Advanced Engineering Forum *Online: 2011-09-09*
ISSN: 2234-991X, Vol. 1, pp 198-203
doi:10.4028/www.scientific.net/AEF.1.198

Identity-Based Multi-Signcryption with Public Verifiability

YU Xiu-ying[1, a] , He Da-ke [2, b]

1.School of Information Since & Technology ,South West Jiao Tong University, 610031, China
2. School of Information Science and Technology,South West Jiao Tong University,610031, China
[a]niniyxy@163.com, [b]dkhe_scce@swjtu.edu.cnl

Key words: signcryption ; identity-based; bilinear pairing; public verifiability

Abstract: Multi-signcryption can meet the requirement of message signcryption with muti-participant. Since the existing identity-based multi-signcryption scheme cannot offer the function of public verifiability, based on identity and bilinear pairing on the Elliptic Curve, a new scheme with public verifiability is proposed. In the scheme, with the steps which is comparatively independent to the signcryption process, it can provide the public verification of each signcryption in need. Therefore, our scheme efficiently achieves the cryptographic functions of multi-signcryption.

1 Introduction

Identity based cryptosystems were introduced by Shamir in1984 ([1]). The idea was to get rid of public key certicates by allowing the user's public key to be the binary sequence corresponding to an information identifying him in a non ambiguous way (e-mail address, IP address combined to a user name, social security number,...).Since Boneh and Franklin gave a practical ID-Based encryption scheme [2] from Weil pairing in 2001, a large number of papers have been published in this area.The concept of public key signcryption schemes was found by Zheng in 1997 ([3]). The idea of this kind of primitive is to perform encryption and signature in a single logical step in order to obtain confidentiality, integrity, authentication and non-repudiation more efficiently than the sign-then-encrypt approach. Many schemes have been designed as the extension of signcryption such as proxy signcryption, Multi-proxy-signcryption, ID-based signcryption,ect, and many research have been proposed[4-8].

With the continue growth of the internet, user sends and forwards an original message to other users. Through this process, the message may be modified, improved and added a convenient feature by many users. But we must detect the malicious attackers and prevent the malicious code from damaging the receiver or prevent the attackers from obtaining the private messages. Therefore the concept of multi-signcryption was proposed in[9] which can meet with the requirement of multi-signers performing together the signcryption operation on messages and a specific scheme called Seo-Lee scheme was proposed in [10]. It efficiently provides message flexibility, order flexibility, message verifiability, order verifiability, message confidentiality, message unforgeability, non-repudiation and robustness. Based on Seo-Lee scheme, a Multi-signcryption scheme using identity and bilinear pairing was proposed. It greatly decreases the cost of building and managing public key infrastructures ; the expense of the users' management of public-key and their certificates is avoided. Up to the present, various studies on ID-Based multi-signcryption have been proposed[12,13].

Most of the existing ID-Based multi-signcryption scheme don't provide the public verifiability though it is a very important property in many practical application. Even there are some schemes can provide the verification, they need the plaintext or the private key of verifier. In this paper, we propose a new ID-Based multi-signcryption that can provide public verification together with other security properties fulfilled and we also give the analysis of the scheme.

2 Preliminary Works

2.1 Bilinear Pairings

We consider two groups G_1 (additive) and G_2 (multiplicative) of the same prime order q. We need bilinear maps $e: G_1 \times G_1 \to G_2$ satisfying the following properties:

1. Bilinearity: $\forall P, Q \in G_1$,$\forall a, b \in F_q^*$,we have $e(aP, bQ) = e(P, Q)^{ab}$.

2. Non-degeneracy: The map does not send all pairs in $G_1 \times G_1$ to the identity in G2. Observe that since G1,G2 are groups of prime order this implies that if P is a generator of G1 then e(P,P) is a generator of G2.

3. Computability: there exists an efficient algorithm to compute $e(P, Q) \forall P, Q \in G_1$.

There are two problems that our scheme base on as follows:

DBDHP: Given two groups $G_1$and G_2 of the same prime order q, a bilinear map$e: G_1 \times G_1 \to G_2$ and a generator P of $G_1$the Decisional Bilinear Diffie-Hellman problem (DBDHP) in (G_1 , G_2 , e) is to decide whether$h = e(p, p)^{abc}$ given (P,aP,bP,cP) and an element $h \in G_2$.

CBDHP: Given two groups $G_1$and G_2 of the same prime order q, a bilinear map $e: G_1 \times G_1 \to G_2$ and a generator P ofG_1, the Computational Bilinear Diffie-Hellman problem (CBDHP) in (G_1,G_2,e) is to compute $h = e(p, p)^{abc}$ given(P,aP,bP,cP).

No algorithm is known to be able to solve any of them so far, though **DBDHP** is no harder than **CBDHP**.

2.2 Security properties

Due to the identity-based nature of singncryption, and the combined requirements on confidentiality and non-repudiation, the security requirements are multifaceted and quite stringent. We assume Alice is the recipient, I_i are the signers and Charlie is a third party. The properties a multi-signctyption should meets are as follows:

Confidentiality: It is impossible for the attacker to compute the secret messages m_1 , m_2 , ···, m_n, or compute the private information of Alice by the signcryption .

Unforgeability: It is impossible for any attacker to forge a valid multi-signcryption even any one of I_i or Alice.

Non-repudiation: Charlie can judge the validity of a signcryption when dispute occurs for sender and recipient.

3 a new ID-Based multi-signcryption

This section proposes a new ID-Based multi-signcryption schemes with flexibility and verifiability for both message and order.

Setup

The PKG chooses the system parameters that include two groups $(G_1, +)$ and $(G_2 , \cdot)$, a bilinear map $e : G_1 \times G_1 \to G_2$ between these groups, a generator P of G1, a master secret $s \in Z_q^*$, and a public key $Ppub = sP \in G_1$. It also chooses a secure symmetric scheme (E;D) and hash functions , $H_0:\{0,1\}^* \to Z_q^*$, $H_1:\{0,1\}^* \to G_1$ and $H_2:\{0,1\}^* \times \{0,1\}^n \times G_1 \to Z_q^*$, n is the length of plaintext. The public key and private key of Alice is $Q_a = H_0(ID_a)$, $S_a = sQ_a$,the keys of Ii (1 ≤i ≤n) is $Q_i = H_0(ID_i)$, $S_i = sQ_i$. PKG keeps the s, the public parameters are G1, G2, P, PPub, e, H0, H1, H2.

Signcrypt

We assume that Alice wants n signers Ii (1 ≤i ≤n) to generate a signcryption on a fixed message M according to order fixed beforehand. First Alice send the original message m and the public key $Q_a = H_0(ID_a)$ to all the signers Ii (1 ≤i ≤n),each signer changes the message m into m_i which includes the secret information for Alice.

Assume I_1 is the first signer and I_{i+1} is the next one to I_i.

I_1: choose $k_1 \in Z_q^*$ in random, compute

$K_1 = e(P_{pub}, Q_a)^{k_1}$, $r_1 = H_1(m_1 \| Q_1 \| K_1)$, $c_1 = E_{K_1}(m_1 \| \mathrm{Q}_1)$, $s_1 = (k_1 P_{pub} - r_1 S_1)$,

$X_1 = k_1 P$, $R_1 = H_2(ID_1, c_1, X_1)P_{pub}$, $Z_1 = S_1 + k_1 R_1$

I_1 sends $(Q_1, s_1, r_1, c_1, X_1)$ to I_2, and sends Z_1 to Alice.

According to each signer I_i .the signcryption process is as follows:

I_i: receive $(Q_{i-1}, s_{i-1}, r_{i-1}, c_{i-1}, X_{i-1})$,choose $k_i \in Z_q^*$ in random, compute:

$K_i = e(P_{pub}, Q_a)^{k_i}$, $r_i = H_1(m_i \| Q_i \| K_i) \cdot r_{i-1}$, $c_i = E_{K_i}(m_i \| \mathrm{Q}_i \| Q_{i-1} \| s_{i-1} \| c_{i-1})$,

$s_i = (k_i P_{pub} - r_i S_i) \in G_1$, $X_i = H_1(c_i, Q_i, K_i)X_{i-1}$

And sends $(Q_i, s_i, r_i, c_i, X_i)$ to the next signer I_{i+1}. Until the last signer I_n sends $(Q_n, s_n, r_n, c_n, X_n)$ to Alice, Alice take the steps as follow to unsigncrypt the multi-signctyption and verify.

Unsigncrypt

Alice :

Receives $(Q_n, s_n, r_n, c_n, X_n)$,with the private key Sa to compute the session key with $I_n: K_n = e(s_n, Q_a)e(Q_n, S_a)r_n$,

With $m_n \| Q_n \| Q_{n-1} \| s_{n-1} \| c_{n-1} = D_{K_n}(c_n)$,get message m_n , Q_n , Q_{n-1} , s_{n-1} , c_{n-1} ;from $r_{n-1} = H_1(m_n \| Q_n \| K_n)^{-1} r_n$ to recover r_{n-1} ,from $X_{n-1} = H_1(c_n \| Q_n \| K_n)^{-1} X_n$ to recover X_{n-1}. Then Alice computes each session key $K_i = e(s_i, Q_a)e(Q_i, S_a)r_i$ with $I_i, 1 \le i \le n$, get all the part signcryption $(Q_i, s_i, r_i, c_i, X_i)$ and message m_i together with the order of signer.

Do the same steps until Alice compute $X_1 = H_1(c_2 \| Q_2 \| K_2)^{-1} X_2$, $r_1 = H(m_2 \| Q_2 \| K_2)^{-1} r_2$,and unsigncrypt m$_1$, Q$_1$ through K$_1$.

Finally ,Alice accepts the signcryption if $r_1 = H(m_1 \| Q_1 \| K_1)$ and $e(P, Z_1) = e(P_{pub}, Q_1)e(X_1, R_1)$ are established, else refuses it.

Public verify:

If a signer I$_i$ denies the signcryption, Alice sends (c_1, X_1, Z_1) to the third party to arbitrate.

The third party compute $R_1 = H_2(ID_1, c_1, X_1)P_{pub}$,judge the sincryption is true if $e(P, Z_1) = e(P_{pub}, Q_1)e(X_1, R_1)$ is established.

Proof of correctness

$$e(P,Z_1) = e(P, S_1 + k_1R_1) = e(P, sQ_1 + k_1R_1) = e(P, sQ_1)e(k_1P, R_1) = e(P_{pub}, Q_1)e(X_1, R_1)$$

4 validity and security analysis

Message flexibility: A message does not need to be fixed beforehand. Therefore each signer can modify an original message.

Order flexibility: Neither order of signers nor signers themselves need to be designated beforehand. Therefore we can easily change order of signers, add a new signer and exclude a signer.

Confidentiality: It is impossible for the attacker to compute the secret messages m$_1$, m$_2$, …, m$_n$, from the signcryptions $(Q_i, s_i, r_i, c_i, X_i)$ without $\mathbf{k_i}$,$\mathbf{S_i}$ and $\mathbf{S_a}$. Base on the problem of discrete logarithm,it is also computational impossible for attacker to compute $\mathbf{k_i}$ from $K_i = e(P_{pub}, Q_a)^{k_i}$ or $\mathbf{S_i}$ from $s_i = (k_iP_{pub} - r_iS_i)$. Therefore it is impossible to get $\mathbf{m_i}$.

Unforgeability: It is impossible for any attacker to forge a valid signcryption without $\mathbf{S_i}$,the private key of $\mathbf{I_i}$even any one of I$_i$ or Alice.

Non-repudiation: Since the signcryption of each $\mathbf{I_i}$ is unforgeable, once the multi-signcryption is generated, it cannot be denied.

Public verification: When dispute occurs for sender and recipient, the recipient can send$(c_1, X_1, Z_1)$to the judge. The judge can verify the validity of the signcryption without the private key of recipient. And the information still kept secret since the verify uses cipher text. The judge first compute $R_1 = H_2(ID_1, c_1, X_1)P_{pub}$, then judge the sincryption is true if $e(P, Z_1) = e(P_{pub}, Q_1)e(X_1, R_1)$ is established.

Assume that an attacker or Alice choose $k_1' \in Z_q^*$ in random, compute $X_1' = k_1'P$, $R_1' = H_2(ID_1, c_1', X_1')P_{pub}$, $Z_1' = S_1' + k_1'R_1'$, forge a message (c_1', X_1', Z_1') , if $e(P, Z_1') = e(P_{pub}, Q_1)e(X_1', R_1)$established, namely

$$e(P,Z_1') = e(P,S_1' + k_1' R_1') = e(P,s'Q_1 + k_1' R_1') = e(P,sQ_1)e(k_1P,R_1) = e(P_{pub},Q_1)e(X_1,R_1)$$

Because the attacker doesn't know value of s, if $e(P,s'Q_1 + k_1' R_1') = e(P,sQ_1)e(k_1P,R_1)$ is satisfied, the problems of ECDL and BDH are solvable.

Verification flexibility: The public verification is alternative and calculates of X_i can be omitted. Therefore it will be computed only when we need public verification.

5 Conclusions

This paper proposed a new ID-Based multi-signcryption with its analysis. The scheme can provides the public verification of signcryption and the signer. It also satisfies the security properties efficiently with short cipher text. It can be applied in e-commerce or e-voting.

Supported by:

Fundamental Research Funds for the Central Universities (No. SWJTU09BR119). National Natural Science Foundation of China (Grant No.61003245)

REFERENCES

[1] Shamir A. Identity-based Cryptosystems and Signature Schemes [C]//Advances in Cryptology , Crypto'84 : LNCS 196.New York : Springer Verlag ,1984 : 47-53.

[2] Boneh D, Franklin M. Identity-based encryption from the weil pairing[C]// Kilian J, ed. Advances in Cryptology-CRYPTO 2001, LNCS 2139. Berlin, Heidelberg: Springer-Verlag, 2001:213- 229.

[3] ZHEN G Y. Digital signcryption or how to achieve cost (signature &encryption) < < cost (signature) +cost (encryption) [M]// KAL ISKI B. A dvances in Cry ptolog y : CRYPTO 1997 , Berlin : Springer ,1997 : 165-179.

[4] Ma C, Chen K. publicly verifiable authenticated encryption[J].Electronics Letters, 2003; 39(3) : 281~282

[5]. Wang G L, Bao F , Ma C S . Efficient Authenticated Encryption Schemes with Public Verifiability[C].In: Proc of the 60th IEEE Vehicular Technology Conference (VTC 2004- Fall) IEEE Computer Society, 2004.

[6]Chan W K, Wei V K. A Threshold Proxy Signcryption [C]. Proc. Of International Conference on Security and Management, Monte Carlo Resort, Las Vegas, Nevada, USA, 2002: 24-27.

[7] Peng Y Q, Xie S Y, Chen Y F et al. A Publicly Verifiable Authenticated Encryption Scheme with Message Linkages.ICCNMC 2005, LNCS 3619, springer- Verlag Berlin Heidelberg, 2005: 1271~1276

[8] Dent Alexander W. Hybrid signcryption schemes wit h insider security. In : Proceedings of t he Information Security and Privacy ACISP 2005 , Brisbane , Aust ralia , 2005 , 253～266.

[9]Mitomi S , Miyaji A. A General Model of Multisignature Schemes with Message Flexibility , Order Flexibility , and Order Verifiability [J] . IEICE Trans on Fundamentals , 2001 , E842A(10):88-99.

[10] Seo S H , Lee S H.. A Secure and Flexible Multi-signcryption Scheme [C]/ / ICCSA 2004 : LNCS 3 046. Berlin : Springer Verlag , 2004 : 689-697.

[11]Zhang C R,Xiao G Z. Multi2signcryption scheme using identity and bil inear pairing [J]. JOURNAL OF XID IAN UNIVERSITY, 2007, 34(2):270-274 (in Chinese).

[12] Zhang J H,Wang J L, Wang Y M. A multi-signcryption model and its application [J] - Journal of Xidian University(Natural Science 2004(3) (in Chinese).

[13] Meng T, Zhang X P,Sun S H.identity-Based Multi-Sincryption scheme[J]. Journal of Electronics,2007,35(6):115-117 (in Chinese).

[14] Duan S, Cao Z. Efficient and Provably Secure Multi-receiver Identity-based Signcryption[C]//Proc. of Australasian Conference on Information Security and Privacy. [S. l.]: Springer-Verlag, 2006: 195-206.

[15] Yu Yong, Yang Bo, Huang Xinyi, et al. Efficient Identity-based Signcryption Scheme for Multiple Receivers[C]//Proc. of ATC’07. [S. l.]: Springer-Verlag, 2007.