2007 International Conference on Computational Intelligence and Security

Controlled Secret Leakage

Tianjie Cao, Shi Huang, Hui Cui, Yipeng Wu, Qihan Luo
School of Computer, China University of Mining and Technology, Xuzhou, 221116, China
tjcao@cumt.edu.cn

Abstract

How to leak authoritative secrets in an elegant way? The paper aims to solve this problem. The desired security properties i.e. Semantic-Security; Recipient-Designation; Verification-Dependence; Designated-Verifier Signature-Verifiability; Public Signature-Verifiability; Recipient-Ambiguity; Designated-Verifier Recipient-Verifiability; Public Recipient-Verifiability; Signer-Ambiguity; Signer-Verifiability are specified in secret leakage. Based on Chow-Yiu-Hui's ID-based ring signature scheme and techniques of zero-knowledge proof, an ID-based controlled secret leakage scheme is proposed. The proposed scheme satisfies all specified security properties and can be used in trust negotiation.

1. Introduction

The most common definition of privacy is the one by Westin: "Privacy is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others" [1]. According to Westin's definition, individuals as well as groups and institutions have a right to privacy. In a fully networked society, privacy is seriously endangered and cannot be sufficiently protected by privacy legislation. Cryptography technologies now are valuable tools for privacy protection in addition to privacy legislation.

We consider the following scenario of secret leakage [2]: If a police wants to arrest a criminal but knows few clues about him, so it promises to give an award to a person in some group who could provide the most important clue after the criminal is arrested. A group member Alice can provide something to a designated policeman Bob, but she is not sure whether her message could be the most important one. How to leak this clue in an elegant way? To protect the authoritative secret from propagating and anonymity of the member Alice and the policeman Bob, we propose controlled secret leakage scheme.

Trust negotiation is now wide used in electronic commerce [3]. In order for strangers to conduct secure transactions, a sufficient level of mutual trust must be established. Trust negotiation is an approach to establishing trust between strangers through the exchange of authoritative secrets. Thus, controlled secret leakage scheme can be used in trust negotiation.

Horster et al. first proposed an authenticated encryption scheme [4]. Authenticated encryption scheme aimed to achieve the purpose that the signature can only be verified by some specified recipients while keeping the message secret from the public.

Rivest et al. introduced the notion of a ring signature in the paper "How to leak a secret" [5]. Ring signature makes it possible to specify a set of possible signers without revealing which member actually produced the signature.

Lv et al. combined the two notations of ring signature and authenticated encryption together and obtained a new type of authenticated encryption, called ring authenticated encryption [2]. Ring authenticated encryption has the following security properties: semantic-security, recipient-designation, verification-dependence, verification-convertibility, recipient-ambiguity, recipient-verifiability, signer-ambiguity and signer-verifiability. In [2], Lv et al. also presented a ring authenticated encryption scheme based on discrete logarithm problem. In [6], Cao et al. found some weaknesses in Lv et al.'s scheme that Lv et al.'s scheme cannot achieve signer-verifiability and recipient-verifiability properties. Cao et al. also proposed an improved ring authenticated encryption scheme to eliminate these weaknesses.

Identity based public key cryptography proposed by Shamir in 1984 [7] can simplify key management and remove the necessity of public key certificates. This is desirable, especially for these applications which involve a large number of public keys in each execution, such as ring signatures. In [8], based on Boneh and Frankliny's ID-Based encryption scheme [9][10] and Zhang and Kim's ID-Based ring signature scheme [11] Cao et al. construct an ID-based ring authenticated encryption scheme.

0-7695-3072-9/07 $25.00 © 2007 IEEE
DOI 10.1109/CIS.2007.79

In 1985, Goldwasser et al. introduced the notion of zero-knowledge (ZK) proof [12]. A zero-knowledge proof is an interactive method for one party (the prover) to prove to another (the verifier) that a statement is true, without revealing anything other than the verity of the statement. An interactive proof usually takes the form of a challenge-response protocol, in which the prover and the verifier exchange messages and the verifier outputs either "accept" or "reject' at the end of the protocol. Zero-knowledge proofs have the following properties:

Completeness. The verifier always accepts the proof if the fact is true and both the prover and the verifier follow the protocol.

Soundness. The verifier always rejects the proof if the fact is false, as long as the verifier follows the protocol.

Zero-knowledgeness. The verifier learns nothing beyond the validity of the fact and cannot even later prove the fact to anyone else.

In this paper, our main contribution is to specify security properties of secret leakage, define controlled secret leakage scheme to protect the secret from propagating and anonymity of the participants, design an ID-based controlled secret leakage scheme.

2. Definitions

2.1. Definition of controlled secret leakage scheme

Definition 1: (Controlled secret leakage scheme). The controlled secret leakage scheme is specified by seven algorithms (protocols).

Signature Generation: The algorithm takes as input message M, the recipient *Bob*'s public key, the signer *Alice*'s private key and all the ring members' identity list L which includes the signer *Alice*, and outputs a ring signature S. The ring signature S will be published in Bulletin Board System (BBS) or send to the recipient *Bob*. We assume that anyone can intercept the signature S in transit.

Message Recovery and Verification: The algorithm takes as input a signature S and the recipient *Bob*'s secret key, outputs the authenticated message M and returns 1 or 0 meaning accept or reject the information that the signature S is created by a ring member, respectively. We require that the algorithm outputs the authenticated message M and returns 1 if the ring signature S is generated by the signer honestly.

Zero Knowledge Proof of a Ring Signature: Zero-knowledge proof of a ring signature is a method for the recipient *Bob* to prove to a verifier *Carol* that the message M is signed by a ring member listed in the ring set L without revealing any other information. Zero-knowledge proof can control the secret leakage and prevent secret propagation. The algorithm takes as input a signature S, a message M, the verifier's private key and a parameter Δ_1 that can only be computed by the recipient *Bob*, and outputs 1 or 0 meaning accept or reject the information that the signature S is really created by a ring member, respectively. We require that the algorithm 1 returns 1 if two parties do the protocol honestly.

Zero Knowledge Proof of Recipient: Zero-knowledge proof of recipient is an interactive method for the recipient *Bob* to prove to a verifier *Carol* that *Bob* is actually the designated recipient without revealing any other information. The algorithm takes as input a signature S, a message M, the verifier's private key and a parameter Λ_1 that can only be computed by the recipient *Bob*, and outputs 1 or 0 meaning accept or reject the information that the signature S is really sent to *Bob*, respectively. We require that the algorithm returns 1 if two parties do the protocol honestly.

Publicly Verifiable Proof of a Ring Signature: The algorithm takes as input a signature S, a message M and a parameter Δ_2 that can only be computed by the recipient *Bob*, and outputs 1 or 0 meaning accept or reject the information that the signature S is really created by a ring member, respectively. We require that the algorithm returns 1 if *Bob* does the protocol honestly.

Publicly Verifiable Proof of Recipient: The algorithm takes as input a signature S, a message M and a parameter Λ_2 released by *Bob*, and outputs 1 or 0 meaning accept or reject the information that the signature S is really sent to *Bob*, respectively. We require that the algorithm returns 1 if *Bob* is the real recipient.

Signer Verification: The algorithm takes as input the signature S and a parameter Σ produced when *Alice* creates the signature, and outputs 1 or 0 meaning accept or reject the information that *Alice* is the actual signer, respectively. We require that the algorithm returns 1 if the signature S is really produced by *Alice*. The algorithm should satisfy the condition that only the actual signer *Alice* could provide such a parameter Σ that makes it equal 1 corresponding to the certain signature S and that will not release the signer's private key.

2.2. Security properties of controlled secret leakage scheme

Definition 2: (Security properties of controlled secret leakage scheme). A controlled secret leakage scheme has the following security properties.

Semantic-Security: Any adversary cannot determine whether his guessed message is the actual message signed by the original signer, although he gets a valid signature.

Recipient-Designation: Only the designated recipient can recover the message and verify the ring signature.

Verification-Dependence: If the actual signer and the legal recipient do not reveal some parameters, any verifier cannot check the validity of the signature even though he gets the message and the corresponding signature.

Designated-Verifier Signature-Verifiability: A designated verifier can be convinced that the message M is signed by a ring member listed in the ring set L by the actual signer or the legal recipient, but the designated verifier is unable to convince anyone else of this fact.

Public Signature-Verifiability: Anyone can verify whether a ring signature is actually produced by at least one of the possible signers after the recipient reveals some parameters.

Recipient-Ambiguity: Anyone cannot know to whom a signature is sent while verifying its validity except the actual signer and the legal recipient.

Designated-Verifier Recipient-Verifiability: A designated verifier can be convinced who is actually the designated recipient by the legal recipient, but the designated verifier is unable to convince anyone else of this fact.

Public Recipient-Verifiability: Anyone can be convinced who is actually the designated recipient by the actual signer or the legal recipient.

Signer-Ambiguity: Anyone cannot determine the identity of the actual signer in a ring of size r with probability greater than $1/r$ if the actual signer is unwilling to expose himself.

Signer-Verifiability: The actual signer can prove to the recipient that it is he who actually signs the signature.

3. ID-Based Controlled Secret Leakage Scheme

Our scheme can be built from any bilinear map e: $\mathbf{G}_1 \times \mathbf{G}_1 \rightarrow \mathbf{G}_2$ between two groups $\mathbf{G}_1$, $\mathbf{G}_2$ as long as BDHP in $\mathbf{G}_1$ is hard and the DDHP in $\mathbf{G}_1$ is easy.

Setup: Let $(\mathbf{G}_1, +)$ and $(\mathbf{G}_2, \bullet)$ denote cyclic groups of prime order q, let P be a generator of $\mathbf{G}_1$ and the bilinear pairing is given as e: $\mathbf{G}_1 \times \mathbf{G}_1 \rightarrow \mathbf{G}_2$. Pick a random $s \in Z_q^*$ and set $P_{pub} = sP$. Choose cryptographic hash function H: $\{0, 1\}^* \rightarrow Z_q^*$, H_1: $\{0, 1\}^* \rightarrow \mathbf{G}_1^*$, H_2: $\mathbf{G}_2 \rightarrow \{0, 1\}^n$, H_3: $\{0, 1\}^n \times \{0, 1\}^n \rightarrow Z_q^*$ and H_4: $\{0, 1\}^n \rightarrow \{0, 1\}^n$. Choose a pseudorandom generator F: $\{0, 1\}^n \rightarrow \mathbf{G}_1$. The message space is $\mathbf{M} = \{0, 1\}^n$. The **master-key** is $s \in Z_q^*$.

Extract: For a given string $ID \in \{0, 1\}^*$ the PKG computes $Q_{ID} = H_1(ID)$, and sets the private key d_{ID} to be $d_{ID} = sQ_{ID}$ where s is the master key.

Signature Generation: Let ID_i be a ring member's identity, and d_{ID_i} be the private key associated with ID_i for $i = 0, 1, \ldots, N-1$, where N is the measure of the anonymity set. Let $L = \{ID_i: 0 \le i \le N-1\}$ be the set of identities. The real signer *Alice*'s identity ID_{Alice} is ring member ID_k listed in L.

Step 1. To sign a message $M \in \{0, 1\}^n$, the signer, *Alice* say, who knows the identity ID_{Bob} of the recipient *Bob*, whose corresponding secret key is $d_{ID_{Bob}}$. Using Boneh-Frankliny's ID-based encryption scheme [9][10] *Alice* encrypts M under the public key ID_{Bob}.

Compute $Q_{ID_{Bob}} = H_1(ID_{Bob}) \in \mathbf{G}_1^*$,

- Choose a random $\sigma \in \{0, 1\}^n$,
- Set $r = H_3(\sigma, M)$,
- Set the ciphertext of M to be $<U, V, W>$: $U = rP$, $V = \sigma \oplus H_2(g_{ID_{Bob}}^r)$ and $W = M \oplus H_4(\sigma)$ where $g_{ID_{Bob}} = e(Q_{ID_{Bob}}, P_{pub}) \in \mathbf{G}_2$.

Step 2. Choose a random $r_1 \in Z_q^*$, and compute $X = r_1 P$, $Y = g_{ID_{Bob}}^{r_1}$ and $Z = H(U \| V \| W \| M \| X \| Y)$.

Step 3. To sign Z *Alice* utilizes Chow-Yiu-Hui's ID-based ring signature scheme [13].

- Choose a random seed $A \in \{0, 1\}^n$, for $i = k + 1, \ldots, N-1, 0, 1, \ldots, k-1$(i.e., the value of i all modulo N), compute $A_i = F((A + i - k) \bmod N)$, and $h_i = H(Z, L, A_i)$.
- Choose a random integer $r' \in Z_q^*$, compute $A_k = r' Q_{ID_k} - \sum_{i \neq k} (A_i + h_i Q_{ID_i})$.
- Compute $h_k = H(Z, L, A_k)$ and $c = (h_k + r') d_{ID_k}$ where $d_{ID_k} = d_{ID_{Alice}}$.
- Choose a random $r_2 \in Z_q^*$, and compute $X_1 = r_2 P$, $Y_1 = g_{ID_{Bob}}^{r_2}$ and $c_1 = c + H_1(Y_1)$.
- Select 0 (i.e., N) as the glue value, the resulting ring signature S is the $(N + 7)$-tuple $(L, U, V, W, X, A_0, \ldots, A_{N-1}, X_1, c_1)$.

Step 4. Finally, *Alice* sends S to the recipient *Bob* and keeps the seed A secret. An adversary can intercept S in this step.

Message Recovery and Verification: After receiving the signature $S = (L, U, V, W, X, A_0, \ldots, A_{N-1}, X_1, c_1)$, the recipient *Bob* does the following.

Step 1. If $U \notin \mathbf{G}_1^*$ reject the signature.

- Compute $\sigma = V \oplus H_2(e(d_{ID_{Bob}}, U))$.
- Compute $M = W \oplus H_4(\sigma)$.
- Set $r = H_3(\sigma, M)$. Test that $U = rP$. If not, reject the signature.

Step 2. Compute $Y = e(d_{ID_{Bob}}, X)$ and $Z = H(U \| V \| W \| M \| X \| Y)$.

Step 3. Compute $Y_1 = e(d_{ID_{Bob}}, X_1)$ and $c = c_1 - H_1(Y_1)$.

Step 4. The validity of the signature is verified by checking that $h_i = H(Z, L, A_i)$ $(0 \le i \le N-1)$ and that

$$e(P, c) = e(P_{pub}, \sum_{i=0}^{N-1}(A_i + h_i Q_{ID_i}))$$

Zero Knowledge Proof of a Ring Signature: If *Bob* (or the signer *Alice*) wants to prove to any designated verifier *Carol* that the message M is signed by a ring member listed in L without revealing any other information, they can do as follows.

Step 1. *Bob* computes $W_1 = e(Q_{ID_{Carol}}, c)$ and sends the message M, the parameter Y and the parameters $(L, U, V, W, X, A_0, \ldots, A_{N-1}, W_1)$ to *Carol*.

Step 2. *Carol* computes $Z = H(U \| V \| W \| M \| X \| Y)$. *Carol* can be convinced that the message M is signed by a ring member listed in L if $h_i = H(Z, L, A_i)$ $(0 \le i \le N-1)$ and $W_1 = e(d_{ID_{Carol}}, \sum_{i=0}^{N-1}(A_i + h_i Q_{ID_i}))$.

Zero Knowledge Proof of Recipient: If *Bob* wants to prove to any designated verifier *Carol* that the signature S is actually sent to *Bob* without revealing any other information, they can do as follows:

Step 1. *Bob* chooses a random nonce $r_3 \in \{0, 1\}^n$ and computes $W_1 = e(Q_{ID_{Carol}}, c)$.

Step 2. *Bob* sends the message M, the nonce r_3, the parameter Y and the parameters $(L, U, V, W, X, A_0, \ldots, A_{N-1}, W_1)$ to *Carol*.

Step 3. *Carol* computes $Z = H(U \| V \| W \| M \| X \| Y)$. *Carol* can be convinced that the message M is signed by a ring member listed in L if $h_i = H(Z, L, A_i)$ $(0 \le i \le N-1)$ and $W_1 = e(d_{ID_{Carol}}, \sum_{i=0}^{N-1}(A_i + h_i Q_{ID_i}))$.

Otherwise, terminate the protocol.

Step 4. *Carol* chooses random integers $r_4, r_5, r_6 \in Z_q^*$, and computes $T_1 = r_4 P + r_5 X$, $U_1 = r_6 Q_{ID_{Carol}}$, $V_1 = (r_6 + H(r_3, T_1, U_1)) d_{ID_{Carol}}$. *Carol* sends (T_1, U_1, V_1) to *Bob*. Here to sign (r_3, T_1) *Carol* utilizes Cha-Cheon's ID-based signature scheme [14].

Step 5. *Bob* checks the freshness of r_3 and the validity of the signature of (r_3, T_1) by checking whether $(P, P_{pub}, U_1 + H(r_3, T_1, U_1) Q_{ID_{Carol}}, V_1)$ is a valid Diffie-Hellman tuple.

Step 6. *Bob* computes $W_2 = H(e(d_{ID_{Bob}}, T_1))$ and then sends W_2 to *Carol*.

Step 7: *Carol* checks whether $W_2 = H(g_{ID_{Bob}}^{r_4} \cdot Y^{r_5})$ where $g_{ID_{Bob}} = e(Q_{ID_{Bob}}, P_{pub})$. Only if they hold does *Carol* accept that the signature is sent to *Bob*.

Publicly Verifiable Proof of a Ring Signature: If *Bob* (or the signer *Alice*) wants to prove to any verifier that the message M is signed by a ring member listed in L, they can do as follows.

Step 1. *Bob* publishes the message M, the parameter Y and the parameters $(L, U, V, W, X, A_0, \ldots, A_{N-1}, c)$.

Step 2. The verifier computes $Z = H(U \| V \| W \| M \| X \| Y)$. The validity of the ring signature is verified by checking that $h_i = H(Z, L, A_i)$ $(0 \le i \le N-1)$ and that

$$e(P, c) = e(P_{pub}, \sum_{i=0}^{N-1}(A_i + h_i Q_{ID_i})).$$

Publicly Verifiable Proof of Recipient: If *Bob* (or the signer *Alice*) wants to prove to any verifier that the signature S is actually sent to *Bob*, they can do as follows:

Step 1. *Bob* publishes the message M, the parameter Y, σ and the parameters $(L, U, V, W, X, A_0, \ldots, A_{N-1}, c)$.

Step 2. The verifier computes $Z = H(U \| V \| W \| M \| X \| Y)$. The validity of the ring signature is verified by checking that $h_i = H(Z, L, A_i)$ $(0 \le i \le N-1)$ and that

$$e(P, c) = e(P_{pub}, \sum_{i=0}^{N-1}(A_i + h_i Q_{ID_i})).$$

Otherwise, terminate the protocol.

Step 3. The verifier does the following.

- Compute $Q_{ID_{Bob}} = H_1(ID_{Bob})$,
- Set $r^* = H_3(\sigma, M)$,
- Compute $U^* = r^* P$, $V^* = \sigma \oplus H_2(g_{ID_{Bob}}^{r^*})$ and $W^* = M \oplus H_4(\sigma)$ where $g_{ID_{Bob}} = e(Q_{ID_{Bob}}, P_{pub})$.

Step 4: The verifier checks whether $U^* = U$, $V^* = V$, and $W^* = W$. Only if they hold does the verifier accept that the signature is sent to *Bob*.

Signer Verification: The actual signer *Alice*'s identity ID_{Alice} is a ring member listed in L. If *Alice* is willing to prove to the recipient *Bob* that she actually leaked the message M, then she does the following.

Step 1. *Bob* verifies that the signature $S = (L, U, V, W, X, A_0, \ldots, A_{N-1}, X_1, c_1)$ is sent to him. The method is same as Message Recovery and Verification.

Step 2. *Alice* sends the seed A and her identity ID_{Alice} to *Bob*.

Step 3. For $i = k + 1, \ldots, N - 1, 0, 1, \ldots, k - 1$, compute $A_i^* = F((A + i - k) \bmod N)$ and checks if $A_i^* = A_i$. If they all hold, then *Bob* convinces that *Alice* is the real signer. Reject, otherwise.

4. Conclusion

In this paper, we defined secret leakage scheme which consist of seven procedures to protect the secret from propagating and anonymity of the participants. We also specified ten security properties of secret leakage scheme. At last, based on Chow-Yiu-Hui's ID-based ring signature scheme and techniques of zero-knowledge proof we construct an ID-based controlled secret leakage scheme. The proposed scheme satisfies all security properties. And can be used to establish trust in electronic commerce applications.

Acknowledgment

This work was supported by the Natural Science Foundation of Jiangsu Province (No. BK2007035), the Science and Technology Foundation of CUMT, and the Student Science Research Project of Jiangsu Province.

References

[1] A. Westin, Privacy and Freedom, New York, Atheneum, 1967.

[2] J. Lv, K. Ren, X. Chen and K. Kim, Ring Authenticated Encryption: A New Type of Authenticated Encryption, SCIS 2004, The 2004 Symposium on Cryptography and Information Security, Sendai, Japan, Jan.27-30, 2004, pp.1179-1184.

[3] Elisa Bertino, Elena Ferrari, Anna Squicciarini. Trust Negotiations: Concepts, Systems, and Languages, Computing in Science and Engineering, vol. 06(4), pp. 27-34, 2004.

[4] P.Horster, M.Michels and H.Petersen, Authenticated Encryption Schemes with Low Communication Costs. Electronics Letters, 30(15), 1994, pp.1212-1213.

[5] R.L.Rivest, A.Shamir and Y.Tauman, How to Leak a Secret. Advances in Cryptology- ASIACRYPT2001, LNCS 2248, Springer-Verlag, 2001, pp.257-265.

[6] T. Cao, D. Lin and R. Xue. Improved Ring Authenticated Encryption Scheme, In Proceedings of Tenth Joint International Computer Conference, International Academic Publishers World Publishing Corporation, 2004, pp.341-346.

[7] A. Shamir, Identity-based cryptosystems and signature schemes, Advances in Cryptology-Crypto 84, LNCS 196, Springer-Verlag, 1984, pp.47-53.

[8] T. Cao, D. Lin and R. Xue. ID-based Ring Authenticated Encryption. In Proceedings of 19th International conference on Advanced Information Networking and Applications, IEEE Computer Society, pp591-596, 2005

[9] D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, Advances in Cryptology-Crypto 2001, LNCS 2139, Springer-Verlag, 2001, pp.213-229.

[10] D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, SIAM Journal on Computing, 32(3), 2003, pp.586-615.

[11] F. Zhang and K. Kim, ID-Based Blind Signature and Ring Signature from Pairings, Asiacrpto02, December 1-5, Queenstown, New Zealand, LNCS 2501, Springer-Verlag, 2002, pp. 533-547.

[12] S. Goldwasser, S. Micali, and C. Rackoff. Knowledge Complexity of Identification Proof Schemes. In 17th ACM Symposium on the Theory of Computing STOC, pp 291–304. SACM, 1985.

[13] Sherman S.M. Chow, Siu-Ming Yiu, and Lucas C.K. Hui, Efficient Identity Based Ring Signature, Applied Cryptography and Network Security, Third International Conference, ACNS 2005, LNCS 3531, Springer-Verlag, pp.499-512

[14] JC Cha, JH Cheon, An Identity-Based Signature from Gap Diffie-Hellman Groups, Practice and Theory in Public Key Cryptography - PKC'2003, LNCS 2567, Springer-Verlag 2003, pp. 18-30.