. [20] pointed out that it could not resist tracking attack and put forward an improvement protocol. Later, Ko et al. [21] found that the protocol of Lv et al. [20] had a defect and proved that his protocol did not work, and put forward an improvement protocol to resist tracking attack. In 2012, Lin et al. [22] put forward a grouping-proof protocol and improved the efficiency of the protocol by Batina et al. [19]. Hermans et al. [23] brought up a new tag grouping-proof protocol and claimed that it reached narrow-strong privacy. Hermans's tag grouping-proof protocol required a trusted time stamping authority (TTSA) which generated time stamps. Similarly, some later documents [24,25] proved that above protocol had security and privacy problems, and put forward relevant improvement measures. The group verification protocol which was based on public key cryptosystem especially ECC was constantly put forward and revised, but still had some deficiencies. Generally speaking, tags did not contain clocks and there was no direct communication among tags. Instead, they communicated through readers. In the group authentication environment, readers were not trusted, which meant that any reader could provide the verifier with a group authentication. This important characteristic was always

neglected by researchers, which caused a lot of security problems. On the basis of analyzing the protocol by Batina et al. [19], this paper puts forward an improved authentication protocol based on ECC and analyzes its privacy and security.

3. Analysis on Grouping-Proof Protocol by Batina et al.

The notations used in the protocol are shown in Table 1.

Table 1. Notations in the Protocol.

Notations	Meaning
P	Base point in the EC group
y	Server's private key
Y	Server's public key
k , K	Reader's private key and public key
s_a, s_b	Tag's private key
S_a, S_b	Tag's public key
$x(T)$	The x-coordinate of T
r_a, r_b	Random number

3.1. Grouping-Proof Protocol by Batina Et al.

Literature [19] puts forward the grouping-proof protocol based on ECC. Before the protocol is executed, each tag has its own private key and the verifier's public key. The verifier stores the public key of each registered tag in the backend database, whose framework is demonstrated in Figure 1. The descriptions of protocol are as follows:

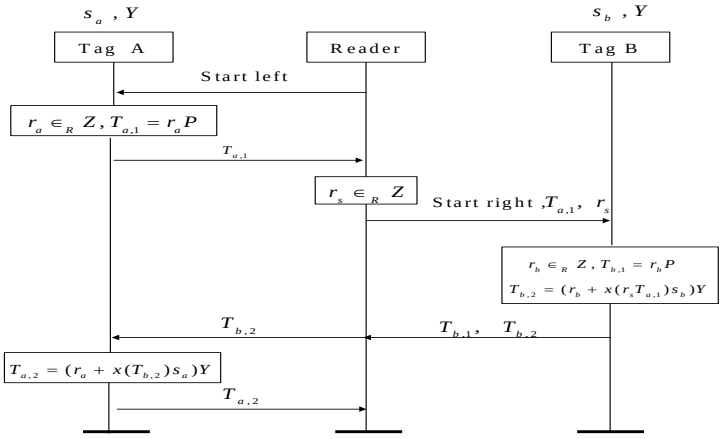

Figure 1. Batina Et Al. 's Protocol

1) The reader sends activating signal "start left" to Tag A ;

2) Tag A generates a random number r_a , calculates corresponding EC point $T_{a,1} = r_a P$ and sends it to the reader;

3) The reader generates a random number r_s , sends activating signal "start right", $T_{a,1}$ and r_s to Tag B ;

4) Tag B generates a random number r_b , calculates corresponding EC points $T_{b,1} = r_b P$ and $T_{b,2} = (r_b + x(r_s T_{a,1}) s_b) Y$, and sends $T_{b,1}$ and $T_{b,2}$ to the reader;

5) The reader sends $T_{b,2}$ to Tag A. Tag A calculates $T_{a,2} = (r_a + x(T_{b,2})s_a)Y$ and sends $T_{a,2}$ to the reader;

6) The reader collects grouping proof $(T_{a,1}, T_{a,2}, r_s, T_{b,1}, T_{b,2})$ and sends it to the backend server;

7) The backend server verifies $S_a = (y^{-1}T_{a,2} - T_{a,1})x(T_{b,2})^{-1}$ and $S_b = (y^{-1}T_{b,2} - T_{b,1})x(r_s T_{a,1})^{-1}$ to determine whether it accepts grouping proof. When the public keys of Tag A and Tag B have been registered at the verifier's backend database, the grouping proof is accepted, or otherwise refused. The grouping proof protocol between two tags can be easily expanded to the grouping proof protocol among multiple tags.

3.2. Attack on Grouping-Proof Protocol by Batina et al

In this part, we analyze the security of Batina et al. 's protocol, and prove that this protocol fails to resist tracking attack and it is insecure while facing impersonation attack.

Definition 1 Resist tracking attack: In the application protocol of RFID, if the adversary fails to access relevant information from the messages transmitted through the protocol to determine which tags are participants of a given communication session, then the protocol is said to be tracking attack resistant.

Definition 2 Resist to impersonation attack: If the adversary is unable to reuse the relevant information eavesdropped from the session between protocols to make fake messages and masquerade themselves as legitimate participants, then the RFID application protocol is said to be impersonation attack resistant.

Theorem 1 (Tracking attack) If the attacker can eavesdrop the messages $\{x(r_s T_{a,1}),\ T_{b,1},\ T_{b,2}\}$ in a normal communication process between the reader and Tag B, the attacker can detect any tag and determine whether or not the tag is Tag B.

Proof Tracking attack on Tag B is demonstrated in Figure 2. The detailed descriptions of this process are as follows:

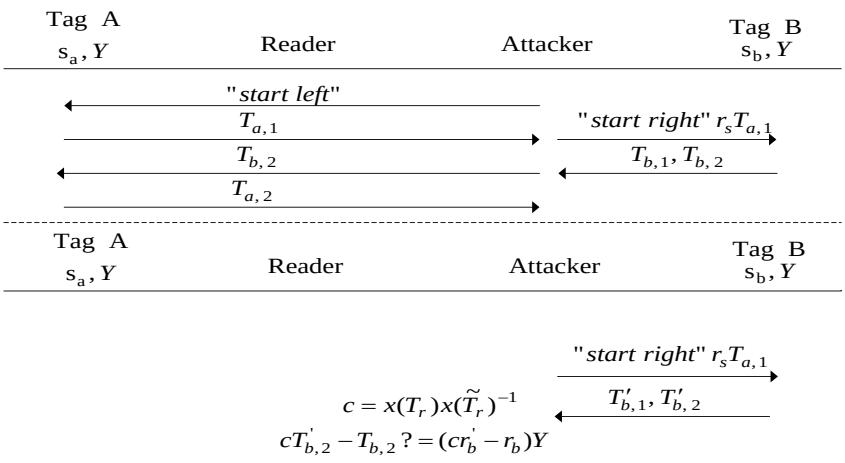

Figure 2.Tracking Attack on Tag

1) During normal communication, the attacker eavesdrops tuple $\{x(r_s T_{a,1}),\ T_{b,1},\ T_{b,2}\}$.

2) The attacker selects a Tag $\hat{B}$ and determine whether Tag $\hat{B}$ is Tag B. Suppose that Tag $\hat{B}$ is Tag B, the attacker selects a random number $\tilde{r}_s$ and calculates $\tilde{\tilde{T}}_r = \tilde{r}_s T_{a,1}$. Impersonated reader sends "start right" and $\tilde{\tilde{T}}_r$ to Tag $\hat{B}$. Tag $\hat{B}$ generates a random number r'_b and calculates $T'_{b,1} = r'_b P$ and $T'_{b,2} = (r'_b + x(\tilde{\tilde{T}}_r)Y$, and then sends them to the

attacker. The attacker calculates $c = x(T_r)x(\tilde{T}_r)^{-1}$. Because $T_{b,2} = r_b Y + x(r_s T_{a,1})Y$, we calculate $cT'_{b,2} - T_{b,2} = (cr'_b - r_b)Y + (cx(\tilde{T}_r) - x(r_s T_{a,1}))s_b Y$, Since $cx(\tilde{T}_r) - x(r_s T_{a,1}) = 0$, we get $cT'_{b,2} - T_{b,2} = (cr'_b - r_b)Y$. Consequently, the attacker can determine whether Tag $\hat{B}$ is Tag B by checking whether the equation $cT'_{b,2} - T_{b,2} = (cr'_b - r_b)Y$ holds. Using the same method, we can determine whether or not Tag $\hat{A}$ is Tag B . According to Definition 1, this protocol cannot resist tracking attack.

Theorem 2 (Impersonation attack) If the attackers can eavesdrop information $\{x(T_{b,2}),\ T_{a,1},\ T_{a,2}\}$ and $\{x(r_s T_{a,1}),\ T_{b,1},\ T_{b,2}\}$ in the normal communication process between the reader and the honest tag, the attacker can impersonate Tag T_b to generate grouping proof protocol.

Proof Impersonation attack on Tag B is demonstrated in Figure 3. The detailed descriptions of this process are as follows:

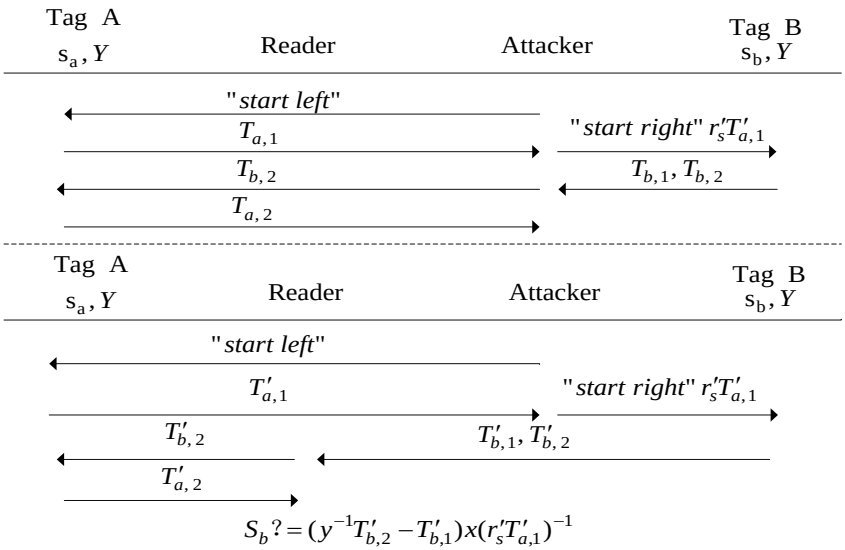

Figure 3. Impersonation Attack on Tag B

1) The attacker collects attack tuple $\{\alpha, T_1, T_2\}$ for which the following relations hold:

$T_1 = rP$ and $T_2 = (r + \alpha s)Y$

for s is the private key of the tag and $r \in_R Z$ an unknown random number.

Above tuple can be obtained by following means: because the reader is not verified and is untrusted, the attacker can query the tags actively to collect attack tuples $\{x(T_{b,2}),\ T_{a,1},\ T_{a,2}\}$ and $\{x(r_s T_{a,1}),\ T_{b,1},\ T_{b,2}\}$.

Among them, $T_{a,1} = r_a P$, $T_{a,2} = (r_a + x(T_{b,2})s_a)Y$

$T_{b,1} = r_b P$, $T_{b,2} = (r_b + x(r_s T_{a,1})s_b)Y$

2) Only when the attacker has tuple $\{\alpha, T_1, T_2\}$, the reader can be tricked to accept $T'_{b,1}$ and $T'_{b,2}$, which means that one can generate arbitrary grouping proof with respect to Tag B . Let $\beta = x(r'_s T'_{a,1})$, then $T'_{b,1}$ and $T'_{b,2}$ can be calculated as follows:

$T'_{b,1} = \gamma T_1 + \delta P$ $\quad T'_{b,2} = \gamma T_2 + \delta Y$ Among them : $\delta \in_R Z$ $\gamma = \beta / \alpha$

The verifier verifies $S_b ? = (y^{-1}T'_{b,2} - T'_{b,1})x(r'_s T'_{a,1})^{-1}$.

$$
\begin{aligned}
S_b &= (y^{-1}T'_{b,2} - T'_{b,1})x(r'_sT'_{a,1})^{-1} \\
&= (y^{-1}(\gamma T_2 + \delta Y) - (\gamma T_1 + \delta P))\beta^{-1} \\
&= (y^{-1}(\gamma (r_b + \alpha s_b)Y + \delta Y) - (\gamma r_b P + \delta P))\beta^{-1} \\
&= (\gamma r_b P + \gamma \alpha s_b P + \delta P - \gamma r_b P - \delta P)\beta^{-1} \\
&= \gamma \alpha s_b P \beta^{-1} \\
&= s_b P \\
&= S_b
\end{aligned}
$$

Consequently, the verification is passed and the attack succeeds. We can achieve the impersonation attack on Tag A in the same way. According to Definition 2, this protocol cannot resist impersonation attack.

4. The Improved Grouping Proof Protocol

Through the analysis in the 3 section, we can easily see that the reason why impersonation attack can be achieved is that there is no reader authentication and the reader can be untrusted. The attacker can carry out any query on the tags and the tags will send the response results back to the attacker, after the attacker collects attack tuple, the real reader can be tricked to accept Tag A .

To overcome the weakness of the grouping proof protocol based on ECC which is put forward by Literature [19] that this protocol cannot resist impersonation attack, based on the original protocol, we come up with improvement scheme, whose framework is demonstrated in Figure 4. The descriptions of the protocol are as follows:

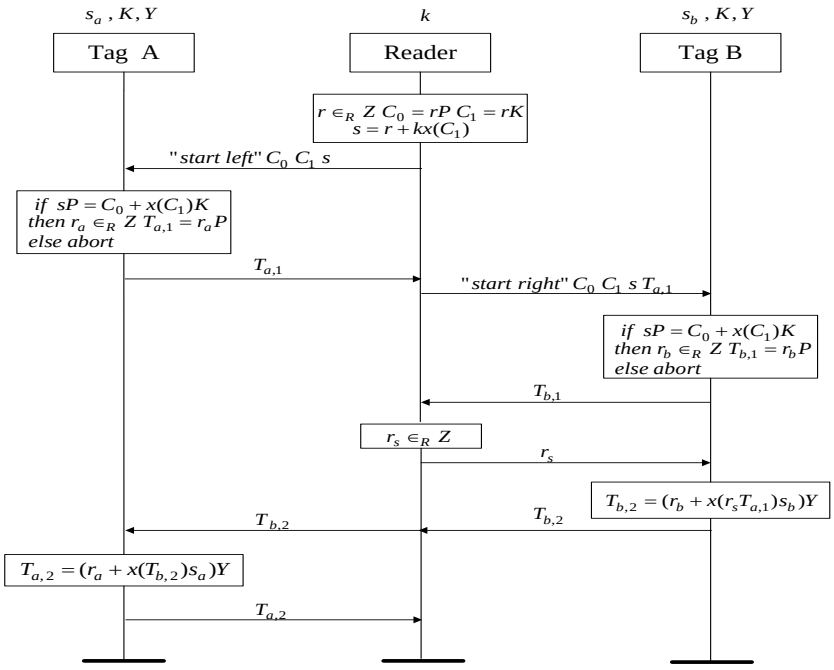

Figure 4. Proposed Protocol

Initialization Stage

The verifier selects a random number $y \in Z_l$ as its private key and calculates $Y(=yP)$ to be its public key. As for Tag T_t, a random number $s_t \in Z_l$ is selected to be its private key and its public key is $S_t = s_t P$, which serves as the identification ID_t for the tag T_t. As for the reader R, a random number $k \in Z_l$ is selected to be its private key and its public key is $K = kP$. $\{ID_t, y\}$ and other relevant information are stored in database while $\{s_t, Y, K\}$ is stored in tags.

Generation stage of grouping proof protocol

1) The reader generates a random number r, and calculates $C_0 = rP$, $C_1 = rK$, $s = r + kx(C_1)$, and sends activating signal "start left" to, and C_0, C_1, s to Tag A;

2) Tag A calculates $sP ? = C_0 + x(C_1)K$. If they are equal, then a random number r_a is generated and corresponding EC point $T_{a,1} = r_a P$ is calculated and sent to the reader, or otherwise the process is terminated;

3) The reader sends activating signal "start right" and $C_0, C_1, s, T_{a,1}$ to Tag B, then Tag B calculates $sP ? = C_0 + x(C_1)K$. If they are equal, then a random number r_b is generated and corresponding EC point $T_{b,1} = r_b P$ is calculated and sent to the reader, or otherwise the process is terminated;

4) The reader generates a random number r_s, and sends r_s to Tag B;

5) Tag B calculates corresponding EC point $T_{b,2} = (r_b + x(r_s T_{a,1})s_b)Y$, and sends $T_{b,2}$ to the reader;

6) The reader sends $T_{b,2}$ to Tag A, then Tag A calculates $T_{a,2} = (r_a + x(T_{b,2})s_a)Y$ and sends $T_{a,2}$ to the reader;

7) The reader collects grouping proof information $(T_{a,1}, T_{a,2}, r_s, T_{b,1}, T_{b,2})$ and sends it to the backend server;

8) The backend server verifies $S_a = (y^{-1}T_{a,2} - T_{a,1})x(T_{b,2})^{-1}$ and $S_b = (y^{-1}T_{b,2} - T_{b,1})x(r_s T_{a,1})^{-1}$ to determine whether to accept the group verification information. When the public keys of Tag A and Tag B have been registered in the verifier's backend database, the grouping proof protocol is accepted, or otherwise refused. The grouping proof protocol between two tags can be easily expanded to the grouping proof protocol among multiple tags.

5. Security Analysis and Comparison

5.1. Security Analysis

Theorem 3 The grouping proof protocol proposed by this paper can resist tracking attack.

Proof Let's Review the process of tracking attack: The attacker selects a Tag $\hat{B}$ and determine whether Tag $\hat{B}$ is Tag B. Suppose that Tag $\hat{B}$ is Tag B, the attacker selects a random number $\tilde{r}_s$ and calculates $\tilde{T}_r = \tilde{r}_s T_{a,1}$. Impersonated reader sends "start right" and $\tilde{T}_r$ to Tag $\hat{B}$. Tag $\hat{B}$ generates a random number $r_b^{'}$ and calculates $T_{b,1}^{'} = r_b^{'} P$ and $T_{b,2}^{'} = (r_b^{'} + x(\tilde{T}_r)Y$, and then sends them to the attacker. The attacker calculates $c = x(T_r)x(\tilde{T}_r)^{-1}$. Because $T_{b,2} = r_b Y + x(r_s T_{a,1})Y$, we calculate $cT_{b,2}^{'} - T_{b,2} = (cr_b^{'} - r_b)Y + (cx(\tilde{T}_r) - x(r_s T_{a,1}))s_b Y$, Since $cx(\tilde{T}_r) - x(r_s T_{a,1}) = 0$, we get

$cT_{b,2}^{'} - T_{b,2} = (cr_b^{'} - r_b)Y$. Consequently, the attacker can determine whether Tag $\hat{B}$ is Tag B by checking whether the equation $cT_{b,2}^{'} - T_{b,2} = (cr_b^{'} - r_b)Y$ holds. The impersonated reader sends "start right" and $\tilde{T}_r$ to Tag $\hat{B}$. In the proposed protocol, after the tag receives "start right" and C_0, C_1, s , firstly it needs to verify $sP ? = C_0 + x(C_1)K$. $sP = (r + kx(rK))P = rP + kx(rK)P$, if $sP = C_0 + x(C_1)K$, the attacker must gets the private key k of the reader, which means that the attackers can get k from $K = kP$. This is equal to solving ECDLP. Or otherwise, the protocol is terminated and the generation process of the protocol cannot be fulfilled. As a result, the attackers cannot determine whether the tags which participate in the protocol are the same tags by eavesdropping the information of session between the tags and the reader. Thus, this protocol can resist tracking attack.

Theorem 4 The group verification protocol put forward by this paper can resist impersonation attack.

Proof If the attackers want the impersonated Tag B to pass the verifier's verification, they need to collect attack tuple $\{\alpha, T_1, T_2\}$. Among them, $T_1 = rP$ and $T_2 = (r + \alpha s)Y$, s is the private key of the tag, $r \in_R Z$.

If the attackers want to get $\{\alpha, T_1, T_2\}$, the impersonated reader must collect tuples $\{x(T_{b,2}), T_{a,1}, T_{a,2}\}$ and $\{x(r_s T_{a,1}), T_{b,1}, T_{b,2}\}$. In the proposed protocol, the tag must firstly verify $sP ? = C_0 + x(C_1)K$. $sP = (r + kx(rK))P = rP + kx(rK)P$, if $sP = C_0 + x(C_1)K$, the attackers must get the private key k of the reader, which means that the attackers can get k from $K = kP$. This is equal to solving ECDLP. Thus the protocol can resist impersonation attack.

5.2. Security Comparison

According to above analysis on the security of the protocol, Table 2 describes the comparison between the improved grouping protocol proposed by this paper and the grouping proof protocol in the reference literature. It can be seen from the comparison that the protocol in this paper basically reaches the requirements of the design objectives, and has the characteristics of having strong privacy protection, resisting tracking attack and resisting impersonation attack, which meet the security demands.

Table 2. Comparison of Security Performance

Protocol	Batina[19]	Lv[20]	Ko [21]	Lin [22]	The protocol of this article
Tracking attack	×	×	×	×	√
replay attack	×	×	×	×	√
impersonation attack	×	×	×	×	√
Man-in-Middle attack	×	√	√	×	√

6. Conclusion

In this paper, we analyzed Batina et al. 's protocol and proved that it could not resist tracking attack and impersonation attack. On this basis, we put forward improved protocol which could resist tracking attack and impersonation attack. This paper gave detailed descriptions on this protocol and proved its security, and compared it with current grouping proof protocol which was based on ECC. The results indicated that the protocol designed by this paper could satisfy the security demands of the grouping proof protocol and had relatively high reliability on the premise of guaranteeing correctness and security.

Acknowledgements

This work was supported by scientific research project of Heze University (No. XY12KJ09) and the science and technology project of the Shandong province universities (No. J14LN21).

References

[1] X. Zhu, S. K. Mukhopadhyay and H. Kurata, "A review of RFID technology and its managerial applications in different industries", Journal of Engineering and Technology Management, vol.29, no.1, **(2012)**, pp.152–167.
[2] D. Nguyen, D. M. Konidala, H. Lee and K. Kim, "A survey on RFID security and provably secure grouping-proof protocols", International Journal of Internet Technology and Secured Transactions, vol.2, no.2, **(2010)**, pp.222-249.
[3] M. Burmester, T. V. Le, B. D. Medeiros and G. Tsudik, "Universally composable RFID identification and authentication protocols", Acm Burmester Magkos & Chrissikopoulos Transactions on Information & System Security, vol.12, no.4, **(2003)**, pp.60-61.
[4] Y. H. Lien, C. T. Hsi, X. Leng, J. H. Chiu and K. C.Chang, "An RFID-based Multi-batch Supply Chain Systems", Wireless Personal Communications, vol.63, no.2, **(2012)**, pp.393-413.
[5] C.L. Chen and C.Y. Wu, "Using RFID yoking proof protocol to enhance inpatient medication safety", Journal of Medical Systems, vol.36, no.5, **(2012)**, pp.2849-2864.
[6] H.Y. Chien, C.C. Yang, T.C. Wu and C.F. Lee, "Two RFID-based solutions to enhance inpatient medication safety", Journal of Medical Systems, vol.35, no.3, **(2011)**, pp.369-375.
[7] P. Peris-Lopez, A. Orfila, J. C.Hernandez-Castro and J. C. A. V. D. Lubbe, "Flaws on RFID grouping-proofs Guidelines for Future Sound Protocols", Journal of Network and Computer Applications, vol.34, no.3, **(2011)**, pp.833-845.
[8] A. Juels, "Yoking-Proofs" for RFID Tags", Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, **(2004)**, pp.138-143.
[9] J. Saito and K. Sakurai, "Grouping Proof for RFID Tags", IEEE International Conference on Advanced Information Networking and Applications, **(2005)**, pp.621-624.
[10] S. Piramuthu "On Existence Proofs for Multiple RFID Tags", IEEE International Conference on Pervasive Services, **(2006)**, pp.317-320.
[11] L. Bolotnyy and G. Robins, "Generalized "Yoking-Proofs for a Groupof RFID Tags", Annual International Conference on Mobile and Ubiquitous Systems, **(2006)**, pp.1-4.
[12] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador and Arturo Ribagorda, "Solving the Simultaneous Scanning Problem Anonymously: Clumping Proofs for RFID Tags", IEEE International Conference on Pervasive Services, Workshop on Security, Privacy and Trust in Pervasive andUbiquitous Computing, **(2006)**, pp.55-60.
[13] M. Burmester, B. de Medeiros and R. Motta, "Provably Secure Grouping-Proofs for RFID Tags", Gilles Grimaud and Francois-Xavier Standaert, Editors. Proceedings of the 8th Smart Card Research and Advanced Applications, Royal Holloway University of London, United Kingdom, **(2008)**, pp.176–190.
[14] Y. Lien, X. Leng, K. Mayes and J.-H. Chiu, "Reading order independent grouping proof for RFID tags", IEEE International Conference on Intelligence and Security Informatics, **(2008)**, pp.128–136.
[15] L. Batina, Y. K. Lee, S. Seys, D. Singel´ee and I. Verbauwhede, "Extending ECC-based RFID authentication protocols to privacy-preserving multi-party grouping proofs", Personal and Ubiquitous Computing, vol.16, no.3, **(2012)**, pp.323-335.
[16] S. Vaudenay, "On privacy models for RFID", Lecture Notes in Computer Science", vol.4833, **(2007)**, pp.68-87.
[17] Y. K. Lee, K. Sakiyama, L. Batina and I. Verbauwhede, "Elliptic Curve Based Security Processor for RFID", IEEE Transactions on Computer, vol.57, no.11, **(2008)**, pp.1514–1527.
[18] D. Hein, J. Wolkerstorfer and N. Felber, "ECC is Ready for RFID - A Proof in Silicon", Lecture Notes in Computer Science, Vol. 5381, **(2009)**, pp.401-413.
[19] L. Batina, L. Y.ee, S. Seys, D. Singele and I. Verbauwhede, "Privacy-preserving ECC-based grouping proofs for RFID", Lecture Notes in Computer Science, **(2011)**, vol. 6531, pp.159-165.
[20] C. Lv, H. Li, J. Ma, B. Niu and H. Jiang, "Security analysis of a privacy-preserving ECC-based grouping-proof protocol", Journal of Convergence Information Technology, vol.6, no.3, **(2011)**, pp.113-119.
[21] W. Ko, S. Chiou, E. Lu and H. Chang, "An improvement of privacy-preserving ECC-based grouping proof for RFID", Cross Strait Quad-Regional Radio Science and Wireless Technology Conference, **(2009)**, pp.1062-1064.
[22] Q. Lin and F. Zhang, "ECC-based grouping-proof RFID for inpatient medication safety", Journal of Medical Systems, vol.36, no.6, **(2012)**, pp.3527-3531.
[23] J. Hermans and R. Peeters, "Private yoking proofs: attacks, models and new provable constructions", Lecture Notes in Computer Science, vol. 7729, **(2013)**, pp.96-108.

[24] W.T. Ko, S.Y. Chiou, E.H. Lu and H.K. Chang, "Modifying the ECC-Based Grouping-Proof RFID System to Increase Inpatient Medication Safety", Journal of Medical Systems, Vol.38, No.9, **(2014)**, pp.1-12.
[25] C. Guo, Z.J. Zhang, L.H. Zhu, Y.A. Tan and Z. Yang "A novel secure group RFID authentication protocol", The Journal of China Universities of Posts and Telecommunications, vol.21, no.1, **(2014)**, pp.94-103.

Authors

Hong-yan Kang, he received the B.E. degree in computer application from Shandong University, Jinan, China, in 1999, and the M.S. degree in computer application from Shandong University of technology, Zibo, in 2006. Currently, he is an Assistant Professor in Department of Computer and Information Engineering at Heze University. His current research interests include embedded system, IoTs and ubiquitous sensor networks.

