Send Orders for Reprints to reprints@benthamscience.ae

A Scalable ECC-Based Grouping-proof Protocol for RFID Systems

Kang Hong-yan*

Department of Computer and Information Engineering, Heze University, Heze, Shandong, 274015, China

Embedded Systems and Internet of Things institute, HeZe University, Heze, Shandong, 274015, China

Abstract: The paper has proposed a grouping-proof protocol that can conduct parallel processing, specific to the problem of low generation efficiency of the grouping-proof protocol of the existing RFID grouping proof scheme, based on the difficulty of the elliptic-curve discrete logarithm, by analyzing the insufficiency of the existing grouping-proof protocol design proposal. Besides, the paper has described the presented grouping-proof protocol, and proved it from security, correctness and privacy. The analysis shows that, the proposal can meet security and privacy requirements, and has higher security and lower tag calculation complexity compared with the similar protocols.

Keywords: Scalable, ECC, grouping-proof, security, privacy, RFID.

1. INTRODUCTION

RFID technology identifies target objects in the open system environment with radio frequency signals. Compared with the bar code, RFID is non-contacting, inexpensive, flexible in deployment, easy to manage and moving object identifiable, etc. So, it has gradually become one of the most popular automatic identification technologies. Although the existing RFID single tag identification and authentication protocol has been widely used in the supply chain management, automatic identification of people or objects, inventory management, identity recognition, etc. [1-3], it is unable to meet group authentication requirements.

In the process of the rapid development and practical application of the RFID, tags needing identification on some special occasions usually have the obvious group feature, i.e. two or more tags are required to be scanned "simultaneously" within a definite range, and the evidence that two or more tags are scanned simultaneously by one reader within its communication range shall be provided [4]. Usually, such problem is referred to as the tag grouping proof, and the multi-tag identification and authentication has increasingly aroused people's concern. There are numbers of application for such problem [5-7]: medicines prescribed by doctors are of the same prescription, so as to reduce the drug risk of patients; in the pharmaceuticals industry, drug manufacturers will assure that medicines will be sold along with the prescriptions; at the airport, the boarding check, passport and luggage, etc. will be generated to be one group to guarantee security. In such applications, it is not enough to only guarantee the security of single entities, information security and integrity can only be assured when several entities belonging to the same group is verified. Such grouping application characteristics of the RFID technology require that the authentication protocol shall be able to handle multi-tag simultaneous access and prove.

2. RELATED WORK

Juels [4] had first made a research on the issue of multi-tag in 2004, and come up with a yoking-proof protocol. However, Saito *et al.* [8] pointed out that, this protocol could not resist the replay attack, because attackers could make up a legitimate grouping proof from several authentication sessions and introduce the timestamp mechanism to improve such protocol. Thus, an improved grouping-proof protocol was proposed. However, Piramuthu *et al.* [9] considered that there was still a vulnerability, i.e. the protocol was unable to resist the replay attack. So, a new grouping-proof protocol was proposed to overcome such deficiency. Although the new protocol had improved the security level, security threats such as privacy disclosure, forward security and DoP attack, etc. failed to be settled. Burmester *et al.* [10] considered that it was not secure enough to only assure the tag coexistence, and proposed 3 grouping authentication protocols based on the share group key, where the third protocol is featured by anonymity and forward security.

The grouping-proof protocol can be divided into two classes as per the different data collection methods: chain-linking grouping-proof protocol and broadcast-style grouping-proof protocol. As to the former [11], during the collection of the group data, an inquiry command will be created by the reader, sent to the first tag. After a response is made by the first tag, the reader will conduct data processing to it, and send the inquiry command to the second tag, and so on, a grouping proof will be generated only after a response from the last tag is obtained by the reader. As to the latter [12, 13], an inquiry command is broadcast by the reader, and responded by all tags, and a grouping proof is generated according to all the responses collected by the reader.

1874-4443/15

For the above-mentioned random number based grouping-proof protocol, share group ID based grouping-proof protocol and tree-based yoking-proof protocol, most of which have applied the hash function, message authentication code and pseudo random number, etc. Studies on the grouping-proof protocol are mainly based on the hash function, random function, secret sharing function, pseudo random function and symmetric cryptographic algorithm, with problems of scalability, security and privacy, etc. Therefore, only basic privacy protections can be provided.

Vaudenay [14] pointed out that it is essential to introduce the public key encryption algorithm into the RFID authentication protocol, so as to provide strong privacy protection agaisnt tag ID information disclosure. It was proposed by Lee *et al.* [15] and Hein *et al.* [16] that a public key cryptography especially elliptic curve cryptography (ECC) shall be introduced into the RFID protocol. Batina *et al.* [17] proposed the ECC-based RFID grouping-proof protocol with privacy protection at the earliest. However, it was pointed out by Lv et al.[18] as tracking attack irresistible, and an improved protocol was proposed. Later, Ko et al.[19] discovered that, there was a deficiency in the protocol proposed by Lv *et al.* [19], proved that such protocol does not work, and proposed an improved protocol to resist the tracking attack. In 2012, a grouping-proof protocol was proposed by Lin *et al.* [20], which had improved the efficiency of the protocol proposed by Batina *et al.* [17]. Later, some literatures [21-23] 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. So, after analyzing the existing ECC-based grouping-proof protocols, the paper has presented a new ECC-based grouping-proof protocol, and analyzed its privacy and security.

The paper has made the following arrangements: Section 3 briefly reviewed the safety requirement and attacker model of grouping-proof protocol. New proposed parallel grouping-proof protocol was introduced in section 4. Security and performance analyses of proposed protocol were addressed in section 5. Finally, we gave the concluding remarks in section 6.

3. SAFETY REQUIREMENT AND ATTACKER MODEL OF GROUPING-PROOF PROTOCOL

In order to guarantee the validity and safety of grouping-proof protocol, the protocol design should be based on the following principles:

(1) In the grouping-proof protocol generation process, not only should the validity of tag grouping-proof protocol be guaranteed, but also the identities of single tag and reader-writer should be verified, and only the grouping-proof information provided by legal tag and reader can be accepted;

(2) In the grouping-proof protocol generation process, the privacy and safety of both single tag and group tag as a whole must be considered;

(3) How to improve the efficiency of group authentication should be considered from the complexities, single tag processing, integral tag group processing and authentication processing.

Suppose an attacker A is a probabilistic polynomial time algorithm, and it can observe, change and play back all information exchanged between reader and tag and even produce new information. We use the oracle machine model defined by Hermans *et al.* [24] to give a group of tags and readers and suppose A can interact with the system via the same oracle.

Definition 1 A grouping-proof protocol is correctness provided that the probability of grouping-proof protocol's rejection of legal tag can be neglected.

Authentication game:

Initialization: select a tag T_i and a reader R;

Learning phase: An attacker randomly calls oracle $Launch()$, $SendTag()$, $Send\,\mathrm{Re}ader()$ and $Corrupt()$ to query the tag T_i and R for several times;

Challenge phase: An attacker calls $SendTag()$, $Send\,\mathrm{Re}ader()$and $Corrupt()$ to simulate the reader and tag to participate in authentication in the protocol;

End phase: If a valid tag or reader can authenticate the legality of reader or tag counterfeited by an attacker, then the attacker A wins the game.

Definition 2 If the successful probability a polynomial time attacker A in the authentication game can be neglected, then the RFID grouping-proof protocol is deemed to have the authentication property.

Privacy Game

Initiation: An attacker selects n tags T_i and a reader R;

Learning phase: An attacker selects two tags T_0 and T_1, calls oracle $Launch()$, $SendTag()$ and $Send\,\mathrm{Re}ader()$ to randomly query the same tags and reader, and randomly calls oracles $Launch()$, $SendTag()$, $Send\,\mathrm{Re}ader()$ and $Corrupt()$ to query other tags;

Challenge phase: The bit $b \in \{0,1\}$ randomly selected by an attacker services as a challenge and $T_b \in \{T_0, T_1\}$ is sent to the attacker, and if $b = 0$, then $T_b = T_0$,otherwise $T_b = T_1$; the attacker can call oracle machines $Launch()$, $SendTag()$ and $Send\,\mathrm{Re}ader()$ to randomly query T_b and R;

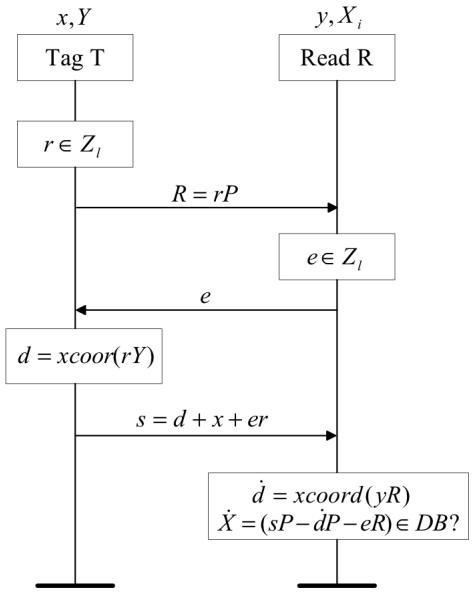

Fig. (1). Private RFID identification protocol of Jens Hermans.

Table 1. Notations in the protocol.

Notations	Meaning
P	Base point in the EC group
y , Y	Server's private key and public key
x_i , X_i	Tag's private key and public key
$\dot{r}(x)$	The x-coordinate of x
r, k	Random number

Speculation phase: The attacker stops to interact with the challenger and a bit b' is output; if $b' = b$, the attacker wins the game.

Definition 3 The probability of winning the privacy game of an attacker can be defined as $\left|\Pr[b' = b] - 1/2\right|$, and if the advantage of an attacker A can be neglected, then a RFID grouping-proof protocol has privacy protection property.

4. RFID GROUPING-PROOF PROTOCOL

The literature [25] proposed a new privacy model on the basis of analysis the existing adversary model and redefines the privacy level under the proposed privacy model. The new ECC-based RFID identification protocol with higher efficiency is proposed, as shown in the Fig. (**1**).

This article considers the above principles comprehensively and constructs the new RFID grouping-proof protocol on the basis of the identification protocol. The notations used in the protocol are shown in Table **1**.

The description of the protocol is as below:

(1) Initialization phase

A reader selects a random number $y \in Z_l$ as its private key and calculates $Y(= yP)$ as its public key. Meanwhile the reader selects a random number $x_i \in Z_l$ as the private key of a tag and calculates $X_i (= x_i P)$ as the identity ID_i of the i tag, and stores $\{ID_i, y\}$ and other related information in the database as well as $\{x_i, Y, P\}$ in the tag.

(2) Grouping-proof generation

Step 1: Query

R broadcasts the "start" command to all tags;

Step 2: T-R Response

After receiving the broadcast command of a reader R, the tag T_i selects a random number k_i and sends $K_i = k_i P$ to the reader R ;

Step 3: R-T Reply

After receiving $K_1, K_2, \cdots\cdots K_n$, a reader R generates a random number ts, calculates $h = hash(\dot{r}(K_1) \oplus \dot{r}(K_2) \oplus \cdots\cdots \oplus ts)$ and broadcasts to all tags.

Step 4: T-R Reply

After receiving h, a tag T_i calculates $s_i = \dot{r}(k_i Y) + x_i + hk_i$ and sends s_i to the reader R;

Step 5: After receiving the n^{th} s_i, the reader R sends $p = \{K_1, K_2, \cdots\cdots, s_1, s_2, \cdots\cdots, h, ts\}$ as the grouping-proof to the background sever for verification.

Step 6: After the server verifies the received grouping-proof protocol p, the grouping-proof protocol can be verified only by verifier by using the private key y, with the proof procedure as follows:

$$h' = hash(\dot{r}(K_1) \oplus \dot{r}(K_2) \oplus \cdots\cdots \oplus ts) \tag{1}$$

$$X_1 = s_1 P - \dot{r}(yK_1) - h'K_1 \tag{2}$$

$$X_2 = s_2 P - \dot{r}(yK_2) - h'K_2 \tag{3}$$

$$\vdots$$

$$X_n = s_n P - \dot{r}(yK_n) - h'K_n \tag{4}$$

5. SECURITY PROOF AND EFFICIENCY ANALYSIS

5.1. Security Analysis

Theorem 1: This protocol is correctness in accordance with definition 1.

Suppose that the grouping-proof is obtained based on the above-mentioned calculation process, the proof procedure is described as follows:

(1) Calculation:

$$h' = hash(\dot{r}(K_1) \oplus \dot{r}(K_2) \oplus \cdots\cdots \oplus ts) \tag{5}$$

(2) Proof:

$$\begin{aligned} & s_i P - \dot{r}(yK_i)P - h'K_i \\ & = (\dot{r}(k_i Y) + s_i + hk_i)P - \dot{r}(yK_i)P - h'K_i \\ & = \dot{r}(k_i Y)P + s_i P + hk_i P - \dot{r}(yk_i P)P - h'k_i P \\ & = X_i \end{aligned} \tag{6}$$

Based on CDH hypothesis, $k_i Y = yK_i$, and to calculated its value, k_i or y must be given, and since these two values are stored in the tag or reader, they are impossible to be affected by an attacker. Accordingly, this protocol is correctness.

Theorem 2 For a polynomial time attacker, the protocol proposed in this paper has the authentication property in accordance with definition 2.

The authentication property is based on one more discrete logarithm (OMDL) hypothesis put forward by Bellare *et al.* [26]. Let P be a generator of a group G_l with order of l, after n challenge inquiries in the oracle $O_1(\,)$ and m discrete logarithm inquiries in the oracle $O_2(\,)$, $m < n$ is satisfied and the discrete logarithms of n random points are calculated. Wherein, for the oracle $O_1(\,)$, the inquiry is preset to output a random element $h \in G_l$; for the oracle $O_2(\,)$, the inquiry z is preset to output $s \in G_l$ and satisfy $z = gs$.

Proof: suppose that an opponent A can counterfeit a grouping-proof protocol, we construct an opponent B to win the OMDL game in the following manner:

(1) $X = O_1(\cdot)$, wherein X is used as the public key of target tag;

(2) B executes A, and at the first stage, B simulates the i^{th} SendTag() oracle machine to query in the following manner:

a) $SendTag(\cdot) \to K_i$: $K_i = O_1(\cdot)$;

b) $SendTag(h) \to s_i$: $s_i = O_2(\dot{r}(k_i Y)P + X + h_i K_i)$

Next, the executing processes of A and B are as follows:

a) During the first execution, A sends K_i to the reader and calculates $\dot{r}(yK_i)$ and s_i, and during the second execution of the protocol, A uses the oracle machine $Send\,\text{Re}ader()$ and return to h';

b) During the second execution, A sends K_i to the reader-writer and calculates $k = (s_i - s_i')/(h - h')$ and $x = s_i - \dot{r}(k_i Y) - hk$, and returns to x and $h_i^{-1}(s_i - x - \dot{r}(k_i Y))$.

The opponent B simulates the above procedures. If B is required to finally win the OMDL game, it is required that $s_i = s_i'$; since ts is a random number, h and h' are random numbers, but under the condition where h and h' are random numbers and $K_i \neq 0$, the triumph probability of B can be neglected, so this protocol has the authentication property.

Theorem 3 For a polynomial time attacker, the RFID grouping-proof protocol proposed in this paper has the privacy protection property in accordance with definition 3.

The privacy protection property is based on the proposed ODH hypothesis and XL hypothesis [25]. XL hypothesis: For the point on the elliptic curve, the discrete logarithm problem is equal to the solution of x-coordinate of the point. The difficulty of XL problem is the equivalent to the solution of DDH problem.

Table 2. Performance evaluation of related works.

Protocol	The Number of Point Multiplications of Tag
Batina[17]	3
Lv[18]	3
Ko[19]	3
Our protocol	2

Proof: Suppose that an opponent A wins the narrow strong privacy game with a non-negligible probability, we construct an opponent B to win ODH hypothesis. B_i simulates the operation of the opponent A. According to the oracle machine model proposed in Reference [25] and the hybrid argument, because $s_1 = \dot{r}(k_1 Y) + x_1 + hk_1$, $s_2 = \dot{r}(k_2 Y) + x_2 + hk_2$, $\cdots$ and $K_1 = k_1 P$, $K_2 = k_2 P$, $\cdots$, under the XL assumption, if $\dot{r}(k_1)$, $\dot{r}(k_2)$, $\cdots$ and $h \neq 0$, then s_1, s_2, $\cdots$ are independent of x_1, x_2, $\cdots$.

As a result, A^k wins the game with a probability of $1/2$, because it cannot acquire any information via x_1, x_2, $\cdots$.

$$\left\| \Pr\left[A^0 wins \right] - \Pr\left[A^k wins \right] \right\| = \left\| \Pr[Awins] - 1/2 \right\| = \frac{1}{2} Adv_A^{privacy} \leq \sum Adv_{B_i} \quad (7)$$

That is, there is at least one B_i which wins the ODH game with a non-negligible probability.

5.2. Efficiency Analysis

Most of ECC-based grouping-proof protocols generate the grouping-proofs based on the thought of chain-linking, and the generation efficient of chain-linking grouping-proof is far below that of broadcast-style grouping-proof. Table **2** describes the efficiency comparison between the protocol proposed in this paper and the grouping-proof protocol in the references.

CONCLUSION

This paper analyzes the disadvantage of existing grouping-proof protocol design scheme and designs an ECC-based unordered grouping-proof protocol, which reduces the computation complexity as far as possible under the premise of meeting the grouping-proof protocol security requirement and is proven from the aspects of correctness, security and privacy, and the analysis result shows that this protocol has strong security and privacy protection property. Compared with the past protocol scheme, the generation efficiency of the grouping-proof protocol in this paper is greatly improved.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflicts of interest.

ACKNOWLEDGEMENTS

This work 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

[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, pp. 152-167, 2012.

[2] Y. Chen, and J.S. Chou. "ECC-based untraceable authentication for large-scale active-tag RFID systems," *Electronic Commerce Research,* vol. 15, no. 1, pp. 97-120, 2015.

[3] M. Burmester, T.V. Le, B.D. Medeiros, and G. Tsudik, "Universally composable RFID identification and authentication protocols," *ACM Trans Inf Syst Secur*., vol. 12, pp. 1-33, 2009.

[4] A. Juels, "Yoking-Proofs" for RFID Tags. In: *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*, pp. 138-143, 2004.

[5] C.L. Chen, and C.Y. Wu, "Using RFID yoking proof protocol to enhance inpatient medication safety," *Journal of Medical Systems*, vol. 36, pp. 2849-2864, 2012.

[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, pp.369-375, 2011.

[7] P. Peris-Lopez, A. Orfila, J. Hernandez-Castro, and J. C.A. van der Lubbe, "Flaws on RFID grouping-proofs Guidelines for Future Sound Protocols," *Journal of Network and Computer Applications*," vol. 34, pp. 833-845, 2011.

[8] J. Saito, and K. Sakurai, "Grouping Proof for RFID Tags," In: *IEEE International Conference on Advanced Information Networking & Applications*, pp. 621-624, 2005.

[9] S. Piramuthu, "On Existence Proofs for Multiple RFID Tags," In: *IEEE International Conference on Pervasive Services*, pp. 317-320, 2006.

[10] M. Burmester, B. de Medeiros, and R. Motta, "Provably Secure Grouping-Proofs for RFID Tags," *Lecture Notes in Computer Science*, vol. 5189, pp. 176-190, 2008.

[11] N. W. Lo, and K. H. Yeh, "Anonymous coexistence proofs for RFID tags," *Journal of Information Science and Engineering*, vol. 26, pp. 1213-1230, 2010.

[12] Z. Zhang, and Q. L. Xu, "Universal composable grouping-proof protocol for RFID tags in the Internet of Things," *Chinese Journal of Computers*, vol. 34, pp. 1188-1194, 2011.

[13] D. N. Duc, 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. 222-249, 2010.

[14] S. Vaudenay, "On privacy models for RFID," *Lecture Notes in Computer Science*, vol. 4833, pp. 68-87, 2007.

[15] Y. K. Lee, K. Sakiyama, L. Batina, and I. Verbauwhede, "Elliptic Curve Based Security Processor for RFID," *IEEE Transactions on Computer*, vol. 57, no. 1514-1527, 2008.

[16] D. Hein, J. Wolkerstorfer, and N. Felber, „ECC is Ready for RFID - A Proof in Silicon," *Lecture Notes in Computer Science*, vol. 5381, pp. 401-413, 2009.

[17] L. Batina, Y. Lee, S. Seys, D. Singele, and I. Verbauwhede, "Privacy-preserving ECC-based grouping proofs for RFID," *Information Security, Lecture Notes in Computer Science*, vol. 6531, pp.159-165, 2011.

[18] 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, pp. 113-119, 2011.

[19] W. Ko, S. Chiou, E. Lu, and H. Chang, "An improvement of privacy-preserving ECC-based grouping proof for RFID," In: *Cross Strait Quad-Regional Radio Science and Wireless Technology Conference*, pp. 1062-1064, 2011.

[20] Q. Lin, and F. Zhang, "ECC-based grouping-proof RFID for inpatient medication safety," *Journal of Medical Systems*, vol. 36, pp. 3527-3531, 2012.

[21] J. Hermans, and R. Peeters, "Private yoking proofs: attacks, models and new provable constructions," *Lecture Notes in Computer Science*, vol. 7739, pp. 96-108, 2012.

[22] 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, pp. 1-12, 2014.

[23] 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, pp. 94-103, 2014.

[24] J. Hermans, A. Pashalidis, F. Vercauteren, and B. Preneel, "A New RFID Privacy Model," *Lecture Notes in Computer Science*, vol. 6879, pp. 568-587, 2011.

[25] J. Hermans, R. Peeters, and B. Preneel, "Proper RFID Privacy: Model and Protocols," *IEEE Transactions on Mobile Computing*, vol. 13, pp. 2888-2902, 2014.

[26] M. Bellare, and A. Palacio, "GQ and Schnorr identi schemes: Proofs of security against impersonation under active and concurrent attacks," *Crypto Lecture Notes for Computer Science*, vol. 2442, pp.162-177, 2002.

Received: June 16, 2015 Revised: July 12, 2015 Accepted: September 11, 2015