On Deng-Zhao Group Signature Scheme

Zhengjun Cao

Key Lab of Mathematics Mechanization, Academy of Mathematics and Systems Science,

Chinese Academy of Sciences, Beijing, P.R. China. 100080 zjcamss@hotmail.com

Abstract Deng and Zhao recently proposed an efficient group signature scheme in [1]. We find that the scheme is linkable which might be overcome by the authors' suggestion that each group member uses different public/private key pair for each signature. Besides, the group manager can forge group signatures solely. That means the scheme does not satisfy unforgeability.

Keywords group signature scheme, unforgeability.

1 Introduction

Group signatures, introduced by Chaum and Heyst[2], allow individual members to make signatures on behalf of the group. More formally, a secure group signature scheme must satisfy the following properties[3]:

- Unforgeability: Only group members are able to sign messages on behalf of the group.
- Anonymity: Given a valid signature of some message, identifying the actual signer is computationally hard for everyone but the group manager.
- Unlinkability: Deciding whether two different valid signatures were produced by the same group member is computationally hard.
- Exculpability: Neither a group member nor the group manager can sign on behalf of other group member.
- Traceability: The group manager is always able to open a valid signature and identify of the actual signer.
- Coalition-resistance: A colluding subset or group members (even if comprised of the entire group) cannot generate a valid signature that the group manager cannot link to one of the colluding group members.

Recently, Deng and Zhao proposed a new group signature scheme from Gap Deffie-Hellman groups. Obviously, the scheme is linkable which might be overcome by the authors' suggestion that each group member uses different public/private key pair for each signature. Besides, we find that the group manager can forge group signatures solely. That is to say, the scheme does not satisfy unforgeability.

2 Deng-Zhao group signature scheme

2.1 Setup

Let E/F_{k^n} be a supersigular elliptic curve whose order has large prime factor q. Let $P \in E/F_{k^n}$ be a point of order q. The subgroup $< P >$ generated by P is defined as G_1. According to the isomorphism ϕ on the curve, define a bilinear map: $\hat{e} : G_1 \times G_1 \rightarrow G_2$, where G_2 is a subgroup of $F^*_{k^{\alpha n}}$. To map a string to a point on curve, we define $H_1 : \{0,1\}^* \rightarrow G_1$ and use the algorithm MapToGroup[4]. We also define $H_2 : \{0,1\}^* \times G_1 \rightarrow z^*_q$. The group manager chooses a random number $s \in Z^*_q$ to be the master key and publishes $P_{pub} = sP$. The initial public key is $(q, P, P_{pub}, H_1, H_2, \hat{e}, \alpha)$ and the secret key is $SK = s$.

2.2 Join

Suppose now that a user u_i wants to join the group. First, u_i randomly chooses $x_i \in Z^*_p$. Then he computes $R_i = x_iP$. Secondly, we assume that communication between the group member and the group manager is secure, i.e., private and authentic. To obtain his membership certificate, each user must perform the following protocol with the group manager:

(1) The user u_i sends R_i to the group manager.

(2) The group manager regards R_i as some ID information and computes

$$D_i = sR_i$$

Then D_i is communicated secretly to the user u_i as group member secret key. R_i is u_i's public key.

2.3 Sign

If user u_i wants to sign a message m on behalf of the group, he does the following things:

(1) Pick a random $r \in Z_q^*$, compute $U = rR_i,\ h = H_2(m,U),\ V = (r+h)D_i$. Then the first part of the signature is $\sigma_1 = (U, V)$.

(2) Compute $P_m = H_1(m) = tP, \quad S_m = x_i P_m$, where $t \in Z_q^*$ and σ_2 is the x-coordinate of S_m.

The final signature of user u_i is $(\sigma_1, \sigma_2, R_i)$.

2.4 Verify

Given a signature $(\sigma_1, \sigma_2, R_i)$ and a message m, verification can be divided into two parts:

(1) The verifier makes sure that the signature is generated by a group member by checking that $\hat{e}(P_{pub}, \phi(U + hR_i)) = \hat{e}(P, \phi(V))$, using σ_1.

(2) The verifier checks that the signature is definitely generated by u_i rather than other members of the group. He does the following :

a) Find a point $S \in E/F_{k^n}$ of order q whose x-coordinate is σ_2 and whose y-coordinate is some $y \in F_{k^n}$. If no such point exists, reject the signature as invalid.

b) Set $c = \hat{e}(P, \phi(S))$ and $d = \hat{e}(R_i, \phi(H_1(m)))$

c) If either $c = d$ or $c^{-1} = d$, accept the signature. Otherwise, reject it.

2.5 Open

The group manager knows the identity of the member for each u_i. As a result, it is easy for the group manage, given a message m and a valid group signature, to determine the identity of the signer corresponding to the public key R_i.

3 Analysis

It's obvious that the scheme is linkable because a user u_i must use his key R_i to make a valid group signature $(\sigma_1, \sigma_2, R_i)$. To overcome the flaw, the authors propose a suggestion that each user uses different public/private key pair for each signature.[1] In a sense, the scheme is not practical. Except the flaw, we find that the group manager can generates valid group signatures solely. That is to say, the scheme does not satisfy unforgeability.

A key observation on the Sign Phase in the original scheme is that user u_i has to use his key triple (x_i, R_i, D_i), where x_i is a random number picked by user u_i in Z_p^*, $R_i = x_i P$, $D_i = sR_i$, P is public, s is the group manager's master key.

Intuitively, we know that the group manager has absolute superiority in Join Phase in the scheme because he can generate an arbitrary $R_0 = x_0 P$ $(x_0 \in_R Z_P^*)$ solely, then he computes $D_0 = sR_0$ using his master key s. Therefore, he obtains a valid key triple (x_0, R_0, D_0) for signing like any group member.

The forgery procedure:

If group manager wants to sign a message m on behalf of the group, he does the following things:

(1) Pick a random $r \in Z_q^*$, compute $U = rR_0,\ h = H_2(m, U),\ V = (r + h)D_0$. Then the first part of the signature is $\sigma_1 = (U, V)$.

(2) Compute $P_m = H_1(m) = tP,\quad S_m = x_0 P_m$, where $t \in Z_q^*$ and σ_2 is the x-coordinate of S_m.

The final signature of group manager is $(\sigma_1, \sigma_2, R_0)$.

The correctness of the forged group signature is obvious.

4 Conclusion

In the paper, we analyze Deng-Zhao group signature scheme, and show its forgeability by a simple attack. We hold that to design a perfect group signature scheme is not easy.

References

[1] Donghua Deng, Yiming Zhao. An Efficient Group Signature from Gap Diffie-Hellman Groups. ChinaCrypt'2004, pp. 186-194 (in English).

[2] D.Chaum, F.Heyst. Group Signatures. Proc. EUROCRYPT'91, 1992, pp.257-265.

[3] M. Bellare, D. Micciancio, B. Warinschi. Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions. EUROCRYPT 2003. LNCS 2656, pp.614-629, 2003.

[4] Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing. Advances in Cryptology-AsiaCrypt'01, LNCS Vol. 2248, C.Boyd ed. Springer-Verlag, 2001.