Unlinkability of a Group Signature

Zhou Sujing[1] and Lin Dongdai[1]

SKLOIS Lab,Institute of Software Chinese Academy of Sciences, Beijing, China
zhousujing@is.iscas.ac.cn

Abstract. Miyaji et.al proposed a fully functional(i.e., satisfying unforgeability, exculpability,anonymity, traceability, unlinkability, and revocability.) group signature over only known-order groups, that is based only on Discrete logarithm related assumptions, specifically, multiple DLP they proposed in the same paper [MU04]. In this paper, we point out their scheme does not have unlinkability.
Keywords: Digital Signature, Group Signature.

1 Introduction

A group signature scheme is a signature scheme that has multiple secret keys corresponding to a single public key. A group signature should at least include the following 5 algorithms: SETUP, JOIN, SIGN, VERIFY and OPEN. SETUP is executed by a group manager, GM for short; JOIN is an interactive protocol between group members and GM; SIGN is an algorithm run by group members; any one can execute VERIFY to check the validity of a given group signature; OPEN is used by GM, or a separate Opener when available, to open a given signature for the identity of its signer.

A secure group signature should at least have the following properties, as defined in [ACJT00]: **unforgeability**, only group members are able to sign on behalf of the group; **exculpability**, neither a group member nor the group manager can sign on behalf of other group members; **unlinkability**, deciding whether two different signatures were signed by the same group member is computationally hard; **anonymity**, identifying the signer given a signature is computationally hard except for the group manager, or Opener; **traceability**, the group manager or Opener is able to open a signature and identify the signer; moreover, a signer cannot prevent the opening of a valid signature; **coalition-resistance**, a colluding subset of group members cannot generate valid group signatures that cannot be opened.

Miyaji et.al proposed a fully functional(i.e., satisfying unforgeability, exculpability,anonymity, traceability, unlinkability, and revocability.) group signature over only known-order groups, that is based only on Discrete logarithm related assumptions, specifically, multiple DLP they proposed in the same paper [MU04].

In this paper, we point out their scheme does not have unlinkability.

2 Miyaji and Umeda's Group Signature

1. SETUP. The group manager GM chooses two groups G_q, G_P with order $q, P(= pq)(p, q$ are primes) respectively, randomly chooses $g_1, g_2, g_3, g_4 \in G_q$, and $h \in_R G_P$, and $x \in_R Z_q$, set$y_1 = g_1^x$, $y_2 = g_3^x$. Group public keys are $Y = \{q, P, G_q, G_P, g_1, g_2, g_3, g_4, h, y_1, y_2\}$. GM's secret key is $S = \{x\}$.
2. JOIN. When a user denoted as P_i wants to join the group, he runs an interactive protocol with GM
   - P_i randomly selects one of his secret keys $x_i \in Z_q$ and sets $z_i := g_2^{x_i}$.
   - GM randomly chooses $w_i \in Z_q$, computes $A_i = z_i g_1^{-w_i}$, $b_i = w_i - A_i x$, sends them to P_i.
   - P_i verifies that $A_i y_1^{A_i} g_1^{b_i} = z_i$.

   P_i's secret keys is x_i, and he also got a certificate (A_i, b_i) from GM.
3. SIGN. P_i signs on $m$chooses $w \in_R Z_q$, calculates $T_1 = h^{g_3^w}$, $T_2 = T_1^{g_4^{b_i}}$,$T_3 = g_3^{b_i} g_4^w$, $T_4 := A_i g_3^w$, $T_5 := y_2^w$, generates two signatures of proof of knowledge σ_1, σ_2.
4. VERIFY, OPEN and Revocation. Omitted here because they are unrelated with our analysis of unlinkability.

3 Analysis of Unlinkability

Suppose two group signatures are given: $(T_1, T_2, T_3, T_4, T_5, \sigma_1, \sigma_2)$ and $(T'_1, T'_2, T'_3, T'_4, T'_5, \sigma'_1, \sigma'_2)$, if they are signed by the same member, then we have the following equations:

$$T_1^{T'_4} = h^{g_3^{A_i g_3^{w'}} \bmod P} = h^{A_i g_3^{w+w'} \bmod P} = {T'_1}^{T_4} \tag{1}$$

$$h^{T_4/T'_4} = T_1/T'_1 \tag{2}$$

Either one will be sufficient to link any two signatures.

References

[ACJT00] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik. A practical and provably secure coalition-resistant group signature scheme. In *Crypto'00*, LNCS 1880, pages 255–270. Springer-Verlag Berlin Heidelberg, 2000.

[MU04] Atsuko Miyaji and Kozue Umeda. A fully-functional group signature scheme over only known-order group. In *ACNS 2004*, LNCS 3089, 2004.