ChinaRxiv

AI translation · View original & related papers at
chinarxiv.org/items/chinaxiv-201805.00370

Provably Secure Pairing-Free Certificateless Signcryption Scheme Postprint

Authors: Chen Hong, Zhao Yue, Xiao Chenglong, Xiao Zhenjiu, Song Hao

Date: 2018-05-18T00:00:00+00:00

Abstract

Certificateless signcryption inherits the characteristic of identity-based signcryption that eliminates the need for public key certificates, while improving upon its key escrow problem, thereby offering certain advantages. To address the shortcomings of existing certificateless signcryption schemes, such as low computational efficiency and inadequate security, we propose a novel class of pairing-free certificateless signcryption schemes based on a secure signature scheme. The construction employs a methodology that binds hash functions to user identities and combines public keys with private keys to generate new keys. In the random oracle model, the confidentiality and unforgeability of the proposed scheme are proven based on the computational intractability of the elliptic curve discrete logarithm problem. Compared with previous schemes, our scheme achieves higher efficiency by eliminating the use of bilinear pairings and exponentiation operations while maintaining security.

Full Text

Preamble

Title: Certificateless Signcryption Scheme of Verifiable Security without Pairing

Authors: Chen Hong, Zhao Yue, Xiao Chenlong, Xiao Zhenjiu, Song Hao
Affiliation: College of Software, Liaoning Technical University, Huludao, Liaoning 125105, China

Abstract: The certificateless signcryption scheme inherits the certificate-free property of identity-based signcryption schemes while improving upon their key escrow problem, offering certain advantages. Aiming at the shortcomings of existing certificateless signcryption schemes such as low computational efficiency and poor security, this paper proposes a new certificateless signcryption scheme without pairings based on a secure signature scheme. The construction employs

a method that binds hash functions with user identities and combines public and private keys to generate new keys. Under the random oracle model, the scheme' s confidentiality and unforgeability are proven based on the computational difficulty of the elliptic curve discrete logarithm problem. Compared with previous schemes, this scheme achieves higher efficiency without using bilinear pairings or exponentiation operations while ensuring security.

Keywords: certificateless signcryption; confidentiality; unforgeability; random oracle model

Funding: National Natural Science Foundation of China Youth Project (61404069)

Author Biographies:
Chen Hong (1967–), female, from Fuxin, Liaoning, associate professor, master' s degree, research focus: network security (chh3188@163.com);
Zhao Yue (1992–), female, master' s student, research focus: network security;
Xiao Chenlong (1984–), male, associate professor, Ph.D., research focus: high-level synthesis;
Xiao Zhenjiu (1968–), male, associate professor, Ph.D., research focus: network and information security;
Song Hao (1996–), female, undergraduate, research focus: network security.

0 Introduction

Confidentiality and authentication are two fundamental metrics in cryptography for evaluating information security. Traditional approaches achieve these by first digitally signing messages and then encrypting them, but this incurs computational costs equal to the sum of both operations, resulting in low efficiency. To address this limitation, Zheng[**?**] introduced the concept of signcryption in 1997, which simultaneously provides both signature and encryption functionality in a single logical step with significantly lower computational and communication overhead than traditional methods. Since its inception, signcryption has become a widely studied research topic.

As the technology evolved, PKI-based signcryption schemes emerged, where public key certificates mitigated "public key replacement" attacks by enabling verification of public key legitimacy. However, the complexity of certificate issuance, validation, and management, coupled with substantial computational overhead, hindered their practical adoption. Subsequently, identity-based signcryption schemes were proposed, which eliminated public key certificates and avoided certificate management difficulties. Yet this introduced a critical key escrow problem: the Private Key Generator (PKG) could generate any user' s private key, enabling undetectable forgery of signatures and decryption of messages, posing serious security risks.

To resolve these issues, researchers combined certificateless cryptography with

signcryption to create the Certificateless Signcryption (CL-SC) paradigm, which simultaneously eliminates the certificate management burden of PKI-based schemes and the key escrow vulnerability of identity-based approaches. The first CL-SC scheme was proposed in 2008[**?**], but was later found vulnerable to extended unforgeability attacks. Subsequent proposals included bilinear pairing operations, which are computationally expensive. Selvi et al.[**?**] introduced a pairing-free CL-SC scheme and proved its security, though it relied heavily on exponentiation operations, limiting efficiency. Later schemes by Zhu et al.[**?**] and Liu et al.[**?**] were also pairing-free but have since been proven insecure.

Building upon the efficient and secure signature scheme by Tang et al.[**?**], this paper constructs a novel pairing-free CL-SC scheme that combines the sender' s private key with the receiver' s public key to form the encryption key, and the sender' s public key with the receiver' s private key for decryption. We prove the scheme' s security under the random oracle model and demonstrate through comparative analysis that it offers superior performance relative to recent signcryption proposals.

1.1 Mathematical Hard Problems

Let the elliptic curve equation defined over $\mathbb{F}_p$ (where $\mathbb{F}_p$ denotes a finite field with p elements, p is a prime and $p > 3$) be $y^2 = x^3 + ax + b$, where $a, b \in \mathbb{F}_p$ and $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$. The set consisting of all solutions on the elliptic curve together with a point at infinity O is denoted by $E(\mathbb{F}_p)$, i.e., $E(\mathbb{F}_p) = \{(x, y)|x, y \in \mathbb{F}_p\} \cup \{O\}$, satisfying the equation $y^2 = x^3 + ax + b$. The number of points on the elliptic curve is denoted by $n = |E(\mathbb{F}_p)|$.

Elliptic Curve Discrete Logarithm Problem (ECDLP): Given an elliptic curve $E(\mathbb{F}_p)$, a point P of order q, $Q \in \langle P \rangle$, and $x \in [0, q-1]$ such that $Q = xP$, computing x is computationally infeasible.

2.1 Scheme Description

The proposed pairing-free CL-SC scheme involves three legitimate participants: the Key Generation Center (KGC), a sender ID_i, and a receiver ID_j. A CL-SC scheme typically consists of the following algorithms:

a) System Parameter Setup. The KGC runs the system initialization. This algorithm takes a security parameter k as input; the KGC selects a master key $s \in \mathbb{Z}_q^*$ and outputs system parameters params. The KGC keeps the master key secret and publishes params.

b) User Partial Key Generation. For a user with identity ID_i, the KGC randomly selects $r_i \in \mathbb{Z}_q^*$ and generates the user' s partial private key D_i and partial public key R_i as:

$$D_i = r_i + s \cdot H_1(ID_i, R_i)$$

$$R_i = r_i P$$

The KGC returns (D_i, R_i) to the user.

c) User Secret Value Generation. The user independently runs this algorithm, taking ID_i and params as input, and outputs a secret value $x_i \in \mathbb{Z}_q^*$ as the long-term private key, which remains confidential from the KGC.

d) User Private Key Generation. The user generates the complete private key:

$$SK_i = (x_i, D_i)$$

Thus, user A' s private key is $SK_A = (x_A, D_A)$, and user B' s private key is $SK_B = (x_B, D_B)$.

e) User Public Key Generation. The user computes $X_i = x_i P$ and generates the public key:

$$PK_i = (X_i, R_i)$$

Therefore, user A' s public key is $PK_A = (X_A, R_A)$, and user B' s public key is $PK_B = (X_B, R_B)$.

f) Signcryption. When sender A signcrypts a plaintext message m for receiver B, the following steps are executed:

1. User A randomly selects $t \in \mathbb{Z}_q^*$.
2. Compute $T = tP$.
3. Compute $h_1 = H_1(ID_B, R_B)$ and $h_2 = H_2(m, T, R_A, X_A)$.
4. Compute $u = t + x_A \cdot h_1 + D_A \cdot h_2$.
5. Compute $K_1 = x_A X_B$ and $K_2 = x_A(R_B + P_{pub} \cdot h_1)$.
6. Compute $V = H_3(K_1, K_2)$ and ciphertext $c = m \oplus V$.
7. User A sends the signcryption $\sigma = (c, u, T)$ to user B.

g) Unsigncryption. Upon receiving $\sigma = (c, u, T)$, user B performs the following steps:

1. Compute $h_1' = H_1(ID_A, R_A)$.
2. Compute $T' = uP - X_A \cdot h_1' - (R_A + P_{pub} \cdot h_1') \cdot h_2'$, where $h_2' = H_2(m, T, R_A, X_A)$.
3. Compute $V' = H_3(x_B T', x_B(R_A + P_{pub} \cdot h_1'))$.
4. Recover plaintext $m = c \oplus V'$.

The composition and communication model of the CL-SC scheme is illustrated in Figure 1 [Figure 1: see original paper].

2.2 Correctness Proof

The correctness analysis of the proposed scheme is as follows:

Since sender A encrypts the plaintext by computing $c = m \oplus V$ where $V = H_3(K_1, K_2)$, and receiver B decrypts the ciphertext by computing $m = c \oplus V'$, we must show that $V = V'$ to ensure the receiver obtains the correct plaintext.

The verification proceeds as follows:

$$T' = uP - X_A h_1' - (R_A + P_{pub} h_1') h_2'$$
$$= (t + x_A h_1 + D_A h_2)P - X_A h_1' - (R_A + P_{pub} h_1') h_2'$$
$$= tP + x_A h_1 P + D_A h_2 P - x_A h_1' P - (R_A + P_{pub} h_1') h_2'$$

Since $h_1' = h_1$ and $h_2' = h_2$, and noting that $D_A P = R_A + P_{pub} H_1(ID_A, R_A)$, we have:

$$T' = tP = T$$

Furthermore:

$$V' = H_3(x_B T', x_B(R_A + P_{pub} h_1'))$$
$$= H_3(x_B T, x_B(R_A + P_{pub} h_1))$$
$$= H_3(x_A X_B, x_A(R_B + P_{pub} h_1))$$
$$= H_3(K_1, K_2) = V$$

Thus, $V = V'$, ensuring that the receiver can correctly recover the plaintext and that the decrypted message passes verification.

3.1 Security Definitions

The fundamental conditions for determining the security of a signcryption scheme are that it must satisfy at least confidentiality (i.e., indistinguishability against adaptive chosen-ciphertext attacks, IND-CCA2) and unforgeability (i.e., existential unforgeability against chosen-message attacks, EUF-CMA). According to the discussion in literature[**?**], CL-SC schemes typically face two types of adversaries $\mathcal{A}_1$ and $\mathcal{A}_2$, and four simulation games (Game I, Game II, Game III, Game IV).

For the first type of adversary $\mathcal{A}_1$, the adversary cannot possess the master key generated by the KGC but has the ability to replace any user' s public key. For the second type of adversary $\mathcal{A}_2$, the adversary can obtain the master key generated by the KGC and thus can construct partial private keys for any legitimate user, but cannot replace user public keys.

Literature[**?**] provides detailed definitions of the four simulation games. This paper primarily uses the first type of adversary $\mathcal{A}_1$ as an example, presenting schematic diagrams under adaptive chosen-ciphertext attacks and chosen-message attacks, as shown in Figures 2 [Figure 2: see original paper] and 3 [Figure 3: see original paper].

3.2 Confidentiality Analysis

If an adversary wishes to obtain the plaintext from ciphertext σ, they must compute the encryption key V. To obtain V, the adversary must know user A' s private key. Even under attack by a Type II adversary $\mathcal{A}_2$, a malicious KGC only possesses the partial private key D_A. To derive the other part of the private key x_A from $X_A = x_A P$, the adversary faces the discrete logarithm problem and thus cannot obtain the encryption key or recover the ciphertext. On the other hand, since $V = H_3(K_1, K_2)$, if the adversary can compute $K_1 = x_A X_B$, they can also break the ciphertext. Similarly, to compute K_1, the adversary must compute B' s complete private key, again facing the discrete logarithm problem.

The detailed confidentiality proof is as follows:

Lemma 1 (Confidentiality under $\mathcal{A}_1$). In the random oracle model and under the assumption that ECDLP is hard, if there exists an adversary $\mathcal{A}_1$ that wins the IND-CCA2 game with advantage ε in polynomial time, then there exists a distinguisher $\mathcal{C}$ that solves the ECDLP problem with probability ε'.

Proof. To break the proposed CL-SC scheme, there must exist an algorithm $\mathcal{C}$ that uses $\mathcal{A}_1$ (Type I adversary) to solve the ECDLP problem, i.e., given (P, aP) to find a.

1. **Initialization:** $\mathcal{C}$ runs the system parameter setup algorithm, saves s, and sends params to $\mathcal{A}_1$.
2. **Query Phase:** $\mathcal{A}_1$ can make various queries:
   - H_1 **queries:** $\mathcal{C}$ maintains list L_1 with entries (ID_i, R_i, h_1). For each query, if exists, return h_1; otherwise, randomly select $h_1 \in \mathbb{Z}_q^*$ and return.
   - H_2 **queries:** $\mathcal{C}$ maintains list L_2 with entries $(ID_i, ID_j, m, T, R_i, X_i, h_2)$. Similar handling as H_1.
   - H_3 **queries:** $\mathcal{C}$ maintains list L_3 with entries (K_1, K_2, h_3). Similar handling.
   - **Partial private key queries:** For user ID_i, if $ID_i = ID_I$, $\mathcal{C}$ aborts; otherwise, query L_1 and return D_i.
   - **Public key queries:** $\mathcal{C}$ maintains list L_{PK}. For query on ID_i, first perform H_1 query, then return (X_i, R_i).
   - **Public key replacement:** Replace entries in L_{PK}.
   - **Private secret value queries:** Query L_{PK}; if public key was replaced, return $\perp$.
   - **Signcryption queries:** For query (ID_a, ID_b, m), if $ID_a \neq ID_I$ and public key not replaced, compute normally; otherwise, simulate using known values.
   - **Unsigncryption queries:** For query $\sigma = (c, u, T)$, if $ID_b \neq ID_I$, compute normally; otherwise, abort.
3. **Challenge Phase:** $\mathcal{A}_1$ selects two equal-length plaintexts m_0, m_1 and

challenge users (ID_I, ID_J). If $ID_I = ID_J$, abort. $\mathcal{C}$ randomly selects $b \in \{0,1\}$, computes challenge ciphertext σ^*, and returns to $\mathcal{A}_1$.

4. **Second Query Phase:** Similar to first phase, but cannot query partial private key of ID_I or unsigncryption of σ^*.
5. **Guess Phase:** $\mathcal{A}_1$ outputs guess b'. If $b' = b$, $\mathcal{C}$ wins.

If $\mathcal{A}_1$ did not query partial private key of ID_I and did not query private key of ID_J, the simulation is perfect. Assuming $\mathcal{A}_1$ makes at most q_{pp} partial private key queries and q_{H_1} H_1 queries, the probability that $\mathcal{C}$ solves ECDLP is:

$$\Pr[\mathcal{C} \text{ succeeds}] \geq \frac{\varepsilon}{q_{H_1}} \left(1 - \frac{q_{pp}}{q_{H_1}}\right)$$

Lemma 2 (Confidentiality under $\mathcal{A}_2$). Similar to Lemma 1, but for Type II adversary who knows master key s.

3.3 Unforgeability Analysis

Lemma 3 (Unforgeability against $\mathcal{A}_1$). In the random oracle model and under the assumption that ECDLP is hard, if there exists an adversary $\mathcal{A}_1$ that wins the EUF-CMA game with advantage ε in polynomial time, then there exists a distinguisher $\mathcal{C}$ that solves the ECDLP problem with probability ε'.

Proof. To break the scheme' s unforgeability, there must exist an algorithm $\mathcal{C}$ that uses $\mathcal{A}_1$ to solve ECDLP.

1. **Initialization:** $\mathcal{C}$ runs setup, sends params and master key s to $\mathcal{A}_1$ (simulating $\mathcal{A}_2$ environment).
2. **Query Phase:** Similar to Lemma 1, but no public key replacement allowed.
3. **Forgery Phase:** After polynomially bounded queries, $\mathcal{A}_1$ submits a forgery (ID_I, ID_J, σ^*) where σ^* is a valid signcryption on message m from ID_I to ID_J, with constraints that no partial private key query on ID_I was made and no signcryption query on this message was made.

Using the forking lemma[**?**], $\mathcal{C}$ can obtain two valid signcryptions and compute:

$$u_1 - u_2 = (h_2 - h_2')(x_I + D_I)$$

Thus solving for the discrete logarithm.

The success probability is:

$$\Pr[\mathcal{C} \text{ succeeds}] \geq \frac{\varepsilon}{q_{H_1}} \left(1 - \frac{q_{pp}}{q_{H_1}}\right)$$

Lemma 4 (Unforgeability against $\mathcal{A}_2$). Similar to Lemma 3, for Type II adversary.

4 Performance Analysis

The proposed CL-SC scheme requires no bilinear pairing or exponentiation operations. The signcryption phase uses 6 point multiplication operations: $T = tP$, $X_A h_1$, $D_A h_2$, $x_A X_B$, $x_A R_B$, $x_A P_{pub} h_1$. The unsigncryption phase uses 8 point multiplication operations: uP, $X_A h_1'$, $R_A h_2'$, $P_{pub} h_1' h_2'$, $x_B T'$, $x_B R_A$, $x_B P_{pub} h_1'$, and verification operations.

We compare our scheme with literature[11-14] in terms of computational efficiency, correctness, confidentiality, and non-repudiation. Let E, P, and M denote exponentiation, bilinear pairing, and point multiplication operations respectively. The comparison results are shown in Table 1 .

Table 1. Performance Comparison of Signcryption Schemes

Scheme	Signcryption	Unsigncryption	Correctness	Confidentiality	Non-repudiation
[11]	2E+6M	2P+2E+5M	√	√	√
[12]	2P+5M	2P+5M	√	√	√
[13]	1E+2M	6E+7M	√	×	×
[14]	6M	8M	√	√	√
Ours	6M	8M	√	√	√

As shown in Table 1, the schemes in [11] use bilinear pairings, exponentiation, and point multiplication; [12] uses bilinear pairings and point multiplication. According to Chen et al.[**?**], one bilinear pairing operation consumes computational resources equivalent to 21 point multiplication operations on elliptic curves. Therefore, our scheme is superior in computational efficiency to the above two schemes.

In terms of security, the scheme in [13] does not satisfy confidentiality and non-repudiation, and cannot resist public key replacement attacks by adversary $\mathcal{A}_1$. The scheme in [14] uses temporary secret values generated by KGC during signcryption, exposing it to master key leakage risks and making it unable to resist $\mathcal{A}_1$' s forgery attacks and $\mathcal{A}_2$' s public key replacement confidentiality attacks. Literature[16,17] detail attack methods against [14]. Therefore, our scheme is more secure than those in [13,14].

5 Conclusion

This paper constructs a pairing-free CL-SC scheme based on Tang et al.' s signature scheme and proves its security under the random oracle model. Performance comparisons with other schemes demonstrate its superior efficiency. CL-SC schemes with low computational overhead and high security have broad applications in electronic payments, wireless sensor devices, autonomous vehicles, etc. However, existing schemes still suffer from security weaknesses and

efficiency issues, making the construction of secure and efficient schemes a worthwhile research direction.

References

[1] Zheng Yuliang. Digital signcryption or how to achieve cost(signature&encryption) « cost(signature) + cost(encryption) [C]// Proc of the 17th Annual International Cryptology Conference on Advances in Cryptology. Berlin: Springer-Verlag, 1997: 165-179.

[2] Barbosa M, Farshim P. Certificateless signcryption [C]// Proc of ACM Symposium on Information, Computer and Communications Security. New York: ACM Press, 2008: 369-372.

[3] Selvi S S D, Vivek S S, Rangan C P. Cryptanalysis of certificateless signcryption schemes and an efficient construction without pairing [C]// Proc of the 5th International Conference on Information Security and Cryptology. Berlin: Springer-Verlag, 2010: 75-92.

[4] Zhu Hui, Li Hui, Wang Yumin. Certificateless signcryption scheme without bilinear pairing [J]. Computer Research and Development, 2010, 47(9): 1587-1594.

[5] Liu Wenhao, Xu Chunxiang. Certificateless signcryption scheme without bilinear pairing [J]. Journal of Software, 2011, 22(8): 1918-1926.

[6] Tang Yongli, Wang Feifei, Yan Xixi, et al. Efficient and provably secure certificateless signature scheme [J]. Computer Engineering, 2016, 42(3): 156-160.

[7] Liu Zhenhua, Hu Yupu, Zhang Xiangsong, et al. Certificateless signcryption scheme in the standard model [J]. Information Sciences, 2010, 180(1): 452-464.

[8] Shen Limin, Zhang Futai, Sun Yinxia. Security analysis of a certificateless signcryption scheme without bilinear pairing [J]. Journal of Cryptologic Research, 2014, 1(2): 146-154.

[9] Pointcheval D, Stern J. Security arguments for digital signatures and blind signature [J]. Journal of Cryptology, 2000, 13(3): 361-396.

[10] Zhou Yanwei, Yang Bo, Zhang Wenzheng. Security analysis and improvement of certificateless signcryption scheme without bilinear maps [J]. Chinese Journal of Computers, 2016, 39(6): 1257-1266.

[11] Deng Lunzhi, Li Siwei, Yu Yafeng. Efficient certificateless signcryption scheme [J]. Journal of Xiamen University: Natural Science, 2014, 53(6): 810-816.

[12] Tang Pengzhi, Zhang Qinglan, Yang Junfang. An improved certificateless signcryption scheme based on bilinear pairing [J]. Journal of Hefei University of Technology: Natural Science, 2016, 39(7): 917-923.

[13] Gao Jianxin, Wu Xiaoping, Qin Yanlin, et al. Certificateless secure signcryption scheme without bilinear pairing [J]. Computer Applications Research, 2014, 31(4): 1195-1198.

[14] Xia Ang, Zhang Longjun. A new certificateless secure signcryption scheme without bilinear pairing [J]. Computer Applications Research, 2014, 31(2): 532-535.

[15] Chen L, Cheng Z, Smart N P. Identity-based key agreement protocols from pairings [J]. International Journal of Information Security, 2007, 6(4): 213-241.

[16] Zou Changzhi. Provably secure certificateless signcryption scheme [J]. Computer Applications and Software, 2016, 33(3): 327-333.

[17] Fan Aiwan, Pan Zhongqiang, Zhao Weiting. Cryptanalysis and improvement of two certificateless signcryption schemes [J]. Computer Applications and Software, 2016, 33(7): 313-317, 333.

Note: Figure translations are in progress. See original paper for figures.

Source: ChinaXiv —Machine translation. Verify with original.