Forward/Backward Unforgeable Digital Signature Scheme Using Symmetric-Key Crypto-System

Tzonelih Hwang
Computer Science and Information Engineering,
National Cheng Kung University,
Tainan, Taiwan
hwangtl@ismail.csie.ncku.edu.tw*

Yi-Ping Luo
Institute for Information Industry,
CyberTrust Technology Institute,
Taipei, Taiwan
yipingluo@iii.org.tw

Prosanta Gope
Computer Science and Information Engineering,
National Cheng Kung University,
Tainan, Taiwan
prosanta.nitdgp@gmail.com

Zhi-Rou Liu
Computer Science and Information Engineering,
National Cheng Kung University,
Tainan, Taiwan
weiweiwen@ismail.csie.ncku.edu.tw

***Abstract*—The digital equivalent of a handwritten signature or stamped seal, but offering far more inherent security, a digital signature is intended to solve the problem of tampering and impersonation in digital communications. Digital signatures can provide the added assurances of evidence to origin, identity and status of an electronic document, transaction or message, as well as acknowledging informed consent by the signer. Even though, some signature schemes have already been proposed to address all the requirements of a digital signature scheme. However, they are unable to accomplish forward or backward unforgeability in arbitrated signature scheme, where if the signature key used in the scheme is compromised then an attacker will be able to forge any previous/future signature. In order to resolve this issue, in this article, we propose secure digital signature schemes, which can ensure the security requirements including forward and backward unforgeability supports.**

Keywords-component; Digital Aignature; Arbitrated Digital Signature; Forward Unforgeability; Backward Unforgeability

I. INTRODUCTION

Digital signatures authenticate electronic documents in much the same way that handwritten signatures authenticate printed documents. Recipients of electronic documents accompanied by digital signatures may verify that senders are who they claim to be and that the documents have not been altered from the time of transmission. In other words, senders may not disown digital signatures by claiming that they have been forged, and recipients can verify the identity of senders as well as the integrity of the documents.

1.1 Security Requirements on a Digital Signature Scheme

Designing a secure digital signature scheme is always a challenging task. A secure digital signature scheme should satisfy the following requirements:

- Authentication: Through the verified signature, the signature receiver can verify the identity of signer and the integrity of the message.
- Non-repudiation: A signer who has sent a valid signature to a receiver cannot later deny having provided that signature.
- Unforgeability: Neither the signature receiver nor an attacker can forge a signature or change the content of a signature. The signature should not be reproducible by any other person.
- Forward Unforgeability: Even if the signature key used in the scheme is compromised, then any previous signature will not be forged.
- Backward Unforgeability: Even if the signature key used in the scheme is compromised, then the attacker will not be able to forge any future signature.

1.2 Problem Statement and Motivation

There are several digital signature schemes [1-10] have been proposed in recent years for various application environments. However, none of these signature schemes can satisfy forward/backward forgeability properties, which are greatly important in the sense of a secure digital signature scheme. For example in an e-commerce-based system, if the service provider's (like the e-shopping website server) signature key is compromised, then any previous transaction record would be forged by the attacker to obtain some benefits. Moreover, the attacker may even try to forge the future signature to impersonate as the legal service provider without being detected.

In 1999, Bellare et al. first proposed the concept of the signature with forward-security [14]. In 2001, Abdalla et al. proposed the improved version of [14] with a shorter public key [15]. Later, Malkin et al. presented an efficient forward-secure digital signature scheme [16] where the secret key only can be used in the number of time period by an exponential function of the security parameter. In 2002, Kozlov et al. proposed the signature schemes by using the key update [17], which claimed that frequent key update will enhance the signature security. Since then, many works related to forward security signature have been proposed [18-25]. On the other hand, in 2010, Lin et al. [26] proposed a forward-backward secure signature scheme to enhance the security of [15] by introducing a backward-secure detection. Unfortunately, in 2015, Wang et al. [27] pointed out that their scheme does not satisfy the property of backward security.

The above-mentioned digital signature schemes are based on public-key crypto-system, which certainly causes higher computational overhead and execution time.

978-1-5090-3438-3/16 $31.00 © 2016 IEEE
DOI 10.1109/ICS.2016.55

Furthermore, security of the existing public key based signature systems has already been proven to be insecure in the environment of quantum computation [10-13].

These are the issues, which have been a great inspiration for us to propose forward or backward unforgeability based digital signature schemes using symmetric key crypto-system, which can deal with various security issues like authentication, non-repudiation, etc. Besides, the scheme should also encompass limited computational burden with the lower execution time and reasonable communication overhead.

Therefore, the rest of the article is organized as follows. In Section 2, we describe our proposed schemes. In Section 3, we analyze the security of the proposed schemes. Finally, a concluding remark is given in Section 4.

II. PROPOSED SIGNATURE SCHEMES

This section demonstrates the forward and backward unforgeability based arbitrated digital signature schemes respectively, where a signer (say Alice) signs a message M to obtain the signature Sig_S and then sends the signature to the arbiter (say Trent). After that, Trent sends the verified signature to the receiver (say Bob). Here, Alice and Bob have to register in Trent and they will get $\left(ID_S, K_S^{Sig}, K_S^E\right)$ and $\left(ID_R, K_R^E\right)$ from Trent, respectively. In the proposed schemes, the arbiter is assumed to be honest and he/she maintains all the record of the intermediate information when verifying the signature. When the dispute occurs, all the participants must trust the arbiter to resolve dispute fairly.

TABLE 1 THE DEFINITIONS OF SOME NOTATIONS.

Notation	Definition
S / R	The signer/receiver
ID_U	The identity of the user U, where $U \in \{S, R\}$
K_U^E	The shared encryption key between the arbiter and the user U, where $U \in \{S, R\}$
K_S^{Sig}	The signature key of the signer
K_i^{OSK}	The one-time signature key of the signer
M	A message which would be signed
T	The timestamp
"$\|\|$"	The concatenate operation
N	A random number
Sig_S	The signer's signature
$E_K(\cdot)$	A symmetric key encryption (e.g. AES) by using K
$D_K(\cdot)$	A decryption of $E_K(\cdot)$ by using K
$H(\cdot)$	A one-way hash function: $H(\cdot): \{0,1\}^* \rightarrow \{0,1\}^n$

2.1 Proposed Forward Unforgeable Signature Scheme

The procedures of the proposed scheme can be divided into three phases, i.e., signature phase, verification phase, and receiving phase (see also Figure 1).

1)Signature phase

S1. Alice generates a random number N and then computes $N_X = K_S^E \oplus N$.

S2. Alice computes $h = H\left(M \,||\, ID_S \,||\, ID_R \,||\, T \,||\, N\right)$ and then generates the signature $Sig_S = E_{K_S^E}(h)$.

S3. Alice sends $\left(Sig_S, M, T, ID_S, ID_R, N_X\right)$ to Trent.

2)Verification phase

V1. When Trent receives the request from Alice, he/she computes $N' = K_S^E \oplus N_X$ and decrypts Sig_S to obtain $h = D_{K_S^E}\left(Sig_S\right)$ by using K_S^E. Subsequently, Trent computes $h' = H\left(M \,||\, ID_S \,||\, ID_R \,||\, T \,||\, N'\right)$ and then compares it with h. If $h = h'$, then Trent goes to the next step. Otherwise, Trent rejects this signature.

V2. Trent calculates $H\left(N' \| K_S^E \| ID_S\right)$ to obtain the value V and updates Alice's encryption key to obtain $K_{S\_new}^E = H\left(K_S^E \,||\, ID_S \,||\, N'\right)$.

V3. Trent computes $H(Sig_S \| M \| T \| ID_S \| ID_R)$ to obtain h_R and then encrypts h_R to obtain $I = E_{K_R^E}(h_R)$ by using K_R^E.

V4. Trent sends V and $\left(I, Sig_S, M, T, ID_S, ID_R\right)$ to Alice and Bob, respectively.

3)Receiving phase

R1. When Alice obtains V from Trent, she computes $H\left(N \,||\, K_S^E \,||\, ID_S\right)$ to obtain $V*$, and then compares it with V. If $V = V*$, then Alice updates her encryption key to obtian $K_{S\_new}^E = H\left(K_S^E \| ID_S \| N\right)$.

R2. When Bob receives $\left(I, Sig_S, M, T, ID_S, ID_R\right)$, he decrypts I to obtain $h_R = D_{K_R^E}(I)$ by using K_R^E. After that, Bob computes $H(Sig_S \| M \| T \| ID_S \| ID_R)$ to obtain h_R', and then compares it with h_R. If $h_R = h_R'$, Bob accepts this signature. Otherwise, Bob rejects this signature.

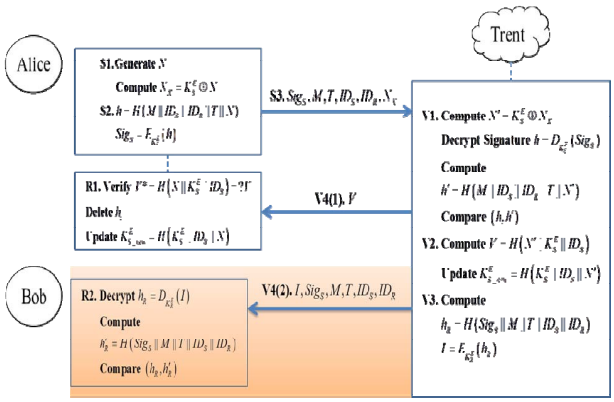

Figure 1: The detailed procedures of the forward unforgeable signature scheme.

2.2 *Proposed Backward Unforgeable Signature Scheme*

Now, in this section, in order to achieve the features of backward unforgeability, the signer calculates n one-time signature keys based on the signature key for generating n signatures as follows, where K_i^{OSK} denotes the i th one-time signature key and $H^{(n-i+1)}(\cdot)$ represents the hash chain function by performing $(n-i+1)$ times hash function, $1 \le i \le n$.

$$K_i^{OSK} = H^{(n-i+1)}(K_S^{Sig} \,||\, ID_S)$$

Here, the signer can store these n one-time signature keys in her database, or she can store the signature key and how many time the signature has been used (i.e., i value) in her database. In the proposed scheme, the signer chooses to store the signature key and i value in her database. Therefore, even though the one-time signature key is compromised during the signature transmission, the attacker cannot forge the future signature on behalf of the signer.

The procedures of the proposed scheme can be divided into three phases, i.e., signature phase, verification phase, and receiving phase (see also Figure 2). The detailed steps are listed in detail, as follows.

1)Signature phase

S1'. Alice computes $h = H(M \,||\, ID_S \,||\, ID_R \,||\, T)$, and then generates the signature $Sig_S = E_{K_i^{OSK}}(h)$.

S2'. Alice sends $(Sig_S, M, T, ID_S, ID_R, i)$ to Trent.

S3'. Alice sets the value i to $i+1$.

2)Verification phase

V1'. When Trent receives the request from Alice, he/she can generate the one-time signature key K_i^{OSK} based on i. After that, Trent decrypts Sig_S to obtain $h = D_{K_i^{OSK}}(Sig_S)$ by using K_i^{OSK}. Subsequently, Trent computes $h' = H(M \,||\, ID_S \,||\, ID_R \,||\, T)$ and then compares it with h. If $h = h'$, then Trent goes to the next step. Otherwise, Trent rejects this signature.

V2'. Trent computes $H(Sig_S, M, T, ID_S, ID_R)$ to obtain h_R and then encrypts h_R to obtain $I = E_{K_R^E}(h_R)$ by using K_R^E.

V3'. Trent sends $(I, Sig_S, M, T, ID_S, ID_R)$ to Bob.

3)Receiving phase

R1'. When Bob receives $(I, Sig_S, M, T, ID_S, ID_R)$, he decrypts I to obtain $h_R = D_{K_R^E}(I)$ by using K_R^E. After that, Bob computes $H(Sig_S \| M \| T \| ID_S \| ID_R)$ to obtain h_R', and then compares it with h_R. If $h_R = h_R'$, Bob accepts this signature. Otherwise, Bob rejects this signature.

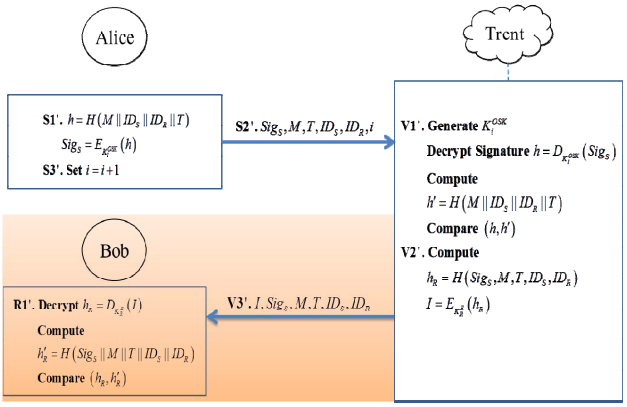

Figure 2: The detailed procedures of the backward unforgeable signature scheme.

III. SECURITY ANALYSIS

Here, we analyze the security of the proposed signature schemes. In this section, we demonstrate that, our proposed signature schemes can ensure several imperative properties, i.e., forward/backward unforgeability, authenticity, and non-repudiation.

In the proposed forward unforgeable signature scheme, since the encryption key is updated in every signature transmission by using a secret random number, therefore, an attacker cannot forge any previous signature without knowing the random number. On the other hand, the security backbone of the proposed backward unforgeable signature scheme is based on the one-way hash function. That is, anyone cannot reconstruct the input of hash function from its hash value alone. Therefore, if the current signature key (i.e., the one-time signature key) is compromised, then the attacker will not be able to forge any future signature.

Besides, in both signature schemes, if, later, Alice (the signer) disavows having produced a signature on the message M, then Bob can send the information

$\{I, Sig_S, M, T, ID_S, ID_R\}$ to Trent. After that, Trent compares the received information with the record in his/her database. If there is a record in his/her database, then Trent can judge that Alice has ever produced a signature Sig_S on M to Bob.

Therefore, the proposed forward/backward unforgeable signature scheme can satisfy all the security requirements, i.e., forward/backward unforgeability, authenticity, and non-repudiation.

IV. CONCLUSIONS

In this article, we have proposed a secure digital signature scheme by using the symmetric-key crypto-system, which can ensure all the security requirements including the features like forward/backward unforgeability, non-repudiation, etc. Security analysis shows that proposed scheme is secure and hence can be useful for various applications. In the proposed schemes, the properties of forward and backward unforgeability have been design to be the forward and backward unforgeable signature schemes, respectively. How to propose a forward-backward unforgeable signature scheme where even if the signature key is compromised then also an attacker will not be able to forge any previous and future signature, could be a very interesting future research.

ACKNOWLEDGMENT

We would like to thank the Ministry of Science and Technology of Republic of China for financial support of this research under Contract No. MOST 105-2221-E-006 - 162 -MY2

REFERENCES

[1] S. Goldwasser, S. Micali and R. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. SIAM Journal of Computing, 17 (2), pp. 281–308 (1988).

[2] J. Herranz. A formal proof of security of Zhang and Kim's ID-based ring signature scheme. Proceedings of WOSIS'04, INSTICC Press, pp. 63–72 (2004).

130 Bibliography

[3] J. Herranz, C. Padr´o and G. S´aez. Distributed RSA signature schemes for general access structures. Proceedings of ISC'03, LNCS 2851, Springer-Verlag, pp. 122–136 (2003).

[4] J. Herranz and G. S´aez. Verifiable secret sharing for general access structures, with application to fully distributed proxy signatures. Proceedings

of Financial Cryptography Conference 2003, LNCS 2742, SpringerVerlag, pp. 286–302 (2003).

[5] J. Herranz and G. S´aez. Forking lemmas for ring signature schemes. Proceedings of Indocrypt'03, LNCS 2904, Springer-Verlag, pp. 266–279,(2003).

[6] J. Herranz and G. S´aez. Ring signature schemes for general access structures. Proceedings of ESAS'04, LNCS 3313, Springer-Verlag, pp. 54–65,(2005).

[7] J. Herranz and G. S´aez. New ID-based ring signature schemes. Proceedings of ICICS'04, LNCS 3269, Springer-Verlag, pp. 27–39 (2004).

[8] J. Herranz and G. S´aez. Revisiting fully distributed proxy signature schemes. Proceedings of Indocrypt'04, LNCS 3348, Springer-Verlag, pp.356–370 (2004).

[9] J. Herranz and G. S´aez. ID-based ring signatures for general families of signing subsets. Submitted (2005).

[10] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on, 1994, pp. 124-134.

[11] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," Siam Journal on Computing, vol. 26, pp. 1484-1509, Oct 1997.

[12] R. Jozsa, "Quantum factoring, discrete logarithms, and the hidden subgroup problem," Computing in Science & Engineering, vol. 3, pp. 34-43, 2001.

[13] J. Proos and C. Zalka, "Shor's discrete logarithm quantum algorithm for elliptic curves," arXiv preprint quant-ph/0301141, 2003.

[14] M. Bellare and S. K. Miner, "A forward-secure digital signature scheme," in Proceedings of CRYPTO, LNCS 1666, 1999, pp. 431-448.

[15] M. Abdalla and L. Reyzin, "A new forward-secure digital signature scheme," in Proceedings of ASIACRYPT, LNCS 2139, 2000, pp. 116-129.

[16] T. Malkin, D. Micciancio, and S. K. Miner, "Composition and efficiency tradeoffs for forward-secure digital signatures," in Cryptology ePrint Archive, Report 2001/034.

[17] A. Kozlov and L. Reyzin, "Forward-secure signatures with fast key update," in Proceedings of Security in Communication Networks, LNCS 2576, 2002, pp. 247-262.

[18] M. Abdalla and M. Bellare, "Increasing the lifetime of a key: A comparative analysis of the security of re-keying techniques," in Proceedings of ASIACRYPT, LNCS 1976, 2000, pp. 431-448.

[19] . G. Itkis and L. Reyzin, "Forward-secure signatures with optimal signing and verifying," in Proceedings of CRYPTO, LNCS 2139, 2001, pp. 332-354.

[20] A. Kozlov and L. Reyzin, "Forward-secure signatures with fast key update," in Proceedings of Security in Communication Networks, LNCS 2576, 2002, pp. 247-262.

[21] H. Krawczyk, "Simple forward-secure signatures from any signature scheme," in Proceedings of the 7th ACM Conference on Computer and Communications Security, 2000, pp. 108-115.

[22] C. F. Lu and S. Shieh, "Secure key-evolving protocols for discrete logarithm schemes," in Proceedings of the Cryptographers' Track at the RSA Conference, LNCS 2271, 2002, pp. 300-309.

[23] C. F. Lu and S. Shieh, "Efficient key-evolving protocol for the GQ signature," Journal of Information Science and Engineering, Vol. 20, 2004, pp. 763-769.

[24] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," Journal of CRYPTOLOGY, Vol. 13, 2000, pp. 0361-369.

[25] W. G. Tzeng and Z. J. Tzeng, "Robust forward-secure signature schemes with proactive security," in Proceedings of Public Key Cryptography, LNCS 1992, 2000, pp. 264-276.

[26] D. R. Lin, C. I. Wang, and D. J. Guan, "A forward-backward secure signature scheme," Journal of Information Science and Engineering, vol. 26, no. 6, pp. 2319–2329, 2010.

[27] L. L. Wang, K. F. Chen, X. P. Mao, and Y. T. Wang, "On the Security of a Forward-backward Secure Signature Scheme," International Journal of Network Security, Vol.17, No.3, PP.307-310, 2015.