Certificateless Group Oriented Signature Secure Against Key Replacement Attack

Chunbo Ma and Jun Ao
School of Information and Communication,
Guilin University of Electronic Technology, Guilin, Guangxi, 541004, P. R. China
machunbo@guet.edu.cn

Abstract. Since Al-Riyami and Paterson presented certificateless cryptography, many certificateless schemes have been proposed for different purposes. In this paper, we present a certificateless group oriented signature scheme based on bilinear pairing. In our scheme, only the members in the same group with the signer can independently verify the signature. We prove the signature scheme is *existential unforgeability* under adaptive chosen message attack in random oracle model.

Keywords. Certificateless, group, signature, identity, random oracle model

1. Introduction

Digital signature is a fundamental cryptographic tool for providing authenticity in communications. To ensure the relationship between a public key and the identity of the holder of the corresponding private key, a certificate signed by CA (Certification Authority) is employed in traditional public key system. However, certification distribution induces additional overload and some potential security issues. For example, some attackers maybe take CA as their target, and if possible they try to forge a valid certification on behalf of their benefit.

Currently, the deployment and management of infrastructures to support the authenticity of cryptographic keys are more important than choosing appropriately secure algorithms or implementing those algorithms in developing secure systems based on public key cryptography. Motivated by this consideration, some public key mechanisms have been deployed. The ID-based public key system [3] is considered as a good alternative for certificate-based public key setting. Its most advantage is that the public key of user is bound with his identity, and this means the certification signed for public key is unnecessary. However, key escrow [4][5] is the inherent drawback in identity-based signature mechanism. In such a scheme, the KGC should always be unconditional trusted, and the KGC has ability to impersonate any single entity since every user's private key is known to the KGC. In many scenarios, such scheme is dangerous and unacceptable.

In order to resolve the escrow problem in Identity-based signature, Al-Riyami and Paterson presented another very different approach called Certificateless Public Key Cryptography (CLPKC) to address the authenticity problem in public key cryptography. The public key used in their mechanism is no longer an arbitrary string. Rather, it is similar to the public key generated in traditional public key system. It is sometimes said that the CLPKC lies in between PKC and IBC, since CLPKC doesn't need certificate to authenticate the public key, and the public key is no longer directly draw from the identity of user.

However, many proposed certificateless public key mechanisms [6][7][8]are vulnerable to replace public key attack. For example, attacker can modify the public key $< X_A, Y_A >=< x_A P, x_A P_{pub} >$ used in Al-Riyami and Paterson's scheme into $< x_A tP, x_A tP_{pub} >$. Obviously, it satisfies the equality $e(X_A, P_{pub}) = e(Y_A, P)$. Then the attacker can produce a signature via an old valid one.

Certificateless signatures have been designed for many purposes [2][19][20]. In this paper, we consider following scenarios. The sender will sign a same message for each member in a specified group, in which each person has his own private/public key pair. An inefficient approach for the sender is that he produces and sends a signature to each person one by one. His alternative approach is to produce a signature for the group and make each member in the specified group to verify the signature independently. Consider the drawback of [1][2], we propose a certificateless group oriented signature scheme based on bilinear pairing for the sender. The public key in our scheme withstands replace public key attack which we have mentioned above. Finally, we prove our signature scheme secure against forgering attack under the assumption that Y-DH problem is intractable.

The rest of the paper is organized as follows. In section2, we introduce some related works. In section3, we give the security model and complexity assumptions. Our signature scheme is presented in section4. The security analysis is given in section5. Finally, we draw the conclusions in section6.

2. Related works

ID-based public key cryptography, first proposed by Shamir [9], tackles the problem of authenticity of keys in a different way to traditional PKI. In ID-PKC, an entity's public key is derived directly from certain aspects of its

identity. Boneh and Franklin [3] presented an alternative ID-PKC from bilinear pairing. Since their scheme is based on elliptic curve, the public key size is shorter than traditional schemes. Subsequently, a mount of ID-based schemes from bilinear pairing have been proposed [12][13][14].However, key escrow is an inherent disadvantage of ID-PKC.

Sattam Al-Riyami and Paterson proposed a certificateless public key cryptography [1] relying on the use of a trusted third party who is in possession of a master key but doesn't suffer from the key escrow property. It can be used to verify the PK before signing a message. Since its first appearance of CLPKC, many researchers made in-depth study on this kind of mechanism and presented lots of schemes [10][15][16].

Yum and Lee [10] presented a generic construction of CLPKC in 2004. From their point of view, one can obtain a CLPKC scheme by combining any IBE and normal public key encryption scheme in proper method.

Despite of the usefulness of CLPKC scheme, it is not easy to design a secure one since the public key authenticated without certificate should withstands forgers attack. One type of such attack is that a forger is allowed to replace public keys of users. Although there are many schemes have been proposed, only few schemes [11] are secure against such attack.

Huang et al. [11] pointed out the drawback of [1] and presented an improved scheme. They show that the scheme [1] does not satisfy the security requirement of certificateless cryptography in the defined adversarial model. And then they show that an attacker allowed to replace the public key can always successfully forge a signature. Furthermore, they provided an improved scheme that withstood replace public key attack. The main idea is to found a way to check whether x_i in X_i and Y_i is identical to that x_i in S_i.

Hwang presented a group-oriented encryption scheme in paper [22]. In this paper, recipient can verify whether he can decrypt the ciphertext correctly or not. The decryption is based on (t,n) threshold, so with the cooperation of at least t members, one can decrypt the ciphertext. There are some other threshold-based group-oriented crypto schemes, such as [23][24[25].

3. Preliminaries

3.1 Bilinear Pairings

Let G_1 be a cyclic multiplicative group generated by g, whose order is a prime q and G_2 be a cyclic multiplicative group of the same order q. Assume that the discrete logarithm in both G_1 and G_2 is intractable. A bilinear pairing is a map $e: G_1 \times G_1 \to G_2$ and satisfies the following properties:

1. *Bilinear:* $e(g^a, p^b) = e(g,p)^{ab}$. For all g, $p \in G_1$ and $a,b \in \mathbb{Z}_q$, the equation holds.
2. *Non-degenerate:* There exists $p \in G_1$, if $e(g,p) = 1$, then $g = O$.
3. *Computable:* For g, $p \in G_1$, there is an efficient algorithm to compute $e(g,p)$.
4. *commutativity:* $e(g^a, p^b) = e(g^b, p^a)$. For all g, $p \in G_1$ and $a,b \in \mathbb{Z}_q$, the equation holds.

Typically, the map e will be derived from either the Weil or Tate pairing on an elliptic curve over a finite field. Pairings and other parameters should be selected in proactive for efficiency and security.

3.2 Complexity Assumptions

Computational Diffie-Hellman Assumption: Given g^a and g^b for some $a,b \in \mathbb{Z}_q^*$, compute $g^{ab} \in G_1$. A (τ,ε)-CDH attacker in G_1 is a probabilistic machine Ω running in time τ such that

$$Succ_{G_1}^{cdh}(\Omega) = \Pr[\Omega(g, g^a, g^b) = g^{ab}] \geq \varepsilon$$

where the probability is taken over the random values a and b. The CDH problem is (τ,ε)-intractable if there is no (τ,ε)-attacker in G_1. The CDH assumption states that it is the case for all polynomial τ and any non-negligible ε.

k-Strong Diffie-Hellman (k-SDH) Assumption[21]: Given $\{g, g^x, g^{x^2}, \cdots, g^{x^k}\}$ for a random number $x \in Z_q^*$, the attacker adaptively chooses random $c \in Z_q^*$ and computes $g^{(c+x)^{-1}}$. A (τ,ε)-k-SDH attacker in G_1 is a probabilistic machine Ω running in time τ such that

$Succ_{G_1}^{k-sdh}(\Omega) = \Pr[\Omega(g, g^x, g^{x^2}, \cdots, g^{x^k}, c) = g^{(c+x)^{-1}}] \geq \varepsilon$.

We say the k-SDH problem is (τ,ε)-intractable if there is no (τ,ε)-attacker in G_1.

k-Exponent (k-E) assumption[21]: Given $\{g, g^x, g^{x^2}, \cdots, g^{x^k}\}$ for a random number $x \in Z_q^*$, compute $g^{x^{k+1}}$. A (τ, ε)-k-SDH attacker in G_1 is a probabilistic machine Ω running in time τ such that

$$Succ_{G_1}^{k-E}(\Omega) = \Pr[\Omega(g, g^x, g^{x^2}, \cdots, g^{x^k}) = g^{x^{k+1}}] \geq \varepsilon$$

We say the **k-E** problem is (τ, ε)-intractable if there is no (τ, ε)-attacker in G_1.

Y-Diffie-Hellman Assumption: Given $\{g, g^x, g^{x^2}, \cdots, g^{x^k}\}$ for a random number $x \in Z_q^*$, the attacker adaptively chooses random $c \in Z_q^*$ and computes $g^{(x^2+x\cdot c))^{-1}}$. (τ, ε)-Y-DH attacker in G_1 is a probabilistic machine Ω running in time τ such that

$$Succ_{G_1}^{YDH}(\Omega) = \Pr[\Omega(g, g^x, g^{x^2}, \cdots, g^{x^k}, c) = g^{(x^2+x\cdot c)^{-1}}] \geq \varepsilon$$

We say the Y-DH problem is (τ, ε)-intractable if there is no (τ, ε)-attacker in G_1.

3.3 Security Notions

The proposed signature scheme consists of four algorithms, i.e. **Setup**, **KeyExtract**, **Sign** and **Verification**. The description of each algorithm is as follows.

- **Setup(1^k)**. It is a probabilistic algorithm. On input the security parameter, outputs system parameters.
- **KeyExtract**. It is a deterministic algorithm that accepts as input a user identity and system parameters to produce the user's public and private keys.
- **Sign**. It is a probabilistic algorithm. On input a message m, the user's private key and the system parameters, outputs a signature σ.
- **Verification**. It is a deterministic algorithm that accepts a message m, a signature σ, the system parameters, the public key and the user's identity ID to output TRUE if the signature is valid, otherwise output $\perp$.

The accepted definition of security for signature schemes is *existential unforgeability* under adaptive chosen message attack, which is described in [17][18]. We say that a signature scheme is secure against an existential forgery under adaptive chosen messages attack if no polynomial bounded adversary has a non-negligible advantage in the following game:

1. **Setup:** the *Challenger* runs the **Setup** algorithm and gives the system parameters to the *Attacker*.
2. **Attack phase:** the *Attacker* performs a polynomial bounded number of requests as follows.
   a) **H** queries. *Attacker* is allowed to request at most q_0 hash queries in form $(m_i \| r_i)$. *Challenger* responds with matching answer V_i.
   b) **Sign** queries. When *Attacker* requests a signature of a designated member in the specified group on a message m_i, the *Challenger* responds a valid signature $\sigma_i = (m_i, V_i, U_i)$ by running **Sign** algorithm. The *Attacker* is allowed to query at most q_{d_s} **sign** queries.
3. **Forge phase:** the *Attacker* gives a new signature (m, U, V) of the designated member, where the message m was never been asked to **sign** oracle in the **Attack phase**, and wins the game if the algorithm **Verification** doesn't output $\perp$.

We define the advantage of the *Attacker* to be Adv(*Attack*)=Pr[*Attack* WIN]. We say that the signature is secure if no polynomial bounded *Attacker* has non-negligible advantage in the game described above.

4. Our Scheme

In this section, we will describe our certificateless group oriented signature in detail. Without loss of generality, we assume that $Alice \in GROUP$ be the signer who wants to sign a message and sends it to each other member in the GROUP by broadcast over the internet. Let G_1 and G_2 be two groups that support a bilinear map as defined in section 3.1. Our signature scheme is consisted of four algorithms i.e. **Setup**, **KeyExtract**, **Sign**, and **Verification**.

- **Setup**. We assume that there exists a Key Generating Center (**KGC**), who performs **Setup** algorithm to initialize the system. **KGC** chooses a random number $k \in \mathbb{Z}_q^*$, and computes $< P_{pub\_1}, P_{pub\_2} >=< g^{k^2}, g^{k^3} >$ as a system parameter. There exist two cryptographic one-way functions $H_0 : \{0,1\}^* \to \mathbb{Z}_q^*$ and $H_1 : \{0,1\}^* \to \mathbb{Z}_q^*$.

- **KeyExtract**. The **KeyExtract** can be described as follows.

  Step1. KGC produces a partial private key $SK_{partial\_A} = g^{(k+H_1(ID_A))^{-1}k^{-1}}$ and sends to Alice in a secure way.

  Step2. After receiving the message, Alice chooses a random number $x_A \in \mathbb{Z}_q^*$ and extracts her private key $SK_A = SK_{partial\_A}^{x_A}$.

  Step3. Alice produces and publishes her public key $< X_A, Y_A >=< P_{pub\_1}^{x_A^{-1}}, P_{pub\_2}^{x_A^{-1}} >$.

- **Sign**. Subsequently, we will give the **Sign** algorithm. To sign a message m, Alice performs the following steps.

  Step1. Choose a random number $a \in \mathbb{Z}_q^*$, compute $r = e(SK_A, (X_A)^{H_1(ID_A)} \cdot Y_A)^a$, and then compute $V = H_0(m \| r)$, where "||" denotes concatenation.

  Step2. Compute $U = SK_A^{(a+V)}$, and the signature is $\sigma = (m, V, U)$.

The signature σ will be send to each other member in the GROUP by broadcast over the Internet.

- **Verification**. Finally, we describe the **Verification** algorithm. Without loss of generality, we assume that the recipient Bob who is in the GROUP performs the following steps to verify the validity of the signature.

  Setp1. Compute $r' = e(U, X_A^{H_1(ID_A)} \cdot Y_A) e(SK_B, X_B^{H_1(ID_B)} \cdot Y_B)^{-V}$

  Step2. Check the equality $V = H_0(m \| r')$. If it is true, the signature is valid. Otherwise, reject the signature.

5. Security of the proposed signature scheme

In this section, we prove that the above signature scheme is unforgeable. The completeness is guaranteed by the correctness of the verification process.

Assume that Alice, Bob and Carol belong to the GROUP. Then let's consider such a scenario: Alice wants to show Bob a signature that Carol once sent her and convince Bob that it is Alice's signature. Since Alice sends the signature to Bob, Bob must know Alice's identity. If the signature is not produced by Alice but Carol, and Bob can't detect Alice's fraud, it means

$$r' = r''$$
$$e(U, X_A^{H_1(ID_A)} \cdot Y_A) e(SK_B, X_B^{H_1(ID_B)} \cdot Y_B)^{-V} = e(U, X_C^{H_1(ID_C)} \cdot Y_C) e(SK_B, X_B^{H_1(ID_B)} \cdot Y_B)^{-V}.$$

Then we have $g^{x_A^{-1}k^2(k+H_1(ID_A))} = g^{x_C^{-1}k^2(k+H_1(ID_C))}$. Since $x_A, x_C \in \mathbb{Z}_q^*$ are two random numbers, and H_1 is a cryptographic one-way function, then the probability of equality hold is negligible.

The following theorem claims the security of the scheme in the random oracle model under the Y-DH assumption, which we have described in section3.2.

Theorem. *If there exists an attacker Alice, who is allowed to request at most* q_0 *Hash queries and* q_{d_s} *signature queries, can break the proposed signature scheme with probability* ε *and within a time bound* t, *assume that* $\varepsilon \geq 10(q_{d_s}+1)(q_{d_s}+q_0)/2^k$, *then there exists another attacker Bob, who can solve* ***Y-DH*** *problem by recalling Alice as a subroutine in expected time* $t' \leq 120686 q_0 t / \varepsilon$.

Proof. Assume that if the attacker Alice has ability to break the proposed signature scheme with non-negligible probability ε, then we will show how Bob can solve **Y-DH** problem. In other words, given $g^k, g^{k^2}, g^{k^3} \in G_1$ and $x_c \in \mathbb{Z}_q^*$, Bob can compute $g^{(k^2+k\cdot x_c)^{-1}}$ with non-negligible probability by running Alice as a subroutine.

We assume that Alice wants to forge Carol's signature, where Carol belongs to the specified GROUP. The challenger Bob will simulate Carol and interacts with Alice by $\mathbf{H_0}$ and **Sign** oracles. Since H_1 is only used to transform user's identity information, we don't take it into consideration.

- **Setup phase**

Bob publishes $g^{k^2}, g^{k^3} \in G_1$ as the system parameter and $< X_C, Y_C >=< P_{pub\_1}^{x_C^{-1}}, P_{pub\_2}^{x_C^{-1}} >$ as Carol's public key.

- **Queries phase**

H hash queries. In this phase, attacker Alice is allowed to request at most q_0 hash queries. Bob maintains an empty Δ-list. For each query $(m_i \| r_i)$, Bob first checks the list:

1). If there is an item $(m_i \| r_i \| V_i)$ in Δ list, then Bob return V_i to Alice.

2). If there is no such record in Δ list, Bob chooses a random $V_i \in \mathbb{Z}_q^*$, and returns it to Alice. And then preserves $(m_i \| r_i \| V_i)$ in Δ-list.

Signature queries. In this phase, Alice is allowed to query at most q_{d_s} signature queries. For each query on m_i, Bob performs following step to return an answer.

1). Choose random numbers $\alpha_i, V_i \in \mathbb{Z}_q^*$, and then sets $g^{a_i} = g^{\alpha_i k^2 x_C^{-1}(k+H_1(ID_C))-V_i}$ and $r_i = e(g^{a_i}, g^k)$.

2). If m_i never been asked before, then Bob preserves $(m_i \| r_i \| V_i)$ in Δ-list.

3). If m_i has been asked before, it means that there is an item $(m_i \| r_i \| V_i)$ in Δ-list. Bob performs above step 1), makes sure that r_j and V_j are fresh, and then preserves $(m_i \| r_j \| V_j)$ in Δ-list.

4). Compute $U_i = g^{\alpha_i k}$, and then Bob returns (m_i, U_i, V_i) to Alice as the answer.

Actually, we have

$$U_i = g^{(a_i+V_i)x_C(k+H_1(ID_A))^{-1}k^{-1}}$$
$$= g^{(\alpha_i k^2 x_C^{-1}(k+H_1(ID_C))-V_i+V_i)x_C(k+H_1(ID_C))^{-1}k^{-1}}$$
$$= g^{\alpha_i k}$$

The simulation is perfect in the random oracle. After all the queries, Alice outputs a fresh signature $\sigma_0 = (m^*, U_j, V_j)$, where warrant m^* has never been queried to the **Sign** oracle. According to the forking lemma [20][21], if $\varepsilon \geq 10(q_{d_s}+1)(q_{d_s}+q_0)/2^k$, then Bob has ability to produce two valid signatures $\sigma = (m^*, U_j, V_j)$ and $\sigma_0^{'} = (m^*, U_j^{'}, V_j^{'})$ on the same warrant m^* such that $H(m^* \| r_j) \neq H^{'}(m^* \| r_j)$. Thus means, Bob can compute $g^{(k^2+k\cdot H_1(ID_C))^{-1}}$ as follows

$$g^{(k^2+k\cdot H_1(ID_C))^{-1}} = (U_j / U_j^{'})^{(V_j - V_j^{'})^{-1} x_c^{-1}}$$

Since we have

$$(U_j / U_j^{'}) = g^{(V_j - V_j^{'})x_c(k^2+k\cdot H_1(ID_C))^{-1}}$$
$$= g^{(k^2+k\cdot H_1(ID_C))^{-1}}$$

According to the forking lemma, Bob can solve the **Y-DH** problem in expected time $t^{'} \leq 120686 q_0 t / \varepsilon$.

□

6. Conclusions

Since Riyami and Paterson presented their Certificatless cryptography, many certificateless signature schemes have been proposed. However, most of these schemes are vulnerable to replace public key attack. Then, how to overcome this defect becomes an interesting issue. We design a certificateless group oriented signature scheme in this paper, and prove its *existential unforgeability* under adaptive chosen message attack in random oracle model.

References

1. S. A. Riyami, and K. Paterson. Certificateless public key cryptography. In Proceedings of Asiacrypt'03, LNCS 2894, pp. 452-473, 2003.
2. C. Ma, F. Ao, D. He. Certificateless Group inside Signature. Proceedings of ISADS'05 (7th International Symposium on Autonomous Decentralized Systems, Chengdu. P. R. China), pagers: 194-200.
3. D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. In Proceedings of Crypto'01, LNCS 2139, pp. 213-229.
4. F. Hess. Efficient identity based signature scheme based on pairings. Selected Areas in Cryptography SAC 2002, LNCS 2595, pp. 310-324, 2003.
5. X. Li, K. Chen, and L. Sun. Certificatelss signature and proxy signature schemes from bilinear pairings. Lithuanian Mathematical Journal. Vol. 45, No. 1, pp. 95-103, 2005.
6. B. C. Hu, D. S. Wong, Z. Zhang, and X. Deng. Key Replacement Attack Against a Generic Construction of Certificateless Signature. ACISP 2006, LNCS 4058, pp. 235-246, Springer-Verlag, 2006.

7. D. H. Yum and P. J. Lee. Generic Constructin of Certificateless Signature. ACISP 2004, LNCS 3108, pp. 200-211, Springer-Verlag, 2004.
8. M. C. Gorantla and A. Saxena, An Efficient Certificateless Signature Scheme, CIS 2005, LNAI 3802, pp. 110-116, Springer-Verlag, 2005.
9. A. Shamir. Identity-based cryptosystems and signature schemes. In Advances in Cryptology-Crypto'84, LNCS 196, pp. 47-53, 1984.
10. D. Yum and P. Lee. Generic construction of Certificateless encryption. In Proceedings of ICCSA'04, LNCS 3043, pp. 802-811, 2004.
11. X. Huang, W. Susilo, Y. Mu, and F. Zhang. On the secuirty of certificateless signature schemes form asiacrypt 2003. In Proceedings of CANS 2005, LNCS 3810, pp. 13-25, 2005.
12. J. Cha, J. H. Cheon. An identity-based signature from gap Diffie-Hellman group. In Proceedings of PKC 2003, LNCS 2567:18-30, 2003.
13. C. Gentry, A. Siverberg. Hierarchical ID-based cryptography. In Advances in Cryptology-Asiacrypt 2002, LNCS 2501: 548-566, 2002.
14. K. G. Paterson. ID-based signatures from pairings on elliptic curves. Electron. Lett., 38(18): 1025-1026, 2002.
15. M. C. Gorantla, A. Saxena. An efficient cerfificateless signature scheme. In Proceedings of CIS'05, LNAI, Vol. 3802: 110-116.
16. K. Y. Choi, J. H. Park, J. Y. Hwang, and D. H. Lee. Efficient certificateless signature schemes. In Proceedings of ACNS 2007, LNCS 4521, pp. 443-458, 2007.
17. D. Proincheval and J. Stern. Security aguments for digital signatures and blind signatures[A]. J. of Cryptology, 2000, 13(3):361-396.
18. E. Brickell, D. Pointcheval, S. Vaudenay, M. Yung. Design validations for discrete logarithm based signature schemes. In PKC'2000, Lecture Notes in Computer Science, Vol. 1751. Springer-Verlag (2000) 276-292.
19. M. Barbosa and P. Farshim. Certificateless signcryption. In Proceedings of ASIACCS'08, 369-372.
20. L. Zhang, F. Zhang, and W. Wu. A provably secure ring signature scheme in certificateless cryptography. Lecture Notes in Computer Science. 4784: 103-121.
21. F. Zhang, R. Safavi-Naini, W. Susilo. An Efficient Signature Scheme from Bilinear Pairings and Its Applications. Practice and Theory in Public Key Cryptography-PKC 2004, Lecture Notes in Computer Science 2947, 277-290, Springer-Verlag, 2004.
22. Hwang. Cryptosystem for group oriented cryptography. In Advanced in Cryptology-eurocrypto'91 Lecture Notes in Computer Science 2045: 352-360.
23. S. Saeednia and H. Ghodosi. A self-certified group-oriented cryptosystem without a combiner. In Proceedings of ACISP'99. Lecture Notes in Computer Science 1578:192-201.
24. H. Ghodosi and S. Saeednia. Modification to self-certified group-oriented cryptosystem without combiner. Electronics Letters, 37(2):86-87.
25. C. C. Chang, H. C. Lee. A new generalized group oriented cryptoscheme without trusted center. Selected areas in communications. IEEE Journal on, 11(5):725-729.