A New Forward-Secure Signcryption Scheme

YIN Xin-Chun, CHEN Jue-Wei, WANG Cai-Mei
Department of Computer Science and Engineering
Yangzhou University
Yangzhou, Jiangsu, China
xcyin@yzu.edu.cn

***Abstract*—Signcryption scheme combines digital signature and encryption functions. In regular signcryption, once the long-term private key is compromised, all signatures even those were issued by the honest signer before the compromise, will not be trustworthy any more. In the paper, we present a new forward-secure signcryption scheme. The forward security is that this key update function is one-way and, given the secret key for the current period, it is hard to compute any of the previously used secret keys. So even the adversary gets the secret key, it is still hard to compute any of the previously used secret keys. In this paper, we combine signcryption and forward-secure to present a new signcryption scheme with forward secrecy.**

I INTRODUCTION

Message security and sender's authentication for communication in the open channel is a basic and important technology of internet. For keeping message confidential and unforged, the sender uses a digital signature algorithm with his private key to sign the message, and encrypts the message and digital signature using a symmetric encryption algorithm using a randomly chosen secret key. The sender uses a public key encryption algorithm with the recipient's public key to encrypt this secret key as envelope. Then, the sender sends the envelope and cipher text to the recipient. After the recipient receives the cipher text and envelope, the recipient uses his private key to decrypt the envelope to get secret key and decrypts cipher text to get plain text and signature by using this secret key. Finally, the recipient verifies the message based on this signature.

Zheng [6] first proposed a new cryptography technique named "Signcryption" which combines the functions of digital signature and encryption algorithm for authentication and confidentiality. In the signcryption scheme, the sender uses the recipient's public key to derive a secret key for symmetric encryption. After the recipient receives the cipher text and digital signature, he uses his private key to derive the same secret key.

Exposure of secret keys can be a devastating attack on a cryptosystem since such an attack typically implies that all security guarantees are lost. Indeed, standard notions of security offer no protection whatsoever once the secret key of the system has been compromised. With the threat of key exposure becoming more acute as cryptographic computations are performed more frequently on poorly protected devices (smart-cards, mobile phones, even PCs), new techniques are needed to deal with this concern.

Forward security was first formalized in the context of signature and identification scheme by Bellare and Miner [1], building on earlier ideas of Anderson [2]. Subsequently, numerous constructions of forward-secure signature schemes have been proposed [3, 4, 7], but a forward-secure encryption scheme has been constructed recently by Canetti, Halevi and Katz [5]. It is based on the binary tree encryption scheme. In forward-secure scheme, the lifetime of the system is divided into N intervals (or time periods) labeled 0, ... , N-1. The signer initially stores secret key SK_0 and this secret key "evolves" with time. Namely, at the beginning of time period i, the receiver applies some function to the "previous" key SK_{i-1} to derive the "current" key SK_i, key SK_{i-1} is then erased and SK_i is used for all sign operations during time period i. The public key remains fixed throughout the lifetime of the scheme, this is crucial for making such a scheme viable. A forward-secure signature scheme guarantees that even if an adversary learns SK_i, signature can't be forged during all time periods prior to i.

In this paper, we combine signcryption and forward -secure to present a new signcryption scheme with forward secrecy based on Bo's scheme.

II THE PROPOSED SIGNCRYPTION SCHEME

A *Initialization phase*

Let G_1, G_2 be two cyclic groups of prime order q, where G_1 is represented additively and G_2 is represented multiplicatively. And let $P \in G_1$ be a generator of G_1.

- Computation Diffe-Hellman (CDH) problem: Given (P, aP, bP) where $a, b \in Z_q^*$, compute abP. The advantage of an algorithm $\mathscr{A}$ in solving the CDH problem in a group G is

$$\mathrm{AdvCDH_A} = \Pr[\mathscr{A}(P, aP, bP) = abP \{a, b \overset{r}{\leftarrow} Zq^*\}$$

We say that $\mathscr{A}$ (t, e)-breaks CDH in G if $\mathscr{A}$ runs in time at most t, and $\mathrm{AdvCDH}_{\mathscr{A}} \geq e$.

- Decision Diffe-Hellman (DDH) problem: Given (P,

Supported by the National Natural Science Foundation of China under Grant No.60473012

aP, bP, cP) where a, b, $c \in Z_q^*$, decide whether $c = ab$ in Z_q^*. If so, (P, aP, bP, cP) is called a valid Diffe-Hellman tuple.

Definition 1. A prime order group G is a (t, e)-GDH group if DDH problem can be solved in polynomial time but no probabilistic algorithm (t, e)-breaks CDH in G.

We use a full binary tree with depth l, then the number of time periods is $N = 2^{l+1}-1$. The root of the tree is called node ε.

Denote the node (represented by bit string) and its secret key corresponding to the time period i by w^i and Sw^i, respectively. Let w^i0 (w^i1) be the left (right) child node and let $w^i|_k$ be a k-prefix of w^i. If w^i is an internal node, then $w^{i+1} = w^i0$. If w^i is a leaf node and $i < N$-1, then $w^{i+1} = w'1$, where w' is the longest string such that $w'0$ is a prefix of w^i. The secret key SK_i can be organized as a stack of node keys ST-SK, with the secret node key Sw^i on top. When the signer runs the key update algorithm, first pops the current secret node key Sw^i off the stack.

B Construction of the scheme

Gen: does the following:

1. Run $\mathcal{IG}_G(1^k)$ to generate groups G_1, G_2 of prime order q and bilinear map e.
2. Select a random generator $P \in G_1$ and a random d_A, $d_B \in Z_q^*$. Set $U_A = d_AP$, $U_B = d_BP$.
3. Chooses cryptographic hash functions $H_1 : \{0, 1\}^* \rightarrow G_1$, and $H_2 : \{0, 1\}^* \times \{0, 1\}^* \times G_1 \rightarrow G_1$.
4. The public key is PK = (G_1, G_2, e, P, U_A, U_B, l, H_1, H_2) and the root secret key is $SN_\varepsilon = d_A H_1(\varepsilon)$.

UPD: It takes as input the tree public key PK, the time period i and the secret key SK_i = ST-SK. Let w be the node corresponding to i. In general, for $w = w_1...w_n$, the secret key of the node w consists of $n + 1$ group elements, Sw = ($Rw|1$, $Rw|2$,...,$Rw|n$-1, Rw, SNw). It first pops the secret node key Sw off the stack ST-SK and then updates a secret key respect to the position of node w in tree as follows.

[1] If w is an internal node, then chooses random ρ_{w0}, $\rho_{w1} \in Z_q^*$, and computes $R_{w0} = \rho_{w0}P$, $R_{w1} = \rho_{w1}P$, $SN_{w0} = SN_w + \rho_{w0}H_1(w_0)$, and $SN_{w1} = S_w + \rho_{w1}H_1(w_1)$. Then pushes Sw_1 = ($Rw|1$, $Rw|2$,...,$Rw|n$-1, Rw, Rw_1, SNw_1) and Sw_0 = ($Rw|1$, $Rw|2$,...,$Rw|n$-1, Rw, Rw_0, SNw_0) in order onto the stack, and erases Sw.

[2] If w is a leaf, then only erases Sw.

SIGCRY: Assume that Alice wants to send a message M to Bob at time i. Alice generates digital signature (R, Fs) of message M and uses the symmetric encryption algorithm and secret key s to encrypt M. Let C be the cipher text. Alice generates the signcrypted text (i, C, R, FS) in the following steps.

1. Randomly selects an integer r, where $r \in Z_q^*$.
2. Computes $R = rP = (r_1, r_2)$.
3. Computes $K = rU_B = (s, s')$.
4. Uses the symmetric encryption algorithm to generate cipher text $C = E_s(M)$, where the s is from K.
5. Pops the top in the stack ST-SK and uses it to generate a signature. Let $w = w_1...w_n$ be the node corresponding to i. Then computes $P_M = H_2(M, i, R)$ and $FS = SN_w + rP_M$. The signer outputs a signature (i, R, FS, C) and $R_{w|m}$ where $1 \le m \le n$.

UNSIGCRY: Bob receives the signcrypted text (i, R, FS, C). He decrypts cipher text C by performing symmetric decryption algorithm with secret key s. He also verifies the signature. Bob gets the plain text as follows. Computes $K = Rd_B = (s, s')$. Uses a symmetric decryption algorithm to generate plain text $M = D_s(C)$. Let $w = w_1...w_n$ be the node corresponding to i, When $P_M = H_2(M, i, R)$, if

$$e(P,FS) = \prod_{m=1}^{n} e(R_{w|_m}, H_1(w|_m)) \cdot e(R, P_M) \cdot e(U_A, H_1(\varepsilon)) \quad (1)$$

then confirms that (i, R, FS, C) is a valid signature.

Completeness: The verification of the signature is justified by the following equations:

$$\begin{aligned}
&\prod_{m=1}^{n} e(R_{w|_m}, H_1(w|_m)) \cdot e(R, P_M) \cdot e(U_A, H_1(\varepsilon)) \\
&= \prod_{m=1}^{n} e(P, \rho_{w|_m} H_1(w|_m)) \cdot e(P, rP_M) \cdot e(P, d_A H_1(\varepsilon)) \\
&= e(P, \sum_{m=1}^{n} \rho_{w|_m} H_1(w|_m) + rP_M + d_A H_1(\varepsilon)) \\
&= e(P, FS)
\end{aligned}$$

III SECURITY PROOF

(1) **Confidentiality**. In our scheme, if the attacker wants to derive the original message, he must get the secret key s. The secret key s is the x-coordinate value of point K. However, to generate secret key s is equal to solve the ECDLP or ECDHP. This two problems are computational infeasible.

(2) **Integrity**. In our proposed scheme, the recipient can verify whether the received message is the original one that was sent by the sender or not. In the **SIGCRY** phase, the sender computes and sends FS to the recipient. The parameter FS is generated where $P_M = H_2(M, i, R)$ and M is the original message. If the attacker changes the original cipher text C as C', the related message is changed to M'. Let $P_{M'} = H_2(M', i, R)$. By the property of one-way hash function, it is computational infeasible for the attacker to modify C as C' such that P_M is equal to $P_{M'}$. Furthermore, the attacker does not get SN_w and r, he cannot compute the

correct FS' from FS and R, such that $FS' = SN_w + rP_M'$. So, if the C is altered, the recipient can verify that the original message is altered in the unsigncryption phase.

(3) **Unforgeability**. In our scheme, the attacker can not forge valid (i, R, FS, C) without the private key of sender, because the CDH.

(4) **Non-repudiation**. When dispute occurs for sender and recipient, the recipient can send (i, R, FS, C) to the judge for settling whether the original message M sent by sender or not. In Judge Verification phase, the judge can determine the signature is generated by the sender if Eq. (1) is hold, because of only the sender can use her own private key d_A to generate correct signature FS. According to the previous analysis about unforgeability, we show that anybody without the private key d_A cannot forge the correct signature of message as the sender. In other words, our proposed scheme satisfies non-repudiation property.

(5) **Forward-secure**. The SK_i is evolving, and even if the adversary get the SK_i but he don't know the ρ_{w0}, $\rho_{w1} \in Z_q^*$. The ρ_{w0} and ρ_{w1} are random chosen, so the adversary can't use SK_i to derive SK_{i-1}.

IV Conclusions

This paper proposed an efficient forward-secure signcryption based on binary tree encryption. In regular signcryption, once the long-term private key is compromised, all signatures even those were issued by the honest signer before the compromise, will not be trustworthy any more. In the paper, we present a new forward-secure signcryption scheme. The forward security is that this Key Update function is one-way and, given the secret key for the current period, it is hard to compute any of the previously used secret keys. So even the adversary gets the secret key, it is still hard to compute any of the previously used secret keys.

References

[1] M. Bellare and S.K. Miner. A forward-secure digital signature scheme. Advances in Cryptology-CRYPTO'99, M. Wiener (Ed.), Lecture Notes in Comput. Sci. 1666, Springer-Verlag, pp. 431-448, 1999.

[2] R. Anderson. Two remarks on public key cryptology. Proc. of CCS'97, ACM, 1997.

[3] M. Abdalla and L. Reyzin. A new forward-secure digital signature scheme. Advances in Cryptology-ASIACRYPT 2000, T. Okamoto (Ed.), Lecture Notes in Comput. Sci. 1976, Springer-Verlag, pp. 116-129, 2000.

[4] G. Itkis and L. Reyzin. Forward-secure signatures with optimal signing and verifying. Advances in Cryptology-CRYPTO 2001, J. Kilian (Ed.), Lecture Notes in Comput. Sci. 2139, Springer-Verlag, pp. 332-354, 2001.

[5] R. Canetti, S. Halevi and J. Katz. A forward-secure public-key encryption scheme. Advances in Cryptology-EUROCRYPT 2003, E. Biham (Ed.), Lecture Notes in Comput. Sci. 2656, Springer-Verlag, pp. 255-271, 2003.

[6] Y. Zheng, Digital signcryption or how to achieve Cost(Signature & Encryption) << Cost(Signature) + Cost(Encryption), in: Advances in Cryptology—Crypto'97LNCS 1294, Springer-Verlag, pp. 165–179, 1997.

[7] Bo Gyeong Kang, Je Hong Park, and Sang Geun Hahn. A New Forward Secure Signature Scheme. 2004, available at http://citeseer.ist.psu.edu.