A Secure ECC-based Mobile RFID Mutual Authentication Protocol and Its Application

Shin-Yan Chiou, Wen-Tsai Ko, and Erl-Huei Lu
(Corresponding author: Shin-Yan Chiou)

Department of Electrical Engineering, Chang Gung University
259, Wen-Hwa 1st Road, Kwei-Shan, Tao-Yuan, Taiwan
(Email: corresponding_ansel@mail.cgu.edu.tw)

(Received Feb. 15, 2017; revised and accepted June 25, 2017)

Abstract

Mobile RFID applications combine RFID technologies and mobile device to create a new convenient application area. However, most of the applications suffer from the security issues due to insecure communication channels among tags, readers and servers. In 2012, Zhou et al. proposed an ECC-based mutual authentication protocol to promote mobile RFID applications security. However, we found their protocol faces to OTRUTS (one time reading and unlimited times service) problem, which means once a reader read the data of a certain tags from a server successfully, the reader can read it unlimited times without reading those tags again. Therefore, their protocol cannot securely support some mobile RFID applications such as the security patrolling application. In this paper, we propose a new secure ECC-based mobile RFID mutual authentication protocol for the safety of mobile RFID applications such as security patrolling.

Keywords: ECC; Mutual Authentication; RFID

1 Introduction

Recently, many researches have concentrated on mobile RFID-based applications [1, 2, 4, 12, 19, 23, 24, 26, 27, 29, 30] as it is believed that this type of applications have advantages of both RFID technology and mobile smart device. In most of the traditional RFID applications, it is assumed that the communication between reader and back end server is wired and secure, while it between tag and reader is wireless and insecure. This is because readers are usually installed at a fixed location but the tags are mobile.

However, in mobile RFID applications, both tag-reader and reader-backend server communication channels are in wireless transmission mode and therefore considered to be insecure. In the mobile RFID based telecommunication service, the tags (different from those of traditional RFID applications) are designed to be stationary and the readers (installed in a mobile device such as a cell phone) are movable. The mobile RFID telecommunication services provide tag information which is stored and maintained in backend database over a reader embedded mobile network to support many applications such as mobile payment [5, 11, 18, 21], emergency response [6, 15, 20, 23], marketing [2], advertisements promotion [14], security patrolling, position reporting, etc. Therefore, the mobile device, with an embedded reader, could be used by a potential customer, a consumer, a security patrolman, etc. That means the holder of the mobile device could also be an adversary to the mobile RFID system.

ECC is proved to be suitable for RFID applications [3, 7, 8, 10, 13, 17, 22, 25]. In 2012, Zhou *et al.* [28] proposed a mutual authentication protocol based on public-key cryptography using ECC for mobile RFID application.

However, their protocol has OTRUTS (one time reading and unlimited times service) problem, which means once a reader read the data of a certain tags from a server successfully, the reader can read it unlimited times without reading those tags again. Therefore, their protocol cannot securely support some mobile RFID applications such as the security patrolling application. In this paper, we propose a new secure ECC-based mobile RFID mutual authentication protocol for the safety of mobile RFID applications such as security patrolling.

The rest of this paper is organized as follows. Second section provides a brief background of ECC. In the third and forth section, we review and analyze Zhon *et al.*'s protocol. The proposed scheme is demonstrated in fifth section. Sixth section provides security analysis. Finally, we draw conclusions in seventh section.

2 Preliminaries

For ECC application, a non-singular elliptic curve should be chosen. All points in a non-singular elliptic curve ($y^2 = x^3 + ax + b (\bmod\ p)$) have tangent lines except one point at infinity, where $p > 3$ and $4a^3 + 27b^2 \neq 0$. The security of ECC is based on the intractability of the following problems.

2.1 Elliptic Curve Discrete Logarithm Problem (ECDLP)

Given an elliptic curve E defined over a finite field F_q, denoted by $E(F_q)$. There is a point $P \in E(F_q)$ with order m and a point $Q \in < P >$. Then the problem of finding the integer $k \in [0, m-1]$ from given P and Q such that $Q = kP$ is defined as ECDLP, where k is the discrete logarithm of Q to the base P, denoted $k = \log_P Q$ [9].

2.2 Elliptic Curve Computational Diffie-Hellman Problem (ECCDHP)

From three given points P, xP and yP over $E(F_q)$, it is hard to compute xyP over $E(F_q)$.

2.3 Elliptic Curve Factorization Problem(ECFP)

From two given points P and Q over $E(F_q)$, where $Q = xP + yP$, it is hard to find two points xP and yP over $E(F_q)$ [16].

3 Zhou *et al.*'s Protocol

In this section, we provide a brief introduction to the notations and Zhou *et al.*'s protocol. Table 1 shows the notations used in our and Zhou *et al.*'s scheme. In table 1, $h()$ is an one-way hash function, where $h : \{0,1\}^* \rightarrow \{0,1\}^{2m}$, m is the bit length of the coordinate x or y of a point over the elliptic curve $E(F_q)$.

Table 1: Notations

Notation	Meaning
P	a base point of a subgroup on elliptic curve $E(F_q)$
ID_i	the identity of Tag_i
$\bar{x}(T)$	the x-coordinate of a point $T = (x_t, y_t)$
$\bar{y}(T)$	the y-coordinate of a point $T = (x_t, y_t)$
t_R	time
k_1, k_2	secrets of *Server*
k_3	private key of *Server*
K	public key of *Server*
T_{P_i}	pseudo-id of Tag_i
R_P	public key of *Reader*
r	private key of *Reader*
$h(\ )$	one-way hash function
$(S)_L$	the left half bits of a binary sequence S
$(S)_R$	the right half bits of a binary sequence S

Zhou *et al.*'s protocol (Figure 1) has four phases: (1) *Initialization Phase*, (2) *Mobile Reader Authentication Phase*, (3) *Tag Authentication Phase* and (4) *Tag Information Sending Phase*. Those phases are described as follows.

3.1 Initialization Phase

In this phase, *Server* chooses an elliptic curve $E(F_q)$ and a base point P over $E(F_q)$ with order n, where n is a large prime number. *Server* randomly chooses his secrets k_1 and $k_2 \in_R Z_q^*$ and his private key $k_3 \in_R Z_q^*$, and computes his public key $K = k_3P$. Next, *Server* computes pseudo-ids $T_{P_i} = k_1^{-1}ID_i + k_2P$ for each tag and writes T_{P_i} into Tagi's memory. On the other hand, Reader randomly chooses his private key $r \in_R Z_q^*$ and computes his public key $RP = rP$.

3.2 Mobile Reader Authentication Phase

In this phase, *Reader* randomly chooses $s \in_R Z_q^*$, computes $Q = sP$, and sends a request Q to Tag_i. After Tag_i receives Q, it chooses a random number $t \in_R Z_q^*$ and sends t to *Reader*. Next, *Reader* computes $v = rt - s$ and sends v to Tag_i. Tag_i checks whether $vP + Q$ is equal to tR_P. If it does, Tag_i authenticates the *Reader* successfully. Otherwise, Tag_i aborts this communication.

3.3 Tag Authentication Phase

In this phase, the Tagi first chooses a random number $c \in_R Z_q^*$, computes $T_1 = cP$, $T_2 = cQ$, $T_3 = cK$, $T_4 = T_{P_i} + T_3$ and $u = h(\bar{x}(T_2), \bar{y}(T_4))$, and sends T_1, T_4 and u to *Reader*. After *Reader* receives them, it computes $R_1 = sT_1$ and $w = h(\bar{x}(R_2), \bar{y}(T_4))$, and checks whether w is equal to u. If it does not, *Reader* aborts this session. Otherwise, *Reader* considers T_1, T_4 and u as valid parameters. Next, *Reader* chooses a random number g, extracts time t_R, computes $R_2 = gP$, $R_3 = (r+g)K$ and $d_R = h(\bar{y}(R_3), \bar{x}(T_1), \bar{x}(T_4), t_R)$, and sends T_1, T_4, R_2, t_R and d_R to *Server*. After *Server* receives those messages, it checks whether t_R is valid. If it does, *Server* computes $B_1 = k_3(R_P + R_2)$ and $d_B = h(\bar{y}(B_1), \bar{x}(T_1), \bar{x}(T_4), t_R)$. Otherwise, *Server* aborts this session. *Server* checks whether $d_B = d_R$ holds, and considers T_1, T_4, R_2, t_R and d_R as valid parameters and authenticates *Reader* successfully. Next, *Server* computes $ID_i = k_1(B_2 - k_2P)$ and checks whether ID_i exists in the database. If it does, *Server* authenticates Tag_i successfully. Otherwise, *Server* aborts this session.

3.4 Tag Information Sending Phase

In this phase, *Server* fetches the related $DATA_i$ of ID_i from the database, encrypts it, and sends the encrypted data to *Reader*. *Server* first chooses a random number $l \in_R Z_q^*$, computes $B_3 = lP$, $B_4 = lR_P$, $B_5 = k_3R_P$, $d_1 = \bar{y}(B_4) \oplus (DATA_i)_L || \bar{x}(B_5) \oplus (DATA_i)_R$ and $d_2 =$

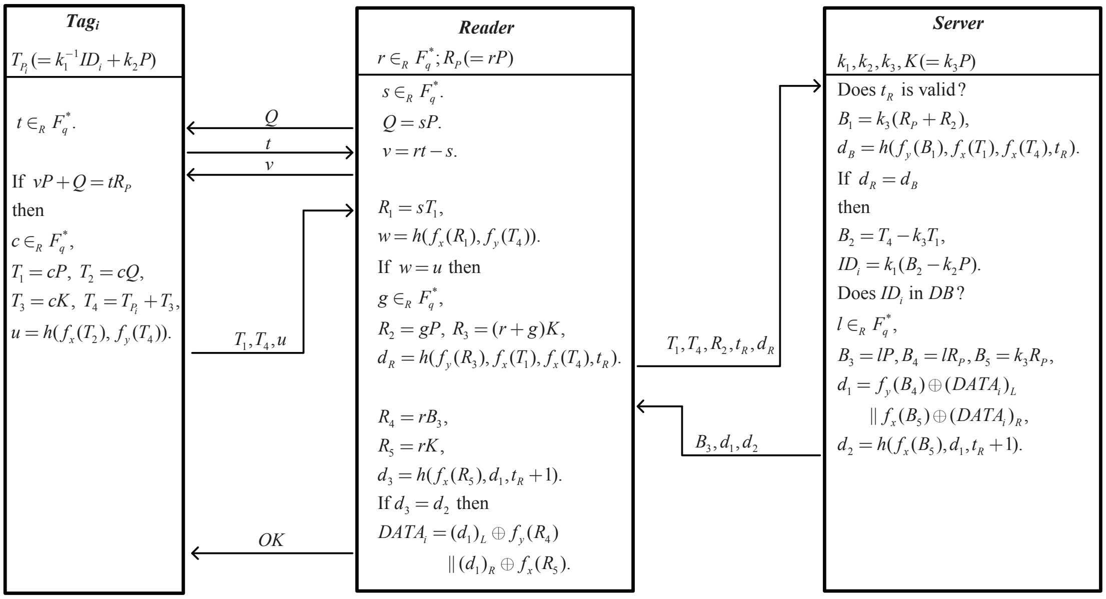

Figure 1: Zhou *et al.*'s protocol

$h(\bar{x}(B_5), d_1, t_R + 1)$, and sends B_3, d_1 and d_2 to *Reader*. When *Reader* receives those messages, it computes $R_4 = rB_3$, $R_5 = rK$ and $d_3 = h(\bar{x}(R_5), d_1, t_R + 1)$, and checks whether $d_3 = d_2$ holds. If it does, *Reader* believe that the parameters B_3, d_1 and d_2 are sent from *Server*, and recovers $DATA_i = (d_1)_L \oplus \bar{y}(R_4)||(d_1)_R \oplus \bar{x}(R_5)$. Otherwise, *Reader* aborts this session.

4 Analysis on Zhou *et al.*'s Protocol

In Zhou *et al.*'s protocol, we find that once *Reader* has read Tag_i's data, then the *Reader* can get Tag_i's data from *Server* without reading Tag_i again. We name this problem as "One Time Reading, Unlimited Times Service (OTRUTS)." The detail of this problem is described as follows and shown in Figure 2.

Assume *Reader* read Tag_i once get the data of Tag_i from *Server* successfully. *Reader* have valid T_1 and T_4. As *Reader* wants Tag_i's new $DATA_i$ from *Server*, he can assign $T'_1 = T_1$, $T'_2 = T_2$, extract a new time t'_R, generate a random number$g' \in_R Z_q^*$, compute $R'_2 = g'P$,$R'_3 = (r + g')K$ and $d'_R = h(\bar{y}(R'_3), \bar{x}(T'_1), \bar{x}(T'_4), t'_R)$, and send $T'_1, T'_4, R'_2, t'_R, d'_R$to *Server* to request the $DATA_i$ of Tag_i. As *Server* received those messages from *Reader*, *Server* authenticates t'_R successfully (with no doubt), computes $B'_1 = k_3(R_P + R'_2)$ and $d'_B = h(\bar{y}(B'_1), \bar{x}(T'_1), \bar{x}(T'_4), t'_R)$, finds out $d'_B = d'_R$ holds, and computes $ID_i = k_1(B'_2 - k_2P)$. Thus *Server* can successfully find ID_i in database because B'_2 has the pseudo-id information T_{P_i}. Therefore, *Server* can fetch the $DATA_i$ and process the "*TagInformationSendingPhase*" to encrypt $DATA_i$ for *Reader*'s request. *Server* then generates a random number $l' \in_R Z_q^*$, computes $B'_3 = l'P$, $B'_4 = l'R_P$, $B'_5 = k_3R_P$, $d'_1 = \bar{y}(B'_4) \oplus (DATA_i)_L||\bar{x}(B'_5) \oplus (DATA_i)_R$ and $d'_2 = h(\bar{x}(B'_5), d'_1, t'_R + 1)$, and sends $B'_3, d'_1$and d'_2 to *Reader*. After *Reader* receives those message, it computes $R'_4 = rB'_3$ and$R'_5 = rK$.Thus, *Reader* can recover $DATA_i = (d'_1)_L \oplus \bar{y}(R'_4)||(d'_1)_R \oplus \bar{x}(R'_5)$. Therefore, in Zhou *et al.*'s protocol, *Reader* just needs to read Tag_i's $DATA_i$ one time, then he can read Tag_i's $DATA_i$ from *Server* with unlimited times without reading Tag_i again.

5 Proposed Protocol

In this section, we propose a mobile RFID-based mutual authentication protocol using elliptic curve cryptography for security patrolling application. In our protocol, we fix the OTRUTS problem of Zhou *et al.*'s protocol and make our protocol suitable to secure applications such as security patrolling.

We take a security patrolling scenario as an instance. In the security patrolling scenario, there are three roles: (1) *Server* as the Security Management Center (*SMC*), (2) *Reader* as the patrolman's *Reader* (*PMR*), and (3)Tag_i as the sentry post's Tag_i (SPT_i). Our protocol has four phases: (1) *Initialization Phase*, (2) SPT_i *to PMR Authentication Phase*, (3) *SMC to PMR and* SPT_i *Authentication Phase* and (4) $DATA_i$ *Sending Phase*. These phases are described as follows and shown in Figure 3.

5.1 Initialization Phase

The initialization phase is same as Zhou *et al.*'s protocol. *SMC* chooses an elliptic curve $E(F_q)$ and a base point P over $E(F_q)$ with order n, where n is a large prime number. *SMC* chooses two secrets k_1, $k_2 \in_R Z_q^*$ and one private

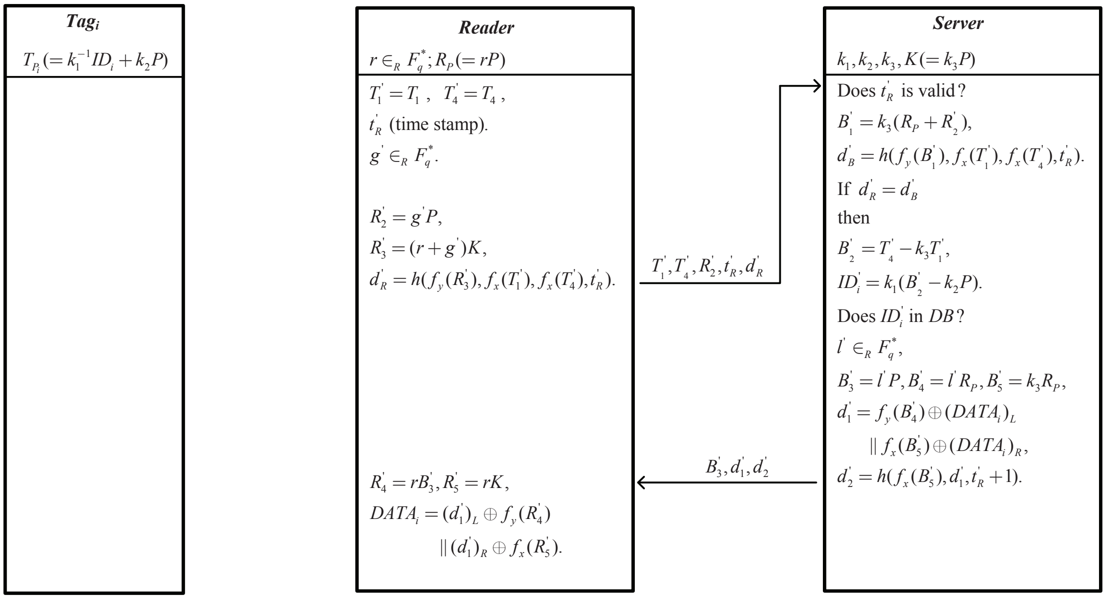

Figure 2: OTRUTS problem

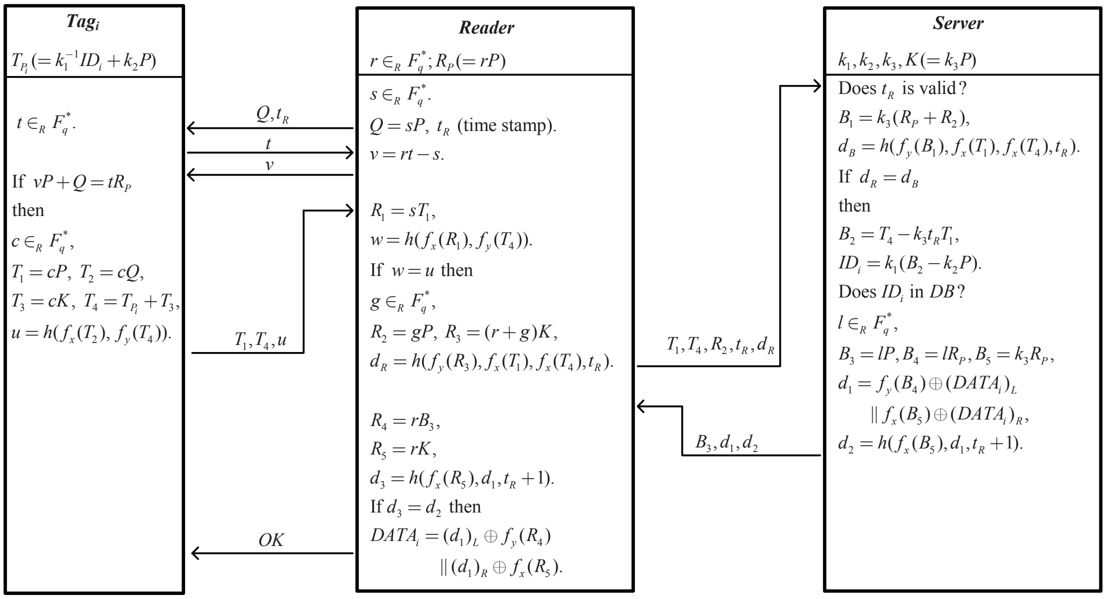

Figure 3: Proposed protocol

key $k_3 \in_R Z_q^*$, and computes his public key $K = k_3P$. Each tag has pseudo-id $T_{P_i} = k_1^{-1}ID_i + k_2P$. On the other hand, PMR chooses his private key $r \in_R Z_q^*$ computes his public key $R_P = rP$.

5.2 SPT_i to PMR Authentication Phase

In this phase, PMR randomly chooses $s \in_R Z_q^*$, extracts times t_R and computes $Q = sP$. Then PMR sends a request, Q and t_R, to SPT_i. After SPT_i receives Q and t_R, it randomly chooses $t \in_R Z_q^*$ and replies t to PMR. After PMR receives t, it computes $v = rt - s$ and sends v to SPT_i. SPT_i checks whether $vP + Q = tR_P$ holds. If it does, SPT_i authenticates the PMR successfully. Otherwise, it aborts the communication.

5.3 SMC to PMR and SPT_i Authentication Phase

SPT_i randomly chooses $c \in_R Z_q^*$, computes $T_1 = cP$, $T_2 = cQ$, $T_3 = ct_RK$, $T_4 = T_{P_i} + T_3$ and $u = h(\bar{x}(T_2), \bar{y}(T_4))$, and sends T_1, T_4 and u to PMR. After PMR receives T_1, T_4 and u, it computes $R_1 = sT_1$ and $w = h(\bar{x}(R_2), \bar{y}(T_4))$, and checks whether $w = u$. If it does, PMR authenticates the messages T_1, T_4 and u successfully. Otherwise, it aborts this session. Then PMR chooses a random number g$\in_R Z_n^*$, computes $R_2 = gP$, $R_3 = (r + g)K$ and $d_R = h(\bar{y}(R_3), \bar{x}(T_1), \bar{x}(T_4), t_R)$, and sends T_1, T_4, R_2, t_R and d_R to *Server*. Then *Server* checks whether t_R is valid. If it does not, *Server* aborts this session. Otherwise, *Server* computes $B_1 = k_3(R_P + R_2)$ and $d_B = h(\bar{y}(B_1), \bar{x}(T_1), \bar{x}(T_4), t_R)$, and checks whether $d_B = d_R$ holds. If it does, *Server* considers T_1, T_4, R_2, t_R and d_R as valid parameters and authenticate *Reader* successfully. Next, *Server* computes $B_2 = T_4 - k_3t_RT_1$and $ID_i = k_1(B_2 - k_2P)$, and checks whether ID_i exists in the database. If it does, *Server* authenticate Tag_i successfully. Otherwise, *Server* aborts this session.

5.4 $DATA_i$ Sending Phase

In this phase, *Server* fetches the related $DATA_i$ of ID_i from the database, encrypts it, and sends the encrypted data to PMR. First, SMC randomly chooses $l \in_R Z_q^*$, computes $B_3 = lP$, $B_4 = lR_P$, $B_5 = k_3R_P$, $d_1 = \bar{y}(B_4) \oplus (DATA_i)_L || \bar{x}(B_5) \oplus (DATA_i)_R$ and $d_2 = h(\bar{x}(B_5), d_1, t_R{+}1)$, and sends B_3, d_1 and d_2 to PMR. After PMR receives those messages, it computes $R_4 = rB_3$, $R_5 = rK$, $d_3 = h(\bar{x}(R_5), d_1, t_R + 1)$, and checks whether $d_3 = d_2$ holds. If it does, PMR believes the parameters B_3, d_1 and d_2 comes from a valid SMC, and recovers $DATA_i = (d_1)_L \oplus \bar{y}(R_4) || (d_1)_R \oplus \bar{x}(R_5)$. Otherwise, it aborts this session.

6 Security Analysis

In the security patrolling scenario, PMR is supposed to visit the assigned SPT in person, read the SPT and send proof back to the SMC for verification in a valid time interval. If a protocol has the OTRUTS problem (described in section 3), PMR just needs to visit SPT_i only one time then he can sit on the chair in the security office and complete the patrolling report without visiting the same SPT again. Therefore, a security patrolling application should avoid the OTRUTS problem in the RFID mobile mutual authentication protocol.

In our protocol, we rearranged $T_3 = ct_RK$ to solve this OTRUTS problem. Thus, we have $T_4 = T_{P_i} + ct_RK$. If PMR tries to read SPT_i's data from SMC without reading SPT_i again, shown as Figure 4, he assigns $T_1' = T_1$ and $T_2' = T_2$, extracts a new time t_R', generates a random number $g' \in_R Z_n^*$, computes $R_2' = g'P$, $R_3' = (r + g')K$ and $d_R' = h(\bar{y}(R_3'), \bar{x}(T_1'), \bar{x}(T_4'), t_R')$, and sends $T_1', T_4', R_2', t_R', d_R'$ to SMC. After SMC receives these messages, it authenticates t_R' successfully (with no doubt), computes $B_1' = k_3(R_P + R_2')$ and $d_B' = h(\bar{y}(B_1'), \bar{x}(T_1'), \bar{x}(T_4'), t_R')$, finds $d_B' = d_R'$ holds, and compute $B_2' = T_4' - k_3t_R'T_1' = T_{P_i} + (t_R - t_R')ck_3P$. Now SMC tries to recover ID_i by computing $ID_i' = k_1(B_2' - k_2P)$ $= k_1(T_{P_i} + (t_R - t_R')ck_3P - k_2P) = ID_i + (t_R - t_R')ck_3P$ $\neq ID_i$. However, SMC finds out ID_i' is not in the database and aborts the session. Therefore, our protocol not only provides the security properties of Zhou *et al.*'s protocol, but also resistants to OTRUTS problem which make our protocol more suitable for security patrolling application.

7 Conclusions

This paper discusses the Zhou *et al.*'s mutual authentication protocol and points out their protocol is faces OTRUTS problem and therefore cannot securely support some mobile RFID applications such as the security patrolling application. This paper proposes a new mutual authentication using ECC and proved the proposed protocol is resistant to OTRUTS problem.

Acknowledgments

This work is partially supported by the Ministry of Science and Technology under Grant MOST 104-2221-E-182-012 and by the CGMH project under Grant BMRPB46. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

References

[1] D. Benedetti, G. Maselli, and C. Petrioli, "Prime: Priority-based tag identification in mobile RFID sys-

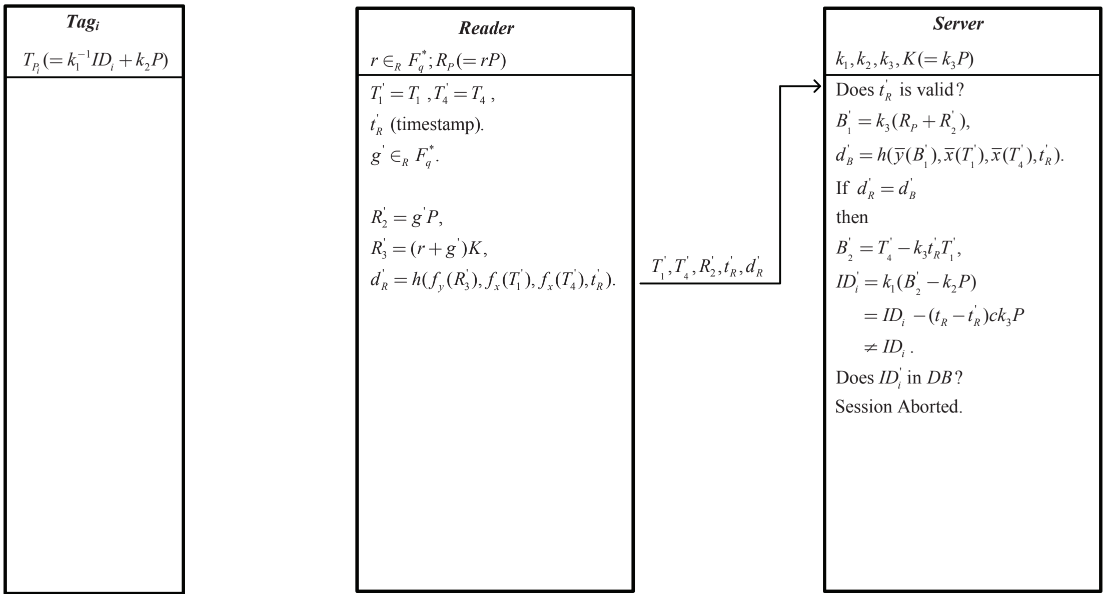

Figure 4: The resistance of OTRUTS problem in our protocol

tems," *Computer Communications*, vol. 108, pp. 64-77, 2017.

[2] C. L. Chen, J. K. Jan, and C. F. Chien, "Based on mobile RFID device to design a secure mutual authentication scheme for market application," in *International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA'10)*, pp. 423–428, 2010.

[3] 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, 2015.

[4] P. Y. Cui, "An improved ownership transfer and mutual authentication for lightweight RFID protocols," *International Journal of Network Security*, vol. 18, no. 6, pp. 1173–1179, 2016.

[5] T. Falk, W. H. Kunz, J. J. Schepers, and A. J. Mrozek, "How mobile payment influences the overall store price image," *Journal of Business Research*, vol. 69, no. 7, pp. 2417–2423, 2016.

[6] G. L. Foresti, M. Farinosi, and M. Vernier, "Situational awareness in smart environments: socio-mobile and sensor data fusion for emergency response to disasters," *Journal of Ambient Intelligence and Humanized Computing*, vol. 2, no. 6, pp. 239–257, 2015.

[7] D. Guo and F. Wen, "A more robust authentication scheme for roaming service in global mobility networks using ECC," *International Journal of Network Security*, vol. 18, no. 2, pp. 217-223, 2016.

[8] L. Han, Q. Xie, and W. Liu, "An improved biometric based authentication scheme with user anonymity using elliptic curve cryptosystem," *International Journal of Network Security*, vol. 19, no. 3, pp. 469-478, 2017.

[9] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer Science & Business Media, 2006.

[10] G. Hou, Z. Wang, "A robust and efficient remote authentication scheme from elliptic curve cryptosystem," *International Journal of Network Security*, vol. 19, no. 6, pp. 904-911, 2017.

[11] G. De Kerviler, N. T. Demoulin, and P. Zidda, "Adoption of in-store mobile payment: Are perceived risk and convenience the only drivers?" *Journal of Retailing and Consumer Services*, vol. 31, pp. 334–344, 2016.

[12] N. Kumar, R. Iqbal, S. Misra, J. J. Rodrigues, and M. S. Obaidat, "Bayesian cooperative coalition game as-a-service for RFID-based secure QOS management in mobile cloud," *IEEE Transactions on Emerging Topics in Computing*, 2016.

[13] N. Kumar, K. Kaur, S. C. Misra, and R. Iqbal, "An intelligent RFID-enabled authentication scheme for healthcare applications in vehicular mobile cloud," *Peer-to-Peer Networking and Applications*, vol. 5, no. 9, pp. 824–840, 2016.

[14] K. Y. Lam, J. K. Y. Ng, J. Wang, et al., "A pervasive promotion model for personalized promotion systems on using wlan localization and nfc techniques," *Mobile Information Systems*, vol. 2015, 2015.

[15] K. M. Lee, M. Runyon, T. J. Herrman, R. Phillips, and J. Hsieh, "Review of salmonella detection and identification methods: Aspects of rapid emergency response and food safety," *Food Control*, vol. 47, pp. 264–276, 2015.

[16] F. Li, X. Xin, and Y. Hu, "Indentity-based broadcast signcryption," *Computer Standards & Interfaces*, vol. 30, no. 1, pp. 89–94, 2008.

[17] D. Liu, Z. Liu, Z. Yong, X. Zou, and J. Cheng, "Design and implementation of an ecc-based digital baseband controller for RFID tag chip," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 7, pp. 4365–4373, 2015.

[18] T. Oliveira, M. Thomas, G. Baptista, and F. Campos, "Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology," *Computers in Human Behavior*, vol. 61, pp. 404–414, 2016.

[19] Q. Qian, Y. L. Jia, R. Zhang, "A lightweight RFID security protocol based on elliptic curve Cryptography," *International Journal of Network Security*, vol. 18, no. 2, pp. 354–361, 2016.

[20] J. Salerno, W. M. Hlaing, T. Weiser, C. Striley, L. Schwartz, F. J. Angulo, and V. S. Neslund, "Emergency response in a global health crisis: epidemiology, ethics, and ebola application," *Annals of Epidemiology*, vol. 26, no. 4, pp. 234–237, 2016.

[21] A. A. Shaikh, P. Hanafizadeh, and H. Karjaluoto, "Mobile banking and payment system: A conceptual standpoint," *International Journal of E-Business Research*, vol. 13, no. 2, pp. 14–27, 2017.

[22] X. Tan, M. Dong, C. Wu, K. Ota, J. Wang, and D. W. Engels, "An energy-efficient ecc processor of uhf RFID tag for banknote anti-counterfeiting," *IEEE Access*, vol. 5, pp. 3044–3054, 2017.

[23] T. Tran, F. Z. Yousaf, and C. Wietfeld, "Rfid based secure mobile communication framework for emergency response management," in *IEEE Wireless Communications and Networking Conference*, pp. 1–6, 2010.

[24] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Authentication mechanism for mobile RFID based smart grid network," in *IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE'14)*, pp. 1–6, 2014.

[25] J. Wolkerstorfer, "Is elliptic-curve cryptography suitable to secure RFID tags," in *Handout of the Ecrypt Workshop on RFID and Lightweight Crypto*, 2005.

[26] R. Xie, B. Y. Jian, and D. W. Liu, "An improved ownership transfer for RFID protocol," *International Journal of Network Security*, vol. 20, no. 1, pp. 149-156, 2018.

[27] L. Yang, Y. Chen, X. Y. Li, C. Xiao, M. Li, and Y. Liu, "Tagoram: Real-time tracking of mobile RFID tags to high precision using cots devices," in *Proceedings of ACM 20th Annual International Conference on Mobile Computing and Networking*, pp. 237–248, 2014.

[28] J. Zhou, Y. Zhou, F. Xiao, and X. Niu, "Mutual authentication protocol for mobile RFID systems," *Journal of Computational Information Systems*, vol. 8, no. 8, pp. 3261–3268, 2012.

[29] Y. Zou, J. Xiao, J. Han, K. Wu, Y. Li, and L. M. Ni, "GRFID: A device-free RFID-based gesture recognition system," *IEEE Transactions on Mobile Computing*, vol. 16, no. 2, pp. 381–393, 2017.

[30] J. M. Zydney and Z. Warner, "Mobile apps for science learning: Review of research," *Computers & Education*, vol. 94, pp. 1–17, 2016.

Biography

Shin-Yan Chiou received the PhD degree in Electrical Engineering from National Cheng Kung University, Taiwan, in 2004. From 2004 to 2009, he worked at Industrial Technology Research Institute as a RD Engineer. Since 2009, he joined the faculty of the Department of Electrical Engineering, Chang Gung University, Taoyuan, Taiwan, where he is currently an Associate Professor. His research interests include information security, cryptography, social network security, and secure applications between mobile devices.

Wen-Tsai Ko received the B.S. degree in Applied Mathematics from Chung Cheng Institute of Technology in 1986, the M.B.A. degree in Defense Information from National Defense Management College in 1998, and the PhD degree in Electrical Engineering from Chang Gung University in 2014. His research interests include information security, visual cryptography and RFID security.

Erl-Huei Lu received the B.S. and M.S. degrees in electrical engineering from Chung Cheng Institute of Technology, Taiwan, in 1974 and 1980, respectively, and the Ph.D. degree electrical engineering from National Cheng Kung University, Taiwan, in 1988. Lu is a professor in the Department of Electrical Engineering, Chang Gung University, Taiwan. His research interests include error-control coding, network security, and systolic architectures.