2011 International Conference on Network Computing and Information Security

An ECDLP-Based Randomized Key RFID Authentication Protocol

Xinglei Zhang, Linsen Li, Yue Wu, Quanhai Zhang
School of Information Security Engineering
Shanghai Jiao Tong University
Shanghai, China
xingxingsjtu@gmail.com, lsli@sjtu.edu.cn, wuyue@sjtu.edu.cn, qhzhang@sjtu.edu.cn

Abstract— **With the expansion of RFID technology application in diverse fields, the security problems attract more and more attention. In the RFID Security authentication protocols used public-key cryptography, the authentication protocol based on the ECDLP (Elliptic Curve Discrete Logarithm Problem) can solve the clone and reply attacks very well, but there are more or less problems in resisting tracking attacks. In this paper, we present a 'Randomized Key' proposal based on ECDLP and improve EC-RAC (Elliptic Curve Based Randomized Access Control) protocol and Schnorr protocol respectively. Our security analysis shows that the proposed improved protocols can resist tracking attack effectively.**

Keywords- RFID security; privacy; tracking attack; ECDLP

I. INTRODUCTION

RFID (Radio Frequency Identification) as a one of the promising information technology in the 21st century has become widely used in various fields of society. But at the same time RFID security issues are increasingly affecting their promotion and application. In the process of RFID authentication mechanisms research, many protocols used hash algorithm and symmetric key algorithms [1] [2] [3] [4] [5]. However, [6] explain hash and symmetric algorithms didn't satisfy RFID system requirements, and present public-key can solve this problem.

Some typical RFID authentication protocols utilize elliptic curve cryptography are: Schnorr protocol [8], Okamoto protocol [9], EC-RAC (ECDLP Based Randomized Access Control) protocol [10] and Revision of EC-RAC protocol [11], etc. These protocols based on ECDLP (Elliptic Curve Discrete Logarithm Problem) can satisfy to resist cloning and reply attack. But Schnorr protocol and Okamoto protocol had been proved vulnerable to tracking attack in [10]. For solving this issue to proposed EC-RAC protocol had also been proved to have privacy problem [12]. Though the Revision of EC-RAC protocol present some way to solve the tracking, but it increase the tag's computing. In this paper, we propose a 'randomized key' method to resolve this issue which is more efficient.

This paper is organized as follows: Section II present related work and established model of the adversary. Section III analyze the security of Schnorr protocol, Okamoto protocol and EC-RAC protocol and present a 'randomized key' proposal. Use this method to improve EC-RAC protocol and Schnorr protocol respectively. The analyses of the security of two protocols are given in Section IV. Then the conclusions are discussed followed.

II. RELATED WORK

In order to discuss the security of authentication protocol better, we should define a reasonable model of the adversary and scope of RFID system security first. The model of the adversary include: assumption of adversary's ability and attack ways.

A. Assumption of adversary's ability

We assume the communication between reader and database are safe. And tag generates random number for adversary is random. Then attackers have (or not have) follow ability:

- Adversary can catch all the information between reader and tag communication.
- Adversary has strong computational ability but only in the polynomial time.
- Adversary cannot get the tag's information through physical method.
- Adversary cannot trespass reader and database.

B. Attack ways

1) Cloning. In [10], assuming that an adversary is able to crack and reveal the secret in tag. However, an adversary should not be able to forge other tags except the cracked. In this paper, we assume that adversary can only use the interactive date between the reader and the tag to crack the secret key in tag. Typically, they use reply method to obtain the multiple feedback from the tag.

2) Tracking. Attackers utilize the obtained data to calculate the output. Although they cannot get secret key, but they can calculate the output that sole corresponding to the tag, then attain the tracking target.

978-0-7695-4355-0/11 $26.00 © 2011 IEEE
DOI 10.1109/NCIS.2011.128

III. Protocol Analyze and Design

A. *Schnorr Protocol (Fig. 1)*

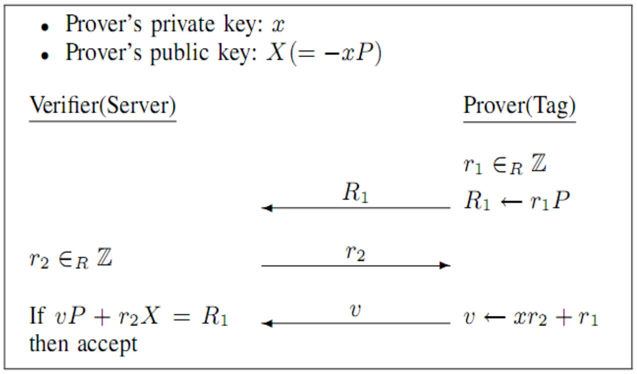
Prover's private key: x
Prover's public key: $X(=-xP)$
Verifier(Server)
Prover(Tag)
$r_1 \in_R \mathbb{Z}$
R_1
$R_1 \leftarrow r_1P$
$r_2 \in_R \mathbb{Z}$
r_2
If $vP + r_2X = R_1$ then accept
v
$v \leftarrow xr_2 + r_1$

Figure 1. Schnorr Protocol.

B. *Okamoto Protocol (Fig. 2)*

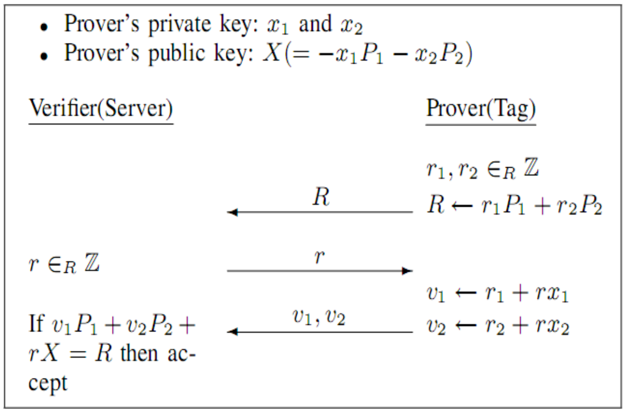
Prover's private key: x_1 and x_2
Prover's public key: $X(=-x_1P_1 - x_2P_2)$
Verifier(Server)
Prover(Tag)
$r_1, r_2 \in_R \mathbb{Z}$
R
$R \leftarrow r_1P_1 + r_2P_2$
$r \in_R \mathbb{Z}$
r
$v_1 \leftarrow r_1 + rx_1$
If $v_1P_1 + v_2P_2 + rX = R$ then accept
v_1, v_2
$v_2 \leftarrow r_2 + rx_2$

Figure 2. Okamoto Protocol.

The above two protocols can resist the clone attack and relay attack, but in [13] prove that they can't resist the tracking attack.

C. *EC-RAC Protocol (Fig.3)*

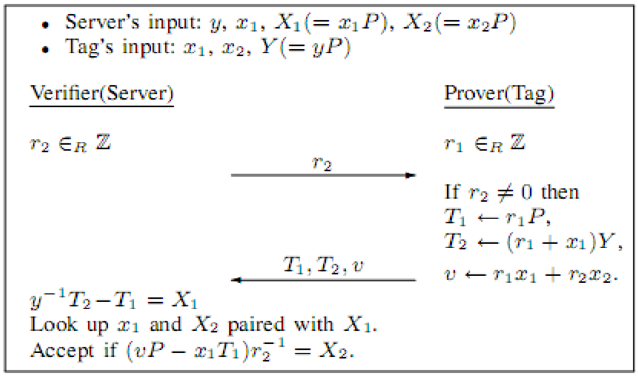
Server's input: y, x_1, $X_1(=x_1P)$, $X_2(=x_2P)$
Tag's input: x_1, x_2, $Y(=yP)$
Verifier(Server)
Prover(Tag)
$r_2 \in_R \mathbb{Z}$
$r_1 \in_R \mathbb{Z}$
r_2
If $r_2 \neq 0$ then
$T_1 \leftarrow r_1P$,
$T_2 \leftarrow (r_1 + x_1)Y$,
T_1, T_2, v
$v \leftarrow r_1x_1 + r_2x_2$.
$y^{-1}T_2 - T_1 = X_1$
Look up x_1 and X_2 paired with X_1.
Accept if $(vP - x_1T_1)r_2^{-1} = X_2$.

Figure 3. EC-RAC Protocol

In [12], attackers simulate reader to send random c twice. By two feedbacks from tag, they can obtain the fixed tag's output. So this protocol can't resist tracking attack. To resolve this problem, Revision of EC-RAC protocol increased the reader authentication module.

In this paper, we combine the ECDLP propose a new solution, the main idea is guarantee the randomized key: x'=x+r. The process is following:

Tag generate random r when authenticate with reader, then calculate x'=x+r. Next, tag send the x'P (or other key handle approach) and r to the reader. Assuming attackers get x'P and r, they still can't achieve the key x through calculate since the difficult to resolve ECDLP.

D. *Improvement of EC-RAC protocol*

Utilize this randomized key method, we improve the EC-RAC protocol. Firstly assume that the background server has strong computational ability.

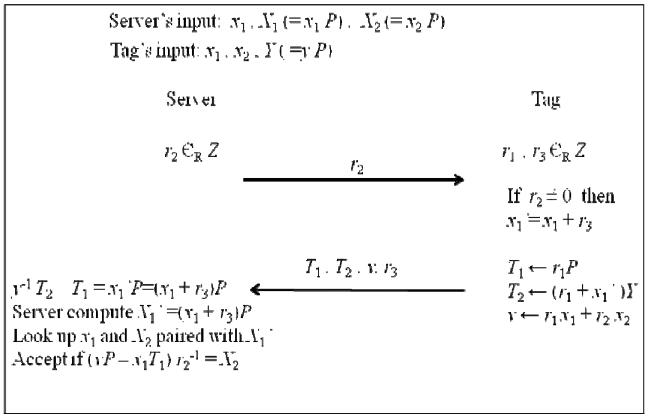
Server's input: x_1 , $X_1(=x_1P)$, $X_2(=x_2P)$
Tag's input: x_1 , x_2 , $Y(=yP)$
Server
Tag
$r_2 \in_R Z$
r_1 , $r_3 \in_R Z$
r_2
If $r_2 \neq 0$ then
$x_1{}' = x_1 + r_3$
T_1 , T_2 , v , r_3
$T_1 \leftarrow r_1P$
$T_2 \leftarrow (r_1 + x_1{}')Y$
$v \leftarrow r_1x_1 + r_2x_2$
$y^{-1}T_2 \quad T_1 = x_1{}'P = (x_1 + r_3)P$
Server compute $X_1{}' = (x_1 + r_3)P$
Look up x_1 and X_2 paired with $X_1{}'$
Accept if $(vP - x_1T_1)r_2^{-1} = X_2$

Figure 4. Improvement of EC-RAC protocol

The flow of the improvement protocol is shown in the Fig.4. The different with the EC-RAC protocol is that tag generate a random r_3, calculate $x_1{}'$=x_1+r_3, exchange x_1 to $x_1{}'$. While the server authenticate tag, database update the all record X_1 to $X_1{}'$=(x_1+r_3)P, then look to match. The behind process same with the origin protocol. But as authentication add to update database, so this action increase in consumption with background server.

E. *Improvement of Schnorr protocol*

Based on this idea, we improve the Schnorr protocol. Protocol flow is shown in Fig.5

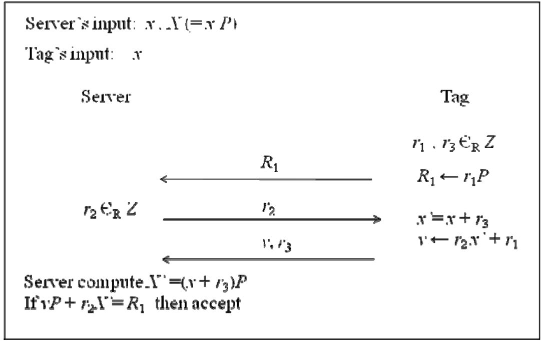
Server's input: x , $X(=xP)$
Tag's input: x
Server
Tag
r_1 , $r_3 \in_R Z$
R_1
$R_1 \leftarrow r_1P$
$r_2 \in_R Z$
r_2
$x' = x + r_3$
v, r_3
$v \leftarrow r_2x' + r_1$
Server compute $X' = (x + r_3)P$
If $vP + r_2X' = R_1$ then accept

Figure 5. Improvement of Schnorr Protocol

Server has pre-share public/private key X/x, and tag has the private key x only. Just like above mention improvement, tag generate a random r_3 when authenticate with reader. Then exchange the private key x to $x'=x+r_3$. Based on the ECDLP, even if attackers know about the r_3 and $x_1'P$, they still can't get any information about x. Furthermore, as the random r_3, adversary also can't track the X'.

IV. Security analysis

According to the previously defined model of the adversary, the following will analyze two improve protocols.

A. Anti-Cloning

As we know, these two original protocols have been proved to resist cloning attack. Since a tag response is randomized in every session, these protocols satisfy many of the security requirements. Adversary can't clone a tag without knowledge of a valid key x except they can resolve ECDLP. Obviously, since we just add a randomized key $x'=x+r$ to exchange the x, the protocols we improved are still secure for cloning.

B. Anti-Tracking

1) Improvement of EC-RAC protocol : In [10], EC-RAC protocol security analysis is suitable for this improvement protocol, since we can treat randomized key x' as x. But EC-RAC protocol is proved vulnerable to tracking in [12]. Let's use this attack ways to test new improvement protocol:

Attacker can generate a random c for r_2 and use it twice to get two different sets of responses from tag. The tag will generate two random numbers k_1 and k_2 for each of the protocol.

$$\{T_1^{(1)}, T_2^{(1)}, v^{(1)}\} = \{k_1P, (k_1 + x_1')Y, k_1x_1' + cx_2\} \qquad (1)$$

$$\{T_1^{(2)}, T_2^{(2)}, v^{(2)}\} = \{k_2P, (k_2 + x_1')Y, k_2x_1' + cx_2\} \qquad (2)$$

Then, an attacker can perform the following calculation.

$$(T_1^{(1)} - T_1^{(2)})(v^{(1)} - v^{(2)})^{-1} = (k_1 - k_2)Y\{k_1x_1^{'(1)} - k_2x_1^{'(2)})\}^{-1} \quad (3)$$

Since the result can't be a fixed value for a specific tag, this method can't be traced by an attacker.

2) Improvement of Schnorr Protocol

In [10] proved vulnerable to tracking. We use the same way in the [10] to test the new protocol's security.

Definition 1: An authentication protocol is secure against the tracking attack if the following polynomial time oracle does not exist.

$$Q\ (param_1, param_2...param_m) = f\,(var^T{}_1, var^T{}_2...var^T{}_n) \quad (4)$$

The specific introduction is in [10]. Based on the ways in [10] construct the $f(\bullet)$:

$$Q\ (r_2, r_1P, r_2x'+r_1, r_3, P) = \{r_1P - (r_2x'+r_1)\ P\}\ r_2^{-1} = -x'P \quad (5)$$

Since $x'=x+r_3$ is random change, so the $f\,(\bullet)$ is not exist.

Improvement of above two protocols, the main change is key randomized. Schnorr protocol and EC-RAC protocol can resist cloning and other attack except tracking. To fundamentally solve the tracking problem is ensure key randomized. Obviously, asymmetric cryptographic can't satisfy this requirement. Also some proposal proposed update secret key when tag authenticate with reader, but it still had some problems. Above two protocols encountered tracking problem is attacker get xP or $x^{-1}P$. But since the key randomized, the $x'P$ or $x'^{-1}P$ which the attacker achieved is continually change. On the other hand, after attackers achieved r and $(x+r)^{-1}P$, they still can't get any information about the key x. Ultimately, the security return on the difficulty of solving the problem on ECDLP.

V. Conclusion

To solve RFID security issues facing huge challenges, although the design of authentication protocols have been able to resist cloning and replay attack, but these still don't have any good solution for tracking and user privacy leak problems, such as EC-RAC protocol and Schnorr protocol. We proposed key randomized based on the characteristics of ECC public cryptography. In the model of the adversary, it not only resists cloning, reply and other attack, but also resolve tracking problem, eliminate the leakage of privacy.

Acknowledgment

This work was supported by the National Natural Science Foundation of China under Grant No. 61071078 and Key Lab of Information Network Security-Ministry of Public Security Foundation of China.

References

[1] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. The First International Conference on Security in Pervasive Computing (SPC'03), March 2003

[2] X. Gao, Z. Xiang, H. Wang, J. Shen, J. Huang and S. Song. An Approach to Security and Privacy of RFID System for Supply Chain. Proceedings of the IEEE International Conference on E-Commerce Technology for Dynamic E-Business (CEC-East'04), 2004

[3] G. Avoine and P. Oechslin. A Scalable and Provably Secure Hash-Based RFID Protocol. The 2nd IEEE International Workshop on Pervasive Computing and Communication Security (Persec'05), March 2005.

[4] M. Feldhofer. An Authentication Protocol in a Security Layer for RFID Smart Tags. IEEE Mediterranean Electrotechnical Conference (IEEE MELECON'04), May 2004.

[5] M. Burmester, T. van Le and B. de Medeiros. Provably secure ubiquitous systems: Universally composable RFID authentication protocols. In Proceedings of the 2nd IEEE/CreateNet International Conference on Security and Privacy in Communication Networks (SECURECOMM 2006). IEEE Press, 2006.

[6] M. Burmester, B. Medeiros and R. Motta. Robust, anonymous RFID authentication with constant key-lookup. Cryptology ePrint Archive: listing for 2007 (2007/402), 2007.

[7] J. Wolkerstorfer. Is Elliptic-Curve Cryptography Suitable to Secure RFID Tags? Workshop on RFID and Light-weight Cryptography, Graz, Austria, August 2005.

[8] P. Tuyls and L. Batina. RFID-tags for Anti-Counterfeiting. In D.Pointcheval, editor, Topics in Cryptology - CT-RSA 2006, volume 3860 of LNCS, pages 115-131. Springer Verlag, February 13-17 2006.

[9] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I.Verbauwhede. Public-Key Cryp-tography for RFID-Tags. In Proceedings of IEEE International Workshop on Pervasive Computing and Communication Security , 6 pages, 2007.

[10] Y. K. Lee, L. Batina, and I. Verbauwhede. EC-RAC (ECDLP Based Randomized Access Control): Provably Secure RFID authentication protocol. In 2008 IEEE International Conference on RFID , pages 97–104,2008.

[11] Y. K. Lee, L. Batina, and I. Verbauwhede. Untraceable RFID Authentication Protocols: Revision of EC-RAC. In 2009 IEEE International Conference on RFID, 2009.

[12] J.Bringer, H.Chabanne, and T.Icart. Cryptanalysis of EC-RAC, a RFID Identification Protocol. In International Conference on Cryptology and Network Security-CANS'08, Lecture Notes in Computer Science. Springer-Verlag, 2008.

[13] C.-P.Schnorr. Efficient Identification and Signatures for SmartCards. In GillesBrassard, editor, Advancesin Cryptology-CRYPTO'89, volume 435 of LNCS, pages239-252. SpringerVerlag,1989.

[14] T.Okamoto. Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes. InE.F.Brickell, editor, Advances in Cryptology-CRYPTO'92, volume740 of LNCS, pages31-53. Springer Verlag, 1992.