The Identity Escrow (Group Signature) Scheme at CT-RSA'05 Is Not Non-frameable

Sujing Zhou, Dongdai Lin
SKLOIS Lab, Institute of Software,
Chinese Academy of Sciences, 100080, Beijing , P.R. China.
Email: {zhousujing,ddlin}@is.iscas.ac.cn

Abstract

Following an attack against exculpability, put forward on Asiacrypt'06, of ACJT's group signature, we further found Nguyen's identity escrow (group Signature) scheme did not satisfy non-frameabiliy either.

Keywords: Group Signature, Identity Escrow, Bilinear Pairing.

1 The Attack

The attack [1] breaks exculpability of ACJT scheme [2](please refer to Appendix A for a review): GM can forge a valid group signature of member i (represented by A_i) on the condition that $t = \log_{a_0} a$ is known to itself.

In fact there exists another attack: let $\hat{e} = k_1\phi(n)$, $\hat{x} = -t^{-1} + k_2\phi(n)$ (select appropriate k_1, k_2 so that $\hat{e} \in \Gamma$, $\hat{x} \in \Lambda$), then $A_i^{\hat{e}} = a^{\hat{x}}a_0$. GM can generate group signatures on behalf of A_i using $(\hat{e}, \hat{x})$.

To foil the attacks, i is better represented by a^{x_i} rather than A_i, as in a new version (unpublished) of ACJT scheme where $T_1 = A_i h^w$, $T_2 = g^w$, $T_3 = a^{x_i} y^w$.

We examined the identity escrow (group signature) scheme of [3], and found that a similar attack exist against the non-frameability, i.e., an adversary who even knows the opening key and the issuing key is not able to impersonate an honest member to pass the membership authentication (forge a valid group signature of an honest member).

GM—who knows the issuing key (x, s) that $P_{pub} = xP$, $Q_{pub} = sQ$—can choose $P_0 = t^{-1}P$, then set $\hat{a_i} = -x$, $\hat{x_i} = -t^{-1}$, and calculate $W_{i,j} = (s - x)^{-1}V_j$ (V_j is the published accumulator). It is evident that $e(\hat{a_i}P + P_{pub}, S_i) = e(\hat{x_i}P + P_0, P)$, and $e(\hat{a_i}Q + Q_{pub}, W_{i,j}) = e(Q, V_j)$ then of course GM can impersonate S_i (generate group signatures on behalf of S_i).

The reason for this attack successful is because member i is represented by S_i instead of x_iP.

2 Review of the Identity Escrow (Group Signature) with Membership Revocation [3]

The original [3] was found flawed [4], we follow the modified version of [3].

It begins by choosing security parameters l, as well as a collision resistent Hash function $\mathrm{H} : \{0,1\}^* \rightarrow \mathrm{Z_p}$,and a bilinear map $e : G_1 \times G_1 \rightarrow G_M$, $ord(G_M) = p, G_1 = \langle P \rangle$.

GKg. GM randomly chooses $x, s, x' \in Z_p^*, P_0, G, H \in_R G_1$, computes $P_{pub} = xP, \Theta = e(G,G)^{x'}, Q_{pub} = sQ$. Group public keys are $\{P, P_0, P_{pub}, H, G, \Theta\}$, GM's issuing key is (x, s), opening key is x'.

(Join, Iss). When a user denoted as i want to join the group, he runs an interactive protocol with GM, and in the end, user i holds secret key x_i, and (a_i, S_i) called a certificate from GM, Δ_i as his identity, where $e(a_iP+P_{pub}, S_i) = e(P, x_iP + P_0)$, and $\Delta_i = e(P, S_i)$.

Suppose the current group accumulated value is V_{j-1}, GM computes a new accumulate value $V_j = (a_i+s)V_{j-1}$. The witness of i in the group is $W_{i,j} = V_{j-1}$.

(IEID_P, IEID_V). An user i running IEID_P computes $E = tG$, $\Lambda = \Delta_i \Theta^t$, then shows knowledge of $(a_i, S_i, x_i, W_{i,j})$ that $e(a_iP+P_{pub}, S_i) = e(x_iP+P_0, P)$, and $e(a_iQ + Q_{pub}, W_{i,j}) = e(Q, V_j)$, and $e(P, S_i)$ has been encrypted in $E = tG$, Λ.

Open. To open an IEID transcript $(E, \Lambda, ...)$, GM computes $\Delta_i = \Lambda e(E,G)^{-x'}$ and a non-interactive zero-knowledge proof of knowledge of x' so that $\Theta = e(G,G)^{x'}$ and $\Lambda/\Delta_i = e(E,G)^{x'}$.

References

[1] Z. Cao, "Analysis of one popular group signature scheme," in *ASIACRYPT'06* (X. Lai and K. Chen, eds.), LNCS 4284, pp. 460–466, Springer-Verlag, 2006.

[2] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, "A practical and provably secure coalition-resistant group signature scheme," in *CRYPTO'00*, LNCS 1880, pp. 255–270, Springer-Verlag, 2000.

[3] L. Nguyen, "Accumulators from bilinear pairings and applications," in *CT-RSA'05*, LNCS 3376, pp. 275–292, Springer-Verlag, 2005. A modified version is available at Cryptology ePrint Archive: Report 2005/123.

[4] F. Zhang and X. Chen, "Cryptanalysis and improvement of an id-based ad-hoc anonymous identification scheme at ct-rsa 05." Cryptology ePrint Archive, Report 2005/103, 2005.

A Review of ACJT's Group Signature

The ACJT scheme [2] begins by choosing security parameters $\epsilon > 1, k, l_p$, as well as a collision resistent Hash function $\mathrm{H} : \{0,1\}^* \rightarrow \{0,1\}^{\mathrm{k}}$, let $\Delta = [2^{\lambda_1} - 2^{\lambda_2}, 2^{\lambda_1} + 2^{\lambda_2}]$, $\Gamma = [2^{\gamma_1} - 2^{\gamma_2}, 2^{\gamma_1} + 2^{\gamma_2}]$, where $\lambda_1 > \epsilon(\lambda_2 + k) + 2, \lambda_2 > 4l_p$, $\gamma_1 > \epsilon(\gamma_2 + k) + 2, \gamma_2 > \lambda_1 + 2$.

SETUP. GM randomly chooses two safe primes p, q, i.e, $p' = (p-1)/2$ and $q' = (q-1)/2$ are large primes too and $a, a_0, g, h \in_R QR_n$, $x \in_R Z_{p'q'}$, calculates $n = pq, y = g^x \bmod n$. Group public keys are $Y = \{n, a, a_0, y, g, h\}$. GM's secret keys are $S = \{p', q', x\}$.

JOIN. When user U wants to join the group, he runs an interactive protocol with GM, and in the end, U obtains his secret keys $x_u \in \Delta$, his certificate

(A_u, e_u), where $e_u \in_R \Gamma$, and $A_u := (a^{x_u} a_0)^{1/e_u} \bmod n$. (A_u, e_u, x_u) is the signing key of U. (A_u, e_u) and transcripts generated as well as the identity of U are stored in a registration database.

SIGN and VERIFY. U signs on m by generating an honest verifier zero-knowledge proof of $(A_u, e_u \in \Gamma, x_u \in \Delta)$, which is formulated specifically as follows

$$SK\{(\alpha, \beta, \gamma, \delta) : a_0 = T_1^{\alpha}/a^{\beta} y^{\gamma} \bmod n, T_2 = g^{\delta} \bmod n, \\ 1 = T_2^{\alpha}/g^{\gamma} \bmod n, T_3 = g^{\alpha} h^{\delta} \bmod n, \alpha \in \Gamma, \beta \in \Delta\}\{m\},$$

The verification of the group signature is the verification of the above proof.

OPEN. GM calculates $A := T_1/T_2^x \bmod n$, compares it with the registration database, the signature signer is then traced; then GM generates a proof of knowledge $PK\{x : y = g^x \bmod n, T_1/A_u = T_2^x \bmod n\}$ to support his judgement.