# University of Technology Chemnitz-Zwickau

Department of Computer Science

Theoretical Computer Science
and Information Security



Technical Report

**TR-96-3-D**


# Comments on some group signature schemes


Markus Michels



November 1996



Straße der Nationen 62
D-09111 Chemnitz, Germany

Phone: (+49) 371-531-1479
Fax: (+49) 371-531-1810

# Comments on some group signature schemes

Markus Michels
Theoretical Computer Science and Information Security
University of Technology Chemnitz-Zwickau,
Straße der Nationen 62, D-09111 Chemnitz, Germany
E-mail: mmi@informatik.tu-chemnitz.de

Draft

**Abstract**

At Asiacrypt'96 meeting, S.J.Kim, S.J.Park and D.H. Won suggested a convertible group signature scheme, based on a group signature scheme by S.J. Park, I.S.Lee and D.H. Won. In this paper it will be pointed out, that both schemes are vulnerable to a group center attack and moreover, an outsider can process a slightly modified attack, if some parameters are chosen improperly. Finally, it is shown that the identification process fails.

## 1. Introduction

In 1991 Chaum and van Heyst suggested the signature concept of *group signatures* [ChHe91], that can be described in the following manner:

- only a certain number $t$ of a group of $n$ members can sign a message.
- any verifier can verifiy the validity of a given signature, but can not trace whom of the signers has signed the message.
- A trustee is able to trace the identity of the signers from a given signature.

They also propose four different scheme for the case $t = 1$, other schemes for this case were suggested by Chen and Pedersen [ChPe94]. However, the length of the public group key depends on the number of members of the group. This is always the case, if the anonymity of the signers is unconditional [ChPe95].

Recently, S.J.Park, S.Lee and D.H.Won suggested a group signature scheme for the case $t = 1$ where the length of the group key is fixed [PaLW95, PaWo95]. Furthermore, at Asiacrypt'96 meeting, S.J.Kim, S.J.Park and D.H.Won pointed out how a slightly modified version of this scheme can be transformed, such that either all signatures or single signatures can be converted into identity-traceable signatures [KiPW96]. They call this concept *convertible group signature* concept.

In this paper, two attacks will be described. In the first attack it is pointed out, that the group center can forge signatures universally, although he is not aware of the secret key of the signer. More seriously, it can be shown that even an outsider can forge signatures universally, if some parameters are chosen improperly. Furthermore, it seems that the identification process doesn't work as described.

## 2. A group signature scheme

Here we review the group signature scheme given in [KiPW96]. Let $GC$ be a group center and $ID_G$ a public group identity.

### Initialization

The group center picks the primes $p', q', f$ and the numbers $\gamma^d$ and $y$, such that $p := 2\gamma^d fp' + 1$ and $q := 2fq' + 1$ are primes and $(n, \gamma^d, y)$ is an acceptable triple (see [KiPW96] for detail). Furthermore, $n = pq$ and $gcd(\gamma, q') = gcd(\gamma, f) = 1$. Finally, there is a secure hash function $h$.

The group center picks two generators $h_1, h_2$ and computes $b := h_1^{2p'\gamma^d} \cdot h_2^{2q'} \pmod n$. According to [KiPW96], $b$ is of order $f$. GC also picks a special $i$ (the class index of $ID_G$) and publishes $(n, \gamma^d, y^i, b, f, h)$ as the group public key, while $(p', q')$ are kept secret.

### Key generation

The group member *Alice* picks a random number $s_A$ as her secret key and transmits $b^{s_A}$ and $ID_A$ to the group center. The group center can compute $x_A$ such that

$$ID_G = b^{-s_A} \cdot y^{-i} \cdot x_A^{-\gamma^d} \pmod n$$

as he knows the factorization of $n$. He submits $x_A$ to member Alice secretly.

### Signature generation

The signer Alice picks two random numbers $r_1, r_2$ with $0 < r_1 < f$ and $0 < r_2 < n$ and computes $V := b^{r_1} \cdot r_2^{\gamma^d} \pmod n$, $e := h(V, m)$, $z_1 := r_1 + s_A \cdot e \pmod f$, $z_2 := r_2 \cdot x_A^e \pmod n$. The signature of the message $m$ is $(e, z_1, z_2)$.

### Signature verification

Given $(m, e, z_1, z_2)$, any verifier can check the validity of the group signature by computing

$$\bar{V} := (ID_G \cdot y^i)^e \cdot b^{z_1} \cdot z_2^{\gamma^d} \pmod n$$

and checking if $e = h(\bar{V}, m)$ holds.

### Identification of the signer

The group center can trace the identity of the signer. He knows $b^{s_j} \pmod n$ and $x_j$ of a member $j$. Given a signature $(e, z_1, z_2)$ on a message $m$, he computes $r_2 := z_2 \cdot x_j^{-e} \pmod n$ and $\bar{V} := (ID_G \cdot y^i)^e \cdot b^{z_1} \cdot z_2^{\gamma^d} \pmod n$ as above. Then he checks whether

$$b^{z_1} \equiv \bar{V} \cdot r_2^{-\gamma^d} \cdot (b^{s_j})^e \pmod n$$

holds. If this is true, then member $j$ is the signer.

## 3. Cryptanalysis of a group signature scheme

In this section we cryptanalysis the scheme described above. We describe two attacks, one can be processed by the group center and the other one can be processed by anyone knowing the public parameters. The aim of both attack is that the attacker can sign any message he likes, that means he can forge the scheme universally. Finally we point out, that the identification process fails.

### Attack of the group center

As the group center does not know the secret key $s_A$ of group member Alice, he cannot generate signatures by using the signature generation protocol. However, it can be shown that he is able to forge signatures by using the following attack: He chooses a message $\tilde{m}$ arbitrarily, computes a value $\bar{V} \in \mathbf{Z}_n$ at random and computes $e := h(\bar{V}, \tilde{m})$. He picks $z_1 \in \mathbf{Z}_f$ at random and computes $\gamma' := (\gamma^d)^{-1} \pmod{\varphi(n)}$. Note that he can compute $\varphi(n) = 4\gamma^d f^2 p'q'$ as he knows $p'$ and $q'$. Now he computes

$$z_2 := \left(\bar{V} \cdot ((ID_G \cdot y^i)^e \cdot b^{z_1})^{-1}\right)^{\gamma'} \pmod n.$$

As a result, $(e, z_1, z_2)$ is a valid signature for the message $\tilde{m}$. Thus we have proven the following theorem:

**Theorem 3.1** *The group center can forge the group signature scheme universally.*

### Attack of an outsider

It can be pointed out that even an outsider is able to forge signatures by using a slightly different attack, if improper parameters are chosen. Note that an outsider does not know $p'$ and $q'$, thus he can't compute $\varphi(n)$ and, as a result, can't process the attack given above.

However, he chooses a message $\tilde{m}$ arbitrarily, computes a value $g \in \mathbf{Z}_f$, computes $\bar{V} := b^g \pmod{n}$ at random and computes $e := h(\bar{V}, \tilde{m})$. We have to assume that $ID_G \cdot y^i$ is of order $f$. In this case, $a := \bar{V}/((ID_G \cdot y^i)^e) \pmod{n}$ is of order $f$ as well. Moreover $t := a/b^{z_1} \pmod{n}$ is also of order $f$ regardless of the choice of $z_1$. Thus by picking a random $z_1 \in \mathbf{Z}_f$ and computing $\gamma' := (\gamma^d)^{-1} \pmod{f}$, he can compute $z_2 := t^{\gamma'} \pmod{f}$. As a result, $(e, z_1, z_2)$ is a valid signature for the message $\tilde{m}$. Note that the assumption, that $ID_G \cdot y^i$ is of order $f$ holds if $x_A$ is of order $f$. Thus we have proven the following theorem:

**Theorem 3.2** *If the public parameter are chosen inproperly, such that the secret value $x_i$ of the member $i$ is of order $f$, then an outsider can forge the group signature scheme universally.*

### Failure of the identification process

Let us assume that a signature $(e, z_1, z_2)$ on a message $m$ is generated by a group member Bob. In a dispute, Bob accuses group member Alice that she has signed the message.

The group center computes $\tilde{r}_2 := z_2 \cdot x_A^{-e} \pmod{n}$ and $\bar{V} := (ID_G \cdot y^i)^e \cdot b^{z_1} \cdot z_2^{\gamma^d} \pmod{n}$ as above. Then the verification equation

$$b^{z_1} \equiv \bar{V} \cdot \tilde{r}_2^{-\gamma^d} \cdot (b^{s_A})^e \pmod{n}$$

holds, because we have

$$\bar{V} \cdot \tilde{r}_2^{-\gamma^d} \cdot (b^{s_A})^e \equiv (ID_G \cdot y^i)^e \cdot b^{z_1} \cdot z_2^{\gamma^d} \cdot \tilde{r}_2^{-\gamma^d} \cdot (b^{s_A})^e$$

$$\equiv (b^{-s_A} \cdot x_A^{-\gamma^d})^e \cdot b^{z_1} \cdot z_2^{\gamma^d} \cdot (z_2 \cdot x_A^{-e})^{-\gamma^d} \cdot (b^{s_A})^e \equiv b^{z_1} \pmod{n}.$$

Thus the group center will incorrectly trace Alice as the signer of the message. Clearly, any member of the group can be traced. This shows that the verification equation is not suitable.

## 4. Two convertible group signature schemes

Now we review the two convertible group signature schemes briefly.

### First scheme

The difference of this scheme to the one described in the last section, is that $bl := blob(b^{r_1} \pmod{n}, R)$ with random $R$ is computed and is added to the hash function to compute $e$ (that is $e := h(V, m, bl)$. Furthermore $bl$ is part of the signature, to enable the verifier to verify a given signature. The identification process is the same as described above. All signatures can be converted by releasing $x_A$, a single signature can be converted by opening the blob and checking whether $b^{r_1} \equiv b^{z_1} \cdot (b^{s_j}) \pmod{n}$ holds. Clearly, the same attacks as described above work here as well.

### Second scheme

The difference of this scheme to the first scheme is that the initialization is simplified.

The group center picks the primes $p', q', f$, such that $p := 2fp' + 1$ and $q := 2fq' + 1$ are primes. It is recommended that $|f| = 160$ and $|p'| = |q'| = 234$. Furthermore, $n = pq$, the group center selects a parameter $g \in \mathbf{Z}_n^*$ with order $f$, and parameters $\gamma, d$ with $\gamma \cdot d \equiv 1 \pmod{\varphi(n)}$

and $|\gamma| = 160$. Finally, there is a secure hash function $h$. The group center publishes $(n, \gamma, g, f, h)$ as the group public key, while $(d, p', q')$ are kept secret.

The group member Alice picks a random number $s_A$ as her secret key and transmits $b^{s_A}$ and $ID_A$ to the group center. The group center can compute

$$x_A = (ID_G \cdot g^{s_A})^{-d} \pmod{n}$$

and submits $x_A$ to member Alice secretly. Now all the protocols are the same as described above, if $(\gamma, g)$ instead of $(\gamma^d, b)$ is used and $y^i$ is omitted. However, the attacks described above can be applied here as well.

## 5. Conclusion

We have shown that in the analyzed group signature schemes, the group center must be a trusted authority, as he can forge signatures universally. Furthermore, it was pointed out that a slightly modified attack can even be processed by an outsider, provided that some parameters are chosen improperly. Finally, it was shown that the identification process does not work as described. The author would like to thank Seung Joo Kim for the hint that Sang-Jun Park and Sung-Joon Park have observed similar problems in the analyzed scheme as well.

## References


[ChHe91] D.Chaum, E.van Heijst, "Group signatures", Lecture Notes in Computer Science 547, Advances in Cryptology: Proc. Eurocrypt '91, Springer Verlag, (1992), pp. 257–265.

[ChPe94] L.Chen, T.Pedersen, "New group signature schemes", Lecture Notes in Computer Science 950, Advances in Cryptology: Proc. Eurocrypt'94, Springer Verlag, (1995).

[ChPe95] L.Chen, T.Pedersen, "On the efficiency of group signatures providing information-theoretic anonymity", Lecture Notes in Computer Science 921, Advances in Cryptology: Proc. Eurocrypt'95, Springer Verlag, (1995), pp. 39–49.

[KiPW96] S.J.Kim, S.J.Park, D.H.Won, "Convertible group signatures", Lecture Notes in Computer Science 1139, Advances in Cryptology: Proc. Auscrypt'96, Springer Verlag, (1996), pp. 311–321.

[PaLW95] S.J.Park, I.S. Lee, D.H.Won, "A practical group signature scheme", Proc. of JW-ISC'95, Japan, (1995), pp. 127–133

[PaWo95] S.J.Park, D.H.Won, "A practical Identity-based group signature scheme", Proc. of ICIEC'95, China, (1995), pp. II64–II67