Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions

Mihir Bellare, Daniele Micciancio, and Bogdan Warinschi

Dept. of Computer Science & Engineering
University of California at San Diego
9500 Gilman Drive, La Jolla, California 92093, USA.
{mihir, daniele, bogdan}@cs.ucsd.edu
http://www-cse.ucsd.edu/users/{mihir, daniele, bogdan}

Abstract. This paper provides theoretical foundations for the group signature primitive. We introduce strong, formal definitions for the core requirements of anonymity and traceability. We then show that these imply the large set of sometimes ambiguous existing informal requirements in the literature, thereby unifying and simplifying the requirements for this primitive. Finally we prove the existence of a construct meeting our definitions based only on the sole assumption that trapdoor permutations exist.

1 Introduction

A central line of work in theoretical cryptography is to provide formal (and strong) definitions of security for cryptographic primitives, and then provide constructions, based on general computational-complexity assumptions (such as the existence of one-way or trapdoor functions), that satisfy the definitions in question. The value and difficulty of such "foundational" work is acknowledged and manifest. A classical example is public-key encryption. Although it might seem like an intuitive goal, much work has been required to formally define and provably achieve it [19, 21, 18, 22, 25, 16], and these advances now serve as the basis for new schemes and applications. This paper provides such foundations for the group signatures primitive.

Background. In the group signature setting introduced by Chaum and Van Heyst [14] there is a group having numerous members and a single manager. Associated to the group is a single signature-verification key *gpk* called the group public key. Each group member i has its own secret signing key based on which it can produce a signature relative to *gpk*. The core requirements as per [14] are that the group manager has a secret key *gmsk* based on which it can, given a signature σ, extract the identity of the group member who created σ (traceability) and on the other hand an entity not holding *gmsk* should be unable, given a signature σ, to extract the identity of the group member who created σ (anonymity). Since then, more requirements, that refine or augment

the core ones, have been introduced (eg. unlinkability, unforgeability, collusion resistance [5], exculpability [5], and framing resistance [15]) so that now we have a large set of unformalized, overlapping requirements whose precise meaning, and relation to each other, is neither always clear nor even always agreed upon in the existing literature.

The state of the art is represented by [5, 2] that identify weaknesses in previous works and present new schemes. The schemes in [2] are claimed to be proven-secure (in the random oracle model). However, while the work in question establishes certain properties, such as zero-knowledge, of certain subprotocols of its scheme, there is no actual definition of the security of a group signature scheme. For example, the anonymity requirement is formulated simply as the phrase "given a valid signature of some message, identifying the actual signer is computationally hard for everyone but the group manager." This is like formulating the privacy requirement for an encryption scheme as the phrase "the ciphertext should not reveal information about the message to anyone except the owner of the secret key," yet to truly capture privacy requires significantly more precise and non-trivial definitions, as evidenced by [19, 21, 18, 22, 25, 16]. In particular the informal requirement of [2] leaves open the issue of what exactly is the attack model and definition of adversarial success. Can the attacker see, or request, previous signatures? Can it call on the group manager to "open" some previous signatures? Can it have partial information ruling out some signers a priori? With such questions unanswered, we believe it is premature to say that proven-security has been achieved.

Furthermore, all claims of proven secure schemes so far have been in the random-oracle model. As far as we know, there are no constructions even claimed to be proven secure in the standard model.

New notions. Providing appropriate definitions has required significantly more than merely formalizing the intuitive informal requirements of previous works. We consider novel attack capabilities and success measures, and then formulate strong versions of the core requirements that we call full-anonymity and full-traceability. Perhaps surprisingly, we are then able to show that these two requirements are enough, in the sense that all the other requirements are implied by them. Our formalisms build on definitional ideas used for encryption [19, 21, 18, 22, 25, 16] and digital signatures [20].

Full-anonymity. We adopt an indistinguishability based formalization under which the adversary produces a message and a pair of group-member identities, is returned a target signature of the given message under a random one of the two identities and then is required to have negligible advantage over one-half in determining under which of the two identities the target signature was produced. Within this framework, we define a strong adversary that may corrupt all the members of the group, including the one issuing the signature. (Formally, the adversary is given the secret keys of all group members.) We also capture (in analogy to the definition of encryption secure against chosen-ciphertext attack [25]) the possibility that the adversary can see the outcome of opening attempts

conducted by the group manager on arbitrary signatures of its choice (except of course the challenge signature).

Full-traceability. Our formulation of traceability is much stronger than what was called traceability in the past, and can be viewed also as a strong form of collusion-resistance. It asks that a group of colluding group members who pool their secret keys cannot create a valid signature that the opening algorithm would not catch as belonging to some member of the colluding group, and this is true even if the colluding group knows the secret key of the group manager under which signatures are opened.

Implications. As indicated above, there is a large and growing list of informal security requirements for group signatures. We show however that all existing requirements are implied by full-anonymity plus full-traceability. This provides a conceptual simplification with a clear advantage: having to check only two security properties makes it easier to give formal proofs of security when new group signature schemes are invented.

These implications might seem surprising at first glance, particularly because the implied properties include seemingly unrelated notions like unforgeability (nobody outside the group can produce valid signatures) or security against framing attacks (no one can produce signatures that will be later attributed to a honest group member that never signed the corresponding document). However the fact that a small number of strong formal notions imply a large number of informal requirements should be viewed, based on historical evidence, as an expected rather than a surprising benefit, and even as a test of the definitions in question. As an analogy, in the absence of a strong formal notion, one might formulate the security of encryption via a list of requirements, for example security against key-recovery (it should be hard to recover the secret key from the public key), security against inversion (it should be hard to recover the plaintext from the ciphertext), security under repetition (it should be hard to tell whether the messages corresponding to two ciphertexts are the same) and so on, and we can imagine these requirements being discovered incrementally and being thought to be quite different from each other. However, strong notions like indistinguishability [19], semantic security [19] and non-malleability [16] imply not only all these, but much stronger properties, and in particular put the different informal requirements under a common umbrella. We believe we are doing the same for group signatures.

Our scheme. With such strong notions of security, a basic theoretical question emerges, namely whether or not a scheme satisfying them even exists, and, if so, what are the minimal computational-complexity assumptions under which this existence can be proven. We answer this by providing a construction of a group signature scheme that provably achieves full-anonymity and full-traceability (and thus, by the above, also meets all previous security requirements) assuming only the existence of trapdoor permutations. We stress that this result is not in the random oracle model. Additionally we note that (1) Our construction is "non-trivial" in the sense that the sizes of all keys depend only logarithmically (rather than polynomially) on the number of group members, (2) It can be extended

to permit dynamic addition of group members, and (3) It can be extended to achieve forward security (cf. [28]).

The construction uses as building blocks an IND-CCA secure asymmetric encryption scheme, known to exist given trapdoor permutations via [16]; simulation-sound adaptive non-interactive zero-knowledge (NIZK) proofs for NP, known to exist given trapdoor permutations via [17, 27]; and a digital signature scheme secure against chosen-message attack, known to exist given trapdoor permutations via [6]. As often the case with constructs based on general assumptions, our scheme is polynomial-time but not practical, and our result should be regarded as a plausibility one only.

The basic framework of our construction builds on ideas from previous works (eg. [2]). Roughly, the secret signing key of a group member includes a key-pair for a standard digital signature scheme that is certified by the group manager. The group member's signature is an encryption, under a public encryption key held by the group manager, of a standard signature of the message together with certificate and identity information, and accompanied by a non-interactive zero-knowledge proof that signature contains what it should. However, our result is still more than an exercise. Previous works did not try to achieve security notions as strong as we target, nor to pin down what properties of the building blocks suffice to actually prove security. For example we found that the encryption scheme had to be secure against chosen-ciphertext attack and not just chosen-plaintext attack. Further subtleties are present regarding the NIZK proofs. We require them to be simulation-sound and also have a strong, adaptive zero-knowledge property [27]. On the other hand, we only require NIZK proofs for a single theorem rather than multiple theorems. We highlight this because at first glance it can sound impossible, but it is due to the strong ZK property, and the situation is not without precedent: single-theorem adaptive ZK proofs have sufficed also for applications in [27].

Related work. As indicated above, the notion of group signature was introduced by Chaum and Heyst in [14]. They also gave the first schemes. Since then, many other schemes were proposed, including [15, 11, 24, 13, 4]. These schemes improve on the performance of the original group signature scheme of [14], but leave open some important security issues, most notably security against coalitions of group members. The importance of achieving provable security against coalitions of group members is pointed out in [5], where a (partial) coalition attack on the scheme of [13] is also described. A subsequent work trying to address the issue of securing group signature schemes against coalition attacks is [2]. On a separate research line, [10, 3, 12] investigate issues related to the dynamics of the group, to support membership revocation, and independent generation of group member keys. Still another extension is that of [28], that combines group signature schemes with forward security [1, 8]. The strong anonymity and traceability issues discussed in this paper are largely independent of the group dynamics or other desirable properties like forward security. So, for ease of exposition, we first present and analyze our definitions for the syntactically simpler case of static groups. Dynamic groups and other extensions are discussed in Section 5.

2 Definitions of the security of group signature schemes

NOTATION AND TERMINOLOGY. If x is a string, then $|x|$ denotes its length, while if S is a set then $|S|$ denotes its size. The empty string is denoted by ε. If $k \in \mathbb{N}$ then 1^k denotes the string of k ones. If n is an integer then $[n] = \{1, \ldots, n\}$. If A is a randomized algorithm then $[A(x, y, \ldots)]$ denotes the set of all points having positive probability of being output by A on inputs $x, y, \ldots$, and by $z \xleftarrow{\$} A(x, y, \ldots)$ the result of running A on the same inputs with freshly generated coins. We say that a function $f\colon \mathbb{N} \to \mathbb{N}$ is *nice* if it is polynomially bounded (i.e. there exists a polynomial $p(\cdot)$ such that $f(k) \leq p(k)$ for all $k \in \mathbb{N}$) and polynomial-time computable. The notion of a function $\nu\colon \mathbb{N} \to \mathbb{N}$ being negligible is standard. In this paper we will need a notion of negligibility of a two-argument function $\mu\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. We say such a μ is negligible if for every nice function $n\colon \mathbb{N} \to \mathbb{N}$, the function $\mu_n\colon \mathbb{N} \to \mathbb{N}$ is negligible, where $\mu_n(k) = \mu(k, n(k))$ for all $k \in \mathbb{N}$.

SYNTAX OF GROUP SIGNATURE SCHEMES. A *group signature scheme* $\mathcal{GS} = (\mathsf{GKg}, \mathsf{GSig}, \mathsf{GVf}, \mathsf{Open})$ consists of four polynomial-time algorithms:

- The randomized *group key generation* algorithm GKg takes input $1^k, 1^n$, where $k \in \mathbb{N}$ is the security parameter and $n \in \mathbb{N}$ is the group size (ie. the number of members of the group), and returns a tuple $(gpk, gmsk, \boldsymbol{gsk})$, where gpk is the *group public key*, $gmsk$ is the *group manager's secret key*, and $\boldsymbol{gsk}$ is an n-vector of keys with $\boldsymbol{gsk}[i]$ being a *secret signing key* for player $i \in [n]$.
- The randomized *group signing* algorithm GSig takes as input a secret signing key $\boldsymbol{gsk}[i]$ and a message m to return a signature of m under $\boldsymbol{gsk}[i]$ ($i \in [n]$).
- The deterministic *group signature verification* algorithm GVf takes as input the group public key gpk, a message m, and a candidate signature σ for m to return either 1 or 0.
- The deterministic *opening* algorithm Open takes as input the group manager secret key $gmsk$, a message m, and a signature σ of m to return an identity i or the symbol $\perp$ to indicate failure.

For simplicity we are assigning the members consecutive integer identities $1, 2, \ldots, n$. We say that σ is a *true* signature of m if there exists $i \in [n]$ such that $\sigma \in [\mathsf{GSig}(\boldsymbol{gsk}[i], m)]$. We say that σ is a *valid* signature of m with respect to gpk if $\mathsf{GVf}(gpk, m, \sigma) = 1$.

CORRECTNESS. The scheme must satisfy the following *correctness* requirement: For all $k, n \in \mathbb{N}$, all $(gpk, gmsk, \boldsymbol{gsk}) \in [\mathsf{GKg}(1^k, 1^n)]$, all $i \in [n]$ and all $m \in \{0,1\}^*$

$$\mathsf{GVf}(gpk, m, \mathsf{GSig}(\boldsymbol{gsk}[i], m)) = 1 \text{ and } \mathsf{Open}(gmsk, m, \mathsf{GSig}(\boldsymbol{gsk}[i], m)) = i\ .$$

The first says that true signatures are always valid. The second asks that the opening algorithm correctly recovers the identity of the signer from a true signature.

DISCUSSION. The definitions above are for the setting in which the group is static, meaning the number and identities of members is decided at the time the group is set up and new members cannot be added later. We prefer to begin with this setting because, even though dynamic groups (in which members may be added at any time) have been considered, proper definitions of security have not been provided even for the basic static-group case. Furthermore the important definitional issues arise already in this context and can thus be treated in a simpler setting. The extension to dynamic groups is relatively straightforward.

COMPACTNESS. In practice it is preferable that sizes of keys and signatures in a group signature scheme do not grow proportionally to the number of members n. Actually, a polynomial dependency of these sizes on $\log(n)$ can be shown to be unavoidable, but ideally one would not want more than that. In our context, this leads to the following efficiency criterion for a group signature scheme. We call a group signature scheme $\mathcal{GS} = (\mathsf{GKg}, \mathsf{GSig}, \mathsf{GVf}, \mathsf{Open})$ *compact* if there exist polynomials $p_1(\cdot,\cdot)$ and $p_2(\cdot,\cdot,\cdot)$ such that

$$|gpk|, |gmsk|, |\boldsymbol{gsk}[i]| \leq p_1(k, \log(n)) \text{ and } |\sigma| \leq p_2(k, \log(n), |m|)$$

for all $k, n \in \mathbb{N}$, all $(gpk, gmsk, \boldsymbol{gsk}) \in [\mathsf{GKg}(1^k, 1^n)]$, all $i \in [n]$, all $m \in \{0,1\}^*$ and all $\sigma \in [\mathsf{GSig}(\boldsymbol{gsk}[i], m)]$.

FULL-ANONYMITY. Informally, anonymity requires that an adversary not in possession of the group manager's secret key find it hard to recover the identity of the signer from its signature. As discussed in the introduction, our formalization is underlain by an indistinguishability requirement, on which is superimposed an adversary with strong attack capabilities. To capture the possibility of an adversary colluding with group members we give it the secret keys of all group members. To capture the possibility of its seeing the results of previous openings by the group manager, we give it access to an *opening oracle*, $\mathsf{Open}(gmsk, \cdot, \cdot)$, which when queried with a message m and signature σ, answers with $\mathsf{Open}(gmsk, m, \sigma)$.

Let us now proceed to the formalization. To any group signature scheme $\mathcal{GS} = (\mathsf{GKg}, \mathsf{GSig}, \mathsf{GVf}, \mathsf{Open})$, adversary A and bit b we associate the first experiment given in Figure 1. Here, A is an adversary that functions in two stages, a choose stage and a guess stage. In the choose stage A takes as input the group members secret keys, $\boldsymbol{gsk}$, together with the group public key gpk. During this stage, it can also query the opening oracle $\mathsf{Open}(gmsk, \cdot)$ on group signatures of his choice, and it is required that at the end of the stage A outputs two valid identities $1 \leq i_0, i_1 \leq n$, and a message m. The adversary also outputs some state information to be used in the second stage of the attack. In the second stage, the adversary is given the state information, and a signature on m produced using the secret key of one of the two users i_0, i_1, chosen at random. The goal is to guess which of the two secret keys was used. The adversary can still query the opening oracle, but not on the challenge signature. We denote by

$$\mathbf{Adv}^{\text{anon}}_{\mathcal{GS},A}(k,n) = \Pr\left[\mathbf{Exp}^{\text{anon-1}}_{\mathcal{GS},A}(k,n) = 1\right] - \Pr\left[\mathbf{Exp}^{\text{anon-0}}_{\mathcal{GS},A}(k,n) = 1\right]$$

the advantage of adversary A in breaking the full-anonymity of $\mathcal{GS}$. We say that a group signature scheme is *fully-anonymous* if for any polynomial-time

Experiment $\mathbf{Exp}^{\text{anon-b}}_{\mathcal{GS},A}(k,n)$
$(gpk, gmsk, \boldsymbol{gsk}) \xleftarrow{\$} \mathsf{GKg}(1^k, 1^n)$
$(\mathrm{St}, i_0, i_1, m) \xleftarrow{\$} A^{\mathsf{Open}(gmsk,\cdot,\cdot)}(\mathsf{choose}, gpk, \boldsymbol{gsk})$; $\sigma \xleftarrow{\$} \mathsf{GSig}(\boldsymbol{gsk}[i_b], m)$
$d \xleftarrow{\$} A^{\mathsf{Open}(gmsk,\cdot,\cdot)}(\mathsf{guess}, \mathrm{St}, \sigma)$
If A did not query its oracle with m, σ in the guess stage then return d EndIf
Return 0

Experiment $\mathbf{Exp}^{\text{trace}}_{\mathcal{GS},A}(k,n)$
$(gpk, gmsk, \boldsymbol{gsk}) \xleftarrow{\$} \mathsf{GKg}(1^k, 1^n)$
$\mathrm{St} \leftarrow (gmsk, gpk)$; $\mathcal{C} \leftarrow \emptyset$; $K \leftarrow \varepsilon$; $\mathrm{Cont} \leftarrow \mathsf{true}$
While $(\mathrm{Cont} = \mathsf{true})$ do
$(\mathrm{Cont}, \mathrm{St}, j) \xleftarrow{\$} A^{\mathsf{GSig}(\boldsymbol{gsk}[\cdot],\cdot)}(\mathsf{choose}, \mathrm{St}, K)$
If $\mathrm{Cont} = \mathsf{true}$ then $\mathcal{C} \leftarrow \mathcal{C} \cup \{j\}$; $K \leftarrow \boldsymbol{gsk}[j]$ EndIf
Endwhile
$(m, \sigma) \xleftarrow{\$} A^{\mathsf{GSig}(\boldsymbol{gsk}[\cdot],\cdot)}(\mathsf{guess}, St)$
If $\mathsf{GVf}(gpk, m, \sigma) = 0$ then return 0 ; If $\mathsf{Open}(gmsk, m, \sigma) = \perp$ return 1
If there exists $i \in [n]$ such that the following are true then return 1 else return 0:
1. $\mathsf{Open}(gmsk, m, \sigma) = i \notin \mathcal{C}$
2. i, m was not queried by A to its oracle

Fig. 1. Experiments used, respectively, to define full-anonymity and full-traceability of group signature scheme $\mathcal{GS} = (\mathsf{GKg}, \mathsf{GSig}, \mathsf{GVf}, \mathsf{Open})$. Here A is an adversary, $b \in \{0,1\}$, and St denotes state information passed by the adversary between stages.

---

adversary A, the two-argument function $\mathbf{Adv}^{\text{anon}}_{\mathcal{GS},A}(\cdot,\cdot)$ is negligible in the sense of negligibility of two-argument functions defined at the beginning of this section.

In the above experiment, the adversary issues a request to sign its message m under one of two identities i_0, i_1 that it specifies, and wins if it can guess which was chosen. One might feel that allowing just one such request is restrictive, and the adversary should be allowed a sequence of such requests. (The challenge bit b remains the same in answering all requests). However, a standard hybrid argument shows that, under polynomial-time reductions, allowing a polynomial number of requests is equivalent to allowing just one request, so our definition is not restrictive. This hybrid argument depends on the fact that the adversary has the group public key and the secret signing keys of all members.

Full-traceability. In case of misuse, signer anonymity can be revoked by the group manager. In order for this to be an effective deterrence mechanism, the group signature scheme should satisfy the following, informally described, security requirement. We require that no colluding set S of group members (even consisting of the entire group, and even being in possession of the secret key for opening signatures) can create signatures that cannot be opened, or signatures that cannot be traced back to some member of the coalition. We remark that

giving the opening key to the adversary does not model corruptness of the group manager,[1] but rather compromise of the group manager's key by the adversary. We call our requirement *full-traceability*.

We formally define full-traceability using the second experiment of Figure 1. Here, adversary A runs in two stages, a choose stage and a guess stage. On input the group public key gpk and the secret of the group manager, $gmsk$, the adversary starts its attack by adaptively corrupting a set $\mathcal{C}$ of group members. The identity of the group members that are corrupted and their number is entirely up to it. At the end of the choose stage the set $\mathcal{C}$ contains the identities of the corrupted members. In the guess stage, the adversary attempts to produce a forgery (m, σ), and we say it wins (meaning the experiment returns 1), if σ is a valid group signature on m, but the opening algorithm returns $\perp$ or some valid user identity i such that $i \notin \mathcal{C}$. Otherwise, the experiment returns 0. We define the advantage of adversary A in defeating full-traceability of the group signature scheme $\mathcal{GS}$ by:

$$\mathbf{Adv}^{\text{trace}}_{\mathcal{GS},A}(k, n) = \Pr\left[\, \mathbf{Exp}^{\text{trace}}_{\mathcal{GS},A}(k, n) = 1 \,\right] ,$$

and say that $\mathcal{GS}$ is *fully-traceable* if for any polynomial-time adversary A, the two-argument function $\mathbf{Adv}^{\text{trace}}_{\mathcal{GS},A}(\cdot, \cdot)$ is negligible.

3 Relations to Existing Security Notions

We show that our formulations of anonymity and traceability are strong enough to capture all existing informal security requirements in the literature. This highlights the benefits of strong notions.

Unforgeability. A basic requirement of any digital signature scheme ([14]) is that signatures cannot be forged, i.e., it is computationally unfeasible to produce message signature pairs (m, σ) that are accepted by the verification algorithm, without knowledge of the secret key(s). We did not include unforgeability among the main security properties of group signature schemes, since it immediately follows from full-traceability.

In order to define unforgeability, one can restrict the adversary used in the definition of full-traceability to just the second stage: in the first stage it does not ask for any secret key, and also, the secret key of the group manager is not part of its initial state St. Still, the adversary can obtain digital signatures of its choice using the signing oracle. In this case a successful attack against the full-traceability requirement reduces to producing a valid message signature pair (m, σ) such that message m was not queried to the signing oracle. The condition about the opening algorithm tracing the signature to a nonmember of the set of corrupted users is vacuously satisfied because this set is empty.

Exculpability. Exculpability (first introduced in [5]) is the property that no member of the group and not even the group manager can produce signatures on behalf of other users.

[1] See section 5 for a detailed discussion of this case

Clearly, a group signature scheme secure against full-traceability has also the exculpability property. If either the group manager or a user defeats the exculpability of a group signature scheme, then an adversary against full-traceability can be easily constructed. In the first case, the adversary simply follows the strategy of the group manager and produces a signature that is a forgery in the sense of full-traceability: it can not be traced to the one who produced it. In the second case, say user i can defeat the exculpability property. Then, an adversary as in the full-traceability experiment, which in the first stage makes a single request for $\boldsymbol{gsk}[i]$, and then follows the strategy of the user to produce the forgery, is successful against full-traceability.

Traceability. Originally [14], the name "traceability" was used to denote the *functional* property that if a message is signed with key $\boldsymbol{gsk}[i]$ and the opening algorithm is applied to the resulting signature, the output of the opening algorithm must be i. Later, the term has been overloaded to include an actual *security* requirement, namely that it is not possible to produce signatures which can not be traced to one of the group that has produced the signature. The two requirements seem to be first separated in [2] where the latter was identified with coalition resistance (see below). Nevertheless, a group signature scheme that is fully traceable, is also traceable (under either definition of traceability).

Coalition resistance. The possibility of a group of signers colluding together to generate signatures that cannot be traced to any of them was not part of the original formulation of secure group signature schemes. The requirement of traceability even in the face of attacks by a coalition of group members was explicitly considered for the first time only recently in [2], and termed coalition resistance. In the descriptions of the property, details such as whether the coalition is dynamically chosen or not are left unspecified. A strong formalization of coalition resistance can be obtained using the experiment for full-traceability in which the adversary is not given the secret key of the group manager. The rest remains essentially unchanged. It is then immediate that fully-traceable group signature schemes are also coalition resistant.

Framing. Framing is a version of coalition resistance that was first considered in [15]. Here, a set of group members combine their keys to produce a valid signatures in such a way that the opening algorithm will attribute the signature to a different member of the group. As in the case of coalition resistance, framing has not been formally defined, issues similar to the one discussed above being left unspecified. A strong formalization for framing is the following: consider an experiment in which a user's identity u is chosen at random from the set of all users, and all group secret keys, except the secret key of u, together with the secret key of the group manager are given to the adversary. The adversary wins if it manages to produce a signature which will open as user u, and we call a scheme secure against framing if no efficient adversary can win with non-negligible probability.

A group signature scheme that is fully-traceable, is also secure against framing. Indeed, an adversary B against framing can be turned into an adversary A against full-traceability as follows. It generates a random user identity and

requests the secret keys of all other users. Then it runs adversary B with input these secret keys and the secret key of the group manager and outputs the forgery attempted by B. If B is successful in its framing attempt, then A defeats full-traceability.

ANONYMITY. As we have already discussed, anonymity is just a weaker form of full anonymity, in which the adversary does not have access to the opening oracle, and also, has no information of the member's secret keys. Clearly, a scheme that is fully-anonymous is also anonymous.

UNLINKABILITY. This is related to anonymity rather than full-traceability. The intuition is that a party after seeing a list of signatures, can not relate two signatures together as being produced by the same user. As for anonymity, it was implicit in previous definitions that the attacker was assumed not to be a group member. Again, realistic scenarios exist where this is not necessarily the case. It is thus necessary to consider distinct security notions for the two cases i.e. *insider/outsider unlinkability*. In either case, formalizing unlinkability is not an easy task because it is not clear how (possibly linked) signatures should be produced. For example we can require that it is computationally hard to distinguish between a box that each time receives an input message produces a signature using a fixed secret key $\boldsymbol{gsk}[i]$, or a box where i is chosen uniformly at random for every invocation of the oracle. However, it is not clear why the uniform distribution should be used in the second case. Alternatively, we could let the adversary choose the distribution in the second case, but still in real applications it seems unjustifiable to assume that the signer is chosen each time independently at random and the choice of the signer at different times might be correlated. We considered various possible formalization of the notion of unlinkability, and in all cases we could prove that it follows from anonymity. Also, it seems that for any reasonable formulation of unlinkability, one can prove that anonymity also follows. We conclude that anonymity and unlinkability are technically the same property, and only the easier to define anonymity property needs to be included in the security definition. We postpone a formalization of unlinkability together with a proof of the above fact for the full version of the paper.

4 Our construction

We begin by describing the primitives we use in our construction.

DIGITAL SIGNATURE SCHEMES. A digital signature scheme $\mathcal{DS} = (\mathsf{K_s}, \mathsf{Sig}, \mathsf{Vf})$ is specified, as usual, by algorithms for key generation, signing and verifying. We assume that the scheme satisfies the standard notion of unforgeability under chosen message attack [20]. It is known that such a scheme exists assuming one-way functions exist [26], and hence certainly assuming the existence of a family of trapdoor permutations.

ENCRYPTION SCHEMES. A public-key encryption scheme $\mathcal{AE} = (\mathsf{K_e}, \mathsf{Enc}, \mathsf{Dec})$ is specified, as usual, by algorithms for key generation, encryption and decryption. We assume that the scheme satisfies the standard notion of indistinguishability

under chosen-ciphertext attack (IND-CCA) [25]. It is known that the existence of trapdoor permutations implies that such schemes exists [16].

Simulation-sound Non-interactive zero knowledge proof systems. We will use simulation-sound NIZK proofs of membership in NP languages. Simple NIZK proof systems are provided by [17], and in [27] it is shown how to transform any such proof system into one that also satisfies simulation-soundness. These proofs systems pertain to the witness relations underlying the languages, which is how we will need to look at them. An NP-*relation over domain* Dom $\subseteq \{0,1\}^*$ is a subset ρ of $\{0,1\}^* \times \{0,1\}^*$ such that membership of $(x,w) \in \rho$ is decidable in time polynomial in the length of the first argument for all x in domain Dom. The language associated to ρ is the set of all $x \in \{0,1\}^*$ such that there exists a w for which $(x,w) \in \rho$. Often we will just use the term NP-relation, the domain being implicit. If $(x,w) \in \rho$ we will say that x is a *theorem* and w is a *proof* of x.

Fix a NP relation ρ over domain Dom. Consider a pair of polynomial time algorithms (P,V), where P is randomized and V is deterministic. They have access to a *common reference string*, R. We say that (P,V) form a *non-interactive proof system* for ρ [17, 9] over domain Dom if there exists a polynomial p such that the following two conditions are satisfied:

1. **Completeness:** $\forall k \in \mathbb{N},\ \forall (x,w) \in \rho$ with $|x| \le k$ and $x \in$ Dom–
$$\Pr\left[R \xleftarrow{\$} \{0,1\}^{p(k)} \,;\, \pi \xleftarrow{\$} P(k,x,w,R) \ :\ V(k,x,\pi,R) = 1 \right] \ =\ 1\ .$$
2. **Soundness:** $\forall k \in \mathbb{N},\ \forall \widehat{P},\ \forall x \in$ Dom such that $x \notin L_\rho$–
$$\Pr\left[R \xleftarrow{\$} \{0,1\}^{p(k)} \,;\, \pi \leftarrow \widehat{P}(k,x,R) \ :\ V(k,x,\pi,R) = 1 \right] \ \le\ 2^{-k}\ .$$

We detail the zero-knowledge requirement as well as the simulation-soundness property in the full paper [7].

Specification. We need to begin by specifying the witness relation ρ underlying the zero-knowledge proofs. We will then fix a proof system (P,V) for ρ and define the four algorithms constituting the group signature scheme in terms of P,V and the algorithms of $\mathcal{DS}$ and $\mathcal{AE}$. Consider the relation ρ defined as follows: $((pk_e, pk_s, M, C), (i, pk', \mathrm{cert}, s, r)) \in \rho$ iff $\mathsf{Vf}(pk_s, \langle i, pk' \rangle, \mathrm{cert}) = 1$, $\mathsf{Vf}(pk', M, s) = 1$, and $\mathsf{Enc}(pk_e, \langle i, pk', \mathrm{cert}, s \rangle; r) = C$. Here M is a k-bit message, C a ciphertext and s a signature. We are writing $\mathsf{Enc}(pk_e, m; r)$ for the encryption of a message m under the key pk_e using the coins r, and assume that $|r| = k$. The domain Dom corresponding to ρ is the set of all (pk_e, pk_s, M, C) such that pk_e (resp. pk_s) is a public key having non-zero probability of being produced by $\mathsf{K_e}$ (resp. $\mathsf{K_s}$) on input k, and M is a k-bit string. It is immediate that ρ is a NP relation over Dom, and consequently we can fix a non-interactive zero knowledge proof system (P,V) for it. Based on this, the algorithms defining the group signature scheme are depicted in Figure 2.

Security Results. Fix digital signature scheme $\mathcal{DS} = (\mathsf{K_s}, \mathsf{Sig}, \mathsf{Vf})$, public-key encryption scheme $\mathcal{AE} = (\mathsf{K_e}, \mathsf{Enc}, \mathsf{Dec})$, NP-relation ρ over domain Dom, and its non-interactive proof system (P,V) as above, and let $\mathcal{GS} = (\mathsf{GKg},$

Algorithm $\mathsf{GKg}(k, n)$
$R \xleftarrow{\$} \{0,1\}^{p(k)}$; $(pk_e, sk_e) \xleftarrow{\$} \mathsf{K_e}(k)$; $(pk_s, sk_s) \xleftarrow{\$} \mathsf{K_s}(k)$
For $i \leftarrow 1$ to n do
$(pk_i, sk_i) \xleftarrow{\$} \mathsf{K_s}(k)$; $\mathrm{cert}_i \leftarrow \mathsf{Sig}(sk_s, \langle i, pk_i \rangle)$
$\boldsymbol{gsk}[i] \leftarrow (k, R, i, pk_i, sk_i, \mathrm{cert}_i, pk_e, pk_s)$
Endfor
$gpk \leftarrow (R, pk_e, pk_s)$; $gmsk \leftarrow (n, pk_e, sk_e, pk_s)$; Return $(gpk, gmsk, \boldsymbol{gsk})$

Algorithm $\mathsf{GVf}(gpk, (m, \sigma))$
Parse gpk as (R, pk_e, pk_s) ; Parse σ as (C, π)
Return $V(k, (pk_e, pk_s, M, C), \pi, R)$

Algorithm $\mathsf{GSig}(\boldsymbol{gsk}[i], m)$
Parse $\boldsymbol{gsk}[i]$ as $(k, R, i, pk_i, sk_i, \mathrm{cert}_i, pk_e, pk_s)$
$s \leftarrow \mathsf{Sig}(sk_i, m)$; $r \xleftarrow{\$} \{0,1\}^k$; $C \leftarrow \mathsf{Enc}(pk_e, \langle i, pk_i, \mathrm{cert}_i, s \rangle; r)$
$\pi \xleftarrow{\$} P(k, (pk_e, pk_s, m, C), (i, pk_i, \mathrm{cert}_i, s, r), R)$; $\sigma \leftarrow (C, \pi)$; Return σ

Algorithm $\mathsf{Open}(gmsk, gpk, m, \sigma)$
Parse $gmsk$ as (n, pk_e, sk_e, pk_s) ; Parse σ as (C, π)
If $V(k, (m, C), \pi, R) = 0$ then return $\perp$
Parse $\mathsf{Dec}(sk_e, C)$ as $\langle i, pk, \mathrm{cert}, s \rangle$
If $(n < i$ OR $\mathsf{Vf}(pk, m, s) = 0$ OR $\mathsf{Vf}(pk_s, \langle i, pk \rangle, \mathrm{cert}) = 0)$ then return $\perp$
Else return i

Fig. 2. Our construction: Group signature scheme $\mathcal{GS} = (\mathsf{GKg}, \mathsf{GSig}, \mathsf{GVf}, \mathsf{Open})$ associated to digital signature scheme $\mathcal{DS} = (\mathsf{K_s}, \mathsf{Sig}, \mathsf{Vf})$, public-key encryption scheme $\mathcal{AE} = (\mathsf{K_e}, \mathsf{Enc}, \mathsf{Dec})$, and non-interactive proof system (P, V).

$\mathsf{GSig}, \mathsf{GVf}, \mathsf{Open})$ denote the signature scheme associated to them as per our construction. We claim the following two lemmas, proved in [7]:

Lemma 1. *If $\mathcal{AE}$ is an IND-CCA secure encryption scheme and (P, V) is a simulation sound, computational zero-knowledge proof system for ρ over* Dom *then group signature scheme $\mathcal{GS}$ is fully-anonymous.* ∎

Lemma 2. *If digital signature scheme $\mathcal{DS}$ is secure against forgery under chosen-message attack and (P, V) is a sound non-interactive proof system for ρ over* Dom *then group signature scheme $\mathcal{GS}$ is fully-traceable.* ∎

The scheme we have described is compact. Indeed, keys, as well as sizes of signatures of k-bit messages, are of size $\mathrm{poly}(k, \log(n))$. We also know that the existence of a family of trapdoor permutations implies the existence of the primitives we require [16, 6, 17, 27]. Thus we get:

Theorem 1. *If there exists a family of trapdoor permutations, then there exists a compact group signature scheme that is fully-anonymous and fully-traceable.*

5 Dynamic Groups and Other Extensions

In the previous sections we considered static group signatures schemes. In this section we discuss various extensions of the basic definition, including schemes where the group is dynamic. Following standard terminology [23] we refer to these groups as partially or fully dynamic.

Partially dynamic groups. These are groups supporting either join (incremental) or leave (decremental) operation. Here we concentrate on incremental groups, and postpone the discussion of leave operation to the next paragraph. In an incremental group signature scheme, the key generation algorithm produces (beside the group public key *gpk*) two secret keys: an issuing key *gisk* and an opening key *gmsk*. No signing keys $\boldsymbol{gsk}$ are output by the key generation algorithm. The two keys *gisk*, *gmsk* are given to two different group managers, one of which has authority on the group membership, and the other has authority on traceability. Using *gisk*, the key issuer can generate (possibly via an interactive process) signing keys $\boldsymbol{gsk}[i]$ and distribute them to perspective group members (which we identify with the index i). The basic definition of security is essentially the same as described in the previous sections. Key *gisk* is given to the adversary in the definition of anonymity, but not in the definition of traceability, as knowledge of this key would allow to generate "dummy" group members and use their keys to sign untraceable messages. Alternatively, one can postulate that if the signature opener cannot trace a signature, then he will blame the key issuer. Our construction (and proof of security) from section 4 can be easily extended to support incremental group operations, with the certificate creation key sk_s used as *gisk*.

Although the above definition allows the group to change over time, the security properties are still static: a signer i that join the group at time t, can use the newly acquired key $\boldsymbol{gsk}[i]$ to sign documents that predate time t. This problem can be easily solved enhancing the signatures with an explicit time counter, and using the technique of forward security. Before explaining the connection with incremental groups, we discuss forward security, which may be a desirable security feature on its own. As for standard digital signature schemes [8], forward security for group signatures is defined using a key evolution paradigm. The lifetime of the public key is divided into time periods, and signing keys of the group members change over time, with the key of user i at time j denoted $\boldsymbol{gsk}_j[i]$. At the end of each time period, each user updates his key using an update algorithm $\boldsymbol{gsk}_{j+1}[i] = \mathsf{GUpd}(\boldsymbol{gsk}_j[i])$. Although the forward security requirement for group signature schemes was already considered before [28], that definition has a serious security flaw: [28] only requires that no adversary, given $\boldsymbol{gsk}_t[i]$, can efficiently recover $\boldsymbol{gsk}_j[i]$ for any $j < t$. This is not enough! [2] We define forward secure group signature schemes requiring that an attacker should not be able to produce *valid signatures* for any earlier time period. Our

[2] Consider a scheme where $\boldsymbol{gsk}_j[i] = (k_j; h_j)$ $\mathsf{GUpd}(k_j; h_j) = k_j; g(h_j)$ for some one way permutation g, and only the first part of the key k_j is used by the signing algorithm. Such a scheme would certainly satisfy the definition of [28], but it is

scheme from Section 4 can be easily modified to achieve forward security, by replacing the signature scheme used by group members with a forward secure one $\mathcal{DS} = (\mathsf{K_s}, \mathsf{Vf}, \mathsf{Sig}, \mathsf{Upd})$.

In the context of dynamic group signature schemes, signing keys are not stolen by an adversary, but given by the key issuer to the group members. Still, if the signature scheme is forward secure, then the group member cannot use the (legitimately obtained) key to sign documents the predate the joining time. A (forward) secure partially dynamic group signature scheme supporting the join operation is obtained letting the key issuer generate key $\boldsymbol{gsk}_t[i]$ when user i joins the group at time t.

FULLY DYNAMIC GROUPS. Now consider a group where members can both join and leave the group. The issue of members leaving the group is much more delicate than the one of members joining the group, and several alternative (and incompatible) definitions are possible. As for partially dynamic groups, the signing keys $\boldsymbol{gsk}_j[i]$ may vary over time, but this time also the public key gpk_j is allowed to change. Consider a signature σ produced (using key $\boldsymbol{gsk}_a[i]$) at time a by some user i who belonged to the group at time 1, but not at times 0 and 2, Now, say σ is verified at time b (using key gpk_b). When should σ be accepted by GVf? There are two possible answers: (1) if i was a group member when then signature was generated, or (2) if i belonged to the group at the time verification algorithm is invoked.[3] Clearly, there is no "right" answer, and what definition should be used depends on the application. In either case, different kinds of inefficiency are necessarily introduced in the protocol. In case (2), σ should be accepted if $b = 1$, but not if $b = 0$ or $b = 2$. In particular, the public keys gpk_j must be different. This is undesirable because it requires the verifier to continuously communicate with the group manager to update the group public key.[4] Moreover, this definition raises potential anonymity problems: verifying the same signature against different public keys gpk_j, one can determine when the signer joined and left the group, and possibly use this information to discover the signer identity. Now consider case (1). This time, the public key may stay the same throughout the lifetime of the group, but the key update function $\boldsymbol{gsk}_j[i] = \mathsf{GUpd}(\boldsymbol{gsk}_{j-1}[i])$ should not be publicly computable by the group members. This introduces inefficiency, as the group members now need to interact with the key issuer to update their signing key from one time period to the next.

Our construction can be easily adapted to satisfy either definition of security for fully dynamic groups, e.g., by rekeying the entire group at the end of each

clearly not forward secure: even if the past keys cannot be recovered, the adversary can still forge messages in the past!

[3] Notice that in the first case, signatures should remain valid (and the signer anonymous) even after the signer leaves the group, while in the second case removing the signer from the group should immediately invalidate all of its signatures.

[4] Alternatively, one can consider public keys of the form $gpk_j = (gpk, j)$, where the time dependent part can be supplied autonomously by the verifier. But in this case the life time of secret key $\boldsymbol{gsk}[i]$ needs to be decided in advance when the user i joins the group.

time period. Due to the high (but unavoidable) cost of rekeying operations, fully dynamic group signatures should be used only if required by the application, and in all other situations the simpler incremental groups are clearly preferable.

DISHONEST GROUP MANAGERS. The last extension to the definition we discuss pertains the case where the group manager holding *gmsk* is not honest. The experiments we gave in Section 2, only capture the situation where the adversary obtained the group manager's secret key. If the group manager is truly dishonest, one should also assume that he does not behave as prescribed when applying the opening algorithm. For example, when asked to open a signature he can falsely accuse an arbitrary user (i.e. he does not use his secret key), or claim that the signature can not be open (e.g. he changes the secret key).

We consider a solution in which when opening a signature the group manager (on input opening key *gmsk*, message m and signature σ) outputs not only a user identity i, but also a "proof" τ. This proof can be (publicly) verified by a "judging" algorithm GJudge such that if $\mathsf{Open}(gmsk, m, \sigma) = (i, \tau)$ then $\mathsf{GJudge}(m, \sigma, i, \tau) = \mathsf{true}$. Within this framework, it is possible to formally capture security requirements regarding dishonest behavior of the group manager.

Our scheme from Section 4 can be easily modified accordingly. We use an authenticated encryption scheme $\mathcal{AE}$ in which when decrypting a ciphertext, one also recovers the randomness that was used to create it. Opening a signature (C, π) is done as follows: the group manager recovers the plaintext underlying C as $\langle i, pk_i, \mathrm{cert}_i, s\rangle$ and also recovers the randomness r that was used to create C. Then, it outputs (i, τ), where $\tau = (\langle i, pk_i, \mathrm{cert}_i, s\rangle, r)$, is the "proof" that the signature was created by user i. The judging algorithm GJudge simply checks whether C is the result of encrypting $\langle i, sk_i, pk_i, \mathrm{cert}_i, s\rangle$ with pk_e using randomness r.

Acknowledgments

The first author is supported in part by NSF grant CCR-0098123, NSF grant ANR-0129617 and an IBM Faculty Partnership Development Award. The second and third authors are supported in part by NSF CAREER Award CCR-0093029.

References

1. R. Anderson. Invited talk. Fourth Annual Conference on Computer and Communications Security,1997.
2. G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik. A practical and provably secure coalition-resistant group signature scheme. In M. Bellare, editor, *CRYPTO'00*, volume 1880 of *LNCS*, pages 255–270. Springer-Verlag, 2000.
3. G. Ateniese and G. Tsudik. Quasi-efficient revocation in group signature schemes. Available at http://eprint.iacr.org/2001/101.pdf.
4. G. Ateniese and G. Tsudik. Group signatures à la carte. In *ACM Symposium on Discrete Algorithms*, pages 848–849. ACM Press, 1999.
5. G. Ateniese and G. Tsudik. Some open issues and directions in group signature. In *Financial Crypto'99*, volume 1648 of *LNCS*, pages 196–211. Springer-Verlag, 1999.

6. M. Bellare and S. Micali. How to sign given any trapdoor permutation. *Journal of ACM*, 39(1):214–233, January 1992.
7. M. Bellare, D. Micciancio, and B. Warinschi. Full version of this paper. Available at http://www.cs.ucsd.edu/users/bogdan.
8. M. Bellare and S. Miner. A forward-secure digital signature scheme. In M. Wiedner, editor, *CRYPTO'99*, volume 1666 of *LNCS*, pages 431–448. Springer-Verlag, 1999.
9. M. Blum, A. DeSantis, S. Micali, and G. Persiano. Non-interactive zero-knowledge proof systems. *SIAM Journal on Computing*, 20(6):1084–1118, December 1991.
10. E. Bresson and J. Stern. Efficient revocation in group signatures. In *PKC'2001*, volume 1992 of *LNCS*, pages 190–206. Springer-Verlag, 2001.
11. J. Camenisch. Efficient and generalized group signature. In *EUROCRYPT'97*, volume 1233 of *LNCS*, pages 465–479. Springer-Verlag, 1997.
12. J. Camenisch and M. Michels. A group signature scheme with improved efficiency. In K. Ohta and D. Pei, editors, *ASIACRYPT'98*, volume 1514 of *LNCS*, pages 160–174. Springer-Verlag, 1999.
13. J. Camenisch and M. Stadler. Efficient group signatures schemes for large groups. In B.Kaliski, editor, *CRYPTO'97*, volume 1294 of *LNCS*, pages 410–424. Springer-Verlag, 1997.
14. D. Chaum and E. van Heyst. Group signatures. In D. W. Davis, editor, *EUROCRYPT'91*, volume 547 of *LNCS*, pages 257–265. Springer-Verlag, 1991.
15. L. Chen and T. P. Pedersen. New group signature schemes. In A. DeSantis, editor, *EUROCRYPT'94*, volume 950 of *LNCS*, pages 171–181. Springer-Verlag, 1994.
16. D. Dolev, C. Dwork, and M. Naor. Nonmalleable cryptography. *SIAM Journal of Computing*, 30(2):391–437, 2000.
17. U. Feige, D. Lapidot, and A. Shamir. Multiple non-interactive zero-knowledge proofs under general assumptions. *SIAM Journal on Computing*, 29(1):1–28, September 1999.
18. O. Goldreich. A uniform-complexity treatment of encryption and zero-knowledge. *Journal of Cryptology*, 6(1):21–53, 1993.
19. S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Science*, 28:270–299, 1984.
20. S. Goldwasser, S. Micali, and R. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal of Computing*, 17(2):281–308, April 1988.
21. S. Micali, C. Rackoff, and B. Sloan. The notion of security for probabilistic cryptosystems. *SIAM Journal of Computing*, 17(2):412–426, 1988.
22. M. Naor and M. Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *STOC'90*, pages 427–437, 1990.
23. N. I. of Standards and Technology. Dictionary of algorithms and data structures. http://www.nist.gov/dads/.
24. H. Petersen. How to convert any digital signature scheme into a group signature scheme. In *Proceedings of Security Protocols Workshop'97*, pages 177–190, 1997.
25. C. Rackoff and D. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In *CRYPTO'91*, pages 433–444, 1992.
26. J. Rompel. One-way functions are necessary and sufficient for secure signatures. In *22nd Annual Symposium on Theory of Computing*, pages 387–394. ACM, ACM Press, 1990.
27. A. Sahai. Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security. In *FOCS'99*, pages 543–553, 1999.
28. D. Song. Practical forward-secure group signature schemes. In *ACM Symposium on Computer and Communication Security*, pages 225–234, November 2001.