Foundations of Fully Dynamic Group Signatures

Jonathan Bootle, Andrea Cerulli(✉), Pyrros Chaidos, Essam Ghadafi, and Jens Groth

University College London, London, UK
{jonathan.bootle.14,andrea.cerulli.13,pyrros.chaidos.10,
e.ghadafi,j.groth}@ucl.ac.uk

Abstract. Group signatures are a central cryptographic primitive that has received a considerable amount of attention from the cryptographic community. They allow members of a group to anonymously sign on behalf of the group. Membership is overseen by a designated group manager. There is also a tracing authority that can revoke anonymity by revealing the identity of the signer if and when needed, to enforce accountability and deter abuse. For the primitive to be applicable in practice, it needs to support fully dynamic groups, i.e. users can join and leave at any time. In this work we take a close look at existing security definitions for fully dynamic group signatures. We identify a number of shortcomings in existing security definitions and fill the gap by providing a formal rigorous security model for the primitive. Our model is general and is not tailored towards a specific design paradigm and can therefore, as we show, be used to argue about the security of different existing constructions following different design paradigms. Our definitions are stringent and when possible incorporate protection against maliciously chosen keys. In the process, we identify a subtle issue inherent to one design paradigm, where new members might try to implicate older ones by means of back-dated signatures. This is not captured by existing models. We propose some inexpensive fixes for some existing constructions to avoid the issue.

Keywords: Group signatures · Security definitions

1 Introduction

Group signatures, put forward by Chaum and van Heyst [CvH91], are a fundamental cryptographic primitive allowing a member of a group (administered by a designated manager) to anonymously sign messages on behalf of the group. In the

The research leading to these results has received funding from the European Research Council under the European Union's Seventh Framework Programme (FP/2007-2013) / ERC Grant Agreement n. 307937 and EPSRC grant EP/J009520/1.

P. Chaidos—Was supported by an EPSRC scholarship (EP/G037264/1 – Security Science DTC).

M. Manulis et al. (Eds.): ACNS 2016, LNCS 9696, pp. 117–136, 2016.
DOI: 10.1007/978-3-319-39555-5_7

case of a dispute, a designated tracing manager can revoke anonymity by revealing the signer. In many settings it is desirable to offer flexibility in joining and leaving the group. In static group signatures [BMW03], the group population is fixed once and for all at the setup phase. Partially dynamic group signatures [BSZ05, KY06] allow the enrolment of members in the group at any time but members cannot leave once they have joined. A challenging problem in group signatures is that of revocation, i.e. allowing removal of members from the group.

Related Work. After their introduction, a long line of research on group signatures has emerged. In the early years, security of group signatures was not well understood and early constructions were proven secure via informal arguments using various interpretations of their requirements.

Bellare et al. [BMW03] formalized the security definitions for static groups. In their model, the group manager (which also acts as the tracing authority) needs to be fully trusted. Later on, Bellare et al. [BSZ05] and Kiayias and Yung [KY06] provided formal security definitions for the more practical partially dynamic case. Also, [BSZ05] separated the tracing role from the group management. In both [BSZ05, KY06] models, members cannot leave the group once they have joined. More recently, Sakai et al. [SSE+12] strengthened the security definitions for partially dynamic groups by defining *opening soundness*, ensuring that a valid signature only traces to one user.

Group Signatures Without Revocation. Constructions of group signatures in the random oracle model [BR93] include [CS97, CM98, ACJT00, BBS04, CL04, CG04, NS04, FI05, FY04, KY05, DP06, BCN+10]. Constructions not relying on random oracles include [ACHdM05, Gro06, BW06, Gro07, BW07, AHO10].

Group Signatures With Revocation. Since revocation is an essential feature of group signatures, many researchers investigated the different approaches via which such a feature can be realized. One approach is for the group manager to change the group public key when members are removed and issue new group signing keys to all remaining legitimate members or allow them to update their old signing keys accordingly. This is the approach adopted by e.g. [TX03, CL02].

Bresson and Stern [BS01] realize revocation by requiring that the signer proves at the time of signing that her group membership certificate is not among those contained in a public revocation list. Another approach, which was adopted by e.g. [CL02, TX03, DKNS04, Ngu05], uses accumulators, i.e. functions that map a set of values into a fixed-length string and permit efficient proofs of membership.

Boneh et al. [BBS04] showed that their static group signature scheme supports revocation since it allows members to update their signing keys according to the changes in the group without the involvement of the manager. Camenisch and Groth [CG04] also gave a construction that supports revocation. Song [Son01] gave a fully dynamic group signature with forward security.

A different approach for revocation known as *Verifier Local Revocation* (VLR), which needs relaxation of some of the security requirements, considered by Brickell [Bri04], was subsequently formalized by Boyen and Shacham [BS04] and further used in e.g. [NF05, LV09, LLNW14]. In VLR, the revocation information

(i.e. revocation lists) is only sent to the verifiers (as opposed to both verifiers and signers) who can check whether a particular signature was generated by a revoked member. A similar approach is also used in Direct Anonymous Attestation (DAA) protocols [BCC04]. *Traceable Signatures* [KTY04] extend this idea, as the group manager can release a trapdoor for each member, enabling their signatures to be traced back to the individual user.

More recently, Libert et al. [LPY12b,LPY12a] gave a number of efficient constructions of group signatures supporting revocation without requiring random oracles by utilizing the subset cover framework [NNL01] that was originally used in the context of broadcast encryption.

Shortcomings in Existing Models & Motivation. While the security of the static and partially dynamic group settings has been rigorously formulated [BMW03,BSZ05,KY06,SSE+12] and is now well understood, unfortunately, the security of their fully dynamic groups counterpart, which is more relevant to practice, has received less attention and is still lacking. In particular, the different design paradigms assume different (sometimes informal) models which do not necessarily generalize to other design approaches. This resulted in various models, the majority of which lack rigour. As a consequence, it can be difficult to compare the merits of the different constructions in terms of their security guarantees. Moreover, existing models place a large amount of trust in the different authorities and assume that their keys are generated honestly. This does not necessarily reflect scenarios arising in real applications. Furthermore, some existing models, as we show, fail to take into account some attacks which might be problematic for some applications of the primitive.

"He Who Controls the Present Controls the Past", (George Orwell). Consider a scenario where the new leadership of an organisation or country wants to justify an unpopular policy (e.g. layoffs or removal of personal freedoms). A way to do that would be to back-date documents justifying the policy: thus, any animosity for the policy would be towards the old leadership. The new leadership is only maintaining the status quo.

Re-framing this in technical terms, we show that the notion of traceability in existing models following the revocation list approach, where the group manager periodically publishes information (i.e. revocation lists) about members excluded from the group, is too weak. In those models, the life of the scheme spans over different intervals (epochs) at the start of which the manager updates the revocation lists. Signatures in those models are bound to a specific epoch. It is vital for functionality that old valid signatures (i.e. those produced at earlier epochs by then-legitimate members) are accepted by the verification algorithm.

The issue we identify in those models is that they allow members who joined at recent epochs to sign messages w.r.t earlier epochs during which they were not members of the group. In a sense this may be considered as an attack against traceability, as those members were not in the group at that interval. Technically however, the scenario we describe is allowed by the model: the underlying issue is a gap between one's interpretation of group signatures and what the definition implies. Our expectation is that a signature bound to epoch τ was produced by

a member of the group *at that time*. Current definitions however, allows for all past, current, and future members, as long as they were not revoked at time τ.

One may dismiss this attack as theoretical, since the old leadership might appeal to the opener. However, this might not always be possible: the opener may be controlled by the new leadership, or in a business setting an outgoing CEO or board member might be disinterested or disincentivized from pursuing the issue. Another possible criticism might be that the weakness is trivial, and would be silently fixed in any construction using the model.

We show that some state of the art constructions, as [NFHF09,LPY12b, LPY12a], are susceptible to this attack. Specifically, their membership certificates are not bound to the epochs of their issuance. As a result, a member can sign w.r.t. earlier epochs. We stress that neither the authors of those schemes claimed their schemes were immune against such an issue nor that their models were supposed to capture such an attack. Thus, such an issue might not be a problem for the applications they originally had in mind, but only in a more general case.

In order to have strong security guarantees from the different constructions, a rigorous and unified security model is necessary. This is the aim of this work as we believe this is a challenging problem that needs to be addressed, especially given the relevance of the primitive.

Our Contribution. We take a close look at the security definitions of fully dynamic group signatures. We provide a rigorous security model that generalizes to the different design paradigms. In particular, our model covers both accumulator based and revocation list based approaches. Our model offers stringent security definitions and takes into account some attacks which were not considered by existing models. We give different flavors of our security definitions which capture both cases when the authorities' keys are adversarially generated and when such keys are honestly generated. We also show that our security definitions imply existing definitions for static and partially dynamic group signatures.

In the process, we identify a subtle difference between accumulator based and revocation list based approaches. Specifically, we identify a simple attack against traceability inherent to constructions following the latter approach and which is not captured by existing models. The attack allows a group member of to sign w.r.t. intervals prior to her joining the group. The security notion modelled by current definitions prevents users from signing only if they are explicitly revoked.

To address this, our traceability definition models a stricter security notion: users are not authorised to sign unless they are non-revoked and are active (i.e. part of the group) at the time interval associated with the signature. We note this is already implied in the accumulator based approach: the signer proves membership in the current version of the group at the time of signing. We also propose a number of possible fixes to this issue in some existing schemes.

Finally, we show that a fully dynamic group signature scheme obtained from the generic construction of accountable ring signatures given in [BCC+15] is secure w.r.t. the stronger variant of our security definitions.

Paper Organization. We present our model for fully dynamic group signatures in Sect. 2 and show that it implies existing definitions for static and partially dynamic group signatures. In Sect. 3 we analyse the security of three existing fully dynamic group signature schemes in our model.

Notation. A function $\nu(\cdot) : \mathbb{N} \to \mathbb{R}^+$ is negligible in the security parameter λ if for every polynomial $p(\cdot)$ and all sufficiently large values of λ, it holds that $\nu(\lambda) < \frac{1}{p(\lambda)}$. Given a probability distribution Y, we denote by $x \leftarrow Y$ the operation of selecting an element according to Y. If M is a probabilistic machine, we denote by $M(x_1, \ldots, x_n)$ the output distribution of M on inputs $(x_1, \ldots, x_n)$. By $[n]$ we denote the set $\{1, \ldots, n\}$. By PPT we mean running in probabilistic polynomial time in the relevant security parameter. For algorithms X and Y, $(x, y) \leftarrow \langle \mathsf{X}(a), \mathsf{Y}(b) \rangle$ denotes the the joint execution of X (with input a) and Y (with input b) where at the end X outputs x, whereas Y outputs y. By $\mathsf{X}^{\langle \cdot, \mathsf{Y}(b) \rangle}(a)$, we denote the invocation of Y (with input b) by X (with input a). Note that X does not get the private output of Y.

2 Syntax and Security of Fully Dynamic Group Signatures

The parties involved in a Fully Dynamic Group Signature (FDGS) are: a group manager $\mathcal{GM}$ who authorizes who can join the group; a tracing manager $\mathcal{TM}$ who can revoke anonymity by opening signatures; a set of users, each with a unique identity $\mathsf{uid} \in \mathbb{N}$, who are potential group members. Users can join/leave the group at any time at the discretion of the group manager. We assume the group manager will regularly publish some information info_τ, associated with a distinct index τ (hereafter referred to as epoch). We assume that τ can be recovered given info_τ and vice versa (i.e. there is bijection between the epochs and associated information). The information depicts changes to the group, for instance, it could include the current members of the group (as in accumulator-based constructions) or those who have been excluded from the group (as, e.g. required by constructions based on revocation lists). As in existing models, we assume that anyone can verify the well-formedness and authenticity of the published group information. By combining the group information for the current epoch with that of the preceding one, any party can identify the list of members who have been revoked at the current epoch. We assume that the epochs preserve the order in which their corresponding information was published. More precisely, for all $\tau_1, \tau_2 \in \mathcal{T}$ ($\mathcal{T}$ being the space of epochs) we require that $\tau_1 < \tau_2$ if info_{τ_1} preceded info_{τ_2}.

Unlike existing models, which assume honestly generated authorities' keys, we separate the generation of the authorities' keys from that of the public parameters, which might need to be generated by a trusted party. This allows us (where appropriate) to define stringent security that protects against adversarial authorities who might generate their keys maliciously. Our definitions can be adapted straight away to work for the weaker setting where authorities' keys are generated honestly as in existing models. For the sake of generality, we define

the group key generation as a joint protocol between the group and tracing managers. Clearly, it is desirable in some cases to avoid such interaction and allow authorities to generate their own keys independently. This is a special case of our general definition where the protocol is regarded as two one-sided protocols.

An $\mathcal{FDGS}$ scheme consists of the following polynomial-time algorithms:

- $\mathsf{GSetup}(1^\lambda) \to \mathsf{param}$: is run by a trusted third party. On input a security parameter λ, it outputs public parameters param. The algorithm also initializes the registration table $\mathbf{reg}$.
- $\langle \mathsf{GKGen}_{\mathcal{GM}}(\mathsf{param}), \mathsf{GKGen}_{\mathcal{TM}}(\mathsf{param}) \rangle$: is an interactive protocol between algorithms $\mathsf{GKGen}_{\mathcal{GM}}$ and $\mathsf{GKGen}_{\mathcal{TM}}$ run by $\mathcal{GM}$ and $\mathcal{TM}$, respectively, to generate their respective private keys as well as the rest of the group public key gpk. The input to both algorithms is the public parameters param. If completed successfully, the private output of $\mathsf{GKGen}_{\mathcal{GM}}$ is a secret manager key msk, whereas its public output is a public key mpk, and the initial group information info. The private output of $\mathsf{GKGen}_{\mathcal{TM}}$ is the secret tracing key tsk, whereas its public output is a public key tpk. The group public key is then set to $\mathsf{gpk} := (\mathsf{param}, \mathsf{mpk}, \mathsf{tpk})$.
- $\mathsf{UKGen}(1^\lambda) \to (\mathbf{usk}[\mathsf{uid}], \mathbf{upk}[\mathsf{uid}])$: outputs a secret/public key pair ($\mathbf{usk}[\mathsf{uid}]$, $\mathbf{upk}[\mathsf{uid}]$) for user uid. We assume the public key table $\mathbf{upk}$ to be publicly available (possibly via PKI) so that anyone can get authentic copies of it.
- $\langle \mathsf{Join}(\mathsf{info}_{\tau_{\text{current}}}, \mathsf{gpk}, \mathsf{uid}, \mathbf{usk}[\mathsf{uid}]), \mathsf{Issue}(\mathsf{info}_{\tau_{\text{current}}}, \mathsf{msk}, \mathsf{uid}, \mathbf{upk}[\mathsf{uid}]) \rangle$: is an interactive protocol between a user uid (who has already obtained a personal key pair, i.e. ran the UKGen algorithm) and the group manager $\mathcal{GM}$. Upon successful completion, uid becomes a member of the group. The final state of the Issue algorithm is stored in the registration table at index uid (i.e. $\mathbf{reg}[\mathsf{uid}]$), whereas that of the Join algorithm is stored in $\mathbf{gsk}[\mathsf{uid}]$. The epoch τ_{current} is part of the output of both parties.
  We assume that the protocol takes place over a secure (i.e. private and authentic) channel. The protocol is initiated by calling Join. The manager may update the group information after running this protocol. The registration table $\mathbf{reg}$ stores additional information used by the group manager and the tracing manager for updating and tracing, depending on the scheme specifics.
- $\mathsf{UpdateGroup}(\mathsf{gpk}, \mathsf{msk}, \mathsf{info}_{\tau_{\text{current}}}, \mathcal{S}, \mathbf{reg}) \to \mathsf{info}_{\tau_{\text{new}}}$: is run by the group manager to update the group information while also advancing the epoch. It takes as input the group manager's secret key msk, a (possibly empty) set $\mathcal{S}$ of active members to be removed from the group and the registration table $\mathbf{reg}$, it outputs a new group information $\mathsf{info}_{\tau_{\text{new}}}$ and might also update the registration table $\mathbf{reg}$. If there has been no changes to the group information, the algorithm returns $\perp$ to indicate that no new information has been issued. The algorithm aborts if any $\mathsf{uid} \in \mathcal{S}$ has not run the join protocol.
- $\mathsf{Sign}(\mathsf{gpk}, \mathbf{gsk}[\mathsf{uid}], \mathsf{info}_\tau, m) \to \Sigma$: on input the group public key gpk, a user's group signing key $\mathbf{gsk}[\mathsf{uid}]$, the group information info_τ at epoch τ, and a message m, outputs a group signature Σ on m by the group member uid. If the user owning $\mathbf{gsk}[\mathsf{uid}]$ is not an active member of the group at epoch τ, the algorithm returns $\perp$.

- $\mathsf{Verify}(\mathsf{gpk}, \mathsf{info}_\tau, m, \Sigma) \to 1/0$: is a deterministic algorithm checking whether Σ is a valid group signature on m at epoch τ and outputs a bit accordingly.
- $\mathsf{Trace}(\mathsf{gpk}, \mathsf{tsk}, \mathsf{info}_\tau, \mathbf{reg}, m, \Sigma) \to (\mathsf{uid}, \pi_{\mathrm{Trace}})$: is a deterministic algorithm which is run by the tracing manager. It returns an identity $\mathsf{uid} > 0$ of the group member who produced Σ plus a proof π_{Trace} attesting to this fact. If the algorithm is unable to trace the signature to a particular group member, it returns $(0, \pi_{\mathrm{Trace}})$ to indicate that it could not attribute the signature.
- $\mathsf{Judge}(\mathsf{gpk}, \mathsf{uid}, \mathsf{info}_\tau, \pi_{\mathrm{Trace}}, \mathbf{upk}[\mathsf{uid}], m, \Sigma) \to 1/0$: is a deterministic algorithm which on input the group public key gpk, a user identity uid, the group information at epoch τ, a tracing proof π_{Trace}, the user's public key $\mathbf{upk}[\mathsf{uid}]$ (which is $\perp$ if it does not exist), a message m, and a signature Σ, outputs 1 if π_{Trace} is a valid proof that uid produced Σ, and outputs 0 otherwise.

Additional Algorithm. We will also use the following polynomial-time algorithm which is only used in the security games to ease composition.

$\mathsf{IsActive}(\mathsf{info}_\tau, \mathbf{reg}, \mathsf{uid}) \to 1/0$: returns 1 if the user uid is an active member of the group at epoch τ and 0 otherwise.

2.1 Security of Fully Dynamic Group Signatures

The security requirements of a fully dynamic group signature are: *correctness*, *anonymity*, *non-frameability*, *traceability* and *tracing soundness*. To define those requirements, we use a set of games in which the adversary has access to a set of oracles. The following global lists are maintained: HUL is a list of honest users; CUL is a list of corrupt users whose personal secret keys have been chosen by the adversary; BUL is a list of bad users whose personal and group signing keys have been revealed to the adversary; SL is a list of signatures obtained from the Sign oracle; CL is a list of challenge signatures obtained from the challenge oracle.

The details of the following oracles are given in Fig. 1.

$\mathsf{AddU}(\mathsf{uid})$ adds an honest user uid to the group at the current epoch.
$\mathsf{CrptU}(\mathsf{uid}, \mathsf{pk})$ creates a new corrupt user whose public key $\mathbf{upk}[\mathsf{uid}]$ is chosen by the adversary. This is called in preparation for calling the SndToM oracle.
$\mathsf{SndToM}(\mathsf{uid}, M_{\mathsf{in}})$ used to engage in the $\mathsf{Join\text{-}Issue}$ protocol with the honest, Issue-executing group manager.
$\mathsf{SndToU}(\mathsf{uid}, M_{\mathsf{in}})$ used to engage in the $\mathsf{Join\text{-}Issue}$ protocol with an honest, Join-executing user uid on behalf of the corrupt group manager.
$\mathsf{ReadReg}(\mathsf{uid})$ returns the registration information $\mathbf{reg}[\mathsf{uid}]$ of user uid.
$\mathsf{ModifyReg}(\mathsf{uid}, val)$ modifies the entry $\mathbf{reg}[\mathsf{uid}]$, setting $\mathbf{reg}[\mathsf{uid}] := val$. For brevity we will assume $\mathsf{ModifyReg}$ also provides the functionality of $\mathsf{ReadReg}$.
$\mathsf{RevealU}(\mathsf{uid})$ returns the personal secret key $\mathbf{usk}[\mathsf{uid}]$ and group signing key $\mathbf{gsk}[\mathsf{uid}]$ of group member uid.
$\mathsf{Sign}(\mathsf{uid}, m, \tau)$ returns a signature on the message m by the group member uid for epoch τ assuming the corresponding group information info_τ is defined.

Fig. 1. Details of the oracles used in the security games

$\mathsf{Chal}_b(\mathsf{info}_\tau, \mathsf{uid}_0, \mathsf{uid}_1, m)$ is a left-right oracle for defining anonymity. The adversary chooses an epoch τ, the group information info_τ, two identities $(\mathsf{uid}_0, \mathsf{uid}_1)$, and a message m and receives a group signature by member uid_b for $b \leftarrow \{0,1\}$ for the chosen epoch. It is required that both challenge users are active members at epoch τ. The adversary can only call this oracle once.

$\mathsf{Trace}(m, \Sigma, \mathsf{info}_\tau)$ returns the identity of the signer of the signature Σ on m w.r.t. info_τ if the signature was not obtained from the Chal_b oracle.

$\mathsf{UpdateGroup}(\mathcal{S})$ allows the adversary to update the group. $\mathcal{S}$ here is the set of the active members to be removed from the group.

The following security requirements are defined by the games in Fig. 2.

Correctness. This requirement guarantees that signatures produced by honest, non-revoked users are accepted by the Verify algorithm and that the honest tracing manager can identify the signer of such signatures. In addition, the Judge algorithm accepts the tracing manager's decision.

Experiment: $\mathbf{Exp}^{\text{Corr}}_{\mathcal{FDGS},\mathcal{A}}(\lambda)$
– $\mathsf{param} \leftarrow \mathsf{GSetup}(1^\lambda)$; $\mathsf{HUL} := \emptyset$.
– $\Big((\mathsf{msk}, \mathsf{mpk}, \mathsf{info}), (\mathsf{tsk}, \mathsf{tpk})\Big) \leftarrow \langle \mathsf{GKGen}_{\mathcal{GM}}(\mathsf{param}), \mathsf{GKGen}_{\mathcal{TM}}(\mathsf{param})\rangle$.
– $\mathsf{gpk} := (\mathsf{param}, \mathsf{mpk}, \mathsf{tpk})$.
– $\Big(\mathsf{uid}, m, \tau\Big) \leftarrow \mathcal{A}^{\mathsf{AddU},\mathsf{ReadReg},\mathsf{UpdateGroup}}\Big(\mathsf{gpk}, \mathsf{info}\Big)$.
– If $\mathsf{uid} \notin \mathsf{HUL}$ or $\mathbf{gsk}[\mathsf{uid}] = \perp$ or $\mathsf{info}_\tau = \perp$ or $\mathsf{IsActive}(\mathsf{info}_\tau, \mathbf{reg}, \mathsf{uid}) = 0$ Then Return 0.
– $\Sigma \leftarrow \mathsf{Sign}(\mathsf{gpk}, \mathbf{gsk}[\mathsf{uid}], \mathsf{info}_\tau, m)$.
– If $\mathsf{Verify}(\mathsf{gpk}, \mathsf{info}_\tau, m, \Sigma) = 0$ Then Return 1.
– $(\mathsf{uid}^*, \pi_{\text{Trace}}) \leftarrow \mathsf{Trace}(\mathsf{gpk}, \mathsf{tsk}, \mathsf{info}_\tau, \mathbf{reg}, m, \Sigma)$.
– If $\mathsf{uid} \neq \mathsf{uid}^*$ Then Return 1.
– If $\mathsf{Judge}(\mathsf{gpk}, \mathsf{uid}, \mathsf{info}_\tau, \pi_{\text{Trace}}, \mathbf{upk}[\mathsf{uid}], m, \Sigma) = 0$ Then Return 1, Else Return 0.

Experiment: $\mathbf{Exp}^{\text{Anon-}b}_{\mathcal{FDGS},\mathcal{A}}(\lambda)$
– $\mathsf{param} \leftarrow \mathsf{GSetup}(1^\lambda); \mathsf{HUL}, \mathsf{CUL}, \mathsf{BUL}, \mathsf{SL}, \mathsf{CL} := \emptyset$.
– $\Big(\mathsf{st}_{\mathsf{init}}, \mathsf{msk}, \mathsf{mpk}, \mathsf{info}\Big) \leftarrow \mathcal{A}^{\langle\cdot,\mathsf{GKGen}_{\mathcal{TM}}(\mathsf{param})\rangle}(\mathsf{init} : \mathsf{param})$.
– Return 0 if $\mathsf{GKGen}_{\mathcal{TM}}$ did not accept or $\mathcal{A}$'s output is not well-formed.
– Parse the output of $\mathsf{GKGen}_{\mathcal{TM}}$ as $(\mathsf{tsk}, \mathsf{tpk})$ and set $\mathsf{gpk} := (\mathsf{param}, \mathsf{mpk}, \mathsf{tpk})$.
– $b^* \leftarrow \mathcal{A}^{\mathsf{AddU},\mathsf{CrptU},\mathsf{SndToU},\mathsf{RevealU},\mathsf{Trace},\mathsf{ModifyReg},\mathsf{Chal}_b}\Big(\mathsf{play} : \mathsf{st}_{\mathsf{init}}, \mathsf{gpk}\Big)$.
– Return b^*.

Experiment: $\mathbf{Exp}^{\text{Non-Frame}}_{\mathcal{FDGS},\mathcal{A}}(\lambda)$
– $\mathsf{param} \leftarrow \mathsf{GSetup}(1^\lambda); \mathsf{HUL}, \mathsf{CUL}, \mathsf{BUL}, \mathsf{SL} := \emptyset$.
– $(\mathsf{st}_{\mathsf{init}}, \mathsf{info}, \mathsf{msk}, \mathsf{mpk}, \mathsf{tsk}, \mathsf{tpk}) \leftarrow \mathcal{A}(\mathsf{init} : \mathsf{param})$.
– Return 0 if $\mathcal{A}$'s output is not well-formed otherwise set $\mathsf{gpk} := (\mathsf{param}, \mathsf{mpk}, \mathsf{tpk})$.
– $\Big(m, \Sigma, \mathsf{uid}, \pi_{\text{Trace}}, \mathsf{info}_\tau\Big) \leftarrow \mathcal{A}^{\mathsf{CrptU},\mathsf{SndToU},\mathsf{RevealU},\mathsf{Sign},\mathsf{ModifyReg}}\Big(\mathsf{play} : \mathsf{st}_{\mathsf{init}}, \mathsf{gpk}\Big)$.
– If $\mathsf{Verify}(\mathsf{gpk}, \mathsf{info}_\tau, m, \Sigma) = 0$ Then Return 0.
– If $\mathsf{Judge}(\mathsf{gpk}, \mathsf{uid}, \mathsf{info}_\tau, \pi_{\text{Trace}}, \mathbf{upk}[\mathsf{uid}], m, \Sigma) = 0$ Then Return 0.
– If $\mathsf{uid} \notin \mathsf{HUL} \setminus \mathsf{BUL}$ or $(\mathsf{uid}, m, \Sigma, \tau) \in \mathsf{SL}$ Then Return 0 Else Return 1.

Experiment: $\mathbf{Exp}^{\text{Trace}}_{\mathcal{FDGS},\mathcal{A}}(\lambda)$
– $\mathsf{param} \leftarrow \mathsf{GSetup}(1^\lambda); \mathsf{HUL}, \mathsf{CUL}, \mathsf{BUL}, \mathsf{SL} := \emptyset$.
– $\Big(\mathsf{st}_{\mathsf{init}}, \mathsf{tsk}, \mathsf{tpk}\Big) \leftarrow \mathcal{A}^{\langle\mathsf{GKGen}_{\mathcal{GM}}(\mathsf{param}),\cdot\rangle}(\mathsf{init} : \mathsf{param})$.
– Return 0 if $\mathsf{GKGen}_{\mathcal{GM}}$ did not accept or $\mathcal{A}$'s output is not well-formed.
– Parse the output of $\mathsf{GKGen}_{\mathcal{GM}}$ as $(\mathsf{msk}, \mathsf{mpk}, \mathsf{info})$. Set $\mathsf{gpk} := (\mathsf{param}, \mathsf{mpk}, \mathsf{tpk})$.
– $\Big(m, \Sigma, \tau\Big) \leftarrow \mathcal{A}^{\mathsf{AddU},\mathsf{CrptU},\mathsf{SndToM},\mathsf{RevealU},\mathsf{Sign},\mathsf{ReadReg},\mathsf{UpdateGroup}}\Big(\mathsf{play} : \mathsf{st}_{\mathsf{init}}, \mathsf{gpk}, \mathsf{info}\Big)$.
– If $\mathsf{Verify}(\mathsf{gpk}, \mathsf{info}_\tau, m, \Sigma) = 0$ Then Return 0.
– $(\mathsf{uid}, \pi_{\text{Trace}}) \leftarrow \mathsf{Trace}(\mathsf{gpk}, \mathsf{tsk}, \mathsf{info}_\tau, \mathbf{reg}, m, \Sigma)$.
– If $\mathsf{IsActive}(\mathsf{info}_\tau, \mathbf{reg}, \mathsf{uid}) = 0$ Then Return 1.
– If $\mathsf{uid} = 0$ or $\mathsf{Judge}(\mathsf{gpk}, \mathsf{uid}, \mathsf{info}_\tau, \pi_{\text{Trace}}, \mathbf{upk}[\mathsf{uid}], m, \Sigma) = 0$ Then Return 1 Else Return 0.

Experiment: $\mathbf{Exp}^{\text{Trace-Sound}}_{\mathcal{FDGS},\mathcal{A}}(\lambda)$
– $\mathsf{param} \leftarrow \mathsf{GSetup}(1^\lambda)$; $\mathsf{CUL} := \emptyset$.
– $(\mathsf{st}_{\mathsf{init}}, \mathsf{info}, \mathsf{msk}, \mathsf{mpk}, \mathsf{tsk}, \mathsf{tpk}) \leftarrow \mathcal{A}(\mathsf{init} : \mathsf{param})$.
– Return 0 if $\mathcal{A}$'s output is not well-formed otherwise set $\mathsf{gpk} := (\mathsf{param}, \mathsf{mpk}, \mathsf{tpk})$.
– $\Big(m, \Sigma, \{\mathsf{uid}_i, \pi_{\text{Trace}_i}\}_{i=1}^2, \mathsf{info}_\tau\Big) \leftarrow \mathcal{A}^{\mathsf{CrptU},\mathsf{ModifyReg}}\Big(\mathsf{play} : \mathsf{st}_{\mathsf{init}}, \mathsf{gpk}\Big)$.
– If $\exists i \in \{1, 2\}$ s.t. $\mathsf{Verify}(\mathsf{gpk}, \mathsf{info}_\tau, m, \Sigma) = 0$ Then Return 0.
– If $\mathsf{uid}_1 = \mathsf{uid}_2$ or $\mathsf{uid}_1 = \perp$ or $\mathsf{uid}_2 = \perp$ Then Return 0.
– If $\exists i \in \{1, 2\}$ s.t. $\mathsf{Judge}(\mathsf{gpk}, \mathsf{uid}_i, \mathsf{info}_\tau, \pi_{\text{Trace}_i}, \mathbf{upk}[\mathsf{uid}_i], m, \Sigma) = 0$ Then Return 0.
– Return 1.

Fig. 2. Security games for fully dynamic group signatures

Formally, an $\mathcal{FDGS}$ scheme is *(perfectly) correct* if for all $\lambda \in \mathbb{N}$, the advantage

$$\mathsf{Adv}^{\text{Corr}}_{\mathcal{FDGS},\mathcal{A}}(\lambda) := \Pr[\mathbf{Exp}^{\text{Corr}}_{\mathcal{FDGS},\mathcal{A}}(\lambda) = 1]$$

is negligible (in λ) for all adversaries $\mathcal{A}$.

Note that the above definition of (perfect) correctness protects against even unbounded adversaries. If computational correctness suffices, i.e. when we consider correctness only against computationally-bounded adversaries, we can drop the last three lines from the correctness game in Fig. 2. Computational correctness of the Trace and Judge algorithms is implied by the other requirements.

(Full) Anonymity. This requires that signatures do not reveal the identity of the group member who produced them. In the game, the adversary, $\mathcal{A}$, can corrupt any user and fully corrupt the group manager by choosing her key. We require that both challenge users are active members of the group at the chosen epoch. Also, note that a Trace query on the challenge signature will fail.

As $\mathcal{A}$ can learn the personal secret and group signing keys of any user, including the challenge users, our definition captures full key exposure attacks.

The adversary chooses an epoch, the group information for that epoch, a message and two group members and gets a signature by either member and wins if she correctly guesses the member. Without loss in generality, we allow the adversary a single call to the challenge oracle. A hybrid argument (similar to that used in [BSZ05]) can be used to prove that this is sufficient.

Formally, an $\mathcal{FDGS}$ scheme is *(fully) anonymous* if for all $\lambda \in \mathbb{N}$, the advantage $\mathsf{Adv}^{\text{Anon}}_{\mathcal{FDGS},\mathcal{A}}(\lambda)$ is negligible (in λ) for all PPT adversaries $\mathcal{A}$, where

$$\mathsf{Adv}^{\text{Anon}}_{\mathcal{FDGS},\mathcal{A}}(\lambda) := \left|\Pr[\mathbf{Exp}^{\text{Anon-0}}_{\mathcal{FDGS},\mathcal{A}}(\lambda) = 1] - \Pr[\mathbf{Exp}^{\text{Anon-1}}_{\mathcal{FDGS},\mathcal{A}}(\lambda) = 1]\right|.$$

Non-Frameability. This ensures that even if the rest of the group as well as the tracing and group managers are fully corrupt, they cannot produce a signature that can be attributed to an honest member who did not produce it.

In the game, the adversary can fully corrupt both the group and tracing managers. She even chooses the keys of both managers. Thus, our definition is stronger than existing models. We just require that the framed member is honest.

Formally, an $\mathcal{FDGS}$ scheme is *non-frameable* if for all $\lambda \in \mathbb{N}$, the advantage

$$\mathsf{Adv}^{\text{Non-Frame}}_{\mathcal{FDGS},\mathcal{A}}(\lambda) := \Pr[\mathbf{Exp}^{\text{Non-Frame}}_{\mathcal{FDGS},\mathcal{A}}(\lambda) = 1]$$

is negligible (in λ) for all PPT adversaries $\mathcal{A}$.

Remark 1. In the game variant we give in Fig. 2, we allow the adversary to generate the tracing manager's key herself. While, as we show later, there are schemes which satisfy this strong variant of the definition, such definition might be too strong to be satisfied by some existing schemes. A weaker variant of the definition is where the tracing key is generated by the challenger rather than the adversary. This requires replacing lines 2–4 in the game in Fig. 2 by the following:

– $(\mathsf{st}_{\mathsf{init}}, \mathsf{info}, \mathsf{msk}, \mathsf{mpk}) \leftarrow \mathcal{A}^{\langle\cdot,\mathsf{GKGen}_{\mathcal{TM}}(\mathsf{param})\rangle}(\mathsf{init} : \mathsf{param})$
– Return 0 if $\mathcal{A}$'s output is not well-formed or $\mathsf{GKGen}_{\mathcal{TM}}$ did not accept
– Let $(\mathsf{tsk}, \mathsf{tpk})$ be the output of $\mathsf{GKGen}_{\mathcal{TM}}$. Set $\mathsf{gpk} := (\mathsf{param}, \mathsf{mpk}, \mathsf{tpk})$
– $\Big(m, \Sigma, \mathsf{uid}, \pi_{\mathrm{Trace}}, \mathsf{info}_\tau\Big) \leftarrow \mathcal{A}^{\mathsf{CrptU},\mathsf{SndToU},\mathsf{RevealU},\mathsf{Sign},\mathsf{ModifyReg}}\Big(\mathsf{play} : \mathsf{st}_{\mathsf{init}}, \mathsf{gpk}, \mathsf{tsk}\Big)$.

Traceability. This ensures that the adversary cannot produce a signature that cannot be traced to an active member of the group at the chosen epoch. In the game, the adversary can corrupt any user and even chooses the tracing key of the tracing manager. The adversary is not given the group manager's secret key as this would allow her to create dummy users which are thus untraceable. Note that unlike [LPY12b,LPY12a,NFHF09], our definition captures that a member of the group should not be able to sign w.r.t. epochs prior to her joining the group since we do not restrict the adversary's forgery to be w.r.t. to the current epoch (i.e. the current version of the group information). The adversary wins if she produces a signature whose signer cannot be identified or is an inactive member at the chosen epoch. The adversary also wins if the Judge algorithm does not accept the tracing decision on the forgery.

Formally, an $\mathcal{FDGS}$ scheme is *traceable* if for all $\lambda \in \mathbb{N}$, the advantage

$$\mathsf{Adv}^{\mathrm{Trace}}_{\mathcal{FDGS},\mathcal{A}}(\lambda) := \Pr[\mathbf{Exp}^{\mathrm{Trace}}_{\mathcal{FDGS},\mathcal{A}}(\lambda) = 1]$$

is negligible (in λ) for all PPT adversaries $\mathcal{A}$.

Remark 2. To get an honestly-generated tracing key variant of the game in Fig. 2, we replace lines 2–5 in the game in Fig. 2 by the following lines:

– $\Big((\mathsf{msk}, \mathsf{mpk}, \mathsf{info}), (\mathsf{tsk}, \mathsf{tpk})\Big) \leftarrow \langle \mathsf{GKGen}_{\mathcal{GM}}(\mathsf{param}), \mathsf{GKGen}_{\mathcal{TM}}(\mathsf{param})\rangle$
– Set $\mathsf{gpk} := (\mathsf{param}, \mathsf{mpk}, \mathsf{tpk})$
– $\Big(m, \Sigma, \tau\Big) \leftarrow \mathcal{A}^{\mathsf{AddU},\mathsf{CrptU},\mathsf{SndToM},\mathsf{RevealU},\mathsf{Sign},\mathsf{ReadReg},\mathsf{UpdateGroup}}\Big(\mathsf{play} : \mathsf{st}_{\mathsf{init}}, \mathsf{gpk}, \mathsf{info}, \mathsf{tsk}\Big)$.

Tracing Soundness. As recently defined by [SSE+12] in the context of partially dynamic group signatures, this requirement ensures that even if both the group and the tracing managers as well as all members of the group collude, they cannot produce a valid signature that traces to two different members. Such a requirement is vital for many applications. For example, applications where signers get rewarded or where we need to stop abusers shifting blame to others.

In the definition, the adversary can fully corrupt all parties involved and wins if she produces a valid signature and valid tracing proofs that the signature traces to different (possibly corrupt) users. We may also consider a stronger variant where the adversary wins by producing a signature that traces to different epochs.

Formally, an $\mathcal{FDGS}$ scheme has *tracing soundness* if for all $\lambda \in \mathbb{N}$,

$$\mathsf{Adv}^{\text{Trace-Sound}}_{\mathcal{FDGS},\mathcal{A}}(\lambda) := \Pr[\mathbf{Exp}^{\text{Trace-Sound}}_{\mathcal{FDGS},\mathcal{A}}(\lambda) = 1]$$

is negligible (in λ) for all PPT adversaries $\mathcal{A}$.

Remark 3. To get an honestly-generated tracing key variant of the game in Fig. 2, we replace lines 2–4 in the game in Fig. 2 by the following lines:

– $\left(\mathsf{st}_{\mathsf{init}}, \mathsf{msk}, \mathsf{mpk}, \mathsf{info}\right) \leftarrow \mathcal{A}^{\langle\cdot,\mathsf{GKGen}_{\mathcal{TM}}(\mathsf{param})\rangle}(\mathsf{init} : \mathsf{param})$
– Return 0 if $\mathsf{GKGen}_{\mathcal{TM}}$ did not accept or $\mathcal{A}$'s output is not well-formed
– Parse the output of $\mathsf{GKGen}_{\mathcal{TM}}$ as $(\mathsf{tsk}, \mathsf{tpk})$ and set $\mathsf{gpk} := (\mathsf{param}, \mathsf{mpk}, \mathsf{tpk})$
– $\left(m, \Sigma, \{\mathsf{uid}_i, \pi_{\mathrm{Trace}_i}\}_{i=1}^{2}, \mathsf{info}_\tau\right) \leftarrow \mathcal{A}^{\mathsf{CrptU},\mathsf{ModifyReg}}\left(\mathsf{play} : \mathsf{st}_{\mathsf{init}}, \mathsf{gpk}, \mathsf{tsk}\right)$.

2.2 Comparison with Existing Models

Models used by accumulator-based constructions, e.g. [BS01, CL02, TX03, AST01, Ngu05, NFHF09], the vast majority of which are stated informally, are specific to that particular design paradigm and do not generalize to other construction approaches. Moreover, most of the them do not take into account some of the attacks that arise in a more formal setting. For instance, some models only protect against partially but not fully corrupt tracing managers and do not capture the tracing soundness requirement. On the other hand, models used by other design approaches, e.g. [NFHF09, LPY12b, LPY12a] are also specific to those approaches and have their own shortcomings. For instance, as discussed earlier, the models used by the state-of-the-art constructions by Libert et al. [LPY12b, LPY12a] and Nakanishi et al. [NFHF09] do not prevent a group member from being able to sign w.r.t. time intervals before she joined the group. This is an attack that can be problematic in some applications of the primitive. In the traceability game used in [NFHF09] as well as the misidentification game used in [LPY12b, LPY12a], the adversary is required to output a signature that is valid w.r.t. the current interval (epoch) and therefore the definitions do not capture the attack we highlight. We stress that the authors of the concerned models never claimed that their models cover such an attack as it might not be a problem for their intended applications.

The traceability issue we shed light on does not apply to accumulator based models. In these settings, when the group changes, an update is published containing a list of the currently active group members and most constructions work by having the signer prove membership in such a list. Therefore, even if a malicious member tries to sign w.r.t. an earlier version of the group information, she still has to prove she is a member of the group at the concerned interval.

In addition [NFHF09,LPY12b,LPY12a] only consider a partially but not fully corrupt tracing manager in the non-frameability game. Moreover, they do not capture the requirement that a signature should only trace to one member (i.e. tracing soundness). The latter is vital for many applications of the primitive.

Another distinction from existing models is that our model allows maliciously generated authorities' keys when applicable. Therefore, it offers more stringent security than existing models which rely on such keys being generated honestly.

2.3 Recovering Other Models

We give security reductions which relate our model to other well-known models for group signatures. All these models assume honest key generation, for both group and tracing managers, which is a special case of our model. We consider three models. First, the model for static group signatures given in [BMW03]. We then consider two models for partially dynamic groups from [BSZ05] and [KY06]. Due to lack of space, we present the technical details in the full paper [BCC+16].

Static Group Signatures [BMW03]**.** We note that we can recover static group signatures [BMW03] from our group signatures. We fix the group manager as the designated opener and include tsk in the group master secret key. In the setup, group members generate their key pairs and interact with the group manager to join the group. Their Open algorithm does not output proofs, as their model does not use a Judge algorithm, so we define a variant of our non-frameability game from Fig. 2 where we replace the last 4 lines in the game in Fig. 2 by the ones in Fig. 3.

$$
\begin{array}{l}
- \left(m, \Sigma, \mathsf{info}_\tau\right) \leftarrow \mathcal{A}^{\mathsf{CrptU},\mathsf{SndToU},\mathsf{RevealU},\mathsf{Sign},\mathsf{ModifyReg}}\left(\mathsf{play} : \mathsf{st}_{\mathsf{init}}, \mathsf{gpk}\right). \\
- \text{ If } \mathsf{Verify}(\mathsf{gpk}, \mathsf{info}_\tau, m, \Sigma) = 0 \text{ Then Return } 0. \\
- \left(\mathsf{uid}, \pi_{\mathrm{Trace}}\right) \leftarrow \mathsf{Trace}(\mathsf{gpk}, \mathsf{tsk}, \mathsf{info}_\tau, \mathbf{reg}, m, \sigma) \\
- \text{ If } \mathsf{uid} \notin \mathsf{HUL} \setminus \mathsf{BUL} \text{ or } (\mathsf{uid}, m, \Sigma, \tau) \in \mathsf{SL} \text{ Then Return } 0 \text{ Else Return } 1.
\end{array}
$$

Fig. 3. Modified non-frameability game.

This gives a sensible and compatible definition which allows us to recover the model from the fully dynamic scheme.

Static group signatures are just fully dynamic group signatures with no joining, issuing, or group updates. Correctness follows trivially from the correctness of the fully dynamic group signature scheme. [BMW03]-full-anonymity follows from (full) anonymity of the fully dynamic group signature scheme, while [BMW03]-full-traceability follows from our traceability and non-frameability requirements.

Partially Dynamic Group Signatures [BSZ05]**.** Fully dynamic group signatures also imply the partially dynamic group signatures of [BSZ05] in the

case where nobody is removed from the group. Anonymity, non-frameability and traceability all follow from our corresponding definitions. Correctness follows trivially from the correctness of the fully dynamic group signature scheme.

Partially Dynamic Group Signatures [KY06]**.** Finally, we consider the partially-dynamic model of [KY06]. We fix the group manager as the designated opener and set $(\mathsf{msk}, \mathsf{tsk})$ to be the group master secret key. Our group info and registration table generalize their public state string. Their Join algorithm runs our user key-generation and $\mathsf{Join}/\mathsf{Issue}$ algorithms. The membership certificate is then the user's public key along with the group information, and the membership secret is the user's private key. Again, their Open algorithm does not output proofs, and the model does not have a judge algorithm. Therefore, as in the case of [BMW03] we modify our non-frameability game from Fig. 2 where we replace the last 4 lines in the game in Fig. 2 with those in Fig. 3.

Correctness follows trivially from the correctness of the fully dynamic group signature scheme. Security against misidentification-attacks follows from traceability, security against framing-attacks follows from non-frameability, and anonymity follows from the (full) anonymity of the fully dynamic group signature.

3 On the Security of Some Existing Schemes

Here we take a closer look at some of the existing fully dynamic schemes and investigate whether or not they are secure using our proposed model.

We show that the state-of-the-art certificate-based schemes in [LPY12b, LPY12a, NFHF09] are all susceptible to an attack against traceability which allows any user to sign w.r.t. an epoch predating her joining. In our model this directly breaks traceability, as the signature is w.r.t. an epoch in which the signer was not active. We note that our attack does not contradict the original security proofs of the schemes, but instead highlights that our definition is stronger. We also show that it is easy to repair the schemes at a reasonable cost.

At first glance, our attack is the dual of a well known issue with many revocation systems. If a user is revoked and anonymity is maintained, the revoked user is able to produce back-dated signatures that still verify. The difference here is that while the revoked user *was* authorized to be part of the group for the epoch in question, in our attack the signing user was in fact *not* authorized to sign for the group. If the adversary is able to block the opening of this signature (e.g. via legal action), its existence would implicitly frame the group's past membership.

3.1 Libert et al. Schemes [LPY12b, LPY12a]

In [LPY12a], users are assigned leaves of a complete binary tree and given a membership certificate containing a unique tag identifying the user, and a commitment to the path from the root to the user's leaf in the tree. Note that the certificate is not bound to the epoch at which the user joined the group. In fact, users joining does not change info_τ or the epoch τ itself.

Revocation is based on the subset difference method [NNL01], using disjoint sets S_{k_i,u_i} for $i = 1, \ldots, m$ which cover non-revoked users. Sets are represented by two nodes, a node k_i and one of its descendants node u_i, and cover all leaves of the sub-tree rooted at node k_i which are not leaves of the sub-tree rooted at u_i. Revocations trigger epoch changes with info_τ updated with a new cover.

To sign, the group member anonymously proves that she holds a membership certificate, and that the node indicated by the certificate belongs to one of those sets. More precisely, the user proves that her leaf is a descendant of node k_i but not a descendant of node u_i for some $i \in [m]$.

Since user certificates are not bound to epochs and leaves are covered until their corresponding users are revoked, it is simple to break traceability: a user can join and then produce a signature for an epoch that predates her joining. A similar argument also applies to the variant of the scheme given in [LPY12b].

Theorem 1. *The fully dynamic scheme of Libert et al. [LPY12a] does not satisfy our traceability definition even w.r.t. honestly generated tracing manager's keys.*

Proof. Consider the following strategy in the traceability experiment: the adversary asks to join as a user uid_1 at epoch τ_1. User uid_1 gets assigned the leaf l_1. Then at a later epoch, τ_2, the adversary asks to join as a second user uid_2. Finally, the adversary signs using the credentials of uid_2 but for epoch τ_1.

We can check by inspection that all subproofs in the back-dated signature go through. The crucial observation is that at epoch τ_1, the leaf l_2 is not revoked and thus must be covered by one of the S_{k_i,u_i} sets. As the proof verifies and uid_2 used a legitimate certificate, opening the signature will be successful and indicate uid_2 as the signer. The adversary wins, as uid_2 was not active at epoch τ_1. □

A possible countermeasure against the above attack is to regard unassigned leaves as revoked until they are assigned. This is simple to do as the scheme does not bound the number of revoked users. We do however need to re-examine the number of subsets required to express this, as the $2|\mathcal{R}|-1$ bound for $|\mathcal{R}|$ revoked users may now seem impractical. If we assume leaves are allocated sequentially to users, we can bound the number of subsets by $2|\mathcal{R}_1| + log(|\mathcal{N} \setminus \mathcal{R}_2|)$ where $\mathcal{R}_2$ is the set of leaves pending allocation and $\mathcal{R}_1$ is the set of leaves allocated to users who were later revoked. Thus, our fix is only marginally more expensive than the base system and much more efficient than a naive analysis would indicate.

If proving set membership/intervals can be done efficiently (and depending on how the epoch counter is implemented), another possible fix is to bind membership certificates to the join epoch and then get the signer to prove that their join epoch is not later than the signing epoch.

3.2 Nakanishi et al. Scheme [NFHF09]

The scheme of Nakanishi et al. [NFHF09] is another certificate-based scheme in the random oracle model. It achieves constant time for both signing and signature verification, relative to the size of the group and the number of revoked users.

A user's group membership certificate consists of a signature on (x, ID) produced by the group manager, where x is a secret owned by the user and ID is a unique integer the manager assigned to her. The group manager can revoke users by issuing revocation lists info_τ. Each list consists of a sequence of *open* integer intervals (R_i, R_{i+1}) signed by the manager, whose endpoints are all the revoked ID's. At each epoch τ, a signer fetches the current info_τ and proves, as part of the signature, that her ID is contained in one interval of the revocation list. If the ID lies between two revoked users' identities, it means it is not an endpoint and so she has not been revoked.

As in other certificate-based constructions, verifiers only know of revoked members, not active ones and, similarly to [LPY12a], the time of joining is not taken into account. This allows users to sign with respect to any epoch prior to joining the group, which represents an attack against our traceability definition.

Theorem 2. *The Nakanishi et al. [NFHF09] fully dynamic group signature scheme does not satisfy our traceability definition.*

Proof. Let $\mathcal{A}$ be an adversary against the traceability game. The adversary adds user uid to the group at epoch τ. Since the user is not revoked, her ID is not an endpoint in any interval of the revocation list info_τ, as for all previous epochs. Therefore, $\mathcal{A}$ could easily produce valid signatures for uid to any epoch $\bar{\tau} < \tau$. Since these signatures trace back to a user which was inactive at the interval with which the signature is associated, $\mathcal{A}$ succeeds in the traceability game. □

The scheme could be easily immunized against the above attack. A first solution, as for [LPY12a], is to initialize the revocation list with all ID's of users that have not joined the group yet. When the manager assigns an ID to a new user, he updates **reg** and the revocation list info_τ. This way, the signature size is not affected. On the other hand, revocation lists are now proportional to the size of the maximum number of users, instead of the number of revoked users.

An alternative countermeasure requires the group manager to include the joining epochs in the certificates by signing $(x, \mathrm{ID}, \tau_{\mathrm{join}})$, where x is a secret owned by user ID and τ_{join} is the joining epoch. A signer then needs to include in the signature a proof that τ_{join} is not greater than the signing epoch. To realize the latter, one can use membership proof techniques from [TS06, CCS08] which are already used in the original scheme. This would increase the cost of signing and verifying by only a constant factor. The new membership proof would require the group manager to provide signatures for every elapsed epoch, which could be appended, for instance, to the revocation list. This makes revocation lists grow linearly with the number of revoked users as well as the number of epochs.

3.3 Bootle et al. Scheme [BCC+15]

Recently, Bootle et al. [BCC+15] gave a generic construction of accountable ring signatures, where every signature can be traced back to a user in the ring. They also showed how one can obtain fully dynamic group signatures from accountable

ring signatures. In addition, they gave an efficient instantiation in the random oracle model that is based on the DDH assumption. Their instantiation yields signatures of logarithmic size (w.r.t. the size of the ring), while signing is quasi-linear, and signature verification requires a linear number of operations. Bootle et al. claimed that their instantiation is more efficient than existing group signature schemes based on standard assumptions.

Each user has a secret key and an associated verification key. To sign, users first encrypt their verification key. Then, via a membership proof, they provide a signature of knowledge showing that the verification key belongs to the ring, and that they know the corresponding secret key. In the full version [BCC+16], we prove their construction is secure w.r.t. the stronger variant of our model.

References

[ACHdM05] Ateniese, G., Camenisch, J., Hohenberger, S., de Medeiros, B.: Practical group signatures without random oracles, IACR Cryptology ePrint Archive (2005)

[ACJT00] Ateniese, G., Camenisch, J.L., Joye, M., Tsudik, G.: A practical and provably secure coalition-resistant group signature scheme. In: Bellare, M. (ed.) CRYPTO 2000. LNCS, vol. 1880, pp. 255–270. Springer, Heidelberg (2000)

[AHO10] Abe, M., Haralambiev, K., Ohkubo, M.: Signing on elements in bilinear groups for modular protocol design. IACR Cryptology ePrint Archive (2010)

[AST01] Ateniese, G., Song, D., Tsudik, G.: Quasi-efficient revocation of group signatures. IACR Cryptology ePrint Archive 2001:101 (2001)

[BBS04] Boneh, D., Boyen, X., Shacham, H.: Short group signatures. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 41–55. Springer, Heidelberg (2004)

[BCC04] Brickell, E.F., Camenisch, J., Chen, L.: Direct anonymous attestation. In: Conference on Computer and Communications Security, CCS (2004)

[BCC+15] Bootle, J., Cerulli, A., Chaidos, P., Ghadafi, E., Groth, J., Petit, C.: Short accountable ring signatures based on DDH. In: Pernul, G., Y A Ryan, P., Weippl, E. (eds.) ESORICS 2015. LNCS, vol. 9326, pp. 243–265. Springer, Heidelberg (2015). doi:10.1007/978-3-319-24174-6_13

[BCC+16] Bootle, J., Cerulli, A., Chaidos, P., Ghadafi, E., Groth, J.: Foundations of fully dynamic group signatures. IACR Cryptology ePrint Archive (2016)

[BCN+10] Bichsel, P., Camenisch, J., Neven, G., Smart, N.P., Warinschi, B.: Get shorty via group signatures without encryption. In: Garay, J.A., De Prisco, R. (eds.) SCN 2010. LNCS, vol. 6280, pp. 381–398. Springer, Heidelberg (2010)

[BMW03] Bellare, M., Micciancio, D., Warinschi, B.: Foundations of group signatures: formal definitions, simplified requirements, and a construction based on general assumptions. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656. Springer, Heidelberg (2003)

[BR93] Bellare, M., Rogaway, P.: Random oracles are practical: a paradigm for designing efficient protocols. In: Conference on Computer and Communications Security - CCS (1993)

[Bri04] Brickell, E.: An efficient protocol for anonymously providing assurance of the container of a private key. Submitted to the Trusted Computing Group (2004)

[BS01] Bresson, E., Stern, J.: Efficient revocation in group signatures. In: Kim, K. (ed.) PKC 2001. LNCS, vol. 1992, pp. 190–206. Springer, Heidelberg (2001)

[BS04] Boneh, D., Shacham, H.: Group signatures with verifier-local revocation. In: Conference on Computer and Communications Security, CCS (2004)

[BSZ05] Bellare, M., Shi, H., Zhang, C.: Foundations of group signatures: the case of dynamic groups. In: Menezes, A. (ed.) CT-RSA 2005. LNCS, vol. 3376, pp. 136–153. Springer, Heidelberg (2005)

[BW06] Boyen, X., Waters, B.: Compact group signatures without random oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 427–444. Springer, Heidelberg (2006)

[BW07] Boyen, X., Waters, B.: Full-domain subgroup hiding and constant-size group signatures. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 1–15. Springer, Heidelberg (2007)

[CCS08] Camenisch, J.L., Chaabouni, R., Shelat, A.: Efficient protocols for set membership and range proofs. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 234–252. Springer, Heidelberg (2008)

[CG04] Camenisch, J.L., Groth, J.: Group signatures: better efficiency and new theoretical aspects. In: Blundo, C., Cimato, S. (eds.) SCN 2004. LNCS, vol. 3352, pp. 120–133. Springer, Heidelberg (2005)

[CL02] Camenisch, J.L., Lysyanskaya, A.: Dynamic accumulators and application to efficient revocation of anonymous credentials. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 61–76. Springer, Heidelberg (2002)

[CL04] Camenisch, J.L., Lysyanskaya, A.: Signature schemes and anonymous credentials from bilinear maps. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 56–72. Springer, Heidelberg (2004)

[CM98] Camenisch, J.L., Michels, M.: A group signature scheme with improved efficiency. In: Ohta, K., Pei, D. (eds.) ASIACRYPT 1998. LNCS, vol. 1514, pp. 160–174. Springer, Heidelberg (1998)

[CS97] Camenisch, J.L., Stadler, M.A.: Efficient group signature schemes for large groups. In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 410–424. Springer, Heidelberg (1997)

[CvH91] Chaum, D., van Heyst, E.: Group signatures. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 257–265. Springer, Heidelberg (1991)

[DKNS04] Dodis, Y., Kiayias, A., Nicolosi, A., Shoup, V.: Anonymous identification in *Ad Hoc* groups. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 609–626. Springer, Heidelberg (2004)

[DP06] Delerablée, C., Pointcheval, D.: Dynamic fully anonymous short group signatures. In: Nguyên, P.Q. (ed.) VIETCRYPT 2006. LNCS, vol. 4341, pp. 193–210. Springer, Heidelberg (2006)

[FI05] Furukawa, J., Imai, H.: An efficient group signature scheme from bilinear maps. In: Boyd, C., González Nieto, J.M. (eds.) ACISP 2005. LNCS, vol. 3574, pp. 455–467. Springer, Heidelberg (2005)

[FY04] Furukawa, J., Yonezawa, S.: Group signatures with separate and distributed authorities. In: Blundo, C., Cimato, S. (eds.) SCN 2004. LNCS, vol. 3352, pp. 77–90. Springer, Heidelberg (2005)

[Gro06] Groth, J.: Simulation-sound NIZK proofs for a practical language and constant size group signatures. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 444–459. Springer, Heidelberg (2006)

[Gro07] Groth, J.: Fully anonymous group signatures without random oracles. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 164–180. Springer, Heidelberg (2007)

[KTY04] Kiayias, A., Tsiounis, Y., Yung, M.: Traceable signatures. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 571–589. Springer, Heidelberg (2004)

[KY05] Kiayias, A., Yung, M.: Group signatures with efficient concurrent join. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 198–214. Springer, Heidelberg (2005)

[KY06] Kiayias, A., Yung, M.: Secure scalable group signature with dynamic joins and separable authorities. IJSN **1**(1/2), 24 (2006)

[LLNW14] Langlois, A., Ling, S., Nguyen, K., Wang, H.: Lattice-based group signature scheme with verifier-local revocation. In: Krawczyk, H. (ed.) PKC 2014. LNCS, vol. 8383, pp. 345–361. Springer, Heidelberg (2014)

[LPY12a] Libert, B., Peters, T., Yung, M.: Group signatures with almost-for-free revocation. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 571–589. Springer, Heidelberg (2012)

[LPY12b] Libert, B., Peters, T., Yung, M.: Scalable group signatures with revocation. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 609–627. Springer, Heidelberg (2012)

[LV09] Libert, B., Vergnaud, D.: Group signatures with verifier-local revocation and backward unlinkability in the standard model. In: Garay, J.A., Miyaji, A., Otsuka, A. (eds.) CANS 2009. LNCS, vol. 5888, pp. 498–517. Springer, Heidelberg (2009)

[NF05] Nakanishi, T., Funabiki, N.: Verifier-local revocation group signature schemes with backward unlinkability from bilinear maps. In: Roy, B. (ed.) ASIACRYPT 2005. LNCS, vol. 3788, pp. 533–548. Springer, Heidelberg (2005)

[NFHF09] Attrapadung, N., Emura, K., Hanaoka, G., Sakai, Y.: A revocable group signature scheme from identity-based revocation techniques: achieving constant-size revocation list. In: Boureanu, I., Owesarski, P., Vaudenay, S. (eds.) ACNS 2014. LNCS, vol. 8479, pp. 419–437. Springer, Heidelberg (2014)

[Ngu05] Nguyen, L.: Accumulators from bilinear pairings and applications. In: Menezes, A. (ed.) CT-RSA 2005. LNCS, vol. 3376, pp. 275–292. Springer, Heidelberg (2005)

[NNL01] Naor, D., Naor, M., Lotspiech, J.: Revocation and tracing schemes for stateless receivers. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 41–62. Springer, Heidelberg (2001)

[NS04] Nguyen, L., Safavi-Naini, R.: Efficient and provably secure trapdoor-free group signature schemes from bilinear pairings. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 372–386. Springer, Heidelberg (2004)

[Son01] Song, D.X.: Practical forward secure group signature schemes. In: Conference on Computer and Communications Security, CCS (2001)

[SSE+12] Sakai, Y., Schuldt, J.C.N., Emura, K., Hanaoka, G., Ohta, K.: On the security of dynamic group signatures: preventing signature hijacking. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 715–732. Springer, Heidelberg (2012)

[TS06] Teranishi, I., Sako, K.: k-times anonymous authentication with a constant proving cost. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T. (eds.) PKC 2006. LNCS, vol. 3958, pp. 525–542. Springer, Heidelberg (2006)

[TX03] Tsudik, G., Xu, S.: Accumulating composites and improved group signing. In: Laih, C.-S. (ed.) ASIACRYPT 2003. LNCS, vol. 2894, pp. 269–286. Springer, Heidelberg (2003)