pISSN 1976-913X
eISSN 2092-805X

A Strong Designated Verifiable DL Based Signcryption Scheme

Sujata Mohanty* and Banshidhar Majhi*

Abstract—This paper presents a strong designated verifiable signcryption scheme, in which a message is signcrypted by a signcryptor and only a specific receiver, who called a "designated verifier", verifies it using his own secret key. The scheme is secure, as an adversary can not verify the signature even if the secret key of the signer is compromised or leaked. The security of the proposed scheme lies in the complexity of solving two computationally hard problems, namely, the Discrete Logarithm Problem (DLP) and the Integer Factorization Problem (IFP). The security analysis of the scheme has been done and it is proved that, the proposed scheme can withstand an adaptive chosen ciphertext attack. This scheme can be very useful in organizations where there is a need to send confidential documents to a specific recipient. This scheme can also be applicable to real life scenarios, such as, e-commerce applications, e-banking and e-voting.

Keywords—Designated Verifiable, Discrete Logarithm Problem, Chosen Ciphertext Attack, Nonrepudiation

1. INTRODUCTION

The concept of signcryption, which was first introduced by Zheng [1], is a cryptographic primitive, that simultaneously provides confidentiality and authenticity. It combines both the functions of digital signature and encryption in a logical single step, at a cost that is significantly lower than that required by the traditional signature-then-encryption approach [8]. Following Zheng's proposal, a lot of research has been done in the area of signcryption [2, 3].

In a signcryption scheme, the sender usually uses the recipient's public key for deriving the session key of a symmetric encryption. This is done while the recipient uses his/her private key for deriving the same session key. The exposure of session keys can be a devastating attack to a cryptosystem since such an attack typically implies that all of the security guarantees are lost. In some cases, it will be an advantage that only a specific person, known as "designated verifier", who can verify the signcrypted text. In some applications, it is important for the signer to decide by whom his signatures can be verified due to blackmailing. For example, in an electronic voting system, the voting center presents proof to convince a voter that his/her vote was counted without letting him/her convince others (e.g., a coercer) of his/her vote. This is important in the design of a receipt-free electronic voting scheme preventing vote buying and coercion. This is the motivation of the concept of "designated verifier signature". The concept of designated verifier signature scheme was first established by Jakobsson et al. [4]. Here only a specific recipient,

Manuscript received October 28, 2011; first revision June 5, 2012; accepted August 16, 2012.
Corresponding Author: Sujata Mohanty

* Dept. of Computer Science and Engineering, National Institute of Technology, Rourkela, Orissa, India (sujata.nitr@gmail.com, bmajhi@nitrkl.ac.in)

called a designated verifier can be convinced of the validity of the signature. But a designated verifier scheme has a serious problem, as one can not verify whether the signer or the designated verifier issued the signature. To overcome this problem, Saeednia et al. proposed a strong designated verifier scheme [5]. Here only the designated verifier can verify the validity of the signature in normal communication. The major weakness of this scheme is analyzed by Lee and Chang[6], that, the signature can be verified not only with the designated verifier's secret key but also the signer's secret key. This could make the signer's identity revealed. A strong designated verifier signature scheme was proposed by Lee and Chang [6], in which a signature can be verified only with the designated verifier's secret key. Steinfeld et al. [7] introduced the conception of "universal designated verifier signature", which can be viewed as an extension of designated verifier signature. Universal designated verifier signature allows any holder of the signature (not necessarily the signer) to designate the signature to any desired designated verifier. The verifier can be convinced that the signer indeed generated the signature, but cannot transfer the proof to convince any third party.

Till date, there is no research in the area of signcryption with strong designated verifiability property, which can have huge applications in real life scenarios, such as e-voting or e-cash or online patent submission. For example, suppose a person has to submit a proposal for patent by an organization. In this scenario, the person may act as a signcryptor and the organization may act as a designated receiver. Here the document to be patented can only recovered and verified by the specific receiver, in our case, it is the organization. We combined the mechanism of strong designated verifier signature scheme as proposed in [6] and incorporated in to signcryption scheme.

In this paper, we propose a novel strong designated verifier signcryption scheme, where the signature can only be verified by a specific recipient, known as designated verifier. In this scheme, the property "strong" refers to the requirement that, only a specific receiver, called a "designated verifier", has to use his/her secret key to verify the validity of the signature. Based on the DLP, the scheme is secure as an adversary cannot verify the signature even if the secret key of the signer is compromised or leaked. The security of the proposed scheme lies in the complexity of solving two hard problems, namely, the Discrete Logarithm Problem (DLP) and the Integer Factorization Problem (IFP). The security analysis of the scheme was carried out and it is proved that the proposed scheme is semantically secure against an adaptive choosen ciphertext attack. This scheme can be very useful in organizations, where there is a need to send confidential documents to a specific recipient, such as e-voting, e-cash and e-commerce applications.

The rest of this paper is organized as follows. Section 2 discusses preliminaries of the proposed scheme. The proposed scheme is presented in section 3. Security analysis of the scheme is done in section 4. Finally we conclude in section 5.

2. Preliminaries

This section describes short definition of the hard computational problems in which the security of the proposed scheme relies.

2.1 Integer Factorization Problem

Suppose p and q are unknown distinct primes and n=p.q. If the product n is known, the problem is to find out the primes p and q [14].

2.2 Discrete Logarithm Problem

Given an integer number p, a generator g in Z_{p^*}, and an arbitrary element a in Z_{q^*}, finding the unique number i, $0 \leq i \leq p - 1$ such that, $a \equiv g^i \bmod p$,is a difficult computational problem [13].

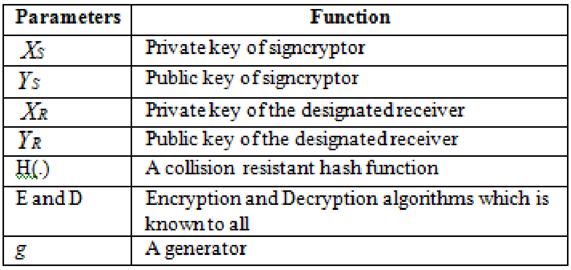
2.3 Safe Prime

Let p is a large prime. We call p a safe prime, if p=2p′+1, such that p′ is also a large prime number [13].

3. Proposed Scheme

The proposed scheme consists of two participants, namely, signcryptor (S) and a designated receiver (R). The scheme consists of three phases, namely, key generation, signcryption and unsigncryption with verification. The parameters used in the scheme are given in Table 1.

Table 1. Parameters used in the proposed scheme



Parameters	Function
X_S	Private key of signcryptor
Y_S	Public key of signcryptor
X_R	Private key of the designated receiver
Y_R	Public key of the designated receiver
H(.)	A collision resistant hash function
E and D	Encryption and Decryption algorithms which is known to all
g	A generator

3.1 Setup

The signcryptor (S) chooses an integer n as the product of two large primes p and q such that $p = 2fp' + 1$ and $q = 2fq' + 1$, where f, p' and q' are all large primes. Then he/she chooses a generator $g \in Z_{p^*}$ with order q and a secure hash function H( ) such as SHA 1. Here p, g and H( ) are public system parameters that are authentically known to all users [13]. Then the signcryptor (S) chooses his/her private key $X_s \in Z_{q^*}$ and computes his/her public key Y_s as follows.

$$Y_s = g^{Xs} \bmod p \tag{1}$$

The designated receiver (R) also chooses his/her private key X_R in random and computes his/her public key as follows.

$$Y_R = g^{X_R} \bmod p \tag{2}$$

The signcryptor and the designated receiver declare their public keys.

3.2 Signcryption

To sign a message M, the signcryptor runs the following steps. He chooses t ∈ Z_{q^*} and computes

$$K = Y_R^t \bmod p \quad (3)$$

$$C = E_K(M) \quad (4)$$

$$r = H(K) \quad (5)$$

$$s = t - r.X_S \bmod q \quad (6)$$

Then he sends $\delta = (r, s, C)$ as the signcrypted text to the designated receiver (R).

3.3 Unsigncryption with verification

After receiving $\delta = (r, s, C)$, the designated receiver (R) computes K' using its own private key (X_R) as given below.

$$K' = (g^s Y_S^r)^{X_R} \bmod p \quad (7)$$

Then he verifies the authenticity of K' by checking the following condition.

$$r = H(K') \quad (8)$$

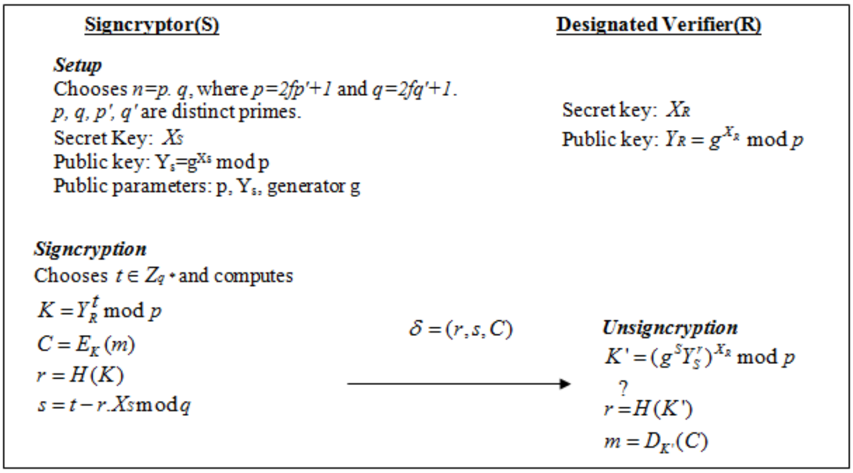
The message M is recovered from the signcrypted text $\delta = (r, s, C)$ as follows.

$$M = D_{K'}(C) \quad (9)$$

4. SECURITY ANALYSIS OF THE PROPOSED SCHEME

In this section, there is a brief discussion of the security aspect of the proposed scheme. Then, the correctness of the proposed signcryption scheme is evaluated. We describe the attacks games used in the security proof to show the semantic security against chosen ciphertext attacks, which was listed in [11, 12]. Finally, we show that the proposed scheme is secure against forgery attack.

In this scheme, the public key generation of both signcryptor and designated receiver are based upon the complexity of solving discrete logarithm problem. It is difficult to extract X_S from Y_S as shown in equation (2). Similarly, extraction of X_R from Y_R is difficult as it is based upn discrete log assumptions. In the signcryption phase, the signcryptor chooses *t* in random and computes *K*, *C*, *r*, *s* as shown in Fig. 1. It is clear that, computation of *K* is also based upon DLP, as it is difficult to obtain the value of *t* from *K*. So, our scheme is still secure if in case the value of *K* is leaked or compromised. Also in our scheme, the signcryptor does not have to send the



Signcryptor(S)

Setup

Chooses $n=p.\,q$, where $p=2fp'+1$ and $q=2fq'+1$.
p, q, p', q' are distinct primes.
Secret Key: X_S
Public key: $Y_s=g^{X_s} \bmod p$
Public parameters: p, Y_s, generator g

Signcryption

Chooses $t \in Z_q{}^*$ and computes
$K = Y_R^t \bmod p$
$C = E_K(m)$
$r = H(K)$
$s = t - r.X_S \bmod q$

$\delta = (r, s, C)$ $\longrightarrow$

Designated Verifier(R)

Secret key: X_R
Public key: $Y_R = g^{X_R} \bmod p$

Unsigncryption

$K' = (g^S Y_S^r)^{X_R} \bmod p$
$r \overset{?}{=} H(K')$
$m = D_{K'}(C)$

Fig. 1. Signcryption and unsigncryption of the proposed scheme

message along with the signature parameter δ . The message is recovered by the designated receiver by using steps as shown in section 3.3. The computational complexity of signcryption phase is $1T_E + 1T_H + 1T_M$ and that of unsigncryption phase is $3T_E + 1T_H + 1T_M$. Here T_E, T_H and T_M are the total number of modular exponentiations, hash operations and multiplication operations. Thus, our scheme has significantly less computational cost.

Correctness

The signcrypted text $\delta = (r, s, C)$ is indeed a valid one; its correctness is discussed below.

(i) $K' = (g^s Y_S^r)^{X_R} \bmod p$
$= (g^s . g^{r.X_s})^{X_R} \bmod p$
$= g^{(s+r.X_S)X_R} \bmod p$
$= g^{t.X_R} \bmod p$, as $s + r.X_S = t \bmod q$ from equation (6)
$= Y_R^t \bmod p$, as $g^{X_R} = Y_R \bmod p$ from equation (2)
$= K$ ▫

(ii) $r = H(K') = H(K)$ as $K' = K$

(iii) $M = D_{K'}(C) = D_K(C)$ as $K' = K$

Definition 1: (Semantic security against chosen ciphertext attacks [11, 12]. A signcryption scheme is semantically secure against chosen ciphertext attacks if no probabilistic polynomial time adversary has a non-negligible advantage in the following game.

1. The challenger runs the key generation algorithm to generate a private/public key pair of receiver (sk_R, pk_R) and gives pk_R to the adversary A.
2. The adversary A submits a number of queries to the signcryption and unsigncryption. In signcryption queries, A chooses a message $m \in M$ (message space) and an arbitrary recipient public key pkr and sends them to the challenger. The challenger runs the signcryption

oracle signcrypt(m, sk_S, pk_R) with private key of signcryptor sk_S and returns the result. In unsigncryption queries, A submits a ciphertext C to the challenger. The challenger runs the signcrypt oracle unsigncrypt (C, sk_R). If the obtained signed plaintext is valid for the recovered signcryptor's public key, then the challenger returns the plaintext to A, otherwise the challenger returns the symbol $\perp$.

3. The adversary A chooses two equal-length messages $m_0, m_1 \in M$ and an arbitrary private key sk_S and then sends them to the challenger. The challenger then flips a coin $b \in \{0,1\}$ to compute a signcrypted text C*=Signcrypt(m_b, sk_S, pk_R) of m_b with the signcryptor's private key sk_S and the under attacked receiver's public key pk_R. Then C* is sent to adversary A as a challenge ciphertext.
4. The adversary A continues to make queries to the signcryption and unsigncryption and he is not allowed to query the unsigncrypt oracle of the challenge ciphertext C*.
5. At the end of the game, the adversary A outputs bit *b* and wins if *b* = *b*. The adversary A's advantage is defined to be $Adv_{IND-CCA}(A) = \Pr[b' = b] - 1/2$.

Based on the above attack game for providing security, we show the proposed scheme is secure against adaptive chosen ciphertext attack.

Assume that, given the receiver's public key Y_R, the adversary A first chooses a signcryptor's private key X_S and a message *m* and sends them to the challenger. The challenger then chooses a random number b and computes the challenge ciphertext δ^* of message m as follows.

$$\delta^* = (r^*, s^*, C^*) \tag{10}$$

After receiving the the challenge ciphertext δ^*, the adversary A first makes a wild guess of b=0 and generates a new ciphertext by choosing a random message m*, whose length is equals to m. Then he chooses a random $X_{S^*} \in Z_{q^*}$. Then the adversary A computes the following.

$$Y_{S^*} = g^{X_{S^*}} \bmod p \tag{11}$$

$$K^* = Y_R^{t'} \bmod p \tag{12}$$

$$C^* = E_{K^*}(m^*) \tag{13}$$

$$r^* = H(K^*) \tag{14}$$

$$s^* = t' - X_{S^*} \bmod p \tag{15}$$

Finally, the adversary A sends the challenge ciphertext δ^* to the challenger for unsigncryption. Upon receiving $\delta^* = (r^*, s^*, C^*)$, the challenger computes

$$K^* = (g^{s^*} Y_S^{r^*})^{X_{R^*}} \bmod p \tag{16}$$

If $r^* = H(K^*)$, then the challenger returns the message m as given below, otherwise rejects the message.

$$m = D_{K^*}(C^*) \tag{17}$$

If the response message m* from the challenger is equals to m, then the adversary A knows that m* is the plaintext for the challenge ciphertext δ^*. The response is automatically rejected because $K^* \neq K$ as X_{R^*} can not be computed from the public key Y_R of receiver, whose complexity lies in solving discrete logarithm problem. Also as $r^* \neq r$ as $K \neq K^*$, which implies message *m* can not be decrypted by using $m = D_{K^*}(C^*)$. Therefore, we conclude that the proposed scheme is secure against adaptive choosen ciphertext attack.

Theorem 1: *It is impossible for any adversary A to forge a valid signcrypted text δ produced by the proposed scheme.*

Proof: To forge a signcrypted text $\delta = (r, s, C)$ of message *m*, the adversary A must know the secret key X_S of the signcryptor who signed the message. The value of X_S is protected under DLP assumption, as shown in equation (1). In case, the value of K is leaked or compromised, it is impossible to compute the parameter s as it requires two secret parameters, X_S and t. Also it is difficult to obtain the designated receiver's secret key (X_R) from the publicly available Y_R, because of the hardness of solving the discrete logarithm problem. Hence, it is almost impossible to produce a valid or authentic signcrypted text by an adversary.

Theorem 2: *No one other than the designated receiver (R) can verify the validity of the signcrypted message.*

Proof: In the proposed scheme, if the secret key of the signcryptor (X_S) is compromised and an adversary A obtains the signcrypted text δ before the designated receiver (R) receives it, the adversary can not verify the signature. This is because the signature can only be verified with the secret key X_R of the designated receiver (R) which is protected under DLP assumption as shown in equation (7). The signcryptor does not have the knowledge of X_R. That indicates the signcryptor also can not verify the validity of the signcrypted text without the help from the designated receiver (R). Therefore, the property *strong designated verifiability* is satisfied.

5. Conclusion

In this paper, we present a new designated verifiable signcrytion scheme based on DLP. Here the property strongly designated verifiability is satisfied. The proposed scheme does not require secure channel in the communication between the signcryptor and the designated verifier. The scheme is proved to be secure against adaptive choosen ciphertext attack. Moreover, an adversary can not verify the signature even if the secret key of the signcryptor is compromised. Therefore, the scheme is suitable for many practical applications, such as e-cash, e-voting and e-commerce.

References

[1] Y. Zheng, "*Digital signcryption or how to achieve cost (signature &encryption) ≪ cost (signature) +*

cost(encryption)", Advances in Cryptology—CRYPTO'97, LNCS 1294, Springer-Verlag, Berlin, 1997, pp.165-179.

[2] H. Petersen and M. Michels, "Cryptanalysis and improvement of signcryption schemes", *IEE Computers and Digital Communications*, Vol.145, No.2, 1998, pp.149-151.

[3] R. Baek,. Steinfeld, Y. Zheng, "*Formal proofs for the security of signcryption"*, Public Key Cryptography 2002, LNCS, vol. 2274, Springer-Verlag, 2002, pp.80-98.

[4] M. Jakobsson, K. Sako, and R. Impagliazzo, "*Designated verifier proofs and their applications"*, Advances in Cryptology-Eurocrypt 1996, LNCS 1070, Springer-Verlag, 1996, pp.143-154.

[5] R. Steinfeld, L. Bull, H.Wang, and J. Pieprzyk, Universal designated-verifier signatures, Advances in Cryptology-Asiacrypt 2003, LNCS 2894, 2003, Springer-Verlag, pp.523-542.

[6] S. Saeednia, S. Kremer, O. Markowitch, "*An efficient strong designated verifier signature scheme"*, ICISC'03,Vol. 2971, Springer, Berlin, 2004, pp.40-54.

[7] J. Lee and J. H. Chang. "Comment on Saeednia et al.'s strong designated verifier signature scheme". *Computer Standards & Interfaces*, Vol.31 (2009), pp.258-260.

[8] J.H. An, Y. Dodis, T. Rabin, "*On the security of joint signature and encryption"*, in Proc. EUROCRYPT 2002, LNCS, Vol.2332, Springer, 2002, pp.83-107.

[9] W.-H. He, T.-C. Wu, Cryptanalysis and improvement of Petersen-Michels signcryption scheme*, IEE Proc.-Comput. Digit. Tech.,* Vol.146, No.2, March, 1999.

[10] Z. Shao, "Efficient deniable authentication protocol based on generalized ElGamal signature scheme", *Computer Standards & Interfaces*, Vol.26, No.5, 2004, pp.449-454.

[11] G. Yang, D.S. Wong, X. Deng, "*Analysis and improvement of a signcryption scheme with key privacy"*, in: Information Security Conference—ISC'05, in: Lecture Notes in Comput. Sci., Vol.3650, Springer-Verlag, Berlin, 2005, pp.218-232.

[12] Chik How Tan, Analysis of improved signcryption scheme with key privacy, *Information Processing Letters,* Vol.99 (2006), pp.135-138.

[13] Shao Z, Signature schemes based on factoring and discrete logarithms, *IEEE Proc., Comput. Digit. Tech.,* Vol.145, No.1, 1998, pp.33-36.

[14] Boris S. Verkhovsky, Integer Factorization: Solution via Algorithm for Constrained Discrete Logarithm Problem*. Journal of Computer Science*, Vol.5 (9), 2009, 674-679.

Sujata Mohanty

She received her MTech degree in Computer Science from College of Engineering and Technology, Bhubaneswar, India in 2008. Presently, she is working as assistant professor in department of Computer Science at National Institute of Technology, Rourkela, India. She is doing her PhD in the area of information security in National Institute of Technology, Rourkela, India.

Banshidhar Majhi

He received his ME degree in Computer Science from National Institute of Technology, Rourkela, Orissa, India in 1998. In 2003 he received his PhD degree in Computer Science from Sambalpur University, Orissa, India. He is working as a professor in department of Computer Science at National Institute of Technology, Rourkela, Orissa, India. His current research interest includes information security, cryptography and biometric security.