Send Orders for Reprints to reprints@benthamscience.ae

The Open Automation and Control Systems Journal, 2015, *7*, 1523-1527

Open Access

Analysis and Design of ECC-Based RFID Grouping-Proof Protocol

Kang Hong-yan*

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

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

Abstract: Aiming at the issues of the existing RFID grouping-proof protocol in security and privacy, an ECC-based RFID grouping-proof protocol is proposed based on the privacy model and the identification protocol proposed by Jens Hermans. This article describes the proposed grouping-proof protocol and demonstrates in correctness, soundness and privacy. The result of theoretical analysis indicates that this scheme meets the requirements of correctness, soundness and privacy, and compared with the similar schemes, this scheme has the higher efficiency. This protocol is low in cost, secure and scalable, and has a certain practicability.

Keywords: Correctness, elliptic curve cryptography, grouping-proof protocol, privacy, security.

1. INTRODUCTION

With the development and wide application of Internet of Things technology, RFID industry has ushered the optimum development opportunity. Compared with bar codes, the RFID technology has the advantages of no contact, long distance, high anti-jamming capability, capability of identifying moving objects, etc., has gradually become one of the most popular technologies in the automatic identification technology, and is widely applied to fields such as supply chain management, identification of commodities and goods, medical management and identity identification, affecting every aspect of the lives of people. In the quick development and actual application processes of RFID, tags to be identified in some special occasions usually have obvious group characteristics, namely two or more tags are needed to be scanned "simultaneously" within a certain range, and the evidence in which two or more tags are scanned simultaneously within their communication range by the reader must be provided [1]. Generally, the issues are referred to as the grouping proof of tags, the identification and authentication of multiple tags arousing more and more concerns of the people. The issues have many scenarios of application [2-4]: medicines prescribed by doctors belong to the same prescription, and thereby reducing the administration risks; in the pharmaceuticals industry, pharmaceutical manufacturers ensure that medicines and prescriptions are sold together; and boarding checks, passports, luggage, etc. are classified as a group to ensure the security and integrity of information.

Researcher firstly studied the proof that two tags exist simultaneously, and then expanded the study to the application. Researches of RFID paid more attention to the privacy and security of RFID, and the grouping-proof of multiple tags, arousing the extensive attention of researchers. In the context of the wide application of RFID, in addition to solve the common security and privacy problems against the RFID system, it also needs to solve problems of preventing attackers from forging the grouping-proof of tags, preventing overtime during identification *etc*. The Yoking-proof protocol, the symmetric cryptosystem-based grouping-proof protocol, the tree-based grouping-proof protocol, etc. [1, 4-6], which are proposed currently have solved the security issues in the RFID grouping-proof to varying degrees, but at the same time, they still have some defects. Lee *et al.* [7] and Hein *et al.,* [8] proposed the possibility of taking public key cryptography, and particularly elliptic curve cryptography, to the RFID system. Vaudenay [9] proposed that the identification and introduction of public key cryptosystem to tags is necessary in order to keep the high privacy of tags. The public key cryptosystem and particularly ECC-based grouping-proof protocols are proposed and modified continuously, but they still have some defects. This article proposes the ECC-based grouping-proof protocol on the basis of analysis of the existing ECC-based grouping-proof protocol, and finally, privacy and security of the proposed system is analyzed.

The arrangement of this paper is as follows: the research effort related to the grouping-proof protocol is introduced in section 2; the design requirements and related number-theoretical assumptions of the grouping-proof protocol are introduced in section 3; the ECC-based grouping-proof protocol is proposed in section 4; the proposed protocol is subjected to the proof of security, soundness and privacy, and security of the new protocol is compared with that of the existing protocol in section 5; and the full text is summarized in section 6.

2. RELATED WORK

Juels *et al.,* [1] proposed a proof program in which two tags existed simultaneously, in 2004 for the first time, which

*Address correspondence to this author at the Department of Computer and Information Engineering, Heze University, Heze, Shandong, 274015, China; Tel: +86 0530 552 5001; Fax: +86 0530 566 8003;
E-mail: khyky@sina.com

1874-4443/15

is called as yoking-proof by the author, and it means that two tags are scanned simultaneously. Later, J. Saito and K. Sakurai [10] proved that Juels's program was easily suffered from replay attack, improved yoking-proof, and added timestamp. They designed the timestamp-based grouping-proof protocol which extended two tags to form multiple tags. However, since the timestamp can be guessed in advance, so attackers can guess multiple timestamps in advance and sign the RFID tags used in the next conversation attack. Therefore, Piramuthu [11] proved that the problem of replay attack is not solved completely, and proposed that the timestamp is changed into random number to resist the attack. Peris-Lopez *et al.,* [12] further indicated that the random number-based grouping-proof protocol was insecure to multi-conversation interference attack. Burmester *et al.,* [13] proposed a security model based on universally compostable security framework aiming at the grouping-proof issue of tags. However, it has proved that the modified protocol is easily attacked by counterfeit in many ways. Lien *et al.,* [14] proposed a grouping-proof protocol which is irrelevant to the response order of tags, improving the efficiency of the grouping-proof protocol of tags. However, Lien's grouping-proof protocol may reveal the identification of tags, and thereby violating the privacy of tags.

In the proposed random number-based grouping-proof protocol, share group ID-based grouping-proof protocol, tree-based grouping-proof protocol, etc., the methods of hash function, message identification codes, pseudo-random numbers, *etc*. are utilized mostly. The study of people on the grouping-proof protocol is mainly focused on the fields of hash and random function-based, sharing secret and pseudorandom function-based and symmetric cryptography-based algorithms, the issues of extensibility, security, privacy, etc. exist, and only some basic privacy protections can be provided.

Vaudenay [9] indicated that it was necessary to introduce the public key cryptography algorithm to the RFID identification protocol in order to provide higher privacy protection in the identity information disclosure of tags. Lee *et al.,* [7] and Hein *et al.,* [8] proposed the possibility of introducing public key cryptography, and particularly elliptic curve cryptography (ECC) into the RFID protocol. At the earliest, Batina *et al.,* [15] proposed ECC-based RFID grouping-proof protocol with privacy protection. Lv *et al.,* [16], however, indicated that it cannot resist tracking attack and proposed an improved protocol. Later, Ko *et al.,* [17] discovered that the protocol of Lv *et al.,* [16] has a defect and proved that the protocol cannot work, and proposed an improved protocol to resist tracking attack. In 2012, Lin *et al.,* [18] proposed a grouping-proof protocol, improving the efficiency of the protocol of Batina *et al.,* [15]. Later, some literatures [19-21] also proved the above protocol has the issues of security and privacy, and proposed corresponding improvement measures.

3. PRELIMINARIES

3.1. The Design Requirement of RFID Grouping-proof Protocol

The basic requirement of designing the RFID grouping-proof protocol is to ensure the privacy, correctness and soundness of the protocol. It is necessary to ensure the security of correctness and soundness of the RFID grouping-proof protocol. Correctness is that a legal label is always accepted by the protocol; and soundness is that the probability of accepting an illegal label is always negligible.

The definition of correctness and soundness is as below:

Definition 1 Correctness: a grouping-proof scheme is correct, and if it is met, the probability of rejecting the legal label by the grouping-proof protocol is negligible.

Definition 2 Soundness: a grouping-proof scheme is sound, and if it is met, the probability of accepting the illegal label by the grouping-proof protocol is negligible.

In accordance with the privacy model proposed by S.Vaudenay [9], the definition of privacy is as below:

Definition 3 Privacy: the privacy game between the challenger and the adversary is divided into two stages: namely the attack stage and the analysis stage. The inquiry of oracle can be issued in the attack stage, the inquiry of oracle cannot be performed in the analysis stage. The adversary can only receive the corresponding sheet of virtual ID and actual ID of tags and output as true or false, and in case of outputting to be true, the adversary wins the game.

3.2. Related Number-theoretical Assumptions

(1) OMDL problem: assume g is the generator of which the order is l in group G_l, after n inquiry of the challenging oracle and the m inquiry of discrete logarithm oracle $O_2()$, meet $m < n$, and calculate the discrete logarithm of n random points. For the oracle $O_1()$, issue the inquiry, and output a random element $h \in G$; for the oracle $O_2()$, issue the inquiry z, and output $s \in G_l$ to meet $z = gs$.

(2) DDH problem: assume g is the generator of which the order is l in group G_l, give $g, ag, bg, cg \in G_l$, and it is hard to distinguish between abg and cg.

(3) CDH problem: suppose g is the generator of which the order is l in group G_l, give $g, ag, bg \in G_l$, and calculate $abg \in G_l$.

(4) XL problem: for points on the elliptic curve, the discrete logarithm problem is equivalent to the solving of x-coordinates of points. The difficulty of XL problem is almost as hard as the DDH problem.

4. PROTOCOL DESCRIPTION

In order to ensure the correctness and security of the grouping-proof protocol, the design of the protocol shall consider the following principles:

(1) In the process of generating the grouping-proof protocol, it shall ensure the correctness of the grouping-proof protocol of tag group and must identify the single tag and the reader is verified, and only the grouping-proof information provided by the legal tags and reader can be received;

(2) In the process of generating the grouping-proof protocol, it shall consider the privacy and security of the single

tag and must consider the privacy and security of the tag as the integral group;

(3) It shall be considered how to improve the efficiency of grouping identification from the processing complexity of the single tag, the processing complexity of the integral tag group, and the processing complexity of identification.

The literature proposed the new privacy model on the basis of the adversary model proposed before analysis and defines the privacy level under the model again. The new ECC-based RFID identification protocol with higher efficiency is proposed, as shown in the Fig. (**1**).

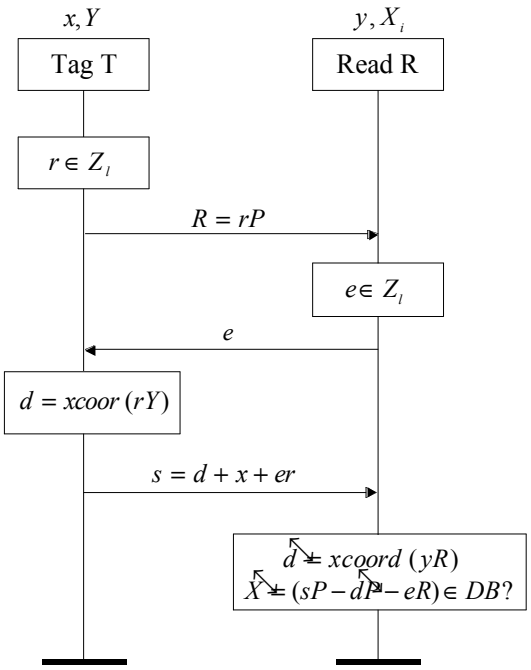

Fig. (1). Private RFID identification protocol of Jens Hermans.

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

Table 1. Notations in the protocol

Notations	Description
P	point on elliptic curve
y, Y	Server's private key and public key
s_i, S_i	Tag's private key and public key
$x(T)$	The x-coordinate of T
r_a, r_b, e	Random number

The block diagram of the protocol is shown in the Fig. (**2**):

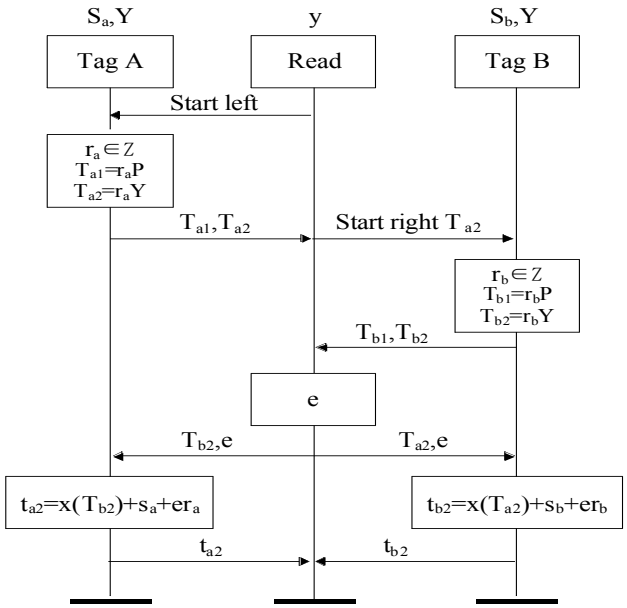

Fig. (2). Proposed grouping-proof protocol.

The description of the protocol is as below:

1) The reader sends the "start left" starting signal to the tag A;

2) The tag A produces random number r_a, calculates the corresponding points $T_{a1} = r_a P$ and $T_{a2} = r_a Y$ and send them to the reader;

3) The reader sends the "start right" starting signal to the tag B and T_{a2};

4) The tag B produces random number r_b, calculates the corresponding points $T_{b1} = r_b P$ and $T_{b2} = r_b Y$, and send T_{b1} and T_{b2} to the reader;

5) The reader produces random number e and sends T_{b2} and e to the tag A and send T_{a2} and e to the tag B;

6) The reader collects grouping-proof information $(T_{a1}, t_{a2}, e, T_{b1}, t_{b2})$ and sends it to the verifier;

7) The verifier verifies that

$$S_a = t_{a2}P - x(yT_{b1})P - eT_{a1} \quad (1)$$

$$S_b = t_{b2}P - x(yT_{a1})P - eT_{b1} \quad (2)$$

If S_a and S_b are registered in the database, verification is successful, and the grouping-proof information of the tags is received.

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:

$$\begin{aligned} & t_{a2}P - x(yT_{b1})P - eT_{a1} \\ & = (x(T_{b2}) + s_a + er_a)P - x(yT_{b1})P - eT_{a1} \\ & = x(r_bY)P + s_aP + er_aP - x(yr_bP)P - eT_{a1} \\ & = S_a \end{aligned} \tag{3}$$

$$\begin{aligned} & t_{b2}P - x(yT_{a1})P - eT_{b1} \\ & = (x(T_{a2}) + s_b + er_b)P - x(yT_{a1})P - eT_{b1} \\ & = x(r_aY)P + s_bP + er_bP - x(yr_aP)P - eT_{b1} \\ & = S_b \end{aligned} \tag{4}$$

In accordance with CDH hypothesis, $r_bY = yT_{b1}$, in order to calculate the value, only r_b or y is given, the two values are saved in the tags and the reader and are influenced by attackers impossibly. Therefore, the protocol is correctness.

Theorem 2 In accordance with the definition 2, the program of this article is correct under OMDL hypothesis.

Then, we prove that the program proposed by this article is correct in the security model of the literature [22].

Proof: we assume that attacker A can forge the grouping-proof protocol, and we construct an attacker B to win the OMDL game in the following way:

(1) $X_a = O_1(\cdot)$, X is used as the public key of the objective label;

(2) B executes A, in the first stage, B simulates the inquiry of SendTag() oracle of the i'th time in the following ways:

a) $SendTag(\cdot) \rightarrow T_{a1,i}$, $T_{a2,i}$:

$$T_{a1,i} = O_1(\cdot); T_{a2,i} = r_{a,i}Y$$

b) $SendTag(e) \rightarrow t_{a2,i}$:

$$t_{a2,i} = O_2(x(T_{b2,i}) + s_aP + e_iT_{a1,i})$$

then, the process of executing A and B is as below:

a) During the first-time execution, A sends $T_{a1}, T_{a2}, T_{b1}, T_{b2}$ to the reader-writer and calculates $x(yT_{b1})$ and t_{a2}, and during the execution of the protocol, A uses the oracle $Send\,\mathrm{Re}ader()$ and returns a new random number e'

b) During the second-time execution, A sends $T_{a1}, T_{a2}, T_{b1}, T_{b2}$ to the reader and calculates

$$r_a = (t_{a2} - t'_{a2})/(e - e') \tag{5}$$

and

$$x = t_{a2} - x(T_{b2}) - er_a \tag{6}$$

and returns $(x, e_i^{-1}(t_{a2,i} - x_i - x(T_{b2,i})))$.

The opponent B simulates the above process, if B wins the OMDL game, $t_{a2} = t'_{a2}$, but e and e' are random numbers, and the occurrence probability is negligible in case of $T_{a1} \neq 0$. Therefore, this protocol is soundness.

Theorem 3 This protocol is privacy in accordance with definition 3.

In the improved protocol of this article, the identification protocol in the literature [22] is utilized, and the security of Jens Hermans protocol is inherited in security.

Proof: It is assumed that opponent A wins privacy game in non-negligible probability (narrow strong privacy). We construct the opponent B to win ODH hypothesis. B_i simulates the operation of opponent A. In accordance with the oracle model and hybrid argument proposed by the literature [22], because $t_{a2} = x(T_{b2}) + s_a + er_a$, $t_{b2} = x(T_{a2}) + s_b + er_b$ and $T_{a1} = r_aP$, $T_{b1} = r_bP$, and if $x(T_{b2}) \neq 0$, $x(T_{a2}) \neq 0$ and $e \neq 0$ under XL assumption, t_{a2} and t_{b2} are independent of s_a and s_b.

A^k wins the game in $1/2$ probability as it cannot acquire any information via s_a and s_b.

$$\begin{aligned} \left|\Pr\left[A^0 wins\right] - \Pr\left[A^k wins\right]\right| &= \left|\Pr[A wins] - 1/2\right| \\ &= \frac{1}{2} Adv_A^{privacy} \\ &\leq \sum Adv_{B_i} \end{aligned} \tag{7}$$

Namely, at least one B_i wins the ODH game in non-negligible probability.

5.2 Efficiency Analysis

In accordance with the security analysis on the above protocol, the Table **2** describes the comparison between the improved grouping-proof protocol proposed by this article and the grouping-proof protocol in the reference. From the comparison, it is observed that the protocol of this article basically meets the requirement of design objective, has the characteristics of high privacy protection, tracking attack resistance, *etc*., and meets the demand for security.

Table 2. Security analysis of related works.

Protocol	Replay attack resistance	MITM attack resistance	Impersonation attack resistance
Batina[15]	√	√	×
Lv[16]	√	√	×
Ko[17]	√	√	×
Our protocol	√	√	√

The Table **3** describes efficiency comparison between the protocol proposed by the protocol and the grouping-proof protocol in the reference.

Table 3. Performance evaluation of related works

Protocol	The number of point multiplications of tag
Batina [15]	3
Lv [16]	3
Ko [17]	3
Our protocol	2

CONCLUSION

This paper reduces the computation complexity as far as possible under the premise of meeting the grouping-proof protocol security requirement; is proven from the aspects of correctness, security and privacy; and the analysis results show that the protocol has strong security and privacy protection property. Compared with the past protocol schemes, the generation efficiency of the grouping-proof protocol in this paper is greatly improved.

CONFLICT OF INTEREST

The author confirms that this article content has no conflict 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] Juels, A, "Yoking-Proofs for RFID Tags," *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*, pp. 138-143, 2004.

[2] 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.

[3] 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.

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

[5] J. Hermans, A. Pashalidis, F. Vercauteren, and B. Preneel, "A new RFID privacy model," *Lecture Notes in Computer Science*, vol. 68, no. 79, pp. 568-587, 2011.

[6] H.Y. Chien, and S.B. Liu, "Tree-based RFID yoking proof. In: Proceedings of International conference on networks security, wireless communications and trusted computing," *Computer Science,* vol. 27, no. 8, pp. 550-553, 2009.

[7] Y. K. Lee, K. Sakiyama, L. Batina, and I.Verbauwhede, "Elliptic curve based security processor for RFID," *IEEE Transactions on Computer* , vol. 57, pp. 1514-1527, 2008.

[8] 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.

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

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

[11] S. Piramuthu, "On existence proofs for multiple RFID tags," In: *Proceedings of International Conference on Pervasive Services*, *Workshop on Security*, 2006, pp. 317-320,

[12] P. Peris-Lopez, and C. Julio, "Solving the simultaneous scanning problem anonymously: clumping proofs for RFID tags," In: *Proceedings of International Conference on Pervasive Services, Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing*, 2007, pp. 55-60.

[13] M. Burmester, B. Medeiros, and R Motta, "Provably secure grouping-proofs for RFID tags," *Lecture Notes in Computer Science,* vol. 5189, pp. 176-190, 2008.

[14] Y. Lien, X. Leng, K. Mayes, and J. H. Chiu, "Reading order independent grouping proof for RFID tags," In: *International Conference on Intelligence and Security Informatics*, 2008, pp. 128-136.

[15] L. Batina, Y. Lee, S. Seys, D. Singele, and I. Verbauwhede, "Privacy-preserving ECC-based grouping proofs for RFID," *Lecture Notes in Computer Science,* vol. 65, no. 31, pp. 159-165, 2011.

[16] 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.

[17] 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*, 2011, pp. 1062-1064.

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

[19] J. Hermans, and R. Peeters, "Private yoking proofs: attacks, models and new provable constructions," *Lecture Notes in Computer Science,* vol. 77, no. 39, pp. 96-108, 2012.

[20] 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. 1-12, 2014.

[21] 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.

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

Received: May 26, 2015 Revised: July 14, 2015 Accepted: August 10, 2015