On the Difficulty of Coalition-Resistance in Group Signature Schemes

Giuseppe Ateniese[*] Marc Joye[†] Gene Tsudik[‡]

June 1, 1999

Abstract

Group signatures allow members of a group to sign *anonymously* on group's behalf. However, in exceptional cases, the anonymity can be revoked by a group manager. One of the most difficult tasks in developing group signature schemes is to prevent coalition attacks: malicious collusions of group members that produce untraceable signatures. This paper describes coalition attacks against some recently proposed group signature schemes. It also presents a candidate scheme resistant against coalition attacks; its security is based on a widely accepted number-theoretic assumption. The paper also includes a survey of notable group signature schemes.

1 Introduction

Group digital signatures are a relatively new concept introduced by Chaum and van Heijst [9] in 1991. A group signature, akin to its traditional counterpart, allows the signer to demonstrate knowledge of a secret with respect to a specific document. A group signature is publicly verifiable: it can be validated by anyone in possession of a group public key. However, group signatures are anonymous in that no one, with the exception of a designated group manager, can determine the identity of the signer. Furthermore, group signatures are unlinkable which makes it computationally hard to establish whether or not multiple signatures are produced by the same group member. In exceptional cases (such as a legal dispute) any group signature can be "opened" by a group manager to reveal unambiguously the identity of the actual signer. At the same time, no one —including the group manager— can misattribute a valid group signature.

The salient features of group signatures make them attractive for many specialized applications, such as voting and bidding. They can, for example, be used in invitations to submit tenders [10]. All companies submitting a tender form a group and each company signs its tender anonymously using the group signature. Once the preferred tender is selected, the winner can be traced while the other bidders remain anonymous. More generally, group signatures can be used to conceal organizational structures, e.g,, when a company or a government agency issues a signed statement. Group signatures can also be integrated with an electronic cash system whereby several banks can securely distribute anonymous and untraceable e-cash. The group property offers the further advantage of concealing the identity of the cash-issuing bank [20].

[*] IBM Zurich Research Laboratory, Saumerstrasse 4, CH-8803 Rüschlikon, Switzerland. Email: gat@ibm.zurich.com

[†] LCIS, Dept of Electrical Engineering, Tamkang University, Tamsui, Taipei Hsien 251, Taiwan, R.O.C. Email: mjoye@geocities.com

[‡] USC ISI, 4676 Admiralty Way, Marina Del Rey, CA 90292, U.S.A. Email: gts@isi.edu

The rest of this paper is organized as follows. In the next section, we formally define group signatures and the associated security properties. Section 3 discusses the difficulty of coalition-resistance and presents some coalition attacks against several recent schemes. As an educational exercise, we review in Section 4 our (failed) attempts to design a coalition-resistant group signature scheme. We then sketch out a new candidate scheme with security based on the strong RSA assumption. We conclude in Section 5. (Additionally, previous and related work in group signatures is surveyed in Appendix A.)

2 Group Signatures

We now present a more formal definition and desired properties of group signatures. For an in-depth discussion of this subject, we refer the reader to [5].

Definition 2.1 A *group signature scheme* is a digital signature scheme comprised of the following procedures:

- `SETUP`: An algorithm for generating the initial group public key $\mathcal{Y}$.
- `JOIN`: A protocol between the group manager and a user that results in the user becoming a new group member.
- `SIGN`: A protocol between a group member and a user whereby a group signature on a user-supplied message is computed by the group member.
- `VERIFY`: An algorithm for establishing the validity of a group signature given a group public key and a signed message.
- `OPEN`: An algorithm that, given a signed message and a group secret key, determines the identity of the signer.

A secure group signature scheme must satisfy the following properties:

- **Unforgeability**: Only group members are able to sign messages on behalf of the group.
- **Anonymity**: Given a signature, identifying the actual signer is computationally hard for everyone but the group manager.
- **Unlinkability**: Deciding whether two different signatures were computed by the same group member is computationally hard.
- **Exculpability**: Neither a group member nor the group manager can sign on behalf of other group members.[1]

  A related definition is that of *framing* [10] which captures the property that a group member is made responsible for a signature he did not produce.
- **Traceability**: The group manager is able to open a signature and identify the actual signer; moreover, a signer cannot prevent the opening of a valid signature.

[1] Note that the above does not preclude the group manager from creating fraudulent signers (i.e., nonexistent group members) and then producing group signatures.

The emphasis of the previous properties is on the fact that a *single* group member cannot generate signatures that are (in case of a dispute) not traceable to him by the group manager. This means that a subset of group members, pooling together their secrets, can generate valid group signatures that cannot be opened by the group manager. In order to avoid this we need the following property:

- **Coalition-resistance**: A colluding subset of group members cannot generate a valid signature that cannot be traced. This property will be discussed in more detail in Section 3.

Definition 2.2 The *efficiency* or *practicality* of a group signature scheme is typically based on the following parameters:

- the size of the group public key $\mathcal{Y}$;
- the size of a group signature;
- the efficiency of `SIGN`, `VERIFY` and `OPEN`; and
- the efficiency of `SETUP` and `JOIN`.

3 Difficulty of Coalition-Resistance

A coalition attack occurs when a subgroup of group members pool their secrets together in order to produce a perfectly valid group signature. Such a signature is *untraceable*, i.e, the `OPEN` algorithm will fail to reveal the signer's identity.

In this section, we discuss several group signature schemes susceptible to coalition attacks. The aim is to gain a better understanding of how a coalition attack happens and, in the long run, to develop coalition-resistant techniques. Our discussion also illustrates that coalition-resistance is certainly one of the most challenging properties in designing a secure group signature scheme.

Following the definition in Section 2, each scheme discussed below is presented as a set of five algorithms: `SETUP`, `JOIN`, `SIGN`, `VERIFY` and `OPEN`. We are mainly concerned with the `JOIN` algorithm which enables a new user to join the group. As a result, the new user is issued a *membership certificate* which is then used to generate group signatures. We show how the knowledge of one or several certificates enables a coalition to derive a new (and valid) membership certificate, thus resulting in untraceable group signatures.

3.1 Camenisch-Stadler Scheme

The coalition-resistance of the (basic) Camenisch-Stadler group signature relies on the following assumption (see Assumption 5.1 in [5, pp. 99–100] and [8, Section 4]).

Assumption 3.1 (Camenisch-Stadler) *Let n be an RSA-modulus, $e \in \mathbb{Z}^*_{\varphi(n)}$, and $a \in \mathbb{Z}^*_n$ an element of large order such that computing discrete logarithms w.r.t. base a is infeasible. We assume that it is hard to compute a pair (x, v) of integers satisfying:*

$$v^e \equiv 1 + a^x \pmod{n} \tag{1}$$

if the factorization of n is unknown. Furthermore, we assume that this is true even when other pairs (x_i, v_i) satisfying the above equation are known.

Specifically, each group member receives a group certificate of the form $(a^x+1)^d \bmod n$, where $de \equiv 1 \pmod{\varphi(n)}$ and, under Assumption 3.1, it is assumed to be hard to generate a new valid group certificate without the aid of the group manager. However, in [3], Ateniese and Tsudik showed that the present scheme does not satisfy the *traceability* property. In fact, it is sufficient to note that $(a^x+1)^d$ can be rewritten as $(a^x+1)^d \equiv a^{xd}(1+a^{-x})^d \pmod{n}$. Then, if $x = ke$ for some integer k, a new certificate can be obtained by computing $a^{-k}(a^x+1)^d \equiv (1+a^{-x})^d \pmod{n}$.[2] In [3], it is also shown that — even when x is a generic value, e.g. if $\gcd(x,e) = 1$ — a colluding subset of group members can easily derive a new certificate, i.e. the scheme does not satisfy the *coalition-resistance* property.

As a fix — also suggested by J. Camenisch (see [3]), the value 1 in the certificate structure $(a^x+1)^d$ can be substituted with a randomly chosen value C. Thus, Assumption 3.1 should be modified as follows.

Assumption 3.2 *Let n be an RSA-modulus, $e \in \mathbb{Z}^*_{\varphi(n)}$, and $a \in \mathbb{Z}^*_n$ an element of large order such that computing discrete logarithms w.r.t. base a is infeasible. We assume that it is hard to compute a pair (x, v) of integers satisfying:*

$$v^e \equiv C + a^x \pmod{n} \tag{2}$$

if the factorization of n is unknown and C is selected randomly. Furthermore, we assume that this is true even when other pairs (x_i, v_i) satisfying the above equation are known.

A further countermeasure is to randomize the value x chosen by the group member, for example by selecting α, β and releasing the certificate $(a^{\alpha x+\beta}+C)^d$ (this has been proposed as a research challenge in [3]).

We stress that C must be chosen randomly, in particular, the discrete logarithm (base a) of C must be unknown. In fact, if the constant 1 in Eq.(1) is replaced by a constant C such that discrete logarithm of C (base a) is known, it is equally easy to derive a new certificate. Suppose that $C \equiv a^c \pmod{n}$ and c is known. Then, replacing 1 by C, Equation (1) becomes

$$v^e \equiv C + a^x \equiv a^{x-c}(a^{2c-x}+a^c) \equiv (a^{(x-c)d})^e(C+a^{2c-x}) \pmod{n} \ . \tag{3}$$

Hence if (x_1, v_1) is a valid pair, also is $(2c - x_1, v_1/a^{(x_1-c)d} \bmod n)$. Assuming that $\gcd(x_1 - c, e) = 1$ and, given two pairs: (x_1, v_1) and (x_2, v_2) with $x_2 = 2c - x_1$, we can compute $T \equiv (v_1/v_2)^\alpha a^\beta \equiv a^{(\alpha(x_1-c)+\beta e)d} \equiv a^d \pmod{n}$ where α and β are given by the extended Euclidean algorithm, i.e., $\alpha(x_1-c)+\beta e = 1$. Therefore, using a a third pair (x_3, v_3), a new pair $(x, v) = (2c-x_3, v_3/T^{(x_3-c)} \bmod n)$ can be derived.

3.2 Tseng-Jan ID-based Scheme

We only give a short description of the signature and refer to the original paper [29] for details. To `SETUP` the system, a trusted authority selects two large primes $p\,(\equiv 3 \bmod 8)$ and $q\,(\equiv 7 \bmod 8)$ such that $(p-1)/2$ and $(q-1)/2$ are smooth, odd and relatively prime [22]. Let $n = pq$. The trusted authority also defines e, d, v and t satisfying $ed \equiv 1 \pmod{\varphi(n)}$ and $vt \equiv 1 \pmod{\varphi(n)}$,

[2] Notice that the group member is required to show knowledge of the a's exponent in $(1+a^{-x})^d$ by means of a standard challenge-response protocol. Even though, the group member does not know $-x \bmod \varphi(n)$, since $\varphi(n)$ is secret, this task can be easily accomplished by changing the sign of cx in the response, where c here represents the challenge. This relative "problem" also affects the Schnorr and Poupard-Stern signature schemes when the signer works in groups of unknown order.

selects g of large order in $\mathbb{Z}_n^*$, and computes $F = g^v \bmod n$. Moreover, the group manager[3] chooses a secret key x and computes the corresponding public key $y = F^x \bmod n$. The public parameters are (n, e, g, F, y); the secret parameters are (p, q, d, v, t, x). When a user U_i (with identity information D_i) wants to JOIN the group, the trusted authority computes $s_i = et \log_g ID_i \bmod \varphi(n)$ where $ID_i = D_i$ or $2D_i$ according to $(D_i|n) = 1$ or -1, and the group manager computes $x_i = {ID_i}^x \bmod n$. The user membership certificate is the pair (s_i, x_i). To SIGN a message m, user U_i chooses two random numbers r_1 and r_2, and computes $A = y^{r_1} \bmod n$, $B = y^{r_2\, e} \bmod n$, $C = s_i + r_1\, h(m\|A\|B) + r_2\, e$ and $D = x_i\, y^{r_2\, h(m\|A\|B)} \bmod n$, where $h(\cdot)$ is a publicly known hash function. Then, to VERIFY that (A, B, C, D) is a valid group signature for message m, one checks whether $D^e A^{h(m\|A\|B)} B \equiv y^C B^{h(m\|A\|B)} \pmod{n}$. In case of disputes, the group manager can OPEN the signature to recover who issued it by checking which identity ID_i satisfies ${ID_i}^{x\, e} \equiv D^e B^{-h(m\|A\|B)} \pmod{n}$.

Let indexes 1 and 2 respectively denote the attributes of user 1 and user 2. If the two users collude, then they can easily evaluate $y^d \bmod n$ from their certificates (s_1, c_1) and (s_2, c_2) as follows. Since $s_1 = et \log_g ID_1 \bmod \varphi(n)$, we have $g^{s_1} \equiv {ID_i}^{et} \pmod{n}$. Hence, from $x_i = {ID_i}^x \bmod n$, it follows that

$$x_i{}^e \equiv ({ID_i}^e)^x \equiv (g^{s_i\, t^{-1}})^x \equiv (g^{v\, x})^{s_i} \equiv y^{s_i} \pmod{n} \ . \tag{4}$$

So, $x_1 = (y^d)^{s_1} \bmod n$, and similarly $x_2 = (y^d)^{s_2} \bmod n$. Assuming w.l.o.g. that $\gcd(s_1, s_2) = 1$, users 1 and 2 can use the extended Euclidean algorithm to find $\alpha, \beta \in \mathbb{Z}$ such that $\alpha s_1 + \beta s_2 = 1$. Consequently, they can recover

$$y^d \equiv y^{d(\alpha s_1 + \beta s_2)} \equiv {x_1}^{\alpha}\, {x_2}^{\beta} \pmod{n} \tag{5}$$

from x_1 and x_2. Once they know $y^d \bmod n$, they can create a new membership certificate as (s', x') with $x' = (y^d)^{s'} \bmod n$ for any s' they choose. Noting that $x'^e \equiv y^{s'} \pmod{n}$, the signatures produced with this certificate will be valid. However since this certificate does not correspond to a known identity, the group manager will not be able to open the resulting signatures.

Remark 3.3 In addition its vulnerability to coalition attacks, the Tseng-Jan ID-based signature is susceptible to *universal* forgery [17], i.e., anyone can forge a valid group signature for an arbitrary message m. There are two known attacks on the scheme. In the first attack, an adversary randomly chooses C and D, computes $B = y^C\, D^{-e} \bmod n$, and sets $A = B$. One can easily see that (A, B, C, D) is a valid signature for any message m.

The second attack allows to choose $A \neq B$. The adversary chooses D and an integer ω. Then he computes $B = D^{-e} \bmod n$, $A = B\, y^{\omega} \bmod n$, and $C = \omega\, h(m\|A\|B)$ (in $\mathbb{Z}$). Here too, one easily verifies that the resulting 4-tuple (A, B, C, D) is a valid signature on message m.

3.3 Tseng-Jan Scheme Based on Self-certified Keys

We begin with a brief review of the scheme and refer to [31] for a thorough description. The SETUP goes as follows: a trusted authority selects $n = pq$ with $p = 2p' + 1$ and $q = 2q' + 1$ where p, q, p', q' are all prime, he also selects g of order $\nu = p'q'$ and $e, d \in \mathbb{Z}_\nu^*$ satisfying $ed \equiv 1 \pmod{\nu}$. The group manager (a.k.a. group authority in [31]), with identity information GD, chooses a secret key x and computes $z = g^x \bmod n$. After receiving z, the trusted authority computes $y = (g^x)^{GID^{-1}} \bmod n$ where $GID = f(GD)$ for a publicly known hash function $f(\cdot)$, and the group secret key $s_G = (g^x)^{-d} \bmod n$. He sends s_G to the group manager. The public parameters are (n, e, g, y); the secret parameters are (p, q, d, x, s_G). To JOIN the group, a user U_i (with identity information D_i) chooses a secret key s_i,

[3] In [29], the authors call it group authority.

computes $z_i = g^{s_i} \bmod n$, and sends z_i to the trusted authority. In return, the trusted authority sends back $p_i = (g^{s_i})^{{ID_i}^{-1} d} \bmod n$ where $ID_i = f(D_i)$. From p_i, the group manager then computes $x_i = {p_i}^{ID_i\, x}\, s_G \bmod n$. The membership certificate of user U_i is the pair (s_i, x_i). When U_i wants to `SIGN` a message m, he chooses r_1, r_2 and r_3 at random and computes $A = r_1\, s_i$, $B = {r_2}^{-eA} \bmod n$, $C = y^{GID\, A\, r_3} \bmod n$, $D = s_i\, h(m\|A\|B\|C) + r_3\, C$ (where $h(\cdot)$ is a publicly known hash function), and $E = x_i\, {r_2}^{h(m\|A\|B\|C\|D)} \bmod n$. To `VERIFY` the validity of signature (A, B, C, D, E) on message m, one checks whether $y^{GID\, A\, D} \equiv (E^{eA}\, B^{h(m\|A\|B\|C\|D)}\, y^{GID\, A})^{h(m\|A\|B\|C)}\, C^C \pmod n$. In case of disputes, the group manager can `OPEN` the signature by checking which x_i satisfies $(x_i)^{eA}\, B^{-h(m\|A\|B\|C\|D)} \equiv E^{eA} \pmod n$.

As before, let indexes 1 and 2 respectively denote the attributes of user 1 and user 2. If the two users collude then they can recover the group secret key $s_G = g^{-xd} \bmod n$. We assume w.l.o.g. that $\gcd(s_1 - 1, s_2 - 1) = 1$. So, by the extended Euclidean algorithm, there exist $\alpha, \beta \in \mathbb{Z}$ such that $\alpha(s_1 - 1) + \beta(s_2 - 1) = 1$. Moreover, we have

$$x_i = p_i^{ID_i\, x}\, s_G \equiv g^{-xd(-s_i+1)} \equiv {s_G}^{-s_i+1} \pmod n\ . \tag{6}$$

Hence, from their membership certificates (s_1, x_1) and (s_2, x_2), users 1 and 2 can find

$$s_G \equiv {s_G}^{\alpha(s_1-1)+\beta(s_2-1)} \equiv {x_1}^{-\alpha}\, {x_2}^{-\beta} \pmod n\ . \tag{7}$$

Consequently, the second Tseng-Jan scheme, too, does not offer coalition-resistance: given s_G, users 1 and 2 can produce a new valid certificate of their choice as (s', x') where $x' = {s_G}^{-s'+1} \bmod n$ for some arbitrary s'.

4 Towards Coalition-Resistance

The previous sections make it fairly evident that finding a group certificate resistant against coalition attacks is not straightforward. As further evidence, the authors of the present paper have been involved in a lengthy process of creating and subsequently breaking many certificate constructs and the underlying number-theoretic assumptions. As a research report and a learning exercise based on our efforts, we now describe some attempts to find a coalition-resistant group certificate. We conclude by sketching out a candidate certificate structure based on a standard assumption widely believed to be hard.

Our starting point is the group signature proposed in [2]. In [2], it was noted that in certain group signature settings (we refer to as *coalition-oblivious*) group members have no incentives to collude. One example application is the *digital lottery*, where each group member anonymously signs its own numbered ticket (to make it valid) and the group manager later distributes prizes to the right holders of the randomly drawn ticket numbers.

For coalition-oblivious settings, [2] presents a viable alternative to costly group signatures that satisfies all the security properties in Section 2, except coalition-resistance.[4]

We now review the certificate used in [2] and then describe one of the (failed) attempts to make it coalition resistant without losing in efficiency.[5]

[4] We note that finding a signature scheme that does not satisfy any other property is quite straightforward. For instance, a group signature not satisfying the *unlinkability* property can be built with just certified pseudonyms.

[5] We are grateful to Jacques Traore for pointing out, via private communication, weaknesses in early proposals of coalition-resistant group signatures.

Let n be product of two safe primes p, q, i.e., $p = 2p' + 1$ and $q = 2q' + 1$ with p', q' appropriately selected primes. Let v, d be elements such that v is prime and $vd \equiv 1 \pmod{\varphi(n)}$. Let a be a generator of a subgroup $G \subset \mathbb{Z}_n^*$ of order $p'q'$, namely G is the set of quadratic residues modulo n and $a = \bar{a}^2 \bmod n$, for a randomly chosen $\bar{a} \in \mathbb{Z}_n^*$ (with overwhelming probability the order of a is $p'q'$; nevertheless, one may test whether $\gcd(a \pm 1, n) = 1$)). The certificate is $A(x) = (a^x\, a_0)^d \bmod n$ where x is the group member's secret (randomized by the group manager) with $0 < x < v$, and $a_0 \in G$ is a constant such that $\log_a a_0$ is unknown. The protocol is run as follows ([2]):

1. Using El Gamal encryption, the signer encrypts $A(x)$ with the group manager's public key $z = a^s \bmod n$.
2. Then, he proves to the verifier that he indeed encrypted his valid certificate, i.e., given $\alpha = A(x)\, z^r \bmod n$ and $\beta = a^r \bmod n$, the verifier computes $\gamma = \alpha^v / a_0 \bmod n$ and checks that γ is a *representation* w.r.t. bases a and z, where the a's exponent is in $]0, v[$ and the z's exponent equals $v \log_a \beta$.

   All these checks can be done via standard and efficient techniques.

Evidently, the certificate is not coalition-resistant: two colluding members can compute a new and untraceable certificate as follows. Assuming $A(x_1)$, $A(x_2)$ are the certificates of the two colluding members, it is sufficient to compute $[A(x_1)]^2 / A(x_2) \bmod n$ which yields $A(2x_1 - x_2)$. It is likely the case that $0 < 2x_1 - x_2 < v$. More importantly, two colluding members can easily compute $a^d \bmod n$, and, thus, generate arbitrary certificates.

To make $A(x)$ coalition-resistant we considered methods forcing the signer to prove some non-linear relations of his secret x. Hence, we came up with the following certificate structure:

$$A(x) = ({a_2}^{x^2}\, {a_1}^{x}\, a_0)^d \bmod n \tag{8}$$

with a_0, a_1, a_2 random quadratic residues of order $p'q'$. First of all, notice that x must be in $]0, v[$ since it is easy to compute $A(x + tv)$ from $A(x)$ for an integer t. Hence, the signer should prove that $0 < x < v$ and that, given $A(x)^v / a_0$, the exponent of a_2 is the square of the exponent of a_1 (via well-known techniques). However, we now show that this certificate, although seemingly *robust*, is not coalition-resistant.

Define $J(x_1, x_2) :\equiv A(x_1)/A(x_2) \equiv {a_2}^{d(x_1^2 - x_2^2)}\, {a_1}^{d(x_1 - x_2)} \pmod{n}$. So, given a third certificate $A(x_3)$ and assuming w.l.o.g. that $\gcd(x_1 - x_2, x_1 - x_3) = 1$, we have

$$J(x_1, x_2)^\alpha\, J(x_1, x_3)^\beta \equiv {a_2}^{d[\alpha(x_1^2 - x_2^2) + \beta(x_1^2 - x_3^2)]}\, {a_1}^d \pmod{n} \tag{9}$$

where α, β are given by the extended Euclidean algorithm, i.e., $\alpha(x_1 - x_2) + \beta(x_1 - x_3) = 1$. Assume furthermore that we are given a fourth certificate $A(x_4)$ such that $\gcd(x_1 - x_2, x_1 - x_4) = 1$. Similarly, the extended Euclidean algorithm yields $\eta, \xi \in \mathbb{Z}$ s.t. $J(x_1, x_2)^\eta\, J(x_1, x_4)^\xi \equiv {a_2}^{d[\eta(x_1^2 - x_2^2) + \xi(x_1^2 - x_4^2)]}\, {a_1}^d \pmod{n}$. Hence, letting $\tau := [\alpha(x_1^2 - x_2^2) + \beta(x_1^2 - x_3^2)] - [\eta(x_1^2 - x_2^2) + \xi(x_1^2 - x_4^2)]$, it follows that

$$K :\equiv \frac{J(x_1, x_2)^\alpha\, J(x_1, x_3)^\beta}{J(x_1, x_2)^\eta\, J(x_1, x_4)^\xi} \equiv {a_2}^{d\tau} \pmod{n}\ . \tag{10}$$

Moreover, noting that v is prime, $\gcd(v, \tau)$ will very likely be 1. Therefore, there exist $\rho, \sigma \in \mathbb{Z}$ s.t. $\rho v + \sigma \tau = 1$ and thus

$${a_2}^d \equiv {a_2}^{d(\rho v + \sigma \tau)} \equiv {a_2}^\rho\, K^\sigma \pmod{n}\ . \tag{11}$$

Once ${a_2}^d$ is known, ${a_1}^d$ is given, for example, by Eq. (9) as

$$ {a_1}^d \equiv \frac{J(x_1,x_2)^\alpha \, J(x_1,x_3)^\beta}{({a_2}^d)^{\alpha(x_1^2-x_2^2)+\beta(x_1^2-x_3^2)}} \pmod{n}\,, \tag{12} $$

and, hence, ${a_0}^d$ is given from any certificate $A(x_i)$ ($i \in \{1,2,3,4\}$) as

$$ {a_0}^d \equiv \frac{A(x_i)}{({a_2}^d)^{x_i^2}\,({a_1}^d)^{x_i}} \pmod{n}\ . \tag{13} $$

In summary, from their respective certificates $A(x_i)$, four colluding group members are able to derive the values of ${a_2}^d, {a_1}^d, {a_0}^d \pmod{n}$, and, thus, compute a new valid membership certificate $A(x) = ({a_2}^d)^{x^2}\,({a_1}^d)^x\,{a_0}^d \bmod n$ whatever the value of x.

4.1 Strong RSA-based Scheme

It is clear that this approach is generally flawed and one must re-examine the problem and look for other solutions. In particular, an ideal solution would have its security based on one or more *well-known* number-theoretic problems.

This was first addressed successfully in a recent work by Camenisch and Michels [6]. The security of their scheme is based on the strong RSA assumption:

Assumption 4.1 (Strong RSA Assumption) *Let $n = pq$ be an RSA-like modulus and let G be a cyclic subgroup of $\mathbb{Z}_n^*$ of order $\#G$, $|\#G| = \ell_G$. There exists a probabilistic polynomial time algorithm K which on input 1^{ℓ_G} outputs a pair (n,z) such that for all probabilistic polynomial-time algorithms A the probability that A can find $u \in G$ and $e \in \mathbb{Z}_{>1}$ satisfying $z \equiv u^e \pmod{n}$ is negligible.*

We now briefly describe the Camenisch-Michels scheme and then show how its efficiency can be improved [1].

Let n be product of safe primes and $G = \langle g \rangle$ be a cyclic subgroup of $\mathbb{Z}_n^*$ such that the Jacobi symbol $(g|n) = 1$. The group manager randomly selects $z, h \in G$ with the same order and publishes (n, g, z, h) and a prior determined range R. These parameters must be publicly verifiable. During the JOIN operation, the group member selects secret primes $e \in R$, $\bar{e}$ and sends $\tilde{e} = e\bar{e}$, $\tilde{z} = z^{\bar{e}} \bmod n$ to the group manager, along with evidences that he knows $\log_z \tilde{z}$, that e is indeed in R, and, finally, that $\tilde{e}$ is product of two primes. Notice that the latter is a quite expensive proof. Later, the group manager computes the value $u = \tilde{z}^{1/\tilde{e}} \bmod n$, which is equivalent to $u = z^{1/e} \bmod n$. The group certificate is the pair (u, e). Notice that the group manager does not know e that thus becomes the group member's secret.[6] In order to SIGN, the group member encrypts, via El Gamal, the value u with the group manager's public key $y = g^x \bmod n$, i.e. $\alpha = u\,y^w \bmod n$, $\beta = g^w \bmod n$, commits e by computing $\gamma = g^e h^w$, and, finally, shows knowledge of two values s_1, s_2 such that $\alpha^{s_1}/y^{s_2} \pmod{n}$ equals z and that $\log_{y^e}(\alpha^e/z) = \log_g \beta$. All without revealing the secret e. This is done via standard non-interactive techniques based on proofs of knowledge.

Let us remark that these techniques may not work properly into the group G suggested in the original scheme [6]. This is because the group member must check that an element $a \in G$, $a \neq \pm 1$ is of large order by testing whether $\gcd(a \pm 1, n) = 1$. Unfortunately, this implies only that the order of a is

[6] Although $z^{e+k/e}$, $k \in \mathbb{Z}$ can be easily derived from $z^{\bar{e}}$ and $z^{\tilde{e}}$, but this does not seem to hurt.

at least $p'q'$, specifically $\mathrm{ord}_G(a) = p'q'$ or $2p'q'$. For the sake of simplicity, we consider the proof of equality of two discrete logarithms, i.e. given $y_1^{x_1}, y_2^{x_2} \pmod{n}$, proving that $x_1 = x_2$. But if $\mathrm{ord}_G(y_1) = \mathrm{ord}_G(y_2) = 2p'q'$, it might be the case that $x_1 \equiv x_2 \pmod{p'q'}$ but $x_1 \not\equiv x_2 \pmod{2}$. A better choice for G is the set of quadratic residues modulo n, denoted by Q_n. In fact, notice that, when n is product of safe primes, Q_n is a cyclic group of order $p'q'$. In this case, either the group manager shows evidences that the public values, like z, are quadratic residues or the group member (and the verifier) modifies the non-interactive proofs by squaring the parameters involved.

4.2 Our Proposal

Finding a more efficient scheme than that in [6] is a difficult task. We can do so only by simplifying the JOIN operation. More precisely, we can avoid the proof that an element is product of two primes (as already mentioned, this is quite an expensive technique). A detailed description of the resulting group signature will appear in an upcoming paper [1], where the new scheme is analyzed in terms of number of exponentiations. We anticipate that the new scheme is a bit more expensive than that in [2] (however it satisfies the coalition-resistance property) yet more efficient than that in [6] since the JOIN operation requires fewer exponentiations.

The basic idea is to extend the certificate structure in [2], i.e., $A(x) = (a^x\, a_0)^d \bmod n$. As already mentioned, n is the product of two safe primes, a is a generator of Q_n (the set of quadratic residues), and $a_0 \in Q_n$ is a constant such that $\log_a a_0$ is unknown. Now, during the JOIN operation the group member P_i receives the certificate $A(x) = (a^{x_i}\, a_0)^{d_i} \bmod n$, where x_i is the group member's secret (randomized by the group manager) with $\lambda_1 < x_i < \lambda_2$. That is, the group manager randomly selects a prime e_i and computes d_i such that $e_i\, d_i \equiv 1 \pmod{\varphi(n)}$ for each group member P_i, with $0 < \lambda_1 < \lambda_2 < e_i$ (λ_1, λ_2 are fixed *a priori*). We explicitly require that for any $i \neq j$, $e_i \neq e_j$ must hold. The protocol carried out by the group member in order to sign a message, proving knowledge of a valid certificate without revealing useful information, is described in [1]. The security of this certificate against any coalition attacks is based on the strong RSA assumption. The main difference with the certificate structure in [6] is that, now, the primes e_i are exclusively selected by the group manager, thus avoiding any further costly checks.

5 Conclusions

This paper discussed the difficulty of developing coalition-resistant group signature schemes. It presented some attacks on newly proposed schemes and provided strategies for making group signature provably secure.

References

[1] Giuseppe Ateniese, Marc Joye, and Gene Tsudik, *A practical group signature*, Manuscript, 1999.

[2] Giuseppe Ateniese and Gene Tsudik, *Group signatures à la carte*, Tenth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA '99), January 1999. To appear.

[3] ______, *Some open issues and new directions in group signatures*, Financial Cryptography (FC '99) (M. Franklin, ed.), Lecture Notes in Computer Science, Springer-Verlag, 1999. To appear.

[4] Jan Camenisch, *Efficient and generalized group signatures*, Advances in Cryptology — EUROCRYPT '97 (W. Fumy, ed.), Lecture Notes in Computer Science, vol. 1233, Springer-Verlag, 1997, pp. 465–479.

[5] ———, *Group signature schemes and payment systems based on the discrete logarithm problem*, Ph.D. thesis, ETH Zürich, Zurich, February 1998, Published in ETH Series in Information Security and Cryptography, vol. 2, Hartung-Gorre, 1998.

[6] Jan Camenisch and Markus Michels, *A group signature scheme with improved efficiency*, Advances in Cryptology — ASIACRYPT '98 (K. Ohta and D. Pei, eds.), Lecture Notes in Computer Science, vol. 1514, Springer-Verlag, 1998, pp. 160–174.

[7] ———, *A group signature scheme based on an RSA-variant*, Tech. Report RS-98-27, BRICS, Aarhus, November 1998. An earlier version appears in [6].

[8] Jan Camenisch and Markus Stadler, *Efficient group signature schemes for large groups*, Advances in Cryptology — CRYPTO '97 (B.S. Kaliski Jr., ed.), Lecture Notes in Computer Science, vol. 1294, Springer-Verlag, 1997, pp. 410–424.

[9] David Chaum and Eugène van Heijst, *Group signatures*, Advances in Cryptology — EUROCRYPT '91 (D.W. Davies, ed.), Lecture Notes in Computer Science, vol. 547, Springer-Verlag, 1991, pp. 257–265.

[10] Lidong Chen and Torben P. Pedersen, *New group signature schemes*, Advances in Cryptology — EUROCRYPT '94 (A. De Santis, ed.), Lecture Notes in Computer Science, vol. 950, Springer-Verlag, 1995, pp. 171–181.

[11] ———, *On the efficiency of group signatures providing information-theoretic anonymity*, Advances in Cryptology — EUROCRYPT '95 (L.C. Guillou and J.-J. Quisquater, eds.), Lecture Notes in Computer Science, vol. 921, Springer-Verlag, 1995, pp. 39–49.

[12] Yvo Desmedt, *Threshold cryptosystems*, Advances in Cryptology – AUSCRYPT '92 (J. Seberry and Y. Zheng, eds.), Lecture Notes in Computer Science, vol. 718, Springer-Verlag, 1993, pp. 3–14.

[13] Yair Frankel, Yiannis Tsiounis, and Moti Yung, *"indirect disclosure proofs": Achieving efficient fair off-line e-cash*, Advances in Cryptology — ASIACRYPT '96 (K. Kim and T. Matsumoto, eds.), Lecture Notes in Computer Science, vol. 1163, Springer-Verlag, 1996, pp. 286–300.

[14] Marc Girault, *Self-certified public keys*, Advances in Cryptology – EUROCRYPT '91 (D.W. Davies, ed.), Lecture Notes in Computer Science, vol. 547, Springer-Verlag, 1991, pp. 491–497.

[15] Marc Joye, Narn-Yih Lee, and Tzonelih Hwang, *On the security of the Lee-Chang group signature scheme and its derivatives*, Tech. Report TR-99-7, Tamkang LCIS, Tamsui, May 1999.

[16] Seungjoo Kim, Sangjoon Park, and Dongho Won, *Convertible group signatures*, Advances in Cryptology — ASIACRYPT '96 (K. Kim and T. Matsumoto, eds.), Lecture Notes in Computer Science, vol. 1163, Springer-Verlag, 1996, pp. 311–321.

[17] Narn-Yih Lee, *Personal communication*, May 19, 1999.

[18] Wei-Bin Lee and Chin-Chen Chang, *Efficient group signature scheme based on the discrete logarithm*, IEE Proc. Comput. Digit. Tech. **145** (1998), no. 1, 15–18.

[19] Chae Hoon Lim and Pil Joong Lee, *Remarks on convertible group signatures of Asiacrypt '96*, Electronics Letters **33** (1997), no. 5, 383–384.

[20] Anna Lysyanskaya and Zulfikar Ramzan, *Group blind signatures: A scalable solution to electronic cash*, Financial Cryptography (FC '98) (R. Hirschfeld, ed.), Lecture Notes in Computer Science, vol. 1465, Springer-Verlag, 1998, pp. 184–197.

[21] Wenbo Mao and Chae Hoon Lim, *Cryptanalysis in prime order subgroups of $\mathbb{Z}_n$*, Advances in Cryptology — ASIACRYPT '98 (K. Ohta and D. Pei, eds.), Lecture Notes in Computer Science, vol. 1514, Springer-Verlag, 1998, pp. 214–226.

[22] Ueli M. Maurer and Yacov Yacobi, *Non-interactive public-key cryptography*, Advances in Cryptology – EUROCRYPT '91 (D.W. Davies, ed.), Lecture Notes in Computer Science, vol. 547, Springer-Verlag, 1991, pp. 498–507.

[23] Markus Michels, *Comments on some group signature schemes*, Tech. Report TR-96-3-D, University of Technology Chemnitz-Zwickau, Chemnitz, November 1996.

[24] Sangjoon Park, Seungjoo Kim, and Dongho Won, *ID-based group signature*, Electronics Letters **33** (1997), no. 19, 1616–1617.

[25] Sangjoon Park, Insook Lee, and Dongho Won, *A practical group signature*, 1995 Japan-Korea Joint Workshop on Information Security and Cryptography (JW-ISC '95), Japan, January 1995, pp. 127–133.

[26] Sangjoon Park and Dongho Won, *A practical identity-based group signature*, 1995 International Conference on Electronics, Informations and Communications (ICEIC '95), China, August 1995, pp. II–64–II–67.

[27] Holger Petersen, *How to convert any digital signature scheme into a group signature scheme*, Pre-proceedings of the 1997 Workshop on Security Protocols, Paris, April 7–9, 1997.

[28] Adi Shamir, *Identity-based cryptosystems and signatures schemes*, Advances in Cryptology – Proceedings of CRYPTO 84 (G.R. Blakley and D. Chaum, eds.), Lecture Notes in Computer Science, vol. 196, Springer-Verlag, 1985, pp. 47–53.

[29] Yuh-Min Tseng and Jinn-Ke Jan, *A novel ID-based group signature*, 1998 International Computer Symposium, Workshop on Cryptology and Information Security (T.L. Hwang and A.K. Lenstra, eds.), Tainan, December 17–19, 1998, pp. 159–164.

[30] ______, *Improved group signature scheme based on discrete logarithm problem*, Electronics Letters **35** (1999), no. 1, 37–38.

[31] ______, *A group signature scheme using self-certified public keys*, Ninth National Conference on Information Security, May 1999, pp. 165–172.

[32] Chih-Hung Wang, Tzonelih Hwang, and Narn-Yih Lee, *Comments on two group signatures*, Information Processing Letters **69** (1999), 95–97.

A Previous Work

As mentioned in the introduction, *group signatures*[7] were first introduced and realized by Chaum and van Heijst [9] in 1991. A number of improvements and enhancements followed. In [10], Chen and Pedersen answer some open questions raised in [9] and realize the first constructions which allow new members to dynamically join the group. Camenisch [4] introduces and constructs *generalized group signatures* which allow some coalitions of group members to sign on the group's behalf. However, all these signature schemes present the main drawback that the length of the group public key depends on the number of group members. Note that this is always the case when *unconditional* anonymity is desired [11].

Based on previous work of Park, I. Lee, and Won [25] (flawed in [23]), Kim, Park, and Won [16] put forth the concept of *convertible group signatures*. In addition to the properties of the standard group signatures, convertible group signatures of a given group member can be turned into ordinary signatures if that member releases some secret information. Later, Lim and P. J. Lee [19] (see also [23]) broke their schemes, showing that the parameters were improperly chosen and, more importantly, that the proposed group signatures were not coalition-resistant. Wang, Hwang, and N.-Y. Lee [32] further comment that their schemes do not allow to uniquely identify the original signer, even if the signer honestly follows the signature procedure. The reverse direction, i.e., converting an ordinary signature into a group signature, was investigated by Petersen [27]. His generic conversion makes use of the 'indirect disclosure proof' technique [13]; the length of the resulting group signatures is, however, linear in the number of group members.

[7] The notion of group signatures is sometimes confused with the notion of *group-oriented signatures* where certain subsets of a group of people are allowed to sign on behalf of the group [12]. However, these latter schemes do not provide a method for identifying the signers.

Following Shamir [28], Park, Kim, and Won [24] (see also [26]) suggest *ID-based group signatures*. Their scheme was broken by Mao and Lim [21]: exploiting the prime order subgroup structure of the scheme, they showed that the anonymity of the signatures was not guaranteed. Moreover, the Park-Kim-Won scheme suffers from being rather expensive and 'static' in the sense that if new group members are added, the previously signed messages can no longer be verified with the updated public-key. A much better ID-based group signature scheme which does not present these limitations was proposed by Tseng and Jan [29]. In [31], Tseng and Jan also propose a group signature scheme based on the related notion of self-certified public keys [14]. See Section 3 for a discussion on the security of these two schemes.

Another efficient group signature scheme was recently proposed by W.-B. Lee and Chang [18], but, unfortunately, it does not enjoy the desirable property of unlinkability. An improved (i.e., unlinkable) version of the Lee-Chang scheme is proposed in [30]. Actually, any obvious attempt to make the Lee-Chang scheme unlinkable would likely fail; furthermore, both the original and the improved Lee-Chang schemes are known to be susceptible to *universal* forgeries [15].

The first group signature suitable for *large groups* is that of Camenisch and Stadler [8]: both the length of the group public key and the group signatures are independent of the group's size. Moreover, a new member addition does not involve re-issuing other members' keys and/or changing the group public key. The Camenisch-Stadler scheme was subsequently improved by Camenisch and Michels in [6] (see also [7]), which now undoubtedly represents the *state-of-the-art* in the field; i.e., the most *practical* group signature scheme (in the sense of Definition 2.2).

Lysyanskaya and Ramzan introduce *group blind signatures* in [20]. These signatures require that a group member signs on group's behalf a document without knowing its content. In [3], Ateniese and Tsudik discuss two other extensions of group signatures, namely *multi-group signatures* and *sub-group signatures*. A multi-group signature is a set of regular group signatures generated by the same signer as a member of multiple groups, whereas a sub-group signature is a group signature generated by a sub-group of group members. The main difference with the generalized group signatures as defined by Camenisch [4] resides in that the size of the sub-group is publicly verifiable.