Threshold Anonymous Credential System

KARYIN FUNG [1], TONY K. CHAN [1], JOSEPH K. LIU [1] AND DUNCAN S. WONG [2]
Department of Information Engineering [1]
The Chinese University of Hong Kong,
HONG KONG
Department of Computer Science[2]
City University of Hong Kong
HONG KONG

Abstract: - A credential system enables a person to identify themselves by their pseudonyms while their privacy is protected. Our scheme preserves the properties in credential system: unforgeability and unlinkability. In practical applications, more than one organization may be needed to issue a valid credential while their identities should be protected. Our construction based on *t*-out-of-*n* threshold blind ring signatures can maintain the requirements of a credential system as well as privacy to the organizations. Transferability of a credential from an organization is retained so that different pseudonyms can be converted into single pseudonym in a *t*-out-of-*n* threshold credential.

Keywords: Blind Ring Signature, Credential System, Threshold

1 Introduction

Credential system is a system in which users can obtain credentials from organizations and demonstrate its possession of these credential while preventing cooperation among organizations from monitoring their activities. In order to protect the privacy of an individual, a system may grant its access based on pseudonym only. Its key features: Unforgeability and Unlinkability, were first studied by David Chaum [11]. Blind signature [6] is an interactive protocol between two parties, namely user and signer, to create a valid signature but the content is unknown to the signer. The signer is unable to figure out the order of two signatures that are signed by it. Ring Signature [5,3] (Spontaneous Anonymous Group(SAG) Signature [4] in some literatures), allows an entity with a set of public keys including its own to generate a signature. Entities except the actual signer are unaware of it. On receiving the signature, verifier is unable to find out the signer.

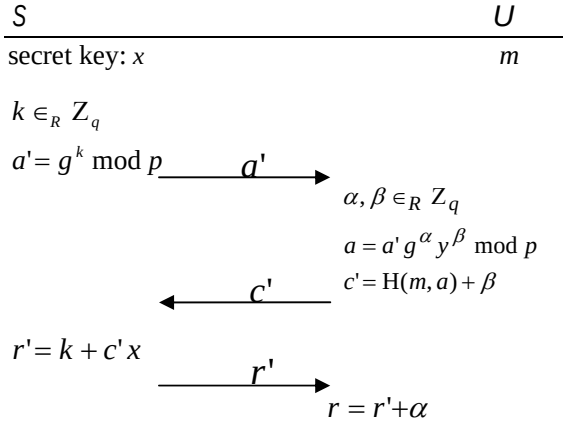
Blind ring signature is a combination of blind signature and ring signature such that blindness and signer-ambiguity are maintained. In [4], Chan, et al. proposed its notion and framework of constructing blind ring signature by any proven secure blind signatures.

1.1 Our contributions

We build a credential system extended from Chen [1] by using *t*-out-of-*n* CDS-type [5] ring signature and Schnorr blind signature. In our system, there are *n* organizations to issue a credential while their identities are protected by signer-ambiguity. Privacy and untraceability are still maintained by the nature of blind signature. The credential showing the user having credentials in *t* out of *n* organizations. Transferability in [1]'s work is remained and all pseudonyms used are unlinkable. This paper is organized as follows. We briefly go through related work and security definitions in Sec. 2. Our main protocol and security proofs are described in Sec. 3 and 4 respectively. After all, open problems are discussed in the last section.

2 Related Work and Definitions

Blind Signature The notion and the properties of blind signature were introduced by Chaum [6]. We now briefly review Schnorr blind signature: Let $G = \langle g \rangle$ be a group modulus prime p by a generator, g with a prime order, q. Let (y, x) be the public and private key of the signer S. User, U requests to sign on the message, m. Let H: $\{0,1\}^* \rightarrow Z_q$ is a hash function.



Signature on m is (c, r).

Fig. 1 Schnorr Blind Signature

CDS-type Blind Ring Signature Blind ring (SAG in original paper) signature [4] is an idea extended from SAG signature from [5] also contains

several properties comparing with traditional blind signature.

1. Blindness: Signer obtains no information about the message during and after the protocol.
2. Signer-ambiguity: except the user, other parties including the signer, cannot find out the actual signers of the signature.
3. Spontaneity: the set of signers are chosen by the user arbitrarily and in general, the public key does not include the user. No setup stage is needed and no group manager gets involved in preprocessing phase.

Definition 1 *(Unforgeability): A scheme is parallel one-more unforgeable against adaptive chosen plaintext, adaptive chosen public-key adversaries, provided that the blind signature is parallel one-more unforgeable by adaptive chosen-plaintext, adaptive chosen public-key, discrete logarithm and ROS problem [9] is hard.*

Definition 2 *(Unlinkability): A credential mechanism is unlinkable if given two pseudonyms and one identity of individual, any polynomial adversary cannot reveal about either the connection between his identity and any of his pseudonyms, or the connection between any of his two different pseudonyms, is information-theoretic minimum.*

Definition 3 *(Signer Ambiguity): A credential mechanism satisfies signer ambiguity if for all probabilistic polynomial time adversaries* A*, security parameter* k*, for all threshold credential, public keys of legitimate issuer list L and actual issuer list* B*, the probability that the adversary output a actual issuer is equal to:*

$$\Pr[O_i \leftarrow A(\sigma) : O_i \in B] \le \frac{|B|}{|L|} + \varepsilon(k) \qquad (1)$$

where ε *is a negligible function.*

Definition 4*: (Collision Property) There exists a polynomial-time algorithm that computes secret key from public key from two accepting conversations (r,c,s) and (r,c',s') where (c,s)≠ (c',s').*

3 Main Protocol

There are three processes: validating process, issuing and transferring process, and three parties involved in these processes: trusted center *C*, organizations $\{O_i : i \in Z^+\}$ and individual *I*. *C* works as a notary office to validate a pseudonym in the correct format. After the validation, *I* has different pseudonym U_i in different organizations O_i. Each O_i issues some types of credential. For $i = 1,...,n$, let (y_i, x_i) be the public and private keys of O_i and *L* be the public key set of *n* organizations. Let (ψ,χ) be the public / private key pair of trusted center, *C*, where $\psi = g^{\chi} \bmod p$. We denote *I* as the individual and U_i as the pseudonym registered for O_i. Let $H: \{0,1\}^* \rightarrow Z_q$ be a secure hash function.

3.1 Validating Protocol

I obtains a pseudonym and a signature on this from trusted Center *C*. *I* registers its pseudonym U_i associated with its unique identification number $u \in G$ stored in *C*. Meanwhile, *C* has to verify that the pseudonym is constructed correctly such that it is in the format of $U_i = ug^{s_i} \bmod p$, s_i is a secret.

Step 1: *C* finds a unique identification number, *u* to the individual *I*.

Step 2: For $i = 1,\ldots,n$, *I* randomly selects s_i and computes pseudonym corresponding to O_i

$$U_i = ug^{s_i} \bmod p \qquad (4)$$

Step 3: For $i = 1,\ldots,n$, *I* requests *C* a blind signature on U_i using the protocol in *Fig.*1.

$$\sigma_{\chi}(U_i) = (V_i, d_i, e_i, h_i) \qquad (5)$$

s.t. $g^{h_i} = d_i \psi^{\varepsilon_i}$ and $U_i^{h_i} = e_i V_i^{\varepsilon_i}$ where $\varepsilon_i = H(U_i, V_i, d_i, e_i)$.

Step 4: For $i = 1,\ldots,n$, stores *C* valid pseudonyms in the form of (U_i, V_i).

Remarks: assume *C* uses the same secret key for *all*.

3.2 Issuing Protocol

Let B be the set of *t* organizations participated in signing a credential to the individual, *I*. For each $O_i \in B$, it signs U_i as

$$\sigma_{x_i} = (Z_i, \overline{a_i}, \overline{b_i}, \overline{r_i}) \qquad (6)$$

s.t. $g^{\overline{r_i}} = \overline{a_i} y_i^{\overline{c_i}}$ and $U_i^{\overline{r_i}} = \overline{b_i} Z_i^{\overline{c_i}}$ where $\overline{c_i} = H(U_i, Z_i, \overline{a_i}, \overline{b_i})$.

3.3 Transferring Protocol

I shows his *t*-out-of-*n* credential associated another pseudonym $U_{(t,n)}$ such that *I* has membership in *t* organizations. To show $O_{(t,n)}$ that it obtains a signature from O_i on pseudonym $U_{(t,n)}$

$$U_{(t,n)} = U_i g^{(s_{(t,n)} - s_i)} \qquad (2)$$

$$Z_{(t,n),i} = Z_i y_i^{(s_{(t,n)} - s_i)} = U_{(t,n)}^{x_i} \qquad (3)$$

It requests *t* organizations to conduct a blind signature protocol. Then *I* transfers the signature on pseudonym U_i in organization O_i to pseudonym, $U_{(t,n)}$ used in $O_{(t,n)}$:

Step 1: For $O_i \notin B$, I randomly picks $Z_{(t,n),i} \in G$ and $r_i, c_i \in Z_q$, and computes $a_i = g^{r_i} y_i^{c_i}$ and $b_i = U_{(t,n)}{}^{r_i} Z_{(t,n),i}^{c_i}$

Step 2: For $O_i \in B$, I requests a blind signature from O_i

Step 2.1: O_i randomly selects k_i and returns $a_i' = g^{k_i}$ and $b_i' = U_i^{k_i}$.

Step 2.2: I randomly selects α_i, β_i in Z_q and computes $a_i = a_i' g^{\alpha_i} y_i^{\beta_i}$ and $b_i = b_i' U_{(t,n)}{}^{\alpha_i} Z_{(t,n),i}^{\beta_i} a_i'^{(s_i - s_{(t,n)})}$

Step 3: I constructs a polynomial of degree no greater than $(n-t)$ by interpolation s.t.

$$f(0) = H(L, U_{(t,n)}, (a_1, b_1, Z_{(t,n),1}), ..., (a_n, b_n, Z_{(t,n),n})) \quad (11)$$

and $f(i) = c_i, \quad O_i \notin B$

Step 4: For $O_i \in B$, I computes $c_i = f(i)$ and sends $c_i' = c_i + \beta_i$ to O_i.

Step 5: On receiving c_i', $O_i \in B$ returns $r_i' = k_i - c_i' x_i$.

Step 6: I computes $r_i = r_i' + \alpha_i$ for O_i.

The credential on pseudonym $U_{(t,n)}$ is

$$(L, (a_1, b_1, Z_{(t,n),1}, r_1), ..., (a_n, b_n, Z_{(t,n)n}, r_n), f)$$

Verification Algorithm

I shows the credential of $U_{(t,n)}$ to $O_{(t,n)}$. The organization performs the following algorithm to verify the credential:

Step 1 For $i = 1, \ldots, n$, $O_{(t,n)}$ compute $c_i = f(i)$.

Step 2 $O_{(t,n)}$ verifies

If $f(0) = H(L, U_{(t,n)}, (a_1, b_1, Z_{(t,n)1}), ..., (a_n, b_n, Z_{(t,n)n}))$

accept; Otherwise, **reject**.

4 Security Proofs of Our Scheme

Our unforgerability proof of our scheme follows a similar fashion in [4, 10].

Theorem 5: Assume our model, which includes the random oracle model and generic model, simulates the adversary with negligible statistical distance. Our scheme is parallel one-more unforgeable against adaptive chosen plaintext, adaptive chosen public key adversaries, provided that discrete logarithm and ROS problem [9] are hard.

Proof (Sketch): [Signing Oracle Simulation]

1. Select (n - t)-degree polynomial f randomly. For each blind signature, I randomly chooses r_i and computes $c_i = f(i)$, $a_i = g^{r_i} y_i^{c_i}$ and $b_i = U_{(t,n)}{}^{r_i} Z_{(t,n),i}^{c_i}$. Set $f(0) = H(L', U'_{(t',n')}, (a_1', b_1', Z'_{(t.n),1}), ..., (a_n', b_n', Z'_{(t.n),n})$
2. Output $(L, (a_1', b_1', Z_1', r_1'), ..., (a_n', b_n', Z_n', r_n'), f)$

[Transfer Prover Oracle TP and Transfer Anonymizer Oracle TA]

1. Forger A requests a blind signature on y_π.
2. TA requests blind signature for $y_i \in L$ to TP.
3. TP commits (a_i, b_i) for each i to TA. TA relays only (a_π, b_π) to A.
4. When A follows up the blind signature with challenge c_π', TA picks c_i' for each $i \neq \pi$ and relays all c_i' to TP.
5. TP returns responses r_i' for each i to TA.
6. TA relays only r_π' to A.

[Witness Extraction and Simulation the Transfer prover oracle]

Dealer D gives n discrete log problem instances $L = \{y_i : i = 1, \ldots, n\}$ to a probabilistic polynomial time simulator M and request M to solve at least one of them.

1. M runs an existential forger A with input (L, U, t) and obtain a forged (t, n)-threshold credential $(L, (a_1, b_1, Z_1, r_1), .., (a_n, b_n, Z_n, r_n), f)$
2. M answers queries at most Q_H times. At q-th query, it replies by $f(0)$ and rewinds to reply by assigning a new value $f(0)'$
3. A returns another blind threshold credential $(L, (a_1, b_1, Z_1', r_1'), .., (a_n, b_n, Z_n', r_n'), f)$,
4. M computes at most t secret keys $\{x_i \mid x_i = \log_g y_i, y_i \in L\}$ by collision property.

By theorem assumption and the results in [9] that ROS problem is hard, therefore, M must have computed a blind signature concerning public key x_π which is never involved in any TP queries. There is non-negligible probability that M rewinds to the challenge of that blind signature.

$$(Z_\pi, (a_\pi, b_\pi), c_\pi, r_\pi) : g^{r_\pi} = a_\pi y_\pi^{c_\pi} \text{ and } U^{r_\pi} = b_\pi Z_\pi^{c_\pi}$$

$$(Z_\pi, (a_\pi, b_\pi), c_\pi', r_\pi') : g^{r_\pi'} = a_\pi y_\pi^{c_\pi'} \text{ and } U^{r_\pi'} = b_\pi Z_\pi^{c_\pi'}$$

Therefore $\log_g y_\pi = \frac{r' - r}{c - c'}$. This is the answer to D's question

Theorem 6: Our scheme satisfies unlinkability even if the center and some organizations collude.

Proof: For any two pseudonyms $U_1 = u_1 g^{s_1}$ and $U_2 = u_2 g^{s_2}$, with uniformly distributed random variable s_1 and s_2, U_1 and U_2 are uniformly distributed and indistinguishable. So it does not reveal any information about u.

Theorem 7: Our scheme is computationally signer-ambiguous in random oracle model provided that the Discrete Logarithm and Decisional Diffie-Hellman (DDH) problem are hard

Proof: M is a polynomial time algorithm that solves t $(\omega_i, \tau, \zeta_i)$, $i \in \{1,...,t\}$ DDH problem and the set of public key $y_i = \omega_i$ and denotes the set of organizations by DDH. Using a probabilistic polynomial time algorithm A, given a *(t, n)*-threshold credential, outputs t organizations O_j' s.t. $O_j' \in B$ with probability no less than $t/n + 1/Q(k)$, Q is a polynomial, k is security parameter. Suppose M is given *(N - t)* organizations denoted by TP with key pair (y_i, x_i), and remaining t *are set as* (ω_i, x_i), $x_i \in_R Z_q$. A set of N public keys is denoted as Y. Once M receives query a *(t', n')* credential on organization set J', $J' \subseteq Y$, $|J'| = n'$, $t' \le n'$. L' be the list of n' public keys. It simulates the following way:

1. Generates a polynomial f, of degree smaller than $n - t$ and set $c_i = f(i)$. Randomly picks $U_{(t',n')}$, $U_{(t',n')} \in G$. Randomly selects a set of t' organizations, B'. If $O_i \in B' \cap TP$, then M initiates a blind signature with O_i to obtain $Z_{(t,n),i}, r_i$. Otherwise, it generates $Z_{(t,n),i} = U_{(t,n)}^{x_i}$ for $O_i \in B' \cap DDH$.
2. Randomly generates $Z_{(t,n),i}$, for $O_i \in J'\text{-}B'$
3. Generates s_i randomly for $O_i \in J' - TP$.
4. Set

$$f(0) = H(L', U_{(t',n')}', (a_1', b_1', Z_{(t.n),1}'), ..., (a_{n'}', b_{n'}', Z_{(t.n'),n'}'))$$

After finishing running q_s times, A chooses n-element subset J of Y. If $DDH \not\subset J$, M halts. Otherwise, set $U_{(t,n)} = \tau$, $Z_{(t.n),i}' = \zeta_i$, for $O_i \in DDH$. The simulation of hash function is same as above.

Then A outputs t organizations, $t \le n$. M outputs *1* if A identifies and outputs organizations in DDH; Otherwise 0. Suppose M outputs *0/1* with equal probability if A cannot identify any organizations in one guess.

Success probability of M on each A guess.

$$\begin{aligned} &= \Pr[M(\omega_i, \tau_i, \zeta_i) = b \mid b = 1] \\ &\quad + \Pr[M(\omega_i, \tau_i, \zeta_i) = b \mid b = 0] \\ &\ge [(k/n + Q(k)) + (1/2(1 - k/n - Q(k)))] \\ &\quad + [0 \cdot (k/n) + 1/2(1 - k/n)] \\ &= 1/2 + 1/(4Q(k)) \end{aligned}$$

5 Conclusion and Open Problems

Our credential system is the first threshold credential system such that an individual can show its membership of more than one organization at one time. It is interesting to extend our one-time show to multi-show in the future. Our scheme provides computational signer-ambiguity to protect identity of the signer. We are welcome to foresee unconditional signer-ambiguity in the future.

References:

[1] L. Chen, Access with Pseudonyms, *Cryptography: Policy and Algorithms*, LNCS No.1029, 1996, pp. 232-243.

[2] J. Camenisch and A. Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. *EUROCRYPT 2001*, pp. 93-118. Springer, 2001.

[3] R. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. *ASIACRYPT 2001*, pp. 552-565. Springer, 2001. LNCS 2248.

[4] T. Chan, K. Fung, J. Liu and V. Wei, Blind Spontaneous Anonymous Group Signatures for Ad-Hoc Groups, *Accepted by ESAS*2004, 2004.

[5] R. Cramer, I. Damgard, and B. Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. *CRYPTO 94*, pp. 174-187. Springer, 1994. LNCS 839.

[6] D. Chaum. Blind signatures for untraceable payments. *CRYPTO 82*, pp. 199-203, 1982

[7] D. Chaum. Security without identification: transaction systems to make big brother obsolete. *CACM*, 29(10):1030-1044, 1985.

[8] D. Pointcheval and J. Stern. Provably secure blind signature schemes. *ASIACRYPT 96*, pp. 252-265. Springer, 1996. LNCS 1163.

[9] C. P. Schnorr. Security of blind discrete log signatures against interactive attacks. In *ICICS*. Springer-Verlag, 2001. LNCS 2229.

[10] M. Abe, M. Ohkubo and K. Suzuki. Efficient threshold signer-ambiguous signatures from variety of keys. *IEICE Trans. Fundamental, vol. E87A, pages 471-479*. No. Feb., 2004.

[11] D. Chaum. Security without identification: transaction systems to make big brother obsolete. *Commun. ACM*, vol. 28, No. 10, pages 1030-1044. ACM Press 1985