A New Signcryption Scheme Based on Elliptic Curves

Wen-jun Cui[1], Zhi-juan Jia[1], Ming-sheng Hu[1(✉)], Bei-Gong[1,2], and Li-peng Wang[1]

[1] College of Information Science and Technology, Zhengzhou Normal University, Zhengzhou 450044, China
cui2361078314@163.com, 2361078314@qq.com
[2] Beijing University of Technology, Beijing 100124, China

Abstract. Based on the intractable problem of discrete logarithm in ECC and the intractability of reversing a one-way hash function, this paper presents a signcryption scheme with public verifiability and forward security. In the process of security proof, the unforgeability ensures that the attacker can't create a valid ciphertext. We verify the cipher text c instead of the plain text m in verification phase. We protect the plain text m, which makes the proposed scheme confidential. Thus, the proposed scheme has the property of public verification. And the scheme ensures that if the sender's private key is compromised, but the attacker can't recover original message m from cipher text (c, R, s). By the performance analysis, our proposed scheme mainly uses the model multiplication. Compared with Zhou scheme, the number of model multiplication has lost one time in signcryption phase, which leads to the significant increase in calculation rate. Moreover, the signature length has lost $2|n|$ compared with Zhou scheme. In other words, the minimum value of complexity is reached in theory. This makes the scheme have higher security and wider applications.

Keywords: Public verifiability · Forward security · Unforgeability · Model multiplication

1 Introduction

From the invention of public key cryptography to the 1990s, delivering an arbitrary length's message in a secure and authenticated way with an expense less than that required by signature-then-encryption seemed to have never been solved. Fortunately, Zheng discovered a new cryptographic primitive termed as "signcryption", which satisfied both the functions of digital signature and public key encryption in a logically single step simultaneously, and with a cost significantly smaller than that required by signature-then-encryption. The saving in cost growed proportionally to the size of security parameters [1]. Based on elliptic curve cryptosystems, a new signcryption was presented, and it saved the communication cost at least 1.25 times and enhanced computation cost 1.19 times over ECDSA-then-PSCE-1 [2]. The signcryption scheme, which can be verified by the third party after the specific recipient removed his key

J. Li et al. (Eds.): SPNCE 2019, LNICST 284, pp. 538–544, 2019.
https://doi.org/10.1007/978-3-030-21373-2_43

information, was a publicly verifiable scheme. Analysis showed that the proposed scheme is secure against the adaptive chosen ciphertext attack [2]. Combining digital signature and encryption functions, an efficient signcryption scheme based on elliptic curve was proposed [3]. The scheme takes lower computation and communication cost to provide security functions. It not only provides message confidentiality, authentication, integrity, unforgeability, and non-repudiation, but also forward secrecy for message confidentiality and public verification. And the judge can verify sender's signature directly without the sender's private key when dispute occurs [3].

A signcryption scheme with public verifiability and forward security was shown in [4]. An open problem on the design of signcryption was successfully solved. And the security properties of this scheme was proved in detail [4]. By using verifiable secret sharing and secure multi-party computation, the authors proposed a protocol for threshold generation of the signcryption [5]. Because point addition couldn't map coordinate addition directly, a linear sum of coordinates to reconstruct the private coordinate was introduced. And the complexity is less than the same schemes based on DLP (Discrete Logarithm Problem) [5]. An enhancement of the e-mail protocol using signcryption based on Elliptic curve was introduced, and it provided confidentiality, authenticity, integrity, unforgeability, non-repudiation, forward secrecy and public verifiability [6]. [7] highlighted limitations of the existing ECC based schemes using signcryption. These limitations include some missing security aspects as well as high computation power requirement, more communication overhead incurred and large memory requirements. Moreover, [7] proposed an efficient lightweight signcryption scheme based on HECC which satisfied all the security requirements. Compared with existing signcryption schemes, the scheme reduced significant amounts of computation, communication costs and message size [7].

New signcryption schemes based on elliptic curve cryptography were introduced [8]. The security of proposed schemes is based on elliptic curve discrete logarithm problem (ECDLP) and elliptic curve Diffie-Hellman problem (ECDHP). The proposed schemes provided various desirable security requirements like confidentiality, authenticity, non-repudiation and forward security as well as chosen ciphertext attack and unforgeability [8]. A public verifiable signcryption scheme with forward security was presented in [9]. In this scheme, the verification process didn't need the sender's private key, a parameter was hided in the index, so attacked who obtained the sender's private key wouldn't get any secret information between these participates before this communication. And furthermore, authentication and message recovery was not separated, but in the process of public verify, the message confidentiality won't be damaged [9]. An improvement scheme was proposed with public verifiability and forward security, the correctness and security were proved in [10]. The efficiency of the scheme was increased significantly compared with two existing schemes. Moreover, a new signcryption scheme based on elliptic curves was proposed with public verifiability and forward security. In the algorithm, both the numbers of model multiplication and model inverse were reached the minimum four times and zero times, the efficiency of the algorithm was increased significantly compared with the existing signcryption scheme [10]. The authors extended hybrid signcryption technique to the certificateless setting, and constructed a provably secure certificateless hybrid signcryption (PS-CLHS) scheme [11]. In the random oracle model,the authors proved that the proposed scheme

satisfies the indistinguishability and unforgeability under the hardness of the bilinear Diffie-Hellman problem and computational Diffie-Hellman problem [11].

2 Preliminaries

For convenience of the readers, we will recall some basic facts and some useful properties. For more details, the readers can refer to [3, 12–14].

2.1 Elliptic Curve

An elliptic curve is defined as a nonsingular cubic curve over finite field in two variables, $f(x, y) = 0$, with a rational point (which may be a point at infinity) which satisfy the equation: $y^2 = x^3 + ax + b$. The field T is generally taken to be the complex numbers, reals, rationales, or a finite field.

2.2 Elliptic Curves Over $GF(p)$

Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller (IBM) and Neil Koblitz as an alternative mechanism for implementing public-key cryptography based on elliptic curve over finite field.

An elliptic curve E over R (real numbers) is defined by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_1, a_2, a_3, a_4, a_6 \in T$. By performing the change of variables, we get one of the simplified Weierstrass equations

$$y^2 = x^3 + ax + b \text{ where } 4a^3 + 27b^2 \neq 0,$$

together with a special point 0 called the point at infinity. G is a generator of elliptic curve. n is the order of G, which satisfies $nG = 0$.

2.3 Elliptic Curve Discrete Logarithm Problem

ECC is based on discrete logarithm that is much more difficult to challenge at equivalent key lengths as compare to other public key cryptography.

Let P and Q be two points of an elliptic curve with order n and n is a prime. The point $Q = kP$ where $k < n$. Given these two points P and Q, find the correct k of Q. Up to now, it is computational infeasible to generate k from P and Q.

2.4 Hash Function

A hash function takes a group of characters and maps it to a value of a certain length called a hash value or message digest. The hash value is representative of the original

string of characters, but is normally smaller than the original. Hash function is mainly used to generate a fixed length of string. Hash function can be divided into weak no-collision hash function and strong no-collision hash function.

Hash function is weak no-collision if a given an information x and there be an information which contents is unfeasible.

Hash function is strong no-collision if an information $x' \neq x$ which contents to $h(x) = h(x')$ is unfeasible.

3 The Proposed Scheme

Most of existing schemes can't simultaneously provide public verifiability and forward security. To solve this problem, based on the intractable problem of discrete logarithm in ECC and the intractability of reversing a one-way hash function, this paper presents a public verifiable signcryption scheme with forward security.

3.1 Initialization Phase

In this phase, we should select and publish some parameters as follows:

Set E is an elliptic curve over $GF(p)$, G is a generator of elliptic curve E. The sender A randomly selects an integer $x_A \in Z_n^*$ as her private key. Meanwhile, A computes her public key $y_A = x_A G$. Similarly, the recipient B also selects private key $x_B \in Z_n^*$ and public key $y_B = x_B G$, (E', D') is the secure encryption and decryption pair.

3.2 Signcryption Phase

The sender A randomly selects $r \in Z_n^*$, then $R = rG$, $K = ry_B = (k, l)$. Generating cipher text $c = E'_k(m)$. Computing Hash function value $e = h(c)$, Hamming weight $d = ham\ (e)$, $s = r + d + x_A \mod n$. A Sends the signcrypted text (c, R, s) to B.

3.3 Unsigncryption Phase

B receives the signcrypted text (c, R, s). Computing $K = x_B R = (k, l)$, Hash function value $e = h(c)$, Hamming weight $d = ham\ (e)$, $t = (s - d) \mod n$. Generating plain text $m = D'_k(c)$.

Verifying $tG - y_A$ is equal to R or not. If it is true then B accepts (c, R, s) which is sent by A.

The signcrypted text (c, R, s) is a valid one, its correctness is given below.

$$(s - d)G - y_A = (r + d + x_A - d)G - x_A G = rG = R.$$

4 Analysis of the Proposed Scheme

In this section, there is a discussion of the security aspects of the proposed scheme.

4.1 Security Proof

The proposed work not only provides unforgeability and non-repudiation (public verification) but also forward secrecy.

1. Unforgeability

Unforgeability ensures that the attacker can't create a valid ciphertext. In the proposed scheme, the attacker cannot create a valid (c, R, s) without the private key of the sender A. If an attacker forges a valid (c', R', s') from previous (c, R, s), the key is to generate a correct s'. Since $s = r + d + x_A$, the attacker must get random r and x_A, which the attacker can't get obviously. To obtain x_A from $y_A = x_A G$ and r from $R = rG$, then the attacker has to solve ECDLP firstly but it is computationally infeasible. Therefore, our proposed scheme satisfies unforgeability.

2. Non-repudiation

The proposed scheme provides the non-repudiation property. Namely, the proposed scheme has the property of public verifiability. When dispute occurs for the sender and recipient, the recipient can send (c, R, s) to the Third-party Trusted Center for settling whether the original cipher text c sent by the sender. During this process, the Third-party Trusted Center can determine whether the signature is generated by the sender, because only the sender can use her own private key x_A to generate correct signature s. Thus, the proposed scheme satisfies non-repudiation property.

Meanwhile, we verify the cipher text c instead of the plain text m in verification phase. We protect the plain text m, which makes the proposed scheme confidential. Therefore, the proposed scheme has the property of public verification.

3. Forward secrecy

The proposed scheme ensures that if the sender's private key is compromised, but the attacker can't recover original message m from cipher text (c, R, s). In the proposed scheme if the attacker tries to derive plain text m, he has to get the secret key k because of $m = D'_k(c)$. There are two ways to deduce k:

(1) We need know r because of $K = ry_B = (k, l)$. However, to obtain r from $R = rG$, then the attacker has to solve ECDLP firstly but it is computationally infeasible.
(2) We need know x_B because of $K = x_B R = (k, l)$. But as B's private key, x_B can't be got.

Therefore our proposed scheme provides forward secrecy.

4.2 Performance Analysis

We compare cost of our proposed work with some elliptic curve cryptography schemes and try to reduce the cost of computation. Recently, our proposed scheme and Zhou

scheme [10] simultaneously provide public verifiability and forward security. Same as Zhou scheme [10], both the numbers of model index and model inverse are reached the minimum zero times. Compared with Zhou scheme [10], the number of model multiplication has lost one time in signcryption phase, which leads to the significant increase in calculation rate. Moreover, the signature length has lost $2|n|$ compared with Zhou scheme. In other words, the minimum value of complexity is reached in theory (Table 1).

Table 1. Performance Comparison

	Zhou scheme [10]		The proposed scheme	
	Signcryption phase	Unsigncryption phase	Signcryption phase	Unsigncryption phase
Model index	0	0	0	0
Model inverse	0	0	0	0
Model multiplication	2	1	1	1
Hash function	1	1	1	1
Signature length	$5\|n\|$		$3\|n\|$	

5 Conclusion

Based on the intractable problem of discrete logarithm in ECC and the intractability of reversing a one-way hash function, this paper presents a public verifiable signcryption scheme with forward security. In the process of security proof, the unforgeability ensures that the attacker can't create a valid ciphertext. We verify the cipher text c instead of the plain text m in verification phase. We protect the plain text m, which makes the proposed scheme confidential. Thus, the proposed scheme has the property of public verification. And the scheme ensures that if the sender's private key is compromised, but the attacker can't recover original message m from cipher text (c, R, s). By the performance analysis, our proposed scheme mainly uses the model multiplication. Compared with Zhou scheme [10], the number of model multiplication has lost one time in signcryption phase, which leads to the significant increase in calculation rate. Moreover, the signature length has lost $2|n|$ compared with Zhou scheme. In other words, the minimum value of complexity is reached in theory. This makes the scheme have higher security and wider applications.

References

1. Zheng, Y.L.: Digital signcryption or how to achieve cost(signature & encryption) $\ll$ cost (signature) + cost(encryption). In: Kaliski, B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 165–179. Springer, Berlin (1997). https://doi.org/10.1007/BFb0052234
2. Han, Y., Yang, X., Hu, Y.: Signcryption based on elliptic curve and its multi-party schemes. In: Proceedings of the 3rd International Conference on Information Security, pp. 216–217. ACM (2004)

3. Hwang, R.J., Lai, C.H., Su, F.F.: An efficient signcryption scheme with forward secrecy based on elliptic curve. Appl. Math. Comput. **167**(2), 870–881 (2005)
4. Qi, M.P., Chen, J.H., Fe, D.B.: Signcryption scheme with public verifiability and forward security. Appl. Res. Comput. **23**(9), 98–106 (2006)
5. Han, Y., Yang, X., Hu, J.: Threshold signcryption based on elliptic curve. In: 2009 International Conference on Information Technology and Computer Science, pp. 370–373. IEEE (2009)
6. Mohapatra, A.K., Kushwaha, J., Popli, T.: Enhancing email security by signcryption based on elliptic curve. Int. J. Comput. Appl. **71**(17), 28–30 (2013)
7. Ch, S.A., Sher, M., Ghani, A., et al.: An efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography. Multimed. Appl. **74**(5), 1711–1723 (2015)
8. Nayak, B.: Signcryption schemes based on elliptic curve cryptography (2014)
9. Qi, M.P., Chen, J.H., He, D.B.: Signcryption scheme with public verifiability and forward security. Appl. Res. Comput. **31**(10), 3093–3094 (2014)
10. Zhou, K.Y.: Attack analysis and improvement on the signcryption scheme with public verifiability and forward security. J. Northwest Normal Univ. (Nat. Sci.) **51**(6), 50–53 (2015)
11. Yu, H.F., Yang, B.: Provably secure certificateless hybrid signcryption. Chin. J. Comput. **38**(4), 804–813 (2016)
12. Al-Somani, T.F., Ibrahim, M.K., Gutub, A.: High performance elliptic curve GF (2m) crypto-processor. Inf. Technol. J. **5**(4), 742–748 (2006)
13. Sun, Y., Chen, X.Y., Du, X.H., et al.: Proxy re-signature scheme for stream exchange. J. Softw. **26**(1), 129–144 (2015)
14. Johnson, D., Menezes, A., Vanstone, S.: The elliptic curve digital signature algorithm (ECDSA). Int. J. Inf. Secur. **1**(1), 36–63 (2001)