Send Orders for Reprints to reprints@benthamscience.ae

1532 *The Open Automation and Control Systems Journal,* 2015, *7,* 1532-1536

Open Access

Design of a Mutual Authentication Protocol for RFID Based on ECC

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: A low-cost, efficient and safe mutual authentication protocol for RFID based on elliptic curve cryptography (ECC) is proposed, specific to the security and privacy problem existed in the existing RFID authentication protocol, on the basis of deep analysis of the existing RFID protocol based on ECC. As to this proposal, mutual authentication between the tag and reader can be realized only through two sessions, under the condition of not destroying the security strength. So, the workload of calculation and system resource expense are reduced. The paper has described the protocol in detail and analyzed its security. The analysis result shows that, the protocol can resist tracking attack, replay attack, man-in-the-middle attack and other attacks, has good forward security and can realize mutual authentication between the server and the tag. Besides, it has definite practicability, due to low cost, security and scalability.

Keywords: Authentication protocol, ECC, Mutual authentication, RFID, Security.

1. INTRODUCTION

With the development and widespread use of the Internet of Things technology, RFID industry enters the age of the best development, influencing people's life in every regard. Compared with bar code, RFID technology gradually becomes one of the most popular automatic identification technologies, due to no contact, low cost, flexible deployment, easy to manage, moving object identifiability and other strengths. It is widely used in supply chain management, automatic identification of people or things, warehouse management, identity recognition and other areas [1-3], and will undoubtedly have far-reaching influence on our way of life.

With the popularization and development of RFID technology, the problem of security and privacy protection has gradually been focused by all walks of life, and become the problem badly in need of solution in the RFID application [4, 5]. In order to solve the problem on security and privacy of RFID in use, scholars have researched and designed lots of RFID authentication protocols. Some of them can provide secure authentication operation and access control among radio frequency units, so as to assure the security and privacy of the radio frequency communication process. Currently, deep and extensive researches have appeared in some literatures [4-8]. However, as restricted by the tag resource, up to now, to design an efficient and secure RFID protocol remains a challenging task, which also becomes a hot issue of RFID research.

*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

People's research of RFID protocol based on password mechanism is mainly centered on the areas of Hash and random function, shared secret and pseudo-random function, and symmetric cryptographic algorithm. This will bring the problem of security and privacy protection, *etc*. In people's impression, public key cryptography is not suitable for RFID tag of low cost and weak computing capability, due to large amount of calculation and complexity. In fact, it is not true. In the literature [9, 10], the author proposes that ECC is suitable for RFID system design, and designs a processor based on ECC used for RFID tag. Great importance is gradually attached to ECC in the RFID protocol design, as it has short key length, small amount of calculation, rapid computation speed and other strengths under the same security level. Besides, it can solve the problems such as scalability and cloning attack, *etc*., and can provide relatively stronger privacy protection [11, 12].

In the RFID system, the malicious reader can get the privacy information stored in the tag by running the fake authentication operation, meanwhile trace or detect the operating record of the tag by intercepting the messages sent by the tag, and then launch malicious attacks on the tag holder. As a result, ensuring the non-disclosure of the tag's privacy information is the basic requirement of the RFID system security. Therefore, a secure RFID authentication protocol shall assure that a legitimate reader can identify a legitimate tag successfully, meanwhile, prevent the illegitimate reader from obtaining any privacy information from the tag. This requires that the security authentication protocol designed by us can not only certify the legitimacy of the tag, but can certify the legitimacy of the reader.

1874-4443/15

2. RELATED WORK

To have higher security and privacy, several authentication protocols based on ECC have been proposed by researchers at home and abroad: Tuyls and Batina [13] proposed the first authentication protocol based on ECC, which can resist passive attack and impersonation attack with the Schnorr authentication scheme. However, such scheme is liable to be subject to tracking attack [14]. When an adversary eavesdrop on the communications between the tag and the reader, and acquires a tuple $\{T, e, y\}$, the tag can be immediately traced by the adversary. Besides, the protocol is liable to be subject to the man-in-the-middle attack, due to the linear relation between the communication data between the reader and the tag and ID-verifier of the tag. Batina [15] had improved the above proposal into the Okamoto authentication method based on ECC, so as to resist the active attack. However, it is still liable to be subject to the tracking attack and man-in-the-middle attack.

Lee [9] proposed a new cryptographic protocol EC-RAC, on the basis of the analysis that Tuyls and Batina [13] and Batina [15] made, which can't provide privacy. What is different from the traditional ECDLP protocol is that, this protocol is aimed at providing anonymity and minimizing workload of the tag. However, afterwards, as the author found that such protocol can't resist the tracking attack and replay attack, without scalability, the author proposed the improved version EC-RAC II. Nevertheless, Lee *et al.* [16] proved that the improved protocol can't resist the man-in-the-middle attack, and proposed EC-RAC IV. EC-RAC IV overcomes the problem of liable to be subject to the tracking attack and man-in-the-middle attack via the nonlinear operation of interactive data. But, the above proposal only considers the one-way authentication from the tag to the reader, without considering the authentication from the reader to the tag, enabling the tag liable to be subject to malicious inquiry.

In 2013, Liao and Hsiao [17] proposed the authentication protocol based on ECC. However, it is proved by Peeters and Hermans [18] that this protocol is liable to be subject to the impersonation attack and cloning attack of the tag, spoofing attack and tracking attack of the reader, etc.

Chou [19] proposed a new authentication protocol based on ECC, and declared that it can resist all kinds of attacks. However, it is proved by Zhang and Qi [20] that, this protocol can't realize forward privacy and mutual authentication, and is liable to be subject to the impersonation attack, tracking attack and cloning attack.

Through the above analysis, it is found by us that, at present, there is till the lack of a secure RFID authentication protocol based on ECC to resist all kinds of possible attacks. Now, a new mutual authentication security protocol is proposed to resist kinds of common attacks.

3. MUTUAL AUTHENTICATION PROTOCOL BASED ON ECC

Based on short key length, high security, greater choice for safety curve and other strengths of ECC, the paper proposes a mutual authentication protocol for RFID based on ECC, on the analysis of existing RFID authentication protocols. In the protocol, the channel between the server and the reader is assumed to be safe.

3.1. Design Objective

The paper has made the following considerations, as to the RFID mutual authentication protocol based on ECC:

- Replay attack resistance: in the RFID system, after the information between the reader and the tag is eavesdropped on by the attacker, it will be sent by the attacker once again, and served as the authentication to the legitimate reader or tag. To resist such attack, in each session, the information sent by the tag shall be changed, so that the attacker is impossible to acquire the identity information of the tag from the information under transmission. In this way, even if the attacker has eavesdropped on and saved all the interactive information during the previous authentication, new authentication information required for passing the authentication process fails to be generated thereupon.
- Man-in-the-middle attack resistance: the man-in-the-middle attack takes place in the process of the data transmission. The attacker can interrupt the communication path, and manipulate the data transmitted to and from the tag and the reader. It is a real-time threat, because the attacker can reveal and tamper the information before the information arrives at the receiving end. Since the tag in the RFID system is small in size, with low cost, it is especially liable to be subject to the man-in-the-middle attack.
- Mutual authentication: it not only requires the authentication from the reader to the tag, enabling only the legitimate tag to be processed by the reader; but requires the authentication from the tag to the reader, ensuring that only authorized users can access to each tag.
- Tracking attack resistance: usually, the attacker will pretend to be a reader to send an authentication request, inveigle the tag to send an authentication response and traces the movement of the tag in accordance with the content of response.
- Forward security: at some time when $t' < t$, tag r and a reader has executed a round of communication protocol; at the time t, the attacker captures this tag and acquires the sensitive information of the tag. However, even under such condition, the attacker can't distinguish whether the entity executing the protocol has contained tag t at the time when $t' < t$.

3.2. Protocol Description

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 , 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

The authentication protocol designed by the paper comprises two steps, described respectively below:

Step 1: Initialization phase

A random number $y \in Z_l$ is chosen by the reader to serve as its private key, and $\{C_0^{(old)}, C_1^{(old)}, s^{(old)}\}$ is worked out as its public key. Meanwhile, a random number $x_i \in Z_l$ is chosen to serve as the private key of the tag, and $X_i (= x_i P)$ is served as the identification ID_i of tag i, which shall be stored in the database along with the tag information such as name, etc., and $\{x_i, Y, P\}$ shall be stored in the tag.

Step 2: Authentication phase

Proposed RFID mutual authentication scheme is shown by Fig. (**1**), the authentication process of the protocol is as follows:

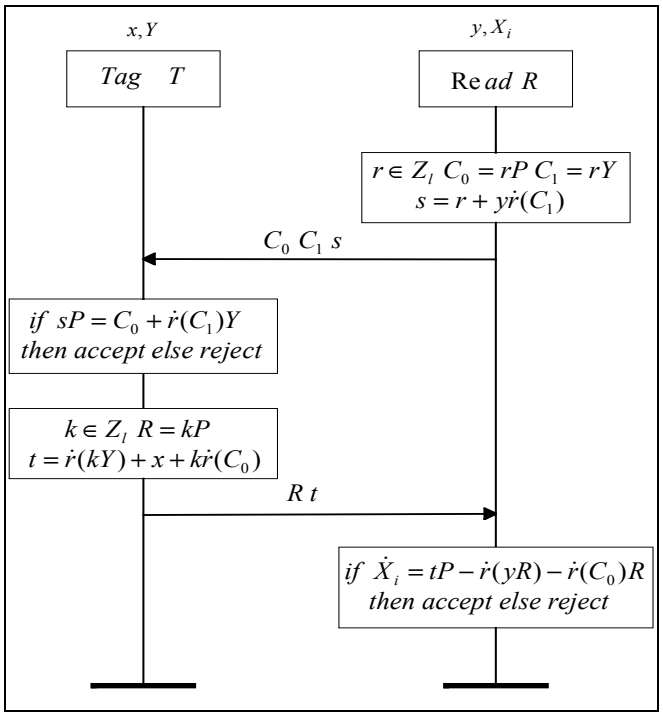

Fig. (1). Proposed RFID mutual authentication scheme.

- The server chooses a random number r?, Z_l, and works out $C_0 = rP$, $C_1 = rY$ and $s = r + y\dot{r}(C_1)$, and sends C_0, C_1 and s to the tag;
- After receiving C_0, C_1 and s, the tag will first check whether $sP = C_0 + \dot{r}(C_1)Y$ can be established, if so, carry out the following operation: choose a random number $k \in Z_l$, work out $R = kP$ and $t = \dot{r}(kY) + x + k\dot{r}(C_0)$, and send R and t to the server; otherwise, authentication from the tag to the reader fails;
- When the server receives R and t, works out $x_i P = tP - \dot{r}(yR) - \dot{r}(C_0)R$ with its private key, and search the identification $ID_i (= X_i = x_i P)$ in the database. If the tag is found, it shall be legitimate; otherwise, it shall be illegitimate, and the authentication will fail.

4. SECURITY AND PRIVACY ANALYSIS

The following security analysis on the protocol is made, in accordance with the objective to be achieved by the authentication protocol proposed by the paper:

4.1. Replay Attack Resistance

When the attacker replays the information flow $\{C_0^{(old)}, C_1^{(old)}, s^{(old)}\}$ to the tag, the tag can't distinguish whether the information flow is the replayed information flow or not. Therefore, the tag will reply the information flow $\{R^{(new)}, t^{(new)}\}$ based on the random number $k^{(new)}$ of the tag. The reader will refuse $\{C_0^{(old)}, C_1^{(old)}, s^{(old)}\}$, because the reader can't acquire the corresponding tag identification (X_i) by means of different $k^{(new)}$ and $k^{(old)}$, namely the probability of $\dot{X}_i = t^{(new)}P - \dot{r}(yR^{(new)}) - \dot{r}(C_0)^{(old)}R^{(new)}$ can be negligible. Therefore, the information flow $\{C_0^{(old)}, C_1^{(old)}, s^{(old)}\}$ under delayed replay shall be of no effect.

4.2. Man-In-The-Middle Attack

Man-in-the-middle attack is shown in Fig. (**2**):

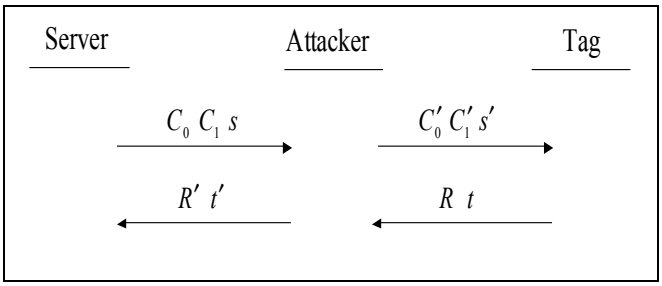

Fig. (2). Man-in-the-middle attack.

The specific process is shown below:

- The server chooses a random number r, works out $C_0 = rP, C_1 = rY, s = r + y\dot{r}(C_1)$, and sends $\{C_0, C_1, s\}$ to the tag;
- The man-in-middle intercepts $\{C_0, C_1, s\}$, chooses the other random number $r^{'}$, works out $C_0' = r^{'}P, C_1' = r'Y, s' = r' + y\dot{r}(C_1')$, and sends $\{C_0', C_1', s'\}$ to the tag by pretending to be the server; since the private key y of the reader can't be obtained, the probability of $s'P = C_0' + \dot{r}(C_1')Y$ can be ignored, therefore, the adversary can't be successfully certified by the tag;
- Assume that the attacker generates an available $s' = r' + y\dot{r}(C_1')$, the tag receives $\{C_0', C_1', s'\}$ and considers the reader as legitimate. The tag generates a random number k, works out $R = kP, t = \dot{r}(kY) + x + k\dot{r}(C_0')$, and sends $\{R, t\}$ to the server;
- The man-in-middle intercepts the tag and sends it to the information $\{R, t\}$ of the server and generates $\{R', t'\}$. As the man-in-middle does not know the private key of the tag, the probability for it to choose $X_i = t'P - \dot{r}(yR') - \dot{r}(C_0)R'$ can be ignored. Therefore, authentication from the server to the tag can't be realized. Through the above analysis, we believe that the man-in-the-middle attack can't work.

4.3. Mutual Authentication

The reader works out $\{C_0 = rP, C_1 = rY, s = r + y\dot{r}(C_1)\}$ and sends it to the tag, the tag verified sP via the public key Y of the reader. On the other hand, the tag generates $\{R = kP, t = \dot{r}(kY) + x + k\dot{r}(C_0)\}$, and the reader verifies the legitimacy of the tag via $x_iP = tP - \dot{r}(yR) - \dot{r}(C_0)R$. This is because the reader can only find the identification X_i of the legitimate tag in the database.

The above analysis shows that, our proposal can realize mutual authentication.

4.4. Tracking Attack Resistance

Since the value k is randomly chosen in each reply, $\{R, t\}$ sent by the tag to the reader is different. Even if the attacker hears the information $\{R, t\}$ and $\{R', t'\}$ of the two sessions sent by the tag to the server, the attacker works out $t - t' = \dot{r}(kY) - \dot{r}(k'Y) + (k - k')\dot{r}(C_0)$. Since $k, k^{'}$ are two random numbers, location clue of the tag can't be found, thus failing to trace to the tag.

4.5. Forward Security

Assume that the attacker acquires the identification $ID_i (= X_i = x_iP)$ of the tag T_i, and steals respectively the session information $\{C_0, C_1, s\}$ and $\{R, t\}$ between the tag and the reader, where $C_0 = rP$, $C_1 = rY$, $R = kP$, $s = r + y\dot{r}(C_1)$, $t = \dot{r}(kY) + x + k\dot{r}(C_0)$. If the adversary wants to distinguish that the information is from the same tag, it must use $R = kP$ and $\dot{r}(kY)$ to work out $\dot{r}(yR)$, indicating that ECDLP is addressed. Therefore, the proposal has forward security.

5. SECURITY COMPARISON

According to the above analysis on the security of the protocol, Table **2** illustrates the comparison of the authentication protocol proposed by the paper with the authentication protocol based on ECC. The comparison shows that, the protocol has basically met the requirements of the design objective, with definite security.

CONCLUSION

The paper has designed an anonymous mutual authentication protocol for RFID based on ECC. The protocol is featured by higher security and privacy protection, can resist tracking attack, replay attack and man-in-the-middle attack, with good forward security, and can realize mutual authentication. The protocol uses only ECC rather than Hash function and so on, and mutual authentication can be realized only through two sessions between the tag and the reader,

Table 2. Security comparison.

	Tuyls's	Batina's	Lee's(2008)	Lee's	Chou's	Ours
Replay Attack	√	√	√	√	√	√
MIMA	×	×	√	√	√	√
Mutual Authentication	×	×	×	×	×	√
Untraceability	×	×	√	√	√	√
Forward Secrecy	×	×	√	√	×	√

thus the amount of calculation and system resource expense are reduced. The comparison and analysis with the currently presented authentication protocol of RFID system shows that, the protocol is a secure, efficient and practical RFID security authentication proposal.

CONFLICT OF INTEREST

The author confirms 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", *J. Eng. Technol. Manag.*, vol. 29, pp. 152-167, 2012.

[2] N.D. Dang, D.M. Konidala, H. Lee and K. Kim, "A survey on RFID security and provably secure grouping-proof protocols", *Int. J. Inter. Technol. Secur. Trans.*, vol. 2, pp. 222-249, 2010.

[3] M. Burmester, T.V. Le, B. D. Medeiros and G. Tsudik, "Universally composable rfid identification and authentication protocols", *ACM Burmester Magkos and Chrissikopoulos Transactions on Information and System Security*, vol. 12, pp. 60-61, 2009.

[4] J. Hermans, A. Pashalidis, F. Vercauteren and B. Preneel, "A new RFID privacy model", *Lect. Notes Comp. Sci.,* vol. 6879, pp. 568-587, 2011.

[5] J. Hermans, R. Peeters and B. Preneel, "Proper RFID privacy: model and protocols", *IEEE Trans. Mobile Comp.*, vol. 13, pp. 2888-2902, 2014.

[6] A. Juels, and S.A. Weis, "Defining strong privacy for RFID". *In: Proceedings of IEEE International Conference on Pervasive computing and Communications Workshops*, New York, USA, pp. 342-347, 2007.

[7] M. Burmester, T.V. Le and B.D. Medeiros, "Provably secure ubiquitous system: Universally composable RFID authentication protocols", In: *Proceedings of the Conference on Security and Privacy in Communication Networks,* Baltimore, Maryland, USA, pp. 1-9, 2006.

[8] Y. Chen and M.T.A.J Jan, "The design of RFID access control protocol using the strategy of indefinite-index and challenge-response", *Comp Commun*, vol. 34, pp. 250-256, 2011.

[9] Y. K. Lee, L. Batina and I. Verbauwhede, "EC-RAC (ECDLP based randomized access control): provably secure RFID authentication protocol", In: *Proceedings of IEEE International Conference on RFID*, Nevada, USA, pp. 97-104, 2008.

[10] D. Hein, J. Wolkerstorfer and N. Felber, "ECC is ready for RFID-a proof in silicon", *Lec. Notes Comp. Sci.*, vol. 5381, pp. 401-413, 2009.

[11] L. Batina, Y.K. Lee, S. Seys, D. Singelée, and I. Verbauwhede, "Extending ECC-based rfid authentication protocols to privacy-preserving multi-party grouping proofs", *Per Ubiq Comp,* vol. 16, pp. 323-335, 2012.

[12] G. Godor, N. Giczi, and S. Imre, "Elliptic curve cryptography based mutual authentication protocol for low computational capacity RFID systems-performance analysis by simulations", *In: Proceedings of IEEE International Conference on Wireless Communications, Networking and Information Security*, Beijing, China, pp. 650-657, 2010.

[13] P. Tuyls and L. Batina, "RFID-tags for anti-counterfeiting", *Lec Notes Comp Sci*, vol. 3860, pp. 115-131, 2006.

[14] Y.K. Lee, K. Sakiyama, L. Batina and I. Verbauwhede, "Elliptic Curve Based Security processor for RFID", *IEEE Transac Comput,* vol. 57, pp. 1514-1527, 2008.

[15] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede, "Public-key cryptography for RFID-tags". *In: Proceedings of the 5th IEEE International Conference on Pervasive Computing and Communications Workshops*, Toronto, Canada, pp. 217-222, 2007.

[16] Y. K. Lee, L. Batina, D. Singelee, B. Preneel and I. Verbauwhede, "Anti-counterfeiting untraceability and other security challenges for RFID systems: Public-key-based protocols and hardware", *In: Proceedings of Information Security and Cryptography*, Seoul, Korea, pp. 237-257, 2010.

[17] Y. Liao and C.A. Hsiao, "A secure ECC-based RFID authentication scheme integrated with id-verifier transfer protocol", *Ad Hoc Networks,* vol. 18, pp. 133-146, 2013.

[18] R. Peeters and J. Hermans, "Attack on Liao and Hsiao's secure ECC based RFID authentication scheme integrated with ID-Verifier transfer protocol", [Available from: http://eprint.iacr.org /2013/399.pdf]

[19] J. Chou, "An efficient mutual authentication RFID scheme based on elliptic curve cryptography", *J. Supercomp.*, vol. 70, pp. 75-94, 2014.

[20] Z. Zhang, and Q. Qi, "An efficient RFID authentication protocol to enhance patient medication safety using elliptic curve cryptography", *J. Med. Syst.,* vol. 38, 47-53, 2014.

Received: June 16, 2015 Revised: August 23, 2015 Accepted: September 28, 2015