Improving Revocation for Group Signature with Redactable Signature

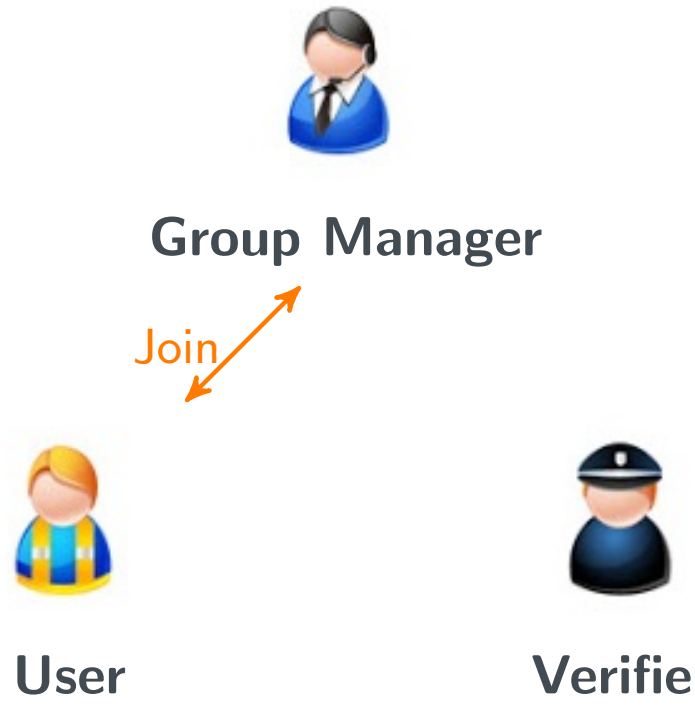
Olivier Sanders
Orange Labs

PKC 2021

orange™

Group Signature

Group Signature



- Users interact with the group manager to join the group

Group Signature

Group Manager

Sign

User → **Verifier**

- Users can sign on behalf of the group
- Signatures are anonymous, except for an appointed entity

GS allows anonymous access to a service

Group Signature

Group Manager

User

Verifier

- Group Signature is standardized at ISO
- Variants (DAA, EPID) are embedded in billions of devices

Group Signature

Group Manager





User 1 **User 2** **User 3** **User 4** **User 5**

Adding users is easy...

Group Signature

Group Manager



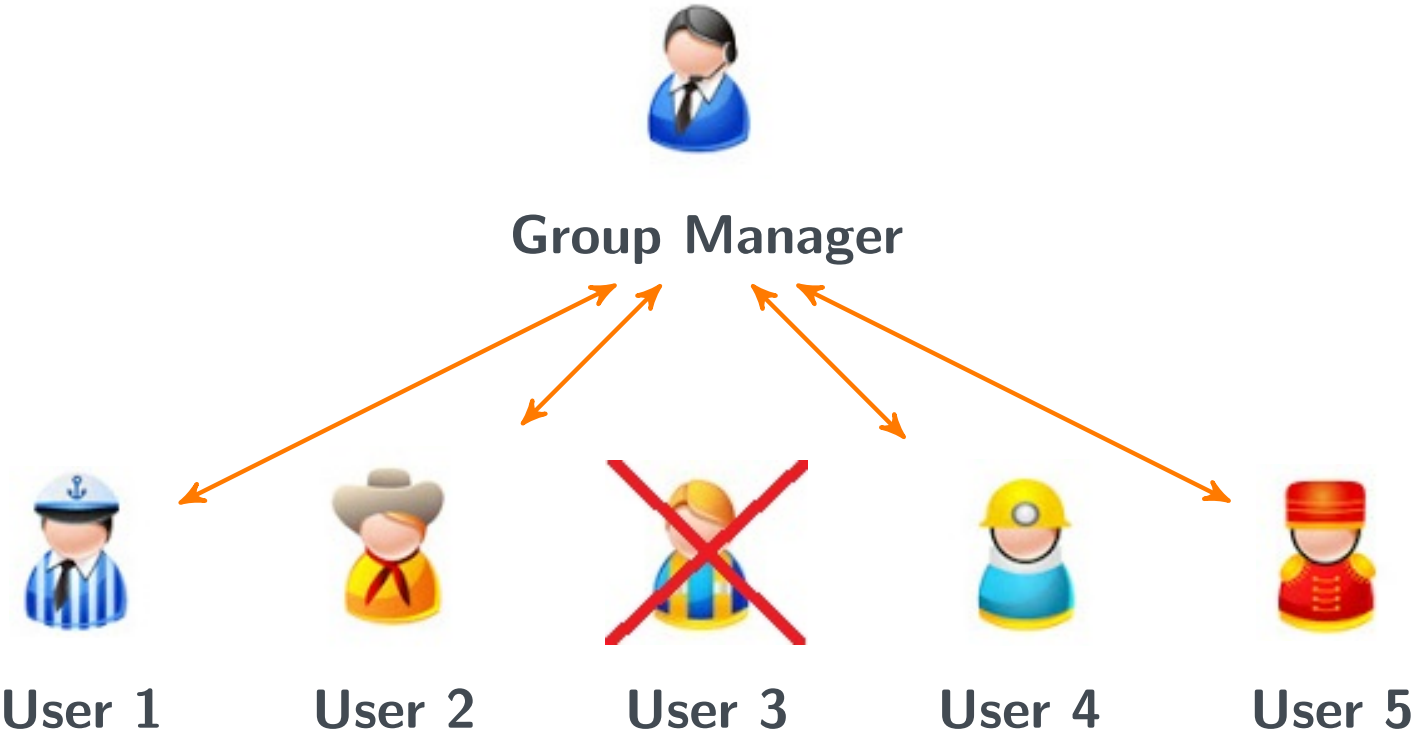


User 1 **User 2** **User 3** **User 4** **User 5**

Adding users is easy... Revoking them is much harder!

common event: end of subscription, loss of credentials, bad behaviour

Revocation Strategy 1



GM generates a new public key and runs `Join` with unrevoked users

	GM	User	Verifier
Practical	✗	↘	∼

	Sign	Verif
Perf	-	-

Revocation Strategy 2

Publication → **Update info E_T**

Group Manager

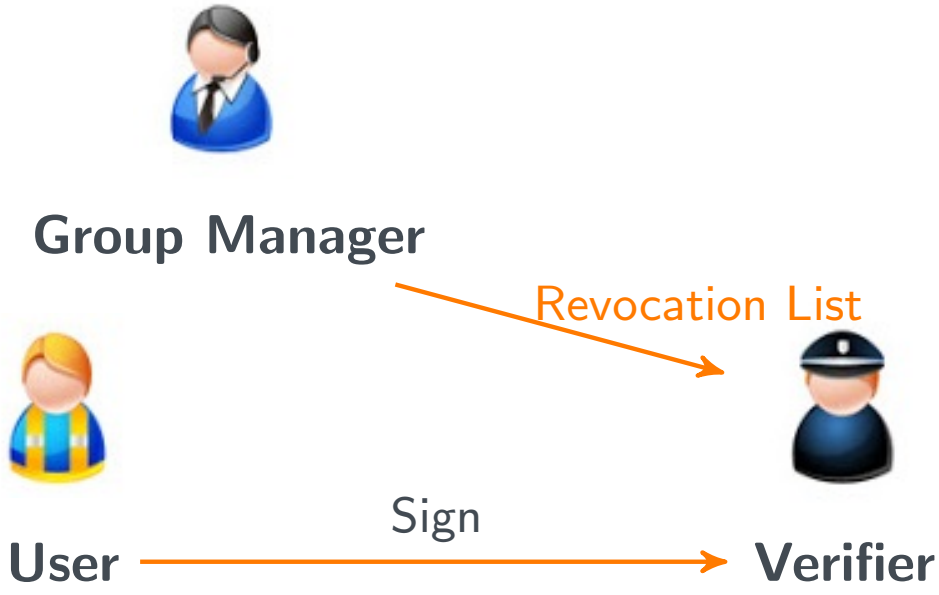
User (E_T) —Sign→ **Verifier (E_T)**

- Every entity must retrieve E_T at each time period T
- User uses E_T to prove that he is still active
- Revocation postponed to the next time period

	GM	User	Verifier
Practical	-	↘	∼

	Sign	Verif
Perf	↘	∼

Revocation Strategy 3



- Revoked users are immediately added to the Revocation List
- Signatures are tested against each element of RL: linear cost

	GM	User	Verifier
Practical	-	-	$\sim$

	Sign	Verif
Perf	-	↘

GS Variants

Variants of GS with some revocation features exist

- Direct Anonymous Attestation:
  - users can be forced to use the same pseudonym
  - remove anonymity of all signers
- EPID:
  - users prove they have not generated revoked signatures
  - complexity increases with the number of revoked signatures

$\Rightarrow$ no fully satisfying solution

GS with Time-Bound Keys

- GS with time-bound keys[1] distinguish two kinds of revocations:
  - natural revocation (NR) predictable at the joining time
  - premature revocation (PR) due to unpredictable events
- NR handled by assigning an expiry period T to each user key

  $\Rightarrow$ signatures can't be generated at time periods $T + i$
- PR handled using Revocation Lists

  $\Rightarrow$ shorter RLs due to NR
- state-of-the-art: Emura *et al* [2] use strategy 2 to instantiate NR

[1] Chu, Liu, Huang and Zhou. *Verifier-local revocation group signatures with time-bound keys*, AsiaCCS, 2012

[2] Emura, Hayashi and Ishida. *Group signatures with time-bound keys revisited: A new model and an efficient construction*, AsiaCCS, 2017

Our Contributions

Better Granularity

Group Manager **User**

T_0 T_0+1 T_0+2 T_0+3 T_0+4 T $T+1$

Current model only considers an expiry time T

- signing keys are useless after T
- signing keys are activated at the period (T_0) of `Join`

Better Granularity

Group Manager **User**

T_0 T_0+1 T_0+2 T_0+3 T_0+4 T_0+5 T_0+6

Our keys can be associated with any set of periods

- Example 1: subscription starts at a later period

Better Granularity

Group Manager **User**

T_0 T_0+1 T_0+2 T_0+3 T_0+4 T_0+5 T_0+6

Our keys can be associated with any set of periods

- Example 2: periodic access to a service (*e.g.* during weekends, etc)

Better Granularity

Group Manager **User**

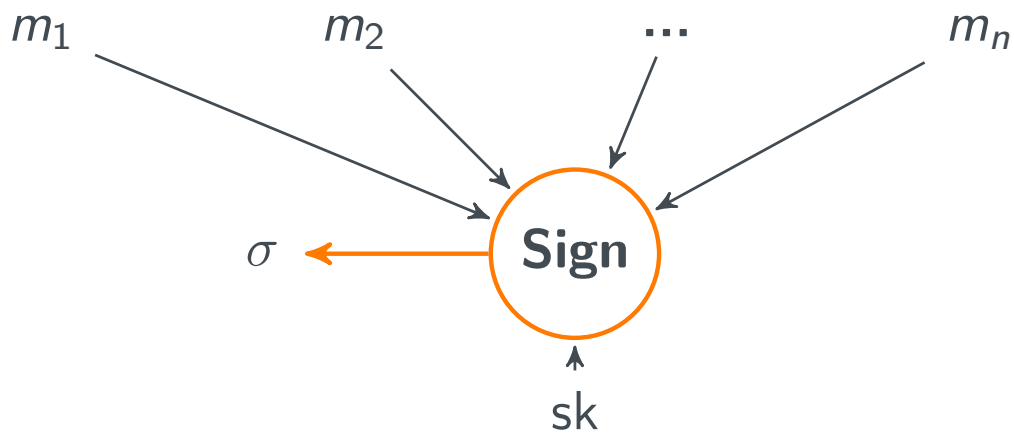
T_0 T_0+1 T_0+2 T_0+3 T_0+4 T_0+5 T_0+6

Our keys can be associated with any set of periods

- Revocation is no longer definitive: key is either active or inactive
- Need to deal with both backward and forward unlinkability

Unlinkable Redactable Signature

We use Unlinkable Redactable Signature[3]

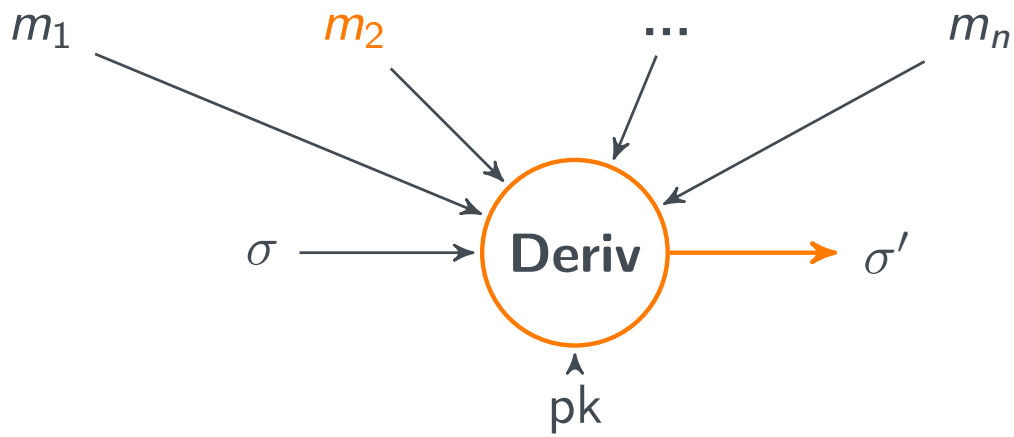


1 signature σ on n messages

[3] Camenisch, Dubovitskaya, Haralambiev and Kohlweiss, *Composable and modular anonymous credentials: Definitions and practical constructions*, Asiacrypt, 2015

Unlinkable Redactable Signature

We use Unlinkable Redactable Signature[3]

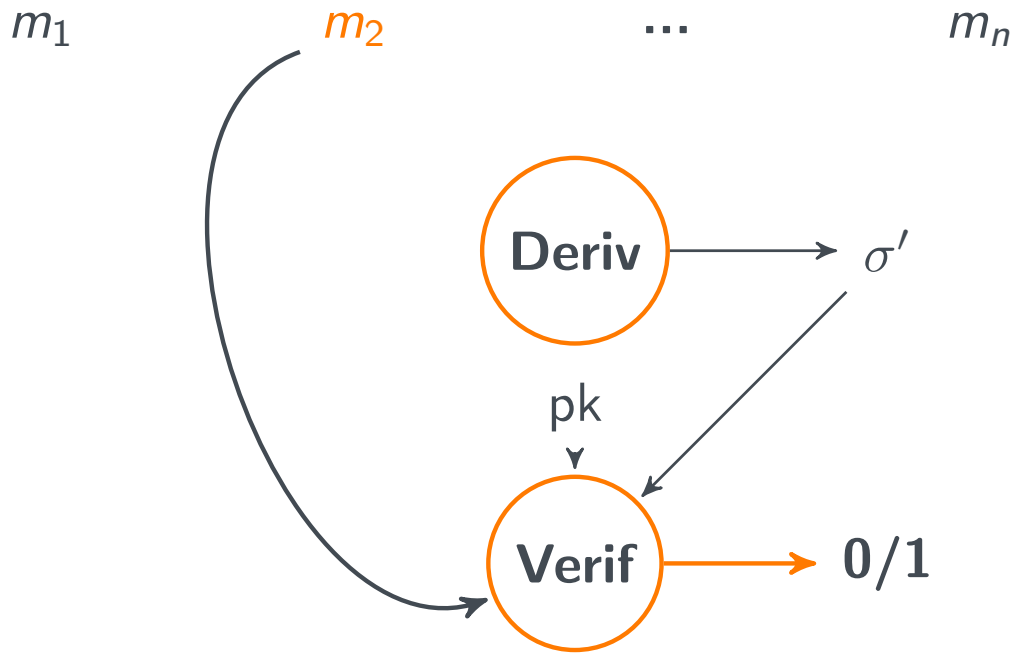


a signature σ' can be derived on a subset of messages

[3] Camenisch, Dubovitskaya, Haralambiev and Kohlweiss, *Composable and modular anonymous credentials: Definitions and practical constructions*, Asiacrypt, 2015

Unlinkable Redactable Signature

We use Unlinkable Redactable Signature[3]

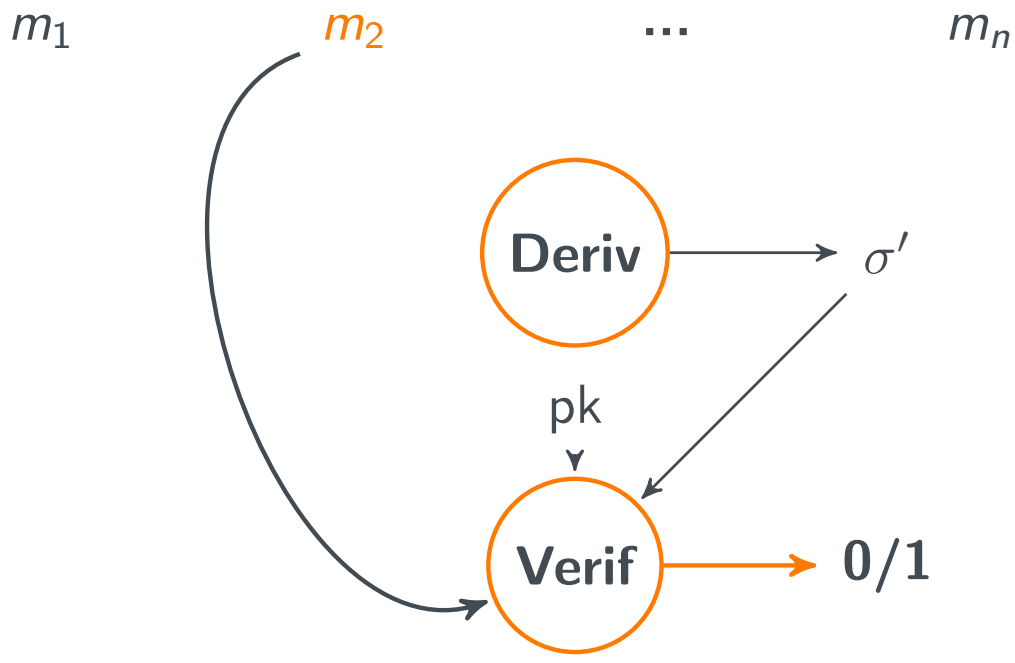


no need to know the redacted messages to check σ'

[3] Camenisch, Dubovitskaya, Haralambiev and Kohlweiss, *Composable and modular anonymous credentials: Definitions and practical constructions*, Asiacrypt, 2015

Unlinkable Redactable Signature

We use Unlinkable Redactable Signature[3]

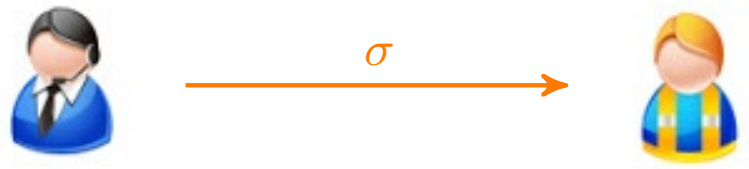


signatures derived from σ are unlinkable

[3] Camenisch, Dubovitskaya, Haralambiev and Kohlweiss, *Composable and modular anonymous credentials: Definitions and practical constructions*, Asiacrypt, 2015

Our Construction

Basic idea:



T_0	T_0+1	T_0+2	T_0+3	T_0+4	T_0+5	T_0+6
m_0	m_1	m_2	m_3	m_4	m_5	m_6

- During `Join`, users obtain a URS σ on $\{m_i\}$

$$m_i = 0 \Leftrightarrow \text{user inactive at } T_0 + i$$

Our Construction

Basic idea:

Group Manager **User** **Verifier**

T_0	T_0+1	T_0+2	T_0+3	T_0+4	T_0+5	T_0+6
m_0	m_1	m_2	m_3	m_4	m_5	m_6

- To sign at period $T_0 + i$, user derives σ' on m_i

  group signature is valid $\Leftrightarrow$ σ' valid and $m_i \neq 0$

No Update information E_T

Security

- Traceability relies on URS unforgeability
- Non frameability: non-zero m_i set as the user's secret key

  $\Rightarrow$ non-zero m_i cannot be revealed
- Premature revocation: Tokens t_i are generated to revoke user at period $T_0 + i$
  - backward unlinkability: t_i useless for signatures issued before $T_0 + i$
  - forward unlinkability: t_i useless for signatures issued after $T_0 + i$

  $\Rightarrow$ anonymity needs more than URS unlinkability

We need specific URS schemes

Instantiation

- A recent URS[4] fulfils these requirements but $O(n^2)$ public key

  not enough practical for large number n of time periods

- We introduce a variant with $O(n)$ public key
  - asymmetric bilinear group $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$
  - GM secret key : $(x, y) \in \mathbb{Z}_p^2$
  - $(\sigma_1, \sigma_1^{x+\sum_{i=1}^{n} y^i m_i})$ signature on $(m_1, \ldots, m_n)$ with $\sigma_1 \xleftarrow{\$} \mathbb{G}_1$

[4] Sanders, *Efficient Redactable Signature and Application to Anonymous Credentials*, PKC 2020

Instantiation

To derive an unlinkable signature σ' on $\{m_i\}_{i \in \mathcal{I}}$, $\mathcal{I} \subset [1, n]$

- $\sigma'_1 \leftarrow \sigma_1^r$ for $r \xleftarrow{\$} \mathbb{Z}_p$
- $\sigma'_2 \leftarrow \sigma_2^r \cdot (\sigma'_1)^t$, for $t \xleftarrow{\$} \mathbb{Z}_p$

Instantiation

To derive an unlinkable signature σ' on $\{m_i\}_{i\in\mathcal{I}}$, $\mathcal{I} \subset [1, n]$

- $\sigma'_1 \leftarrow \sigma_1^r$ for $r \xleftarrow{\$} \mathbb{Z}_p$
- $\sigma'_2 \leftarrow \sigma_2^r \cdot (\sigma'_1)^t$, for $t \xleftarrow{\$} \mathbb{Z}_p$
- $\widetilde{\sigma}' \leftarrow \widetilde{g}^t \prod_{j\in\overline{\mathcal{I}}} (\widetilde{g}^{y^j})^{m_j}$ with $\{\widetilde{g}^{y^j} \in \mathbb{G}_2\}_j \subset \mathsf{pk}$ and $\overline{\mathcal{I}} = [1, n] \setminus \mathcal{I}$

Instantiation

To derive an unlinkable signature σ' on $\{m_i\}_{i\in\mathcal{I}}$, $\mathcal{I} \subset [1, n]$

- $\sigma'_1 \leftarrow \sigma_1^r$ for $r \xleftarrow{\$} \mathbb{Z}_p$
- $\sigma'_2 \leftarrow \sigma_2^r \cdot (\sigma'_1)^t$, for $t \xleftarrow{\$} \mathbb{Z}_p$
- $\widetilde{\sigma}' \leftarrow \widetilde{g}^t \prod_{j\in\overline{\mathcal{I}}} (\widetilde{g}^{y^j})^{m_j}$ with $\{\widetilde{g}^{y^j} \in \mathbb{G}_2\}_j \subset \mathsf{pk}$ and $\overline{\mathcal{I}} = [1, n] \setminus \mathcal{I}$
- $c_i \leftarrow \mathtt{H}(\sigma'_1 || \sigma'_2 || \widetilde{\sigma}' || \mathcal{I} || i)$ for $i \in \mathcal{I}$

Instantiation

To derive an unlinkable signature σ' on $\{m_i\}_{i\in\mathcal{I}}$, $\mathcal{I} \subset [1, n]$

- $\sigma'_1 \leftarrow \sigma_1^r$ for $r \xleftarrow{\$} \mathbb{Z}_p$
- $\sigma'_2 \leftarrow \sigma_2^r \cdot (\sigma'_1)^t$, for $t \xleftarrow{\$} \mathbb{Z}_p$
- $\widetilde{\sigma}' \leftarrow \widetilde{g}^t \prod_{j\in\overline{\mathcal{I}}} (\widetilde{g}^{y^j})^{m_j}$ with $\{\widetilde{g}^{y^j} \in \mathbb{G}_2\}_j \subset \mathsf{pk}$ and $\overline{\mathcal{I}} = [1, n] \setminus \mathcal{I}$
- $c_i \leftarrow \mathtt{H}(\sigma'_1 || \sigma'_2 || \widetilde{\sigma}' || \mathcal{I} || i)$ for $i \in \mathcal{I}$
- $\sigma'_3 = \prod_{i\in\mathcal{I}} [(g^{y^{n+1-i}})^t \cdot \prod_{j\in\overline{\mathcal{I}}} (g^{y^{n+1-i+j}})^{m_j}]^{c_i}$ with $\{g^{y^k} \in \mathbb{G}_1\}_k \subset \mathsf{pk}$

Instantiation

To derive an unlinkable signature σ' on $\{m_i\}_{i\in\mathcal{I}}$, $\mathcal{I}\subset[1,n]$

- $\sigma'_1 \leftarrow \sigma_1^r$ for $r \xleftarrow{\$} \mathbb{Z}_p$
- $\sigma'_2 \leftarrow \sigma_2^r \cdot (\sigma'_1)^t$, for $t \xleftarrow{\$} \mathbb{Z}_p$
- $\widetilde{\sigma}' \leftarrow \widetilde{g}^t \prod_{j\in\overline{\mathcal{I}}}(\widetilde{g}^{y^j})^{m_j}$ with $\{\widetilde{g}^{y^j}\in\mathbb{G}_2\}_j \subset \mathsf{pk}$ and $\overline{\mathcal{I}} = [1,n]\setminus\mathcal{I}$
- $c_i \leftarrow \mathtt{H}(\sigma'_1||\sigma'_2||\widetilde{\sigma}'||\mathcal{I}||i)$ for $i\in\mathcal{I}$
- $\sigma'_3 = \prod_{i\in\mathcal{I}}[(g^{y^{n+1-i}})^t \cdot \prod_{j\in\overline{\mathcal{I}}}(g^{y^{n+1-i+j}})^{m_j}]^{c_i}$ with $\{g^{y^k}\in\mathbb{G}_1\}_k \subset \mathsf{pk}$

Verification of $\sigma' = (\sigma'_1,\sigma'_2,\sigma'_3,\widetilde{\sigma}') \in \mathbb{G}_1^3\times\mathbb{G}_2$

$$e(\sigma'_1, \widetilde{\sigma}'\cdot\widetilde{g}^x\prod_{i\in\mathcal{I}}(\widetilde{g}^{y^i})^{m_i}) = e(\sigma'_2,\widetilde{g}) \wedge e(\sigma'_3,\widetilde{g}) = e(\prod_{i\in\mathcal{I}}(g^{y^{n+1-i}})^{c_i},\widetilde{\sigma}')$$

Our Group Signature

In our case

- $\mathcal{I} = \{i^*\}$ with i^* the current time period
- $m_i =$ usk if $i \in \mathcal{T}$ set of active time periods and $m_i = 0$ otherwise

Complexity

- $\sigma'_1 \leftarrow \sigma_1^r \quad \rightarrow$1exp in $\mathbb{G}_1$
- $\sigma'_2 \leftarrow \sigma_2^r \cdot (\sigma'_1)^t \quad \rightarrow$2exp in $\mathbb{G}_1$
- $\widetilde{\sigma}' \leftarrow \widetilde{g}^t [\prod_{j \in \overline{\mathcal{I}} \cap \mathcal{T}} \widetilde{g}^{y^j}]^{\mathsf{usk}} \quad \rightarrow$2exp in $\mathbb{G}_2$
- $c_{i^*} \leftarrow \mathtt{H}(\sigma'_1 || \sigma'_2 || \widetilde{\sigma}' || \{i^*\} || i^*) \quad \rightarrow$1hash
- $\sigma'_3 = [(g^{y^{n+1-i^*}})^t \cdot [\prod_{j \in \overline{\mathcal{I}} \cap \mathcal{T}} g^{y^{n+1-i^*+j}}]^{\mathsf{usk}}]^{c_{i^*}} \quad \rightarrow$3exp in $\mathbb{G}_1$
- Proof of Knowledge of usk $\quad \rightarrow 1\mathtt{exp}$ in $\mathbb{G}_1 + 1\mathtt{hash} + 1\mathtt{pair}$

Performance

Size in Bytes (B) with BLS381 curve, for R premature revocations

pk	Signing Key	`Update`	RL	σ
$(1+2n)\mathbb{G}_1$ $+(n+1)\mathbb{G}_2$ $= 48(4n+3)$B	$2\mathbb{G}_1 + \mathbb{Z}_p$ $= 128$ B	None	$R\mathbb{G}_2$ $= 96R$ B	$3\mathbb{G}_1 +$ $1\mathbb{G}_2 + 2\mathbb{Z}_p$ $= 303$ B

Computational Complexity

Signature	Verification
$7\text{exp}_1 + 2\text{exp}_2 + 2\text{Hash} + 1\text{pair}$	$3\text{exp}_1 + 2\text{Hash} + (3R+7)\text{pair}$

Conclusion

GS with time-bound keys is an efficient solution for user revocation

- Users can be revoked immediately using Revocation Lists
- RLs not too large thanks to natural revocation

Contributions

- We improve granularity of natural revocation
- We show how to construct it with URS
  - Simple Enrolment, Signature and Verification procedures
  - No need to publish or retrieve update information
- We propose a new URS scheme to implement our construction
  - short, constant size group signature
  - fast signature generation

thank you