Cryptanalysis and Improvement of a Directed Digital Signature Scheme Using Non-interactive Public-key

Jia-Rong Sun[1], Shu-Chen Lin[1], and Min-Shiang Hwang[1,2]
(Corresponding author: Min-Shiang Hwang)
Department of Computer Science and Information Engineering, Asia University, Taiwan, ROC.[1]
Department of Medical Research, China Medical University Hospital, China Medical University[2]

ABSTRACT: Tseng et al. modified a non-interactive public-key distribution system and also proposed several applications based on the Maurer and Yacobi scheme. One of their applications, a directed digital signature scheme, only uses signer's identity to verify the signature. Any pair of users neither interacts to each other nor access to the public files of the system. However, their scheme cannot prevent the forgery attack. Each user can forge the signature for any message successfully and declare that is generated by the other user. In this paper, we also propose a secure directed digital signature scheme using non-interactive public-key.

1 INTRODUCTION

In 1984, Shamir (Shamir, 1984) proposed the idea that let each user's identification information (e.g., name, address, and E-mail address) be his/her public key in a public key cryptosystem. Any pair of users has the ability to verify the signature without exchanging secret and public keys, without keeping key directories, and without using the services of a third party (Hwang et al. 2014, Hwang et al. 2006). Base on Shamir's identity-based concept, many systems have been proposed that named identity-based public-key systems (Hwang & Chen, 1994, Koyama & Ohta, 1987, Tsujii & Itoh, 1989).

Most of the proposed schemes, the receiver must identify himself/herself to the trusted authority center and obtain his/her secret key from the trusted authority center. In other words, the user's ID is not really his/her identification information. Furthermore, the trusted authority center determines the secrets of all users.

In 1991, Maurer and Yacobi proposed an identity-based non-interactive public key distribution system based on a novel trapdoor one-way function of exponentiation modulo a composite number. Their latest version is released in 1996 (Maurer & Yacobi, 1996). The signature of any user is verified by his/her identity information without executing an interactive public key authentication. They adopted the squaring and the Jacobi symbol methods to guarantee that each identity number corresponds to his/her identity information. In their scheme, there are no public keys, certificates and other information except the identity of each user. Many ID-based schemes had been proposed (Awasthi & Lal, 2007, Choo, 2005, Farash & Attari, 2014, He et al. 2013, Kar, 2013, Li et al. 2006, Li et al. 2007, Mohaisen et al. 2009, Quan et al. 2013, Xu et al. 2009, Zhao & Zhang, 2011, Zhao, 2008).

There are many types of digital signature schemes (DSS): Directed DSS (Lu & Cao 2006, Tseng & Jan, 1998), Ring DSS (Awasthi & Lal 2007, Liu & Wong 2008, Qin, et al. 2014, Xiong, et al. 2011, Zheng, et al. 2007), Threshold DSS (Chang, et al. 2004, Chang, et al. 2005, Hwang & Chang 2005, Mashhadi 2013, Tzeng, et al. 2004, Xiong, et al. 2010, Yang, et al. 2004), Blind DSS (Chakraborty & Mehta 2012, Hwang, et al. 2002, Hwang, et al. 2003, Lee, et al. 2003, Moldovyan 2011, Moldovyan & Moldovyan 2010), Proxy DSS (Ma, et al. 2013, Mashhadi 2012, Tian & Huang 2012), Identity-based DSS (Kar 2014, Wang, et al. 2012), Certificateless DSS (He 2009, Wang, et al. 2009, Zhou, et al. 2014).

Tseng et al. (Tseng & Jan, 1998) improved the squaring method based on the Maurer and Yacobi scheme and also proposed a directed signature scheme, a user identification scheme and a conference key distribution system. Nevertheless, in this article, we discuss the security of their directed signature scheme and propose an improved scheme.

The remainder of our paper is organized as follows. In Section 2, we briefly review Tseng et al.'s directed digital signature scheme. An attack on Tseng et al.'s directed digital signature scheme is proposed in Section 3. In Section 4, we propose a secure directed digital signature scheme. Finally, we give a brief conclusion in Section 5.

2 REVIEW OF TSENG ET AL.'S SCHEME

Tseng et al. proposed a directed digital signature scheme that only the specified receiver can verify the signature. The scheme consists of three phases: system initialization, user registration, and the directed digital signature phases. The three phases are described in the following.

System Initialization Phase: The trusted authority generates system parameters as follows: *N* denotes the product of four primes p_j which are between 60 and 70 decimal digits, where the numbers (p_j-1) are odd and pair-wise relatively prime; *e* denotes an integer in $Z^*_{\varphi(n)}$ and the secret value *d* is satisfied the equation $e \cdot d \equiv 1 (\mathrm{mod}\, \varphi(N))$.

User Registration Phase: When a user U_A who wants to join the system, he/she presents his/her unique identity ID_A. The trusted authority randomly chooses a secret number *t* from $Z^*_{\varphi(n)}$, where φ is the Euler's totient function. Then, the trusted authority computes s_A to U_A in secret, where *g* is a primitive element in $GF(p_j)$, $v \equiv t^{-1} (\mathrm{mod}\, \varphi(N))$. A one-way function, $h(\cdot)$, is published by the trusted authority.

$$s_A \equiv e \cdot t \cdot \log_g (ID_A{}^2) (\mathrm{mod}\, \varphi(N)) \tag{1}$$

After generating the above parameters, the trusted authority publishes $\{N, g, e, h(\cdot)\}$ and keeps $\{p_1, p_2, p_3, p_4, t, v, d\}$ secret. The legal er, U_A publishes $\{ID_A\}$ and keeps $\{s_A\}$ secret.

The Directed Digital Signature Phase: Assume the legal user U_A wants to sign a message *M* and send it to the specific receiver U_B. The signature generating procedure is as follows. First of all, U_A chooses a random integer *k* in Z^*_N and computes the signature *(r, s)* for message *M*, where

$$r = g^{e \cdot k} (\mathrm{mod}\, N) \tag{2}$$

$$s = (ID_B{}^2)^{s_A \cdot h(M,r)} \cdot g^k (\mathrm{mod}\, N) \tag{3}$$

Secondly, U_A sends (M, r, s) to U_B. Upon receiving (M, r, s), U_B can verify the signature of message *M* by the following equation:

$$s^e = (ID_A{}^2)^{e \cdot s_B \cdot h(M,r)} \cdot r (\mathrm{mod}\, N) \tag{4}$$

If the above verified equation holds, the signature for message *M* by U_A is verified. The specific verifier only verify the validity of signature for message *M* by the unique identity of the signer.

3 ATTACK ON TSENG ET AL.'S SCHEME

In this section, we will show that Tseng et al.'s directed digital signature scheme cannot withstand the forgery attack. Assume U_A generates the signature (r, s) for the message *M* and sends it to a specified receiver U_B. In general, the values $\{M, r, s\}$ is only generated by U_A. However, in their scheme, the user U_B can forge the signature (r', s') for the sage M' and declare that the signature (r', s') is generated by the U_A. The U_B forges signature (r', s') as follows:

Step1. Choose a random integer k' in Z^*_N

Step2. Compute the signature (r', s') for message M' as follows:

$$r' = g^{e \cdot k'} (\mathrm{mod}\, N)$$
$$s' = (ID_A{}^{s_B})^{2 \cdot h(M', r')} \cdot g^{k'} (\mathrm{mod}\, N)$$

The signature (r', s') for message M' is verified correctly as follows:

$$(s')^e = (ID_A{}^2)^{e \cdot s_B \cdot h(M', r')} \cdot g^{k'} (\mathrm{mod}\, N)$$
$$= ((ID_A{}^{s_B})^{2 \cdot h(M', r')} \cdot g^{k'})^e (\mathrm{mod}\, N)$$

Therefore, U_B can forge the signature for any message and declare the signature is generated by U_A. In other words, the user can forge the signature and declare that is generated by the other user. The problem is that any user U_A or U_B, can obtain $(ID_B{}^2)^{s_A}$ and $(ID_A{}^2)^{s_B}$ respectively by the following equation:

$$(ID_A{}^2)^{s_B} = g^{d \cdot v \cdot s_A \cdot s_B} = (ID_B{}^2)^{s_A} \tag{5}$$

4 THE PROPOSED SCHEME

There are also three phases in the proposed scheme: system initialization, user registration, and the directed digital signature phases. The System Initialization Phase and User Registration Phase of the proposed scheme are the same as in Tseng et al.'s Scheme (Tseng & Jan, 1998).

The Directed Digital Signature Phase: Assume the legal user U_A wants to sign a message *M* and send it to the specific receiver U_B. The signature generating procedure is as follows. First of all, U_A chooses a random integer *k* in Z^*_N and computes the signature *(r, s)* for message *M*, where

$$r = g^k (\mathrm{mod}\, N) \tag{6}$$

$$s = (ID_B{}^2)^{s_A \cdot h(M,r)} \cdot g^{d \cdot k} (\mathrm{mod}\, N) \tag{7}$$

Secondly, U_A sends (M, r, s) to U_B. Upon receiving (M, r, s), U_B can verify the signature of message *M* by the following equation:

$$s^e = (ID_A{}^2)^{e \cdot s_B \cdot h(M,r)} \cdot r (\mathrm{mod}\, N) \tag{8}$$

If the above verified equation holds, the signature for message *M* by U_A is verified. The specific verifier only verify the validity of signature for message *M* by the unique identity of the signer.

The proposed scheme is secure to against forging attack. U_B cannot forge the signature for any message and declare the signature is generated by U_A. The key point is that any user, U_B, cannot obtain the signature

s in Equation (7) because of U_B does not known the U_A's secret value d.

5 CONCLUSION

We have shown that there is a leak in Tseng et al.'s directed digital signature scheme. Their scheme cannot withstand the forgery attack. Hence, anyone can forge the signature for any message and declare that is sent from a specific user. We also proposed a secure directed digital signature scheme using non-interactive public-key.

ACKNOWLEDGMENTS

This study was supported by the National Science Council of Taiwan under grant 103-2221-E-468 - 026, 103-2622-E-468-001-CC2, and 103-2622-H-468-001-CC2.

REFERENCE

Awasthi, A.K. & Lal, S. (2007). ID-based ring signature and proxy ring signature schemes from bilinear pairings, *International Journal of Network Security* 4(2): 187-192.

Chakraborty, K. & Mehta, J. (2012). A stamped blind signature scheme based on elliptic curve discrete logarithm problem. *International Journal of Network Security* 14(6): 316-319.

Chang, T.Y., Hwang, M.S., Yang, W.P. (2005). An improvement on the lin-wu (t, n) threshold verifiable multi-secret sharing scheme. *Applied Mathematics and Computation* 163(1): 169-178.

Chang, T.Y., Yang, C.C., Hwang, M.S. (2004). A threshold signature scheme for group communications without a shared distribution center. *Future Generation Computer Systems* 20(6): 1013-1021.

Choo, K.K.R. (2005). Revisit of McCullagh-Barreto two-party ID-based authenticated key agreement protocols, *International Journal of Network Security* 1(3): 154-160.

Farash, M.S. & Attari, M. A. (2014). A pairing-free ID-based key agreement protocol with different PKGs, *International Journal of Network Security* 16(3): 168-173.

He, D., Khan, M.K., Wu, S. (2014). On the security of a RSA-based certificateless signature scheme. *International Journal of Network Security* 16(1): 78-80.

He D, Zhao W, and Wu S. (2013). Security analysis of a dynamic ID-based authentication scheme for multi-server environment using smart cards. *International Journal of Network Security* 15(5): 282-292.

Hwang M.S. & Chang, T.Y. (2005). Threshold signatures: current status and key issues. *International Journal of Network Security* 1(3): 123-137.

Hwang M.S., Chong S.K., and Chen T.Y. (2010). Dos-resistant ID-based password authentication scheme using smart cards, *Journal of Systems and Software* 83: 163-172.

Hwang, M.S., Lee, C.C., Lai, Y.C. (2002). Traceability on low-computation partially blind signatures for electronic cash. *IEICE Fundamentals on Electronics, Communications and Computer Sciences* E85-A(5): 1181-1182.

Hwang, M.S., Lee, C.C., Lai, Y.C. (2003). An untraceable blind signature scheme. *IEICE Transactions on Foundations* E86-A(7): 1902-1906.

Hwang M.S., Lo J.W., and Lin S.C. (2004). An efficient user identification scheme based on ID-based cryptosystem, *Computer Standards & Interfaces* 26(6): 565-569.

Hwang T and Chen J. L. (1994). Identity-based conference key broadcast system. *IEE Proceedings – Computer Digital Technology* 141(1): 57-60.

Kar, J. (2013). ID-based deniable authentication protocol based on Diffie-Hellman problem on elliptic curve. *International Journal of Network Security* 15(5): 357-364.

Kar, J. (2014). Provably secure online/off-line identity-based signature scheme for wireless sensor network. *International Journal of Network Security* 16(1): 29-39.

Koyama, K. & Ohta, K. (1987). Identity-based conference key distribution system, in *Advances in Cryptology, CRYPTO'87*, Lecture Notes in Computer Science, LNCS 293: 194-202.

Lee, C.C., Hwang, M.S., Yang, W.P. (2003). Untractable blind signature schemes based on discrete logarithm problem. *Fundamenta Informaticae* 55(3-4): 307-320.

Li F., Xin X., and Hu Y. (2006). ID-based signcryption scheme with (t,n) shared unsigncryption, *International Journal of Network Security* 3(2): 155-159.

Li Z., Chong C.F., Hui L.C.K., Yiu S.M., Chow K. P., Tsang W.W., Chan H.W., Pun K.K.H. (2007). An attack on libert et al.'s ID-based undeniable signature scheme. *International Journal of Network Security* 5(2): 220-223.

Liu, J.K. & Wong, D.S. (2008). Solutions to key exposure problem in ring signature. *International Journal of Network Security* 6(2): 170-180.

Lu, R. & Cao, Z. (2006). A directed signature scheme based on RSA assumption. *International Journal of Network Security* 2(3): 182-186.

Ma, C., Xue, K., Hong, P. (2013). A proxy signature based re-authentication scheme for secure fast handoff in wireless mesh networks. *International Journal of Network Security* 15(2): 122-132.

Mashhadi, S. (2013). A novel non-repudiable threshold proxy signature scheme with known signers. *International Journal of Network Security* 15(4): 274-279.

Mashhadi, S. (2012). A novel secure self proxy signature scheme. *International Journal of Network Security* 14(1): 22-26.

Maurer U.M. & Yacobi Y. (1996). A non-interactive public-key distribution system. *Designs, Codes and Cryptography* 9(3): 305-316.

Mohaisen A., Nyang D.H., Lee K.H. (2009). Hierarchical grid-based pairwise key pre-distribution in wireless sensor networks, *International Journal of Network Security* 8(3): 282-292.

Moldovyan, N.A. (2011). Blind signature protocols from digital signature standards. *International Journal of Network Security* 13(1): 22-30.

Moldovyan, N.A. & Moldovyan, A.A. (2010). Blind collective signature protocol based on dis-

crete logarithm problem. *International Journal of Network Security* 11(2): 106-113.
Qin, Z., Xiong, H., Li, F. (2014). A provably secure certificate based ring signature without pairing. *International Journal of Network Security* 16(4): 278-285.
Quan Q., Xiao C.J., and Zhang R. (2013). Grid-based data stream clustering for intrusion detection. *International Journal of Network Security* 15(1): 1-8.
Shamir A. (1984). Identity based cryptosystems & signature schemes, in *Advances in Cryptology, CRYPTO'84*, Lecture Notes in Computer Science, LNCS 196: 47-53.
Tian, M. & Huang, L. (2012). Breaking a proxy signature scheme from lattices. *International Journal of Network Security* 14(6): 320-323.
Tseng Y.M. & Jan J.K. (1998). ID-based cryptographic schemes using a non-interactive public-key distribution system. in *Proceedings of the 14th Annual Computer Security Applications Conference (IEEE ACSAC98)*: pp. 237-243.
Tsujii S & Itoh T. (1989). An ID-based cryptosystem based on the discrete logarithm problem. *Journal of Selected Areas in Communications* 7(4): 467-473.
Tzeng, S.F., Yang, C.Y., Hwang, M.S. (2004). A nonrepudiable threshold multi-proxy multi-signature scheme with shared verification. *Future Generation Computer Systems* 20(5): 887-893.
Wang, C., Long, D., Tang, Y. (2009). An efficient certificateless signature from pairings. *International Journal of Network Security* 8(1): 96-100.
Wang, Z., Wang, L., Zheng, S., Yang, Y., Hu, Z. (2012). Provably secure and efficient identity-based signature scheme based on cubic residues. *International Journal of Network Security* 14(1): 33-38.
Xiong, H., Qin, Z., Li, F. (2010). Identity-based threshold signature secure in the standard model. *International Journal of Network Security* 10(1): 75-80.
Xiong, H., Qin, Z., Li, F. (2011). A certificateless proxy ring signature scheme with provable security. *International Journal of Network Security* 12(2): 92-106.
Xu C., Zhou J., Xiao G. (2008). General group oriented ID-based cryptosystems with chosen plaintext security. *International Journal of Network Security* 6(1): 1-5.
Yang, C.Y., Tzeng, S.F., Hwang, M.S. (2004). On the efficiency of nonrepudiable threshold proxy signature scheme with known signers. *Journal of Systems and Software* 73(3): 507-514.
Zhao X. & Zhang F. (2011). A new type of ID-based encryption system and its application to pay-TV systems. *International Journal of Network Security* 13(3): 161-166.
Zhao Z.M. (2008). ID-based weak blind signature from bilinear pairings. *International Journal of Network Security* 7(2): 265-268.
Zheng, D., Li, X., Chen, K. (2007). Code-based ring signature scheme. *International Journal of Network Security* 5(2): 154-157.
Zhou, M., Zhang, M., Wang, C., Yang, B. (2014). CCLAS: A practical and compact certificateless aggregate signature with share extraction. *International Journal of Network Security* 16(3): 174-181.