

Cryptanalysis on Du-Wen Certificateless Short Signature Scheme

Chun-I Fan, Ruei-Hau Hsu, and Pei-Hsiu Ho

Department of Computer Science and Engineering, National Sun Yat-sen University
Kaohsiung, Taiwan, R.O.C.

cifan@faculty.nsysu.edu.tw, {d943040001, d943040003}@student.nsysu.edu.tw

Abstract. Certificateless signature scheme is a practical solution to confront the drawback, KGC being able to forge the signature of a user, of an identity based signature scheme. Lots of previous research results have shown the security models and the generic constructions for certificateless signatures. However, most of them did not satisfy Girault's level-3 security which the conventional public key infrastructure (PKI) can achieve. Until 2007, Hu et al. introduced a generic construction and security model that can fulfill the requirement of Girault's level-3 security. Recently, Du and Wen proposed a certificateless short signature scheme which is more computation efficient than the previous ones. But a flaw in security proofs and lack of Girault's level-3 security can be still found in their scheme. In this paper, a cryptanalysis on Du-Wen scheme and an improved scheme will be presented.

1 Introduction

In a conventional public key infrastructure (PKI), it requires heavy management and communication cost to achieve authenticity of the public keys of users. Identity based (ID-based) cryptography was proposed by Shamir [15] to conquer the problem of public key certification. Each user is allowed to take her/his public identity information as her/his public key without being certified by any authority or trusted third party. To validate the public key and the corresponding private key of a user, the private key is issued by a Key Generation Center (KGC) to obtain the authorization. However, it has a serious drawback, i.e., KGC can also have the same ability as the user to perform public-key cryptographic operations, such as decryption and signing, by yielding the same key pair via the identity of the user and its master key. Consequently, confidentiality and non-repudiation cannot be satisfied in such ID-based public-key cryptosystems perfectly.

To solve the shortcoming of ID-based cryptosystems, a certificateless cryptosystem, which combines the advantages of PKI and ID-based cryptosystems, was proposed by Al-Riyami and Paterson [1]. In the key issuing phase of a certificateless signature scheme, both the secret of a user and the master key of KGC are required for the generation of the public key and private key of the

user. It prevents KGC from producing the user's private key for signing or decrypting messages. Subsequently, several certificateless signature (CLS) schemes [6][9][12][14][16][19] were proposed where [9][14][16] just provided informal security analyses and [6][12][19] proved that their schemes are secure via a formal manner. Later, key replacement attacks [2][5][18] were proposed against the schemes [9][14][16]. In the development of CLS, some generic constructions [2][10][12] for CLS were introduced to provide versatile abilities, e.g., employing different kinds of signature schemes in the construction of CLS schemes. From the above studies, some proposed schemes [9][14][16] were demonstrated as being insecure under key replacement attacks and [1][12][14] were vulnerable to malicious-but-passive-KGC attacks [2]. Thus, [2][13] presented two provably secure CLS schemes under the presence of some specified adversaries [11].

However, the security model of [2][13] cannot reach the same security level as that of PKI-based signature schemes. The conventional PKI can meet Girault's level-3 security [8], that is, KGC or trusted third party (TTP) cannot find out all secret information of a user nor generate a contradictory public key, which is another public key indistinguishable from the real public key of the user. Therefore, Hu et al. [11] proposed an improved generic model to construct a CLS scheme to achieve Girault's level-3 security. After that, Du and Wen [7] proposed a certificateless short signature scheme with provable security. Nevertheless, a user in Du-Wen scheme can change its public key without being certified again by KGC. Also, there is a flaw in the simulation of the security proofs. In this paper, we will show how a user replaces its public key without the help of KGC to break Girault's level-3 security in Du-Wen scheme and point out the flaw in the security proofs.

The rest of this paper is organized as follows. In Section II, we review Du-Wen certificateless short signature scheme. In Section III, we show the flaw in the simulation of the security proofs and how to perform the public-key replacement attack in Du-Wen scheme. We also propose an improved scheme in this section. Finally, we give a concluding remark.

2 Review of Du-Wen Certificateless Short Signature Scheme

In this section, we will review Du-Wen certificateless short signature scheme from bilinear pairings.

2.1 Bilinear Pairings

Let G_1 be a cyclic additive group, and G_2 be a cyclic multiplicative group of the same prime order q . There exists a bilinear mapping $e : G_1 \times G_1 \rightarrow G_2$ which satisfies the following properties:

1. Bilinearity: $e(aP, bQ) = e(P, Q)^{ab}$, where $P, Q \in G_1, a, b \in Z_q^*$
2. Non-degeneracy: There exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$

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

The modified Tate pairing [3] on a supersingular elliptic curve is such a bilinear pairing.

2.2 Du-Wen Certificateless Short Signature Scheme

Du-Wen scheme consists of seven algorithms defined as follows:

- **Setup:** Given an input k as the system security parameter. Then Key Generation Center (KGC) selects two groups G_1 and G_2 of prime order $q \leq 2^k$, a bilinear mapping $e : G_1 \times G_1 \rightarrow G_2$, a generator P of group G_1 where $e(P, P) = g$. KGC also selects two distinct cryptographic hash functions $H_1 : \{0, 1\}^* \rightarrow Z_q^*$, $H_2 : \{0, 1\}^* \times G_1 \rightarrow Z_q^*$, and chooses a random number $s \in Z_q^*$ as its master key, and then generates its public key $P_{pub} = sP \in G_1$. Thereafter, KGC publishes the system parameters, $params = \{k, G_1, G_2, e, q, P, g, P_{pub}, H_1, H_2\}$, and keeps s secretly.
- **Partial-Private-Key-Extract:** Given a user identity $ID \in \{0, 1\}^*$, KGC computes $Q_{ID} = H_1(ID)$ and $d_{ID} = \frac{1}{s+Q_{ID}}P$. After that, KGC sends d_{ID} to the user with identity ID as her/his partial private key via a secure channel. The partial key can be verified by checking if $e(d_{ID}, P_{pub} + Q_{ID}P) = g$. Let $T = P_{pub} + Q_{ID}P$.
- **Set-Secret-Value:** The user randomly selects $r \in Z_q^*$ and sets it as her/his secret value.
- **Set-Private-Key:** The user sets (d_{ID}, r) as her/his private key.
- **Set-Public-Key:** Take $params$ and the user's secret value r as inputs, and generate the user's public key $pk_{ID} = r(P_{pub} + Q_{ID}P) = rT$.
- **CL-Sign:** To generate the signature of message $m \in \{0, 1\}^*$, the user performs the following steps:
 1. set $h = H_2(m, pk_{ID})$;
 2. compute $S = \frac{1}{r+h}d_{ID} = \frac{1}{(r+h)(s+Q_{ID})}P$. (S is the signature on m of the user.)
- **CL-Verify:** Given $params$, m , pk_{ID} , and the signature S on m of the user with identity ID , the signature can be verified by the followings:
 1. calculate $h = H_2(m, pk_{ID})$;
 2. check if $e(S, pk_{ID} + hT) = g$.

3 Comments on Du-Wen Scheme

There is a flaw in the security proofs of Du-Wen scheme. In the proofs of **Lemma 1** and **Lemma 2**, when attacker \mathcal{A}_1 makes a **Signing Query** (ID_i, m_j) where $ID_i = ID_I$ is the target ID and m_j is not the target message m^* , simulator C cannot generate ID_i 's signature on m_j for \mathcal{A}_1 . It means that the security model is weaker than that of one-more forgery.

Moreover, a certificateless signature scheme should be as secure as a traditional digital signature scheme based on public key infrastructures (PKI). However, Du-Wen scheme is not as secure as PKI-based ones since it cannot achieve Girault's level-3 security [8]. Girault who proposed an aspect of the trust levels of an authority where he classifies the trust of an authority into three levels. Higher level means that users need less trust relied on their authority. Also, the truly non-repudiation can be achieved only when the authority can impersonate no user. There are three different trust levels for certificateless signatures as follows.

Level 1. KGC knows users' secrets and can impersonate any user without being detected.

Level 2. KGC does not know users' secrets but it still can impersonate a user by generating a false partial private key, which is different from the original one, without being detected.

Level 3. KGC does not know users' secrets and cannot impersonate any user by generating any false partial private key since the impersonation of any user can be detected.

To achieve Girault's level-3 security, a certificateless signature scheme should restrict that every user cannot produce any false partial private key which is different from the original one. It leads that only KGC can produce a false partial private key for impersonating the corresponding user. In this case, if KGC produces a false partial private key corresponding to the public key of a specific user and it is different from the original one, the user can sign a message by the original partial private key to show that her/his partial private key is legal.

According to the above definitions, we find that Du-Wen scheme cannot meet the requirement of Girault's level-3 security since the public key and private key, which includes the partial private key, of a user can be replaced without the help of KGC. Thus, KGC can produce a false partial private key and its corresponding public key such that the user cannot convince the others that the false one is not produced by her/him. A user with identity ID can replace its public key and the corresponding private key through the following steps. First, the user randomly selects a new secret value r' and sets its private key as (d_{ID}, r') . The user then computes the corresponding public key $pk'_{ID} = r'(P_{pub} + Q_{ID}P) = r'T$ to replace its original public key pk_{ID} . After generating the new public and private keys, the user can produce a signature $S' = \frac{1}{r'+h'}d_{ID} = \frac{1}{(r'+h')(s+Q_{ID})}P$ on m , where $h' = H_2(m, pk'_{ID})$. The signature can pass the verification due to $e(S', pk'_{ID} + h'T) = e(\frac{1}{r'+h'}d_{ID}, (r' + h')T) = e(P, P) = g$.

3.1 The Proposed Improved Scheme

In order to achieve Girault's level-3 security in Du-Wen scheme, we propose a modified version without increasing much computation cost. The details of the proposed scheme are shown as follows.

- **Setup:** Let k be the system security parameter. Then KGC selects two groups G_1 and G_2 of prime order $q \leq 2^k$, a bilinear mapping $e : G_1 \times G_1 \rightarrow$

G_2 , a generator P of group G_1 where $e(P, P) = g$. KGC also selects two distinct cryptographic hash functions $H_1 : \{0, 1\}^* \rightarrow Z_q^*$, $H_2 : \{0, 1\}^* \times G_1 \rightarrow Z_q^*$, and sets a random number $s \in Z_q^*$ as its master key, and then generates its public key $P_{pub} = sP$. KGC publishes the system parameters, $params = \{k, G_1, G_2, e, q, P, g, P_{pub}, H_1, H_2\}$, and keeps s secretly.

- **User-Key-Gen:** Assume that there exists a secure channel between every user and KGC. A user with identity ID randomly chooses $r \in Z_q^*$ and then computes $pk_{ID} = rP$ and $pk'_{ID} = r(P_{pub} + Q_{ID}P)$ where $Q_{ID} = H_1(ID)$. The user keeps r secretly and sets (pk_{ID}, pk'_{ID}) as its public key.
- **Partial-Private-Key-Gen:** KGC takes $params$, the user's partial public information (Q_{ID}, pk_{ID}) as inputs, and generates the user's partial private key $d_{ID} = \frac{1}{(s+Q_{ID}+H_1(pk_{ID}))}P$. Then KGC returns d_{ID} to the user. After receiving d_{ID} , the user checks the correctness of d_{ID} by the equation $e(d_{ID}, P_{pub}+Q_{ID}P+H_1(pk_{ID})P) = g$. The private key of the user is (r, d_{ID}) .
- **CL-Sign:** To produce the signature on message $m \in \{0, 1\}^*$, the user with identity ID performs the following steps:
 1. set $h = H_2(m, pk_{ID})$;
 2. compute $S = \frac{1}{r+h}d_{ID} (= \frac{1}{(r+h)(s+Q_{ID}+H_1(pk_{ID}))}P)$, where S is the signature on message m of the user.
- **CL-Verify:** Given $params$, message m , pk_{ID} , pk'_{ID} , and the signature S on message m of the user with identity ID , the signature can be verified as follows:
 1. let $h = H_2(m, pk_{ID})$;
 2. if the following formula holds, the signature S is valid.

$$e(S, pk'_{ID} + H(pk_{ID})pk_{ID} + h(P_{pub} + Q_{ID}P + H_1(pk_{ID})P)) = g$$

To clarify how the modified scheme can achieve Girault's level-3 security, we give a brief security analysis below. In the modified scheme, the public key of a user with identity ID consists of $pk_{ID} = rP$ and $pk'_{ID} = r(P_{pub} + Q_{ID}P)$. If the user would like to change pk_{ID} and pk'_{ID} to $pk_{ID} (= r'P)$ and $pk'_{ID} (= r'(P_{pub} + Q_{ID}P))$ with another secret r' , the signature produced with the new secret r' cannot meet the equation $e(S, pk'_{ID} + H(pk_{ID})pk_{ID} + hT') = g$, where $T' = P_{pub} + Q_{ID}P + H_1(pk_{ID})P$. The partial key $d_{ID} = \frac{1}{s+Q_{ID}+H_1(pk_{ID})}$ of the user is issued by KGC and the hashed value of pk_{ID} is embedded into the partial private key. Therefore, if the user changes its public key by itself, she/he cannot produce the corresponding partial private key $\tilde{d}_{ID} = \frac{1}{s+Q_{ID}+H_1(pk_{ID})}$. Hence, the proposed scheme is with Girault's level-3 security, i.e., KGC cannot produce a contradictory public key of the user since only KGC has the ability to certify the public key of the user.

Compared with the original scheme, the additional computations are only two point multiplications in the improved scheme.

4 Conclusions

In this paper, we have shown that the security proof of Du-Wen scheme does not cover one-more forgery. Inadequate proofs cannot convince the people of the security of the scheme. Therefore, strict security proofs will be required in Du-Wen scheme. Moreover, the scheme is also insufficient for Girault's level-3 security. Certificateless signatures with Girault's level-3 security are urgently desired since the improved generic model proposed by [11] has already included the security property. Therefore, we have also proposed an improved Du-Wen scheme to achieve Girault's level-3 security and remove the security flaw in Du-Wen scheme. We take the advantage of the short signature scheme [4], which was proposed by Boneh and Boyen, to design our certificateless short signature scheme. In our future work, we will finish the security proof for the proposed scheme based on that of [4].

References

1. S. Al-Riyami and K.G. Paterson, Certificateless Public Key Cryptography, In Proceedings of ASIACRYPT 2003, LNCS 2894, pp. 452-473, Springer-Verlag, 2003.
2. M.H. Au, J. Chen, J.K. Liu, Y. Mu, D.S. Wong and G. Yang, Malicious KGC Attacks in Certificateless Cryptography, In Proceedings of ASIACCS'07, ACM, pp.302-311, 2007.
3. I. Blake, G. Seroussi and N. Smart, Advances in Elliptic Curve Cryptography, London Mathematical Society Lecture Notes Series, Cambridge University Press, 2005.
4. D. Boneh and X. Boyen, Short Signatures Without Random Oracles and the SDH Assumption in Bilinear Groups, *Journal of Cryptology*, Vol.21, No.2, pp.149-177, Springer-Verlag, 2008.
5. X. Cao, K.G. Paterson and W. Kou, An Attack on a Certificateless signature scheme, Cryptology ePrint Archive: Report 2006/367.
6. K.Y. Choi, J.H. Park, J.Y. Hwang and D.H. Lee, Efficient Certificateless Signature Schemes, In Proceedings of ACNS'07, LNCS 4521, pp.443-458, Springer-Verlag, 2007.
7. H. Du and Q. Wen, Efficient and Provably-Secure Certificateless Short Signature Scheme from Bilinear pairings, *Computer Standards & Interfaces*, Vol.31, pp.390-394, 2009.
8. M. Girault, Self-certified Public Keys. In Proceedings of the EUROCRYPTO'91, LNCS 547, pp.490-497, Springer-Verlag, 1991.
9. M.C. Gorantla and A. Saxena, An Efficient Certificateless Signature Scheme, In Proceeding of CIS'05, LNAI, LNCS 3802, pp.110-116, Spring-Verlag, 2005.
10. B.C. Hu, D.S. Wong, Z.Zhang and X.Deng, Key Replacement Attack against a Generic Construction of Certificateless Signature, In Proceedings of ACISP'06, LNCS 4058, pp.235-246, Springer-Verlag, 2006.
11. B.C. Hu, D.S. Wong, Z.Zhang and X.Deng, Certificateless Signature: A New Security Model and an Improved Generic Construction, *Designs, Codes and Cryptography*, Vol.42, No.2, pp.109-126, Springer-Verlag, 2007.
12. X. Huang, W. Susilo, Y. Mu and F. Zhang, On the Security of Certificateless Signature Schemes from Asiacrypt 2003, In Proceedings of CANS'05, LNCS 3810, pp.13-25, Springer-Verlag, 2005.

13. X.Huang, Y.Mu, W. Susilo, D.S. Wong and W. Wu, Certificateless Signature Revisited, In Proceedings of ACISP'07, LNCS 4586, pp.308-322, 2007.
14. X. Li, K. Chen and L. Sun, Certificateless Signature and Proxy Signature Schemes from Bilinear Pairings, *Lithuanian Mathematical Journal*, Vol.45, No.1, pp.76-83, 2005.
15. A. Shamir, Identity-based Cryptosystems and Signature Schemes, In Proceedings of CRYPTO 1984, LNCS 196, pp.47-53, Springer-Verlag, 1985.
16. W.S. Yap, S.H. Heng and B.M. Goi, An Efficient Certificateless Signature Scheme, Emerging Directions in Embedded and Ubiquitous Computing, In Proceedings of EUC Workshops 2006, LNCS 4097, pp.322-331, Springer-Verlag, 2006.
17. D.H. Yum, P.J. Lee, Generic Construction of Certificateless Signature, In Proceedings of ACISP'04, LNCS 3108, pp.200-211, Springer-Verlag, 2004.
18. Z. Zhang and D. Feng, Key Replacement Attack on a Certificateless Signature Scheme, Cryptology ePrint Archive: Report 2006/453.
19. Z. Zhang, D. Wong, J. Xu and D. Feng, Certificateless Public-Key Signature: Security Model and Efficient Construction, In Proceedings of ACNS'06, LNCS 3989, pp.293-308, Springer-Verlag, 2006.