ID-Based Signcryption Scheme with (t, n) Shared Unsigncryption

Fagen Li[1], Xiangjun Xin[1,2], and Yupu Hu[1]
(Corresponding author: Fagen Li)

Key Laboratory of Computer Networks and Information Security, Xidian University[1]
Xi'an, Shaanxi 710071, P.R. China (Email:fagenli@mail.xidian.edu.cn)
Department of Information and Computing Science, Zhengzhou University of Light Industry[2]
Zhengzhou, Henan 450002, P.R. China

(Received Aug. 14, 2005; revised and accepted Sept. 12 & Oct. 20, 2005)

Abstract

An identity-based signcryption scheme with (t, n) shared unsigncryption is proposed, which is the integration of the signcryption scheme, the (t, n) threshold scheme and zero knowledge proof for the equality of two discrete logarithms based on the bilinear map. In this scheme, any third party can verify the validity of the signature, but only more than t members in the recipient group can cooperatively recover the message m. As compared to the Zhang et al.'s signcryption scheme with (t, n) shared unsigncryption based on discrete logarithms, the proposed scheme has the following advantages: it provides both public verifiability and forward security; the key management problem is simplified because of using identity-based cryptosystem.

Keywords: Cryptography, identity-based cryptography, signcryption, (t, n) threshold, zero knowledge proof

1 Introduction

Confidentiality, integrity, non-repudiation and authentication are the important requirements for many cryptographic applications. A traditional approach to achieve these requirements is to "sign-then-encrypt" the message. Signcryption, first proposed by Zheng [19] in 1997 , is a new cryptographic primitive that performs signing and encryption simultaneously, at a lower computational and communication overhead cost than the "sign-then-encrypt" approach. One of the shortcomings of Zheng's original schemes is that its non-repudiation procedure is more inefficient since they are based on interactive zero-knowledge proofs. To achieve simple and safe non-repudiation procedure, Bao and Deng [3] introduced a signcryption scheme that can be verified by a sender's public key. Furthermore, Jung et al. [10] showed that Zheng's schemes do not provide the forward security. That is, anyone who obtains the sender's private key can recover the original message of a signcrypted text. In addition, Steinfeld and Zheng [17] and Malone-Lee and Mao [14] proposed efficient signcryption schemes based on integer factorization and using RSA, respectively. The formal models and security proofs for signcryption schemes have been studied in [1].

Identity-based (ID-based) cryptography (for examples, [4] and [16]) is rapidly emerging in recent years. The distinguishing property of ID-based cryptography is that a user's public key can be any binary string, such as an email address that can identify the user. This removes the need for senders to look up the recipient's public key before sending out an encrypted message. ID-based cryptography is supposed to provide a more convenient alternative to conventional public key infrastructure. Malone-Lee [13] gave the first ID-based signcryption scheme. Libert and Quisquater [12] pointed out that Malone-Lee's scheme is not semantically secure and proposed a provably secure ID-based signcryption schemes. However, the properties of public verifiability and forward security are mutually exclusive in the their scheme. Chow et al. [5] proposed ID-based signcryption schemes that provide both public verifiability and forward security. The first ID-based ring signcryption scheme was proposed in [9].

All of the above schemes consist of only single recipient. However, In many cases, we need to prohibit a single recipient from recovering a signcrypted message. For example, in a sealed-bid auction scheme [11], the coalition between the service providers and some bidders must be prevented by the way in which at least t service providers must participate, the information about the bid of a bidder can be obtained. In 2002, Zhang et al. [18] proposed a new signcryption scheme with (t, n) shared unsigncryption in which at least t recipients must participate in an unsigncryption process. However their scheme is based on discrete logarithm problem, not ID-based. In addition, in their scheme, only the recipients can verify the signature because the unsigncryption needs the recipients' private keys. That is, Zhang et al.'s scheme does not provide the public verifiability.

In this paper, an ID-based signcryption scheme with (t, n) shared unsigncryption is proposed, which is the integration of the Chow et al.'s signcryption scheme [5], the Shamir's (t, n) threshold scheme [15], and Baek and Zheng's zero knowledge proof for the equality of two discrete logarithms based on the bilinear map [2]. In this scheme, a signcrypted message is decrypted only when more than t members join an unsigncryption protocol and the signature can be verified by any third party. As compared to the Zhang et al.'s signcryption scheme with (t, n) shared unsigncryption, the proposed scheme has the following advantages: it provides both public verifiability and forward security; the key management problem is simplified because of using ID-based cryptosystem.

The rest of this paper is organized as follows. Some definitions and preliminary works are given in Section 2. The proposed signcryption scheme with (t, n) shared unsigncryption is given in Section 3. The security and efficiency of our scheme are discussed in Section 4. Finally, the conclusions are given in Section 5.

2 Preliminary Works

In this section, we briefly describe the basic definition and properties of the bilinear pairings. The Shamir's (t, n) threshold scheme [15] and Baek and Zheng's zero knowledge proof for the equality of two discrete logarithms based on the bilinear map [2] are also briefly described. They are the basic tools to construct our scheme.

2.1 Bilinear Pairings

Let G_1 be a cyclic additive group generated by P, whose order is a prime q, and G_2 be a cyclic multiplicative group of the same order q. Let a, b be elements of Z_q^*. A bilinear pairings is a map $\hat{e} : G_1 \times G_1 \rightarrow G_2$ with the following properties:

1) Bilinearity: $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$.

2) Non-degeneracy: There exists P and $Q \in G_1$ such that $\hat{e}(P, Q) \neq 1$.

3) Computability: There is an efficient algorithm to compute $\hat{e}(P, Q)$ for all P,$Q \in G_1$.

The modified Weil pairing and the Tate pairing [4] are admissible maps of this kind. For more details about bilinear pairings, see [4, 6, 7, 8]. The security of our scheme described here relies on the hardness of the following problems.

Definition 1 *Given two groups* G_1 *and* G_2 *of the same prime order* q*, a bilinear map* $\hat{e} : G_1 \times G_1 \rightarrow G_2$ *and a generator* P *of* G_1*, the Decisional Bilinear Diffie-Hellman problem (DBDHP) in* $(G_1, G_2, \hat{e})$ *is to decide whether* $h = \hat{e}(P, P)^{abc}$ *given* (P, aP, bP, cP) *and an element* $h \in G_2$*.*

Definition 2 *Given two groups* G_1 *and* G_2 *of the same prime order* q*, a bilinear map* $\hat{e} : G_1 \times G_1 \rightarrow G_2$ *and a generator* P *of* G_1*, the Computational Bilinear Diffie-Hellman problem (CBDHP) in* $(G_1, G_2, \hat{e})$ *is to compute* $h = \hat{e}(P, P)^{abc}$ *given* (P, aP, bP, cP)*.section*

The decisional problem is of course not harder than the computational one. However, no algorithm is known to be able to solve any of them so far.

2.2 Shamir's (t, n) Threshold Scheme

In order to share a private key D_{ID}, we need the Shamir's (t, n) threshold scheme. Suppose that we have chosen integers t (a threshold) and n satisfying $1 \leq t \leq n < q$. First, we pick $R_1, R_2, \ldots, R_{t-1}$ at random from G_1^*. Then we construct a function $F(u) = D_{ID} + \sum_{j=1}^{t-1} u^j R_j$. Finally, we compute $D_{ID_i} = F(ID_i)$ for $1 \leq i \leq n$ and send (ID_i, D_{ID_i}) to the i-th member of the message recipient group. When the number of shares reaches the threshold t, the function $F(u)$ can be reconstructed by computing $F(u) = \sum_{j=1}^{t} D_{ID_j} N_j$, where $N_j = \prod_{i=1, i\neq j}^{t} \frac{u - ID_i}{ID_j - ID_i} \bmod q$. The private key D_{ID} can be recover by computing $D_{ID} = F(0)$.

2.3 Baek and Zheng's Zero Knowledge Proof for the Equality of Two Discrete Logarithms Based on the Bilinear Map

To ensure that all decryption shares are correct, that is, to give robustness to threshold unsigncryption, we need a certain checking procedure. we use the Baek and Zheng's zero knowledge proof for the equality of two discrete logarithms based on the bilinear map. We construct a zero-knowledge proof of membership system for the language $L_{EDLog^{G_2}_{P,\tilde{P}}} \overset{def}{=} \{(\mu, \tilde{\mu}) \in G_2 \times G_2 \mid \log_g \mu = \log_{\tilde{g}} \tilde{\mu}\}$ where $g = \hat{e}(P, P)$ and $\tilde{g} = \hat{e}(P, \tilde{P})$ for generators P and $\tilde{P}$ of G_1 as follows.

Suppose that $(P, \tilde{P}, g, \tilde{g})$ and $(k, \tilde{k}) \in L_{EDLog^{G_2}_{P,\tilde{P}}}$ are given to the Prover and the Verifier, and the Prover knows a secret $S \in G_1^*$. The proof system works as follows.

1) The Prover chooses T from G_1 randomly and computes $r = \hat{e}(T, P)$ and $\tilde{r} = \hat{e}(T, \tilde{P})$. The Prover sends r and $\tilde{r}$ to the Verifier.

2) The Verifier chooses h from Z_q^* randomly and sends it to the Prover.

3) On receiving h, the Prover computes $W = T + hS$ and sends it to the Verifier.

4) The Verifier checks if $\hat{e}(W, P) = rk^h$ and $\hat{e}(W, \tilde{P}) = \tilde{r}\tilde{k}^h$. If the equality holds then the Verifier returns *"Accept"*, otherwise, returns *"Reject"*.

As claimed in [2], the above protocol can be easily converted a non-interactive knowledge proof.

3 The Proposed Scheme

In this section, we propose an ID-based signcryption scheme with (t, n) shared unsigncryption scheme. The proposed scheme involves three roles: the Private Key Generator (PKG), the sender Alice, and the message recipient group $L = \{L_1, L_2, \ldots, L_n\}$. It consists of four algorithms: **Setup**, **Extraction**, **Signcryption**, and **Unsigncryption**. The details of them are described as below.

Setup: Given a security parameter k, the PKG chooses groups G_1 and G_2 of prime order q (with G_1 additive and G_2 multiplicative), a generator P of G_1, a bilinear map $\hat{e} : G_1 \times G_1 \to G_2$ and hash functions $H_1 : \{0,1\}^* \to G_1$, $H_2 : G_2 \to \{0,1\}^n$, $H_3 : \{0,1\}^* \times G_2 \to Z_q^*$ and $H_4 : G_2 \times G_2 \times G_2 \to Z_q^*$. It chooses a master-key $s \in Z_q^*$ and computes $P_{pub} = sP$. It also chooses a secure symmetric cipher (E, D). The PKG publishes system's public parameters $\{G_1, G_2, n, \hat{e}, P, P_{pub}, H_1, H_2, H_3, , H_4, E, D\}$ and keeps the master-key s secret.

Extraction: Given an identity ID, the PKG sets the user's public key $Q_{ID} = H_1(ID)$, computes the user's private signcryption key $S_{ID} = s^{-1}Q_{ID}$ and private decryption key $D_{ID} = sQ_{ID}$. Similarly to Chow et al.'s scheme [5], we use two private keys in order to provide both public verifiability and forward security. The sender Alice has a public key Q_{ID_A}, a corresponding private signcryption key $S_{ID_A} = s^{-1}Q_{ID_A}$ and a corresponding private decryption key $D_{ID_A} = sQ_{ID_A}$. The message recipient group L has a public key Q_{ID_L}, a corresponding private signcryption key $S_{ID_L} = s^{-1}Q_{ID_L}$ and a corresponding private decryption key $D_{ID_L} = sQ_{ID_L}$. Suppose that we have chosen integers t (a threshold) and n satisfying $1 \le t \le n < q$. The PKG picks $R_1, R_2, \ldots, R_{t-1}$ at random from G_1^* and constructs a function $F(u) = D_{ID_L} + \sum_{j=1}^{t-1} u^j R_j$. Then, the PKG computes the private key $D_{L_i} = F(ID_i)$ and the verification key $y_i = \hat{e}(D_{L_i}, P)$ for recipient $L_i (1 \le i \le n)$. Subsequently, the PKG secretly sends the private key D_{L_i} and the verification key y_i to L_i. L_i then keeps D_{L_i} as secret while making y_i public.

Signcryption: To send a message m to the recipient group L, the Alice choose x from Z_q^* randomly and computes the ciphertext(c, r, S) as follows:

1) Compute $k_1 = \hat{e}(P, Q_{ID_A})^x$.
2) Compute $k_2 = H_2(\hat{e}(Q_{ID_A}, Q_{ID_L})^x)$.
3) Compute $c = E_{k_2}(m)$.
4) Compute $r = H_3(c, k_1)$.
5) Compute $S = (x - r)S_{ID_A}$.

Unsigncryption: Without lose of generality, let $L' = \{L_1, L_2, \ldots, L_t\}$ be t member of L that want to cooperatively unsigncrypt the received signcrypted message (c, r, S). Each $L_i \in L'$ follows the steps below.

1) Compute $k'_1 = \hat{e}(S, P_{pub})\hat{e}(Q_{ID_A}, P)^r$.
2) Accept the message (signature) if and only if $r = H_3(c, k'_1)$, return *"Reject"* otherwise.
3) Compute $\tilde{y_i} = \hat{e}(D_{L_i}, S)$, $\tilde{u_i} = \hat{e}(T_i, S)$, $u_i = \hat{e}(T_i, P)$, $v_i = H_4(\tilde{y_i}, \tilde{u_i}, u_i)$ and $W_i = T_i + v_i D_{L_i}$ for random $T_i \in G_1$ and send $\sigma_i = (i, \tilde{y_i}, \tilde{u_i}, u_i, v_i, W_i)$ to the other $t - 1$ member in L'.
4) Each $\sigma_j = (j, \tilde{y_j}, \tilde{u_j}, u_j, v_j, W_j)$ from L_j $(j \ne i)$ is verified by the procedure as follows. L_i firstly compute $v'_j = H_4(\tilde{y_j}, \tilde{u_j}, u_j)$ and then check if $v'_j = v_j$, $\hat{e}(W_j, S)/\tilde{y_j}^{v'_j} = \tilde{u_j}$, and $\hat{e}(W_j, P)/y_j^{v'_j} = u_j$. If the test above holds, the σ_j from L_j $(j \ne i)$ is valid decryption share.
5) Compute $k'_2 = H_2(\prod_{j=1}^{t} \tilde{y_j}^{N_j} \hat{e}(Q_{ID_A}, Q_{ID_L})^r)$, where $N_j = \prod_{i=1, i \ne j}^{t} \frac{-ID_i}{ID_j - ID_i} \bmod q$.
6) Recover $m = D_{k'_2}(c)$.

4 Analysis of the Scheme

4.1 Correctness

The correctness can be easily verified by the following equations.

$$\begin{aligned}
k'_1 &= \hat{e}(S, P_{pub})\hat{e}(Q_{ID_A}, P)^r \\
&= \hat{e}(xS_{ID_A}, P_{pub})\hat{e}(S_{ID_A}, P_{pub})^{-r}\hat{e}(Q_{ID_A}, P)^r \\
&= \hat{e}(P, Q_{ID_A})^x
\end{aligned}$$

$$\begin{aligned}
k'_2 &= H_2(\prod_{j=1}^{t} \tilde{y_j}^{N_j} \hat{e}(Q_{ID_A}, Q_{ID_L})^r) \\
&= H_2(\prod_{j=1}^{t} \hat{e}(N_j D_{L_j}, S)\hat{e}(Q_{ID_A}, Q_{ID_L})^r) \\
&\quad \text{(bilinear property of } e\text{)} \\
&= H_2(\hat{e}(\sum_{j=1}^{t} N_j D_{L_j}, S)\hat{e}(Q_{ID_A}, Q_{ID_L})^r) \\
&\quad \text{(bilinear property of } e\text{)} \\
&= H_2(\hat{e}(D_{ID_L}, S)\hat{e}(Q_{ID_A}, Q_{ID_L})^r) \\
&\quad \text{(Shamir's threshold scheme)} \\
&= H_2(\hat{e}(D_{ID_L}, xS_{ID_A})\hat{e}(D_{ID_L}, S_{ID_A})^{-r}\hat{e} \\
&\qquad (Q_{ID_A}, Q_{ID_L})^r) \\
&= H_2(\hat{e}(Q_{ID_A}, Q_{ID_L})^x)
\end{aligned}$$

4.2 Security

Unforgeability: Since the signcryption process is the same as the Chow et al.'s signcryption scheme [5], forging a ciphertext for any message m is equivalent to forge a Chow et al.'s signcryption. Chow et al.'s scheme is proven to have the existential unforgeability against adaptive chosen message attacks (in the random oracle) assuming the CBDHP problem is hard.

Confidentiality: In our scheme, the confidentiality is the same as the Chow et al.'s signcryption scheme [5]. Chow et al.'s scheme is proven to have the indistinguishability against adaptive chosen ciphertext attacks (in the random oracle) assuming the DBDHP problem is hard. In the unsigncryption phase, any $t-1$ or fewer recipients can not recover the k_2, thus they can not recover the message. It is difficult to compute D_{L_i} from $\tilde{y_i}$ since it is difficult to invert the bilinear mapping. Dishonest recipients can not cheat others by present incorrect $\tilde{y_i}$ since we use the checking procedure based on Baek and Zheng's zero knowledge proof for the equality of two discrete logarithms based on the bilinear map [2].

Public verifiability: Any third party can verify the signature by step 1 and 2 of **Unsigncryption**, so our scheme provides the public verifiability.

Forward security: Even though S_{ID_A} is revealed, any third party can not compute k_2' without the knowledge of D_{ID_L}. Therefore, our scheme provides the forward security.

4.3 Efficiency

We only consider the pairing, point multiplication and exponentiation computation and ignore other computation such as *hash* and (E, D). Let TP, TPM and TE be the time for computing pairing, point multiplication and exponentiation. The time complexity required by the signcrypter is $2TP + TPM + 2TE$. The time complexity required by each member in L' is $(2t+4)TP + TPM + (3t-1)TE$.

5 Conclusions

We have successfully integrated the design ideas of the ID-based signcryption scheme, the (t, n) threshold scheme and zero knowledge proof for the equality of two discrete logarithms based on the bilinear map, and have proposed an ID-based signcryption scheme with (t, n) shared unsigncryption. In the proposed scheme, any third party can verify the validity of the signature, but only more than t members in the recipient group can cooperatively recover the message m. As compared to the Zhang et al.'s signcryption scheme with (t, n) shared unsigncryption based on discrete logarithms, the proposed scheme has the following advantages: it provides both public verifiability and forward security; the key management problem is simplified because of using identity-based cryptosystem.

Acknowledgements

We would like to thank the anonymous reviewers for their valuable comments and suggestions. This research is supported by National Natural Science Foundation of China under contract no. 60473029.

References

[1] J. Baek, R. Steinfeld, and Y. Zheng, "Formal proofs for the security of signcryption," in *PKC 2002*, LNCS 2274, pp. 80-98, Springer-Verlag, 2002.

[2] J. Baek and Y. Zheng, "Identity-based threshold decryption," in *PKC 2004*, LNCS 294, pp. 262-2767, Springer-Verlag, 2004.

[3] F. Bao and R. H. Deng, "A signcryption scheme with signature directly verifiable by public key," in *PKC'98*, LNCS 1431, pp. 55-59, Springer-Verlag, 1998.

[4] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *CRYPTO 2001*, LNCS 2139, pp. 213-229, Springer-Verlag, 2001.

[5] S. S. M. Chow, S. M. Yiu, L. C. K. Hui, and K. P. Chow, "Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity," in *International Conference on Information Security and Cryptology (ICISC 2003)*, LNCS 2971, pp. 352-369, Springer-Verlag, 2003.

[6] X. Du, Y. Wang, J. Ge, and Y. Wang. "An ID-based broadcast encryption scheme for key distribution", *IEEE Transactions on Broadcasting*, vol. 51, no. 2, pp. 264–266, 2005.

[7] S. D. Galbraith, K. Harrison, and D. Soldera, "Implementing the Tate pairings," in *The Third International Workshop on Ant Algorithms (ANTS 2002)*, LNCS 2369, pp. 324-337, Springer-Verlag, 2002.

[8] F. Hess, "Efficient identity based signature schemes based on pairings," in *Selected Areas in Cryptography (SAC 2002)*, LNCS 2595, pp. 310-32, Springer-Verlag, 2003.

[9] X. Huang, W. Susilo, Y. Mu, and F. Zhang, "Identity-based ring signcryption schemes: cryptographic primitives for preserving privacy and authenticity in the ubiquitous world," in *19th International Conference on Advanced Information Networking and Applications (AINA'05)*, pp. 649-654, Taipei, Taiwan, 2005.

[10] H. Y. Jung, D. H. Lee, J. I. Lim, and K. S. Chang, "Signcryption schemes with forward secrecy," in *The Second Workshop Information Security Application (WISA 2001)*, pp. 463-475, Seoul, Korea, 2001.

[11] M. Kudo, "Secure electronic sealed-bid auction protocol with public key cryptography," *IEICE Transactions on Fundamentals*, vol. E81-A, no. 1, pp. 20-26, 1998.

[12] B. Libert and J. Quisquater, "A new identity based signcryption schemes from pairings," in *2003 IEEE*

Information Theory Workshop, pp. 155-158, Paris, France, 2003.

[13] J. Malone-Lee, "Identity based signcryption," *Cryptology ePrint Archive*, Report 2002/098, 2002. Available from: http://eprint.iacr.org/2002/098.

[14] J. Malone-Lee and W. Mao, "Two birds one stone: signcryption using RSA," in *Topics in Cryptology-CT-RSA 2003*, LNCS 2612, pp. 211-225, Springer-Verlag, 2003.

[15] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 24, no. 11, pp. 612-613, 1979.

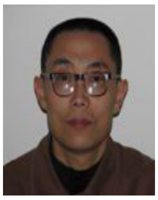
[16] A. Shamir, "Identity-based cryptosystems and signature schemes", in *CRYPTO'84*, LNCS 196, Springer-Verlag, pp. 47–53, 1984.

[17] R. Steinfeld and Y. Zheng, "A signcryption scheme based on integer factorization," in *The Third Information Security Workshop (ISW 2000)*, LNCS 1975, pp. 308-322, Springer-Verlag, 2000.

[18] Z. Zhang, C. Mian, and Q. Jin, "Signcryption scheme with threshold shared unsigncryption preventing malicious receivers," in *IEEE Region 10 Technical Conference on Computers, Communications, Control and Power Engineering (IEEE TENCON'02)*, pp. 196-199, Beijing, China, 2002.

[19] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) $\ll$ cost (signature) + cost(encryption)," in *CRYPTO'97*, LNCS 1294, Springer-Verlag, pp. 165-179, 1997.

Fagen Li received his B.S. degree from Luoyang Institute of Technology, Luoyang, P.R. China in 2001 and M.S. degree from Hebei University of Technology, Tianjin, P.R. China in 2004. He is now a Ph.D. candidate in Key Laboratory of Computer Networks and Information Security, Xidian University, Xi'an, P.R. China. His recent research interests include network security, mobile ad hoc network and cryptography.



Yupu Hu received his B.S. in Mathematics Science and Ph.D. degrees in Cryptography from Xidian University in 1987 and 1999, separately. He is now a professor in the School of Telecommunications Engineering, Xidian University. His recent research interests include network security and cryptography. He is the fellow of CIE and CIC.

Xiangjun Xin received his B.S. degree from Zhengzhou University, Zhengzhou, P.R. China in 1997 and M.S. degree from Xinyang Normal University, Xinyang, P.R. China in 2004. He is now a Ph.D. candidate in Key Laboratory of Computer Networks and Information Security, Xidian University; a lecturer in the Department of Information and Computing Science, Zhengzhou University of Light Industry, Zhengzhou, P.R. China. His recent research interests include cryptography and computer security.