Cryptanalysis of an ID-based Deniable Threshold Ring Authentication

Tzu-Chun Lin[1], Ting-Yi Yeh[1], Min-Shiang Hwang[2,3]
(Corresponding author: Min-Shiang Hwang)
Department of Applied Mathematics, Feng Chia University[1]
100, Wenhwa Road, Taichung 40724, Taiwan, R.O.C.
Department of Computer Science & Information Engineering, Asia University[2]
500, Lioufeng Rd., Wufeng, Taichung 41354, Taiwan
Department of Medical Research, China Medical University Hospital, China Medical University, Taiwan[3]
(Email: mshwang@asia.edu.tw)
(Received Aug. 21, 2018; revised and accepted Dec. 15, 2018)

Abstract

In this paper, we offer analysis of a deniable threshold ring authentication protocol proposed by Jin *et al.* [5]. The Authors in [5] combined the two concepts, namely, threshold ring signature and deniable authentication, to propose a non-interactive deniable (t, n)- threshold ring authentication protocol. The protocol is the first design of this type. We will point out that this protocol cannot guarantee that at least t legal participates generate a valid signature and cannot withstand message modification attacks under certain restrictions.

Keywords: Bilinear Pairing; Deniable Authentication; Ring Signature; Threshold Signature

1 Introduction

The development of digital signature schemes for different needs is one of most important research topics in cryptography. A (t, n)-threshold signature allows any subset of t or more than t out of n participants to generate a valid signature [4]. Since 1991, Desmedt and Frankel [1] presented the concept of a (t, n)-threshold signature, which has been studied widely. A ring signature allows members of a signature group to anonymously sign messages on behalf of the group, and there is no group manager, group setup process and undo mechanism.

A deniable authentication protocol only allows not the message receiver to verify that the received message is indeed the one sent by the sender, but also ensures the sender's privacy so that this means that the following two special characteristics have to satisfy:

1) It enables an intended receiver to identify the source of a given message.

2) The intended receiver cannot prove the identity of the sender to any third party, even if he/she fully cooperates with the third party.

Due to the above two characteristics, the deniable authentication protocol can be broadly used for online shopping, electronic voting systems [9], e-learning systems and negotiation over Internet, *etc.* The concept of interactive deniable authentication protocol was initially introduced by Dwork *et al.* [2]. Since then, many interactive and non-interactive deniable authentication protocols based on various mathematical theories have been developed [6, 8, 10–15, 17, 18, 20, 24, 25]. The concept of deniable ring authentication was first introduced by Noar. This scheme can be extended to generate threshold authentication [17]. However, Noar's scheme requires an interactive zero knowledge protocol. In 2004, Susilo and Mu [22] proposed a non-interactive deniable ring authentication protocol based on Chamelon hash function and bilinear pairing.

In 2015, Jin *et al.* [5] combined the two concepts to propose a non-interactive deniable threshold ring authentication protocol (called IBDTRA) generated by elliptic curves and bilinear pairing [23]. This is the first design of this type. On the surface, all legal signers are involved in the signature. Actually, only t legal signers have used their own private keys to sign. However, the verifier can only verify that the signature was calculated by the group consisting of legitimate signers. The verifier would not know which participants have jointly calculated the signature.

In this article, we will point out that the IBDTRA cannot guarantee that at least t legal participates generate a valid signature and cannot withstand message modification attacks under certain restrictions.

2 Review of IBDTRA Protocol

2.1 Preliminary

Let G_1 be an additive group of prime order q, G_2 be a multiplicative group with the same order q. In the paper, a bilinear map $e : G_1 \times G_1 \longrightarrow G_2$ has to satisfy the following properties:

1) Bilinearity: $e(aP, bQ) = e(P, Q)^{ab}$, where $P, Q \in G_1$, $a, b \in \mathbb{Z}_q^*$.

2) Non-degeneracy: If $e(P, Q) = 1_{G_2}$ for all $Q \in G_1$, then $P = 1_{G_1}$.

3) Computability: There is an efficient algorithm to compute $e(P, Q)$ for any $P, Q \in G_1$.

Note that if a bilinear pairing is used on elliptic curves, then, usually, the Weil pairing or Tate pairing is recommended.

2.2 The IBDTRA Protocol

In this subsection, we will review Jin *et al.*'s IBDTRA protocol [5] . Let $G_1 =< P >$ be an additive group of prime order q, G_2 be a multiplicative group with the same order q and $e : G_1 \times G_1 \longrightarrow G_2$ be a bilinear map. Let $H_1 : \{0,1\}^* \longrightarrow G_1$ and $H_2 : \{0,1\}^* \longrightarrow \mathbb{Z}_q^*$ be two one-way hash functions. Suppose that there are n legitimate signers and one verifier (receiver). A message m requires at least $t(< n)$ participants to sign. Assumed that each legitimate signer $Sig(i)$ and the verifier have their own identity ID_i, $i = 1, \cdots, n$ and ID_r, respectively.

Setup. PKG constructs a pair of keys: (private key, public key) $= (s, P_{pub})$, where $s \in \mathbb{Z}_q$ and $P_{pub} := sP$. PKG publishes system parameters are $\{G_1, G_2, q, P, P_{pub}, e, H_1, H_2\}$.

Key Generation. The PKG computes private key $S_i = sQ_i$ for each user, where $Q_i = H_1(ID_i)$, $i = 1, \cdots, n, r$.

Signature. Without loss of generality, suppose the $Sig(1), \cdots, Sig(t)$ are the participating signers and $Sig(1)$ prepares the authenticate on behalf of other participants $Sig(t+1), \cdots, Sig(n)$.

1) $Sig(1)$ chooses $x_i, h_i \in \mathbb{Z}_q$ as so-called private key for each $Sig(i)$, $i = t+1, \cdots, n$, and computes the public keys

$$U_i = x_i P - h_i Q_i,$$
$$V_i = x_i P_{pub}.$$

2) For $j = 1, \cdots, t$, each $Sig(j)$ chooses the private key $r_j \in \mathbb{Z}_q^*$ and computes the public key

$$U_j = r_j P.$$

3) $Sig(1)$ computes the hash value

$$h_0 = H_2(\{ID_i\}_{i=1}^n, t, m, ID_r, \{U_k\}_{k=1}^n)$$

and then constructs a polynomial $f(x) \in \mathbb{Z}_q[x]$ of degree $n - t$ with the constant term h_0.

4) For $j = 1, \cdots, t$, each $Sig(j)$ uses the value $h_j := f(j)$ to compute another key

$$V_j = r_j P_{pub} + h_j S_j.$$

5) Anyone can calculate the values

$$V = \sum_{k=1}^{n} V_k \quad \text{and} \quad W = e(V, Q_r).$$

6) Also, $\sigma = \{\{U_k\}_{k=1}^n, W, f(x)\}$ is the deniable authentication for the message m.

Verification. After receiving (σ, m), the verifier checks whether

$$h_0 \stackrel{?}{=} H_2(\{ID_i\}_{i=1}^n, t, m, ID_r, \{U_k\}_{k=1}^n).$$

If this is the case, then computes $h_k = f(k)$ for each $k = 1, \cdots, n$, and

$$e(\sum_{k=1}^{n}(U_k + h_k Q_k), S_r).$$

If

$$e(\sum_{k=1}^{n}(U_k + h_k Q_k), S_r) = W,$$

then the massage m is accepted.

Figure 1 shows that the participating signers have different algorithms than the other ring participants in making the authentication of a message.

3 Cryptanalysis of IBDTRA Protocol

In this section, we show that there are two weaknesses in Jin *et al.*'s IBDTRA protocol [5].

Theorem 1. *In IBDTRA protocol, the verifier cannot confirm if at least t members are participating in this signature.*

Proof. Assume that only $t - 1$ members, say $Sig(1), \cdots, Sig(t-1)$, agree to sign. $Sig(1)$ can construct (U_t, V_t) for the absent $Sig(t)$: First, $Sig(1)$ chooses an integer $r_t \in \mathbb{Z}_q$ and computes

$$U_t = r_t P.$$

$Sig(1)$ computes the hash value

$$h_0 = H_2(\{ID_i\}_{i=1}^n, t, m, ID_r, \{U_k\}_{k=1}^n)$$

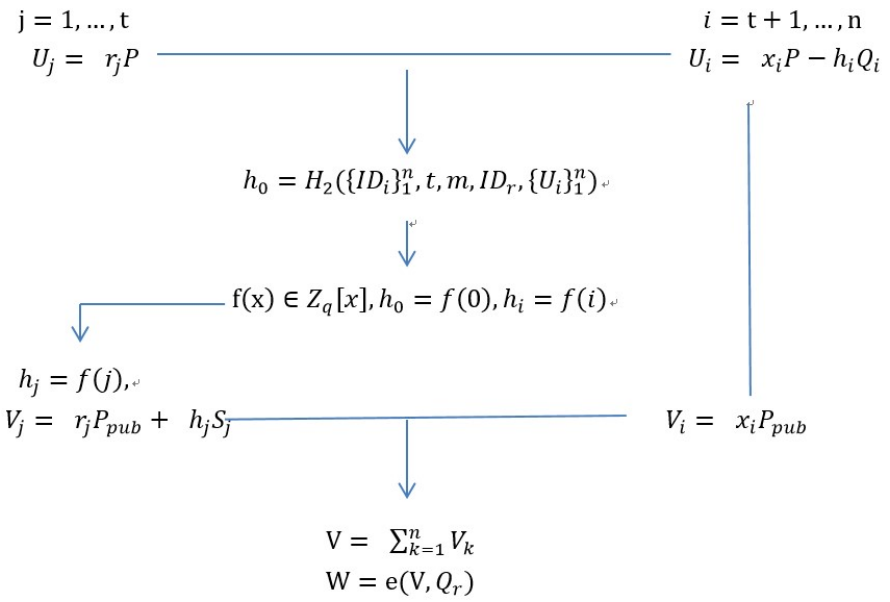

Figure 1: The phase of (t, n)-threshold authentication

and then construces a polynomial $f(x) \in \mathbb{Z}_q[x]$ of degree $n-t$ with the constant term h_0. In order to obtain V_t, $Sig(1)$ needs to find a pair of integers (x_t, y_t) such that

$$r_t \equiv x_t - h_t y_t \bmod q \quad (1)$$
$$Q_t = y_t P. \quad (2)$$

Thus, $V_t := x_t P_{pub}$. □

One of the ways to solve the equation

$$r_t = x_t - h_t y_t$$

in $\mathbb{Z}_q$ relies on the following idea: we choose randomly a pair (x', y') and let $s = x' - h_t y'$. Then $1 = s^{-1}x' - h_t s^{-1} y'$, thus $r_t = s^{-1}x' r_t - h_t s^{-1} r_t y'$. Next, we check whether $Q_t = (s^{-1} r_t y')P$. If it is not the case, then go back to the choice of (x', y'). If G_1 is a subgroup of an elliptic curve over $\mathbb{Z}_q$. To determine an integer y such that $Q = yP$ is just like to solve the ECDLP (Elliptic Curve Discrete Logarithm Problem).

Another way to find the solution (x_t, y_t): assume that (x, y) is a solution of the equation $U_t = xP - h_t Q^*$, where $Q^* = yP$. If $Q^* \neq Q_t$, we consider the point $U^* := xP - h_t Q_t$. Let $aP = U^* - U_t$. Solving the ECDLP is one of the most frequently studied topics in cryptanalysis. So far, there is no known attack of polynomial time for the 160-bit ECDLP [3, 16, 19]. In fact, the difficulty of the ECDLP depends not only on the bit-length of the order $o(P) = q$ but also on the bit-length of the scalar a. In order to invalidate attacks, the bit-length of the selected scalar approximates the bit-length of the prime order q. For this reason, we choose a solution y whose bit-length is approximately the bit-length of the prime order q. If the bit-length of the integer of the subtraction $a \equiv y_t - y \bmod q$ is short enough, then the value of a can be calculated in polynomial time by using exhaustive search. If the value of the integer a is found, then the private key $y_t = y - a h_t^{-1}$ is solved, where $Q_t = y_t P$. Next question, is it easy to find a pair of solution (x, y) such that the bit-length of the scalar a is short enough? In other word, how likely is it to prevent IBDTRA protocol from such attack? Such questions are still open. The following attack uses a similar approach.

Theorem 2. *If $t \leq n/2$, then the IBDTRA protocol is unable to resist the message modify attack.*

Proof. Assume that an eavesdropper intercepts the authenticated message (σ, m) and wants to use the fake message m^* to replace the real message m.

Since $H_2(\cdots, m, \cdots) \neq H_2(\cdots, m^*, \cdots)$, in order for the fake message m^* to pass verification, the eavesdropper must be able to create a new polynomial $g(x) \in \mathbb{Z}_q[x]$ such that the following conditions are satisfied:

1) $h_0^* = g(0)$, where the constant term $h_0^* = H_2(\{ID_i\}_{i=1}^n, t, m^*, ID_r, \{U_k\}_{k=1}^n)$.
2) $\deg g(x) = n - t$.
3) $h_k = g(k)$, $k = 1, \cdots, t$.

Such polynomial $g(x)$ is defined by

$$g(x) := h_0^* + (h_1 - h_0^*)x^l \prod_{i=1, i\neq 1}^{t} \frac{x-i}{1-i} + (h_2 - h_0^*)\frac{x}{2} \prod_{i=1, i\neq 2}^{t} \frac{x-i}{2-i} + \cdots + (h_t - h_0^*)\frac{x}{t} \prod_{i=1}^{t-1} \frac{x-i}{t-i},$$

where $l \geq 0$ is an integer with $t + l = n - t$.

Then, for $i = t + 1, \cdots, n$, set $h_i^* := g(i)$. To find $x_i^* \in \mathbb{Z}_q$ satisfying $U_i = x_i^* P - h_i^* Q_i$, the eavesdropper computes $U_i^* = x_i P - h_i^* Q_i$ and $U_i - U_i^*$. If $U_i - U_i^* = a_i P$ and a_i is a small integer, then the integer a_i can be effectively calculated, and also $x_i^* = a_i + x_i$ and $V_i^* = x_i^* P_{pub}$. □

4 Conclusion

The verifier in IBDTRA protocol uses his/her own private key and public keys of all legal signers together with a bilinear pairing to verify an authenticated message, so he/she can only prove whether a given message is from a legitimate group. The verifier could not know the list of signers who have actually participated in the signature. In this paper we provide a possible way to accomplish the challenge of sender spoofing and modifying messages: First, we give a solution (x, y) of Equation (1) and let $U^* - U_t = aP$ be an element of the cyclic group $< P >$; under the premise that the integer a is small, then the integer a can be effectively calculated by using exhaustive search, so the true solution (x_t, y_t) that satisfies both Equations (1) and (2) is found. Although IBDTRA protocol is not immediately dangerous, due to increased computing power and ongoing research on ECDLP [16,19,21], such attacks still seem to pose a threat to it.

Acknowledgment

This research was partially supported by the Ministry of Science and Technology, Taiwan (ROC), under contract no.: MOST 104-2221-E-468-004 and MOST 105-2410-H-468-009. MOST 106-2221-E-468-002.

References

[1] Y. Desmedt, Y. Frankel, "Shared generation of authentications and Signatures", in *Advances in Cryptology (CRYPTO'91)*, pp. 457–469, 1991.

[2] C. Dwork, M. Naor, A. Sahsi, "Concurrent zero-knowledge", in *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing (STOC'98)*, pp. 409–418, 1998.

[3] J. Hoffstein, J. Pipher, J. H. Silverman, *An Introduction to Mathematical Cryptography*, Springer-Verlag, New York, 2008.

[4] M. S. Hwang and T. Y. Chang, "Threshold signatures: Current status and key issues", *International Journal of Network Security*, vol. 1, no. 3, pp. 123–137, 2005.

[5] C. Jin, C. Xu, L. Jiang, "ID-based deniable threshold ring authentication," in *IEEE 17th International Conference on High Performance Computing and Communications (HPCC'15), IEEE 7th International Symposium on Cyberspace Safety and Security (CSS'15), and IEEE 12th International Conf on Embedded Software and Systems (ICESS'15)*, pp. 1779–1784, 2015.

[6] J. Kar, "ID-based deniable authentication protocol based Diffie-Hellman problem on elliptic curve," *International Journal of Network Security*, vol. 15, no. 5, pp. 357–364, 2013,

[7] H. Krawczyk, T. Rabin, *Chameleon Hashing and Signatures*, 1997.

[8] W. B. Lee, C. C. Wu, W. J. Tsaur, "A novel deniable authentication protocol using generalized ElGamal signature scheme", *Information Sciences*, vol. 177, no. 6, 1376–1381, 2007.

[9] C. T. Li, M. S. Hwang, C. Y. Liu, "An electronic voting protocol with deniable authentication for mobile Ad hoc networks," *Computer Communications*, vol. 31, no. 10, pp. 2534–2540, June 2008.

[10] F. Li, P. Xiong, C. Jin, "ID-based deniable authentication for Ad hoc networks", *Computing*, vol. 96, no. 9, pp. 843–853, 2014.

[11] F. Li, D. Zhong, T. Takagi, "Efficient deniable authenticationed encryption and its application to E-mail," *IEEE Transactions on Inforensics and Security*, vol. 11, no. 11, pp. 2477–2486, 2016.

[12] C. C. Lin, C. C. Chang, "An improved deniable authentication protocol," *International Journal of Computer Science and Network Secruity*, vol. 6, no. 11, pp. 240–242, 2006.

[13] T. C. Lin, "Improvement of an ID-based deniable authentication protocol," *Journal of Electronic Science and Technology*, vol. 16, no. 2, pp. 139–144, 2018.

[14] C. Y. Liu, C. C. Lee, T. C. Lin, "Cryptanalysis of a deniable authentication protocol based on generalized ElGamal signature scheme," *International Journal of Newtork Security*, vol. 12, no. 1, pp. 58–60, 2011.

[15] R. Lu, X. Lin, Z. Cao, L. Qin, X. Liang, "A simple deniable authentication protocol based on the Diffie-Hellman algorithm," *International Journal of Computer Mathematics*, vol. 85, no. 9, pp. 1315–1323, 2008.

[16] S. Miyoshi, Y. Nogami, T. Kusaka, N. Yamai, "Solving 94-bit ECDLP with 70 computers in parallel," *International Journal of Computer and Information Engineering*, vol. 9, no. 8, pp. 1966–1969, 2015.

[17] M. Naor, "Deniable ring authentication," *Advances in Cryptology (Crypto'01)*, LNCS, vol. 2442, pp. 481–498, 2002.

[18] M. D. Raimondo, R. Gennaro, "New approaches for deniable authentication," *Journal of Cryptology*, vol. 22, pp. 572–615, 2009.

[19] O. Schwarz, *General Attacks on Elliptic Curve Based Cryptosystems*, Project Report in Winter 2012-2013, Project Advisor: Barukh Ziv.

[20] Z. Shao, "Efficient deniable authentication protocol based on generalized ElGamal signature scheme," *Computer Standards & Interfaces*, vol. 26, no. 5, pp. 449–454, 2004.

[21] K. Somsuk, C. Sanemueang, "The new modified methodology to solve ECDLP based on brute force attack," *Recent Advances in Information and Communication Technology*, pp. 255–264, Springer, 2018.
[22] W. Susilo, Y. Mu, "Non-interactive deniable ring authentication," in *International Conference on Applied Cryptography and Network Security (ACNS'04)*, LNCS, vol. 3089, pp. 149–163, Springer, 2004.
[23] S. F. Tzeng, M. S. Hwang, "Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 61–71, Mar. 2004.
[24] E. J. Yoon, "Security analaysis of Kar's ID-based deniable authentication protocol," *Contemporary Engineering Sciences*, vol. 8, no. 17, pp. 765–771, 2015.
[25] E. J. Yoon, E. K. Ryu, K. Y. Yoo, "Improvement of Fan *et al.*'s deniable authentication protocol based on Diffie-Hellman algorithm," *Applied Mathematics and Computation*, vol. 167, pp. 274–280, 2005.

Biography

Tzu-Chun Lin received the PhD in Mathematics from the Faculties for Mathematics and Science of the Georg-August-University at Göttingen in Germany. She is an associate professor in the Department of Applied Mathematics of Feng Chia University in Taiwan, R.O.C.. Her current research interests include commutative algebras, invariant theory of finite groups and public-key cryptography.

Ting-Yi Yeh received his B.S. degree from the Department of Applied Mathematics at Feng Chia University, Taiwan, ROC. His research interests on information security and public key cryptography.

Min-Shiang Hwang received M.S. in industrial engineering from National Tsing Hua University, Taiwan in 1988; and Ph.D. degree in computer and information science from National Chiao Tung University, Taiwan in 1995. He was a professor and Chairman of the Department of Management Information Systems, NCHU, during 2003-2009. He was also a visiting professor with University of California (UC), Riverside and UC. Davis (USA) during 2009-2010. He was a distinguished professor of Department of Management Information Systems, NCHU, during 2007-2011. He obtained the 1997, 1998, 1999, 2000, and 2001 Excellent Research Award of National Science Council (Taiwan). Dr. Hwang was a dean of College of Computer Science, Asia University (AU), Taichung, Taiwan. He is currently a chair professor with Department of Computer Science and Information Engineering, AU. His current research interests include information security, electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr. Hwang has published over 300+ articles on the above research fields in international journals.