Efficient Redactable Signature and Application to Anonymous Credentials

Olivier Sanders
Orange Labs

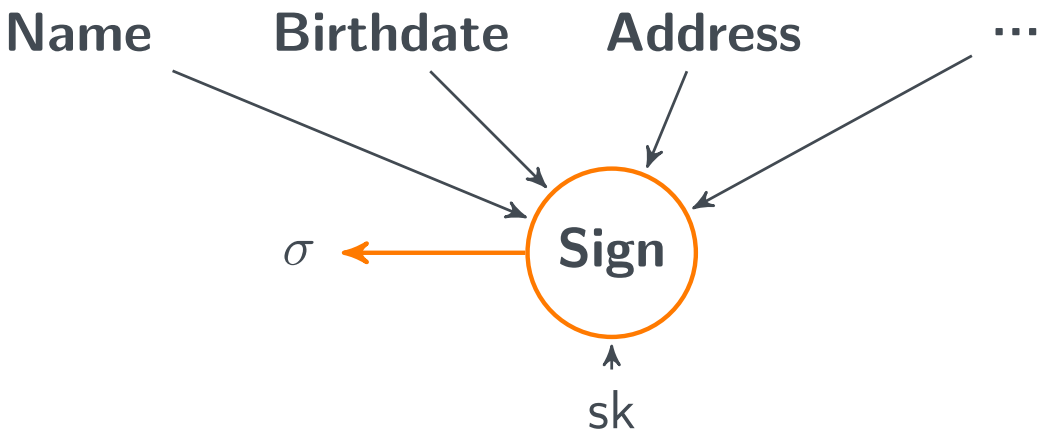
PKC 2020

orange™

Context

Digital Signature

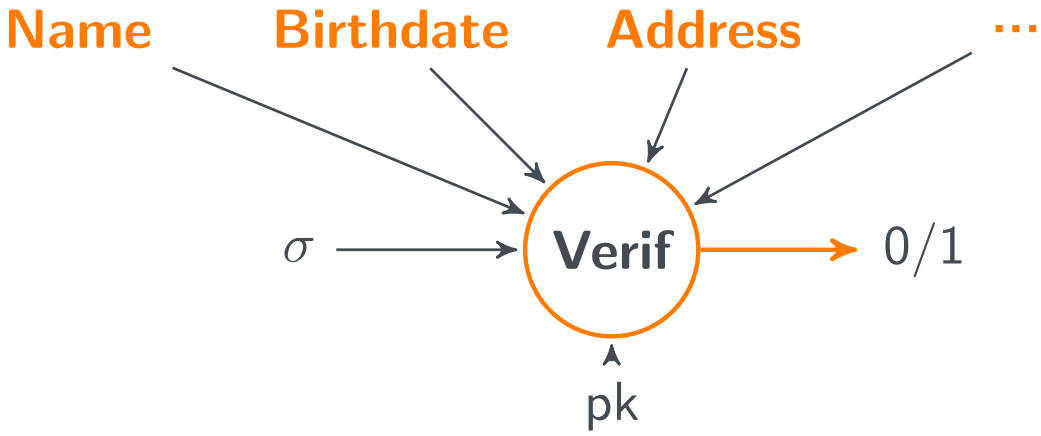
Digital signature can be used to authenticate digital data



not even one bit can be modified

Digital Signature

Digital signature can be used to authenticate digital data



verification requires knowledge of all signed data

Limits of Digital Signature

Use Case: One just needs to verify that age ≥ 18

- Efficiency: ✗ (n messages to send)
- Privacy: ✗ (reveals all signed data to the verifier)

How to efficiently and privately check that k out of n messages are certified or satisfy some relations?

Standard Alternatives:

- Alternative 1: 1 signature per message
  - Efficiency: $\sim$ (n signatures to store)
  - Privacy: ↗

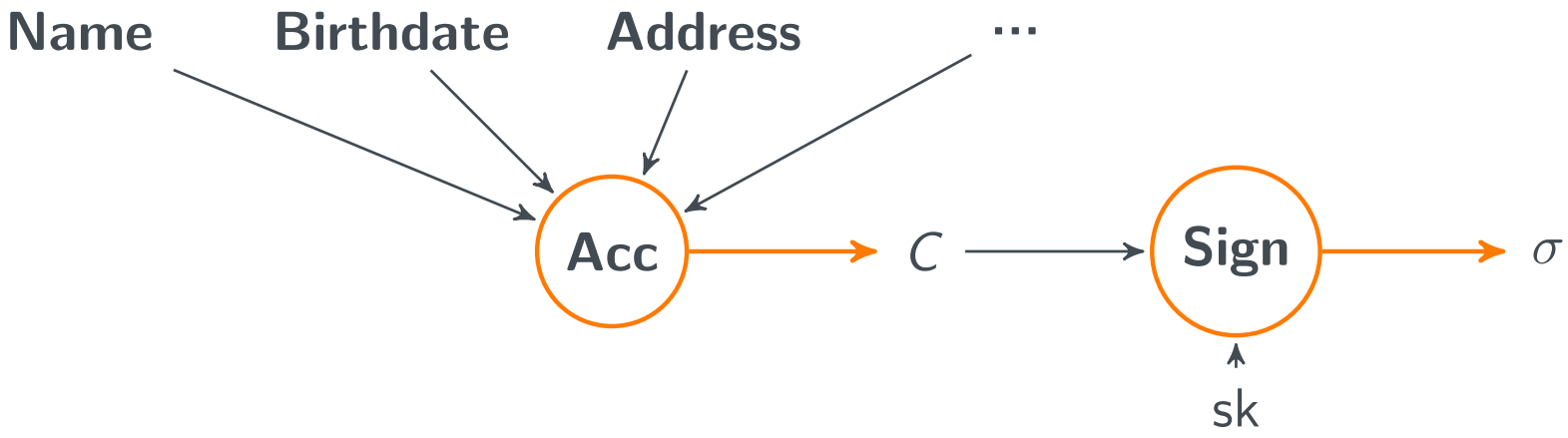
Limits of Digital Signature

- Alternative 2: Merkle's tree
  - Efficiency: ↗ ($\log(n)$ elements to send)
  - Privacy: $\sim$ (prevents zero-knowledge proofs)
- Alternative 3: proof of knowledge of the n messages
  - Efficiency: ↘
  - Privacy: ✓

$\Rightarrow$ no satisfying solution

Accumulators

Solution from [FHS19][1]

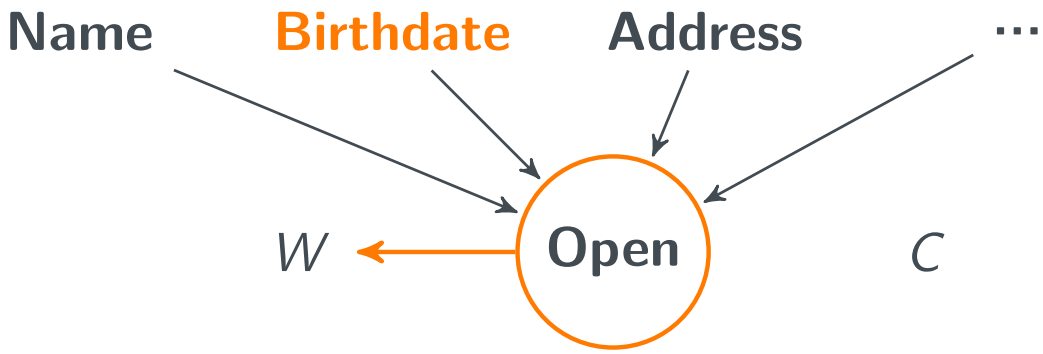


messages are accumulated and then signed

[1] Fuchsbauer, Hanser and Slamanig, *Structure-preserving signatures on equivalence classes and constant-size anonymous credentials*, Journal of Cryptology, 2019

Accumulators

Solution from [FHS19][1]

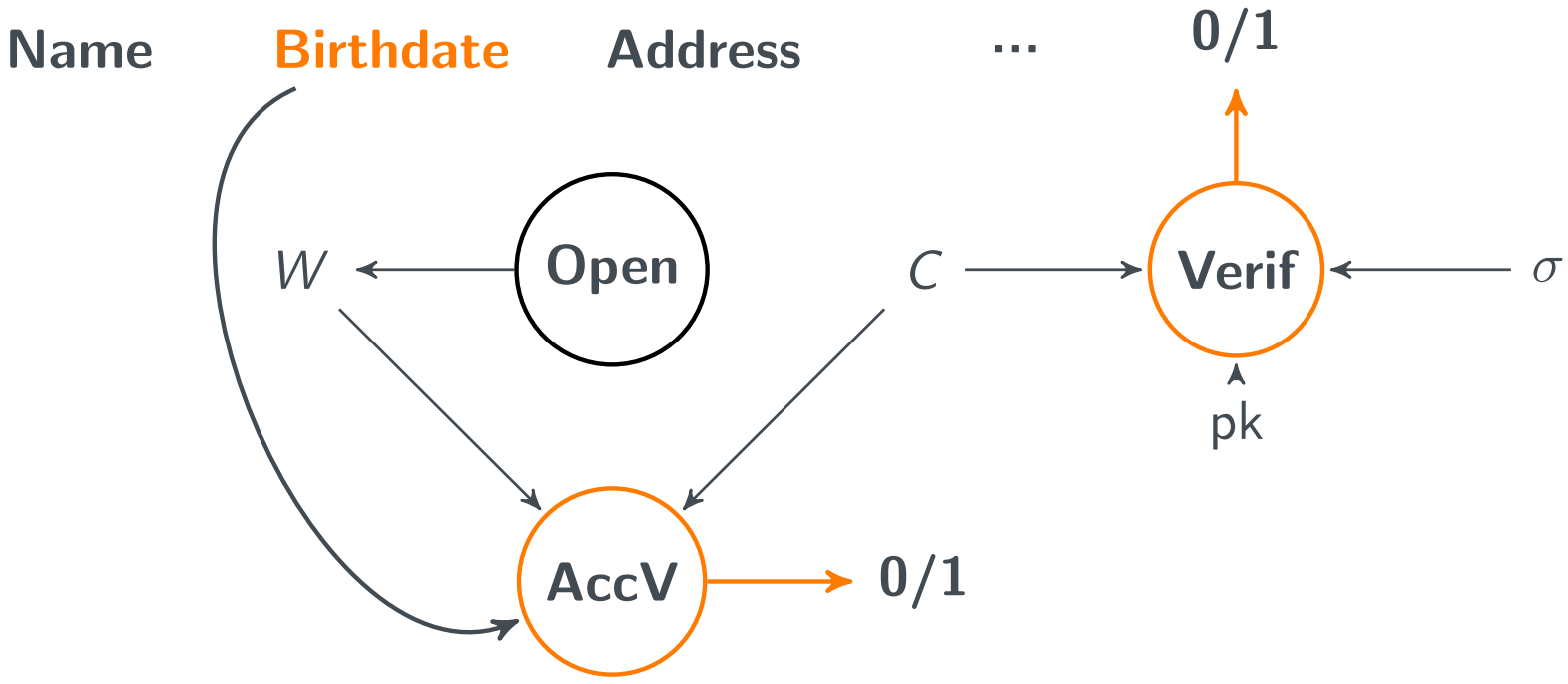


a witness W that "birthdate" has been accumulated can be computed

[1] Fuchsbauer, Hanser and Slamanig, *Structure-preserving signatures on equivalence classes and constant-size anonymous credentials*, Journal of Cryptology, 2019

Accumulators

Solution from [FHS19][1]



Given C, W, σ, one can check that "birthdate" has been signed

[1] Fuchsbauer, Hanser and Slamanig, *Structure-preserving signatures on equivalence classes and constant-size anonymous credentials*, Journal of Cryptology, 2019

Accumulators

Assessment of FHS solution (compared to basic signature):

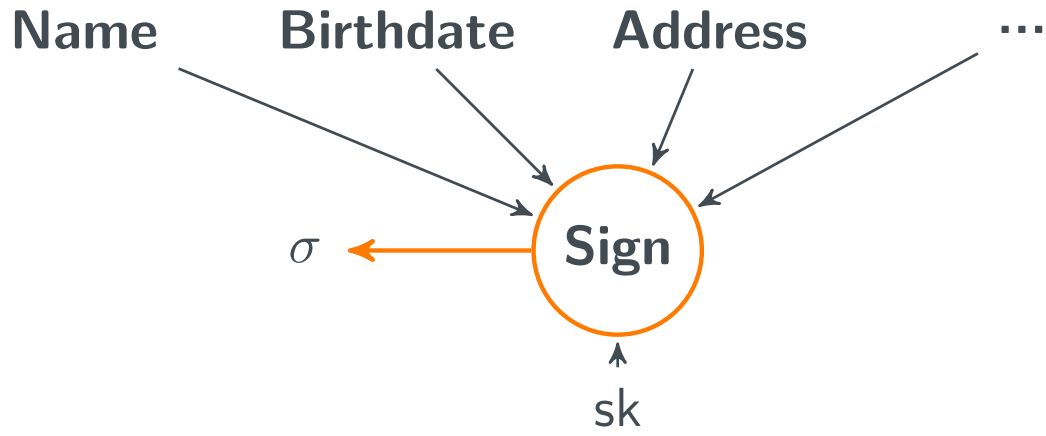
- Efficiency: ✓
  - $O(1)$ certificate size
  - $O(1)$ communication complexity[2]
  - $O(k)$ verification complexity
- Privacy: $\sim$
  - the k messages must be disclosed, no ability to prove that they satisfy some relations (*e.g.* age ≥ 18)

$\Rightarrow$ not fully satisfying

[2] excluding the k disclosed messages

Unlinkable Redactable Signature

Solution from [CDHK15][3]

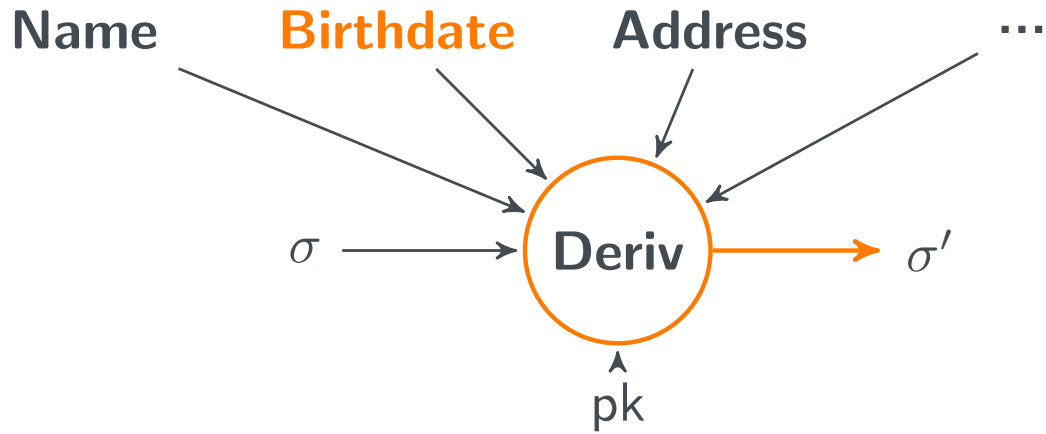


1 signature σ on all messages

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

Unlinkable Redactable Signature

Solution from [CDHK15][3]

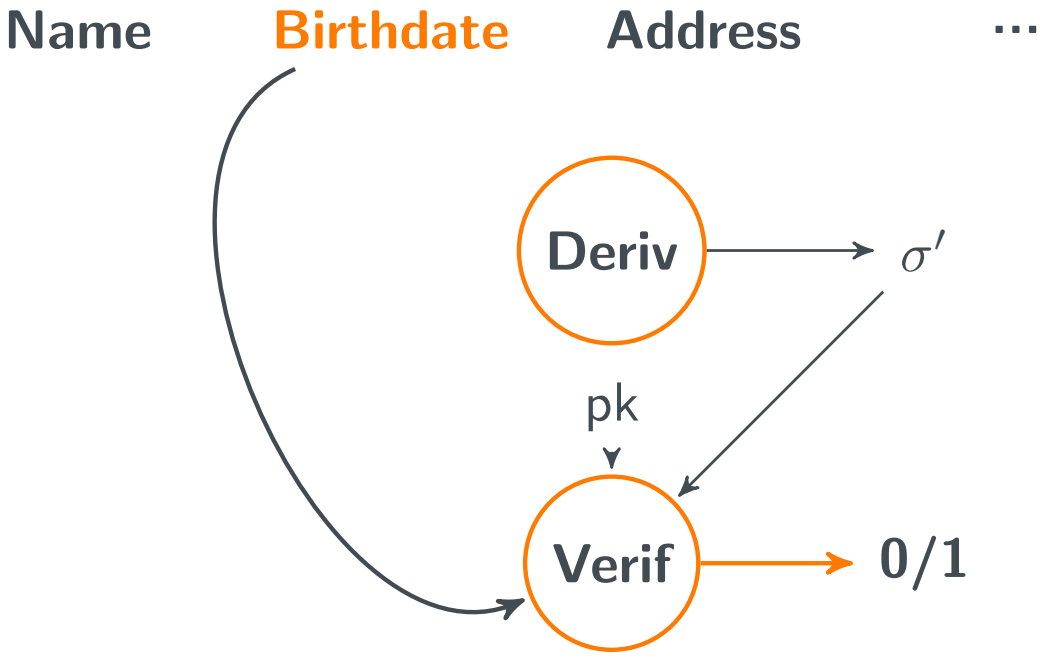


a signature σ' can be derived on a subset of messages

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

Unlinkable Redactable Signature

Solution from [CDHK15][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

Assessment of CDHK solution (compared to basic signature):

- Efficiency: ↗
  - $O(1)$ certificate size
  - $O(1)$ communication complexity[4]
  - very large constant
  - $O(k)$ verification complexity
- Privacy: $\sim$
  - the k messages must be disclosed, no ability to prove that they satisfy some relations (*e.g.* age ≥ 18)
  - derived signatures can be unlinkable

$\Rightarrow$ not fully satisfying

[4] excluding the k disclosed messages

Our Contribution

Unlinkable Redactable Signature

We want an unlinkable redactable signature scheme with:

- Efficiency:
  - short, constant-size (derived) signatures
  - verification of k out of n messages in $O(k)$
- Privacy:
  - unlinkability: to link signatures derived from the same σ is hard
  - relations about non-redacted messages can be proved in ZK

Pointcheval-Sanders Signature

Our starting point: PS signature[5]

- use asymmetric bilinear group $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$
- secret $(x, y_1, \ldots, y_n)$ and public $X = g^x$, $Y_i = g^{y_i}$ in $\mathbb{G}_1$
- a signature on $(m_1, \ldots, m_n)$ is $\widetilde{\sigma}_1 \xleftarrow{\$} \mathbb{G}_2$ and $\widetilde{\sigma}_2 \leftarrow \widetilde{\sigma}_1^{x+\sum_{i=1}^{n} y_i m_i}$
- verification:

$$e(g, \widetilde{\sigma}_2) \stackrel{?}{=} e(X \prod_{i=1}^{n} Y_i^{m_i}, \widetilde{\sigma}_1)$$

designed to support proofs of knowledge of m_i

[5] Pointcheval and Sanders, *Short Randomizable Signature*, CT-RSA 16

Pointcheval-Sanders Signature

- Use Case: $\mathcal{V}$ wants to check that a subset $\{m_i\}_{i\in\mathcal{I}}$ of messages is signed and/or satisfies some relations

  $\Rightarrow$ messages $\{m_i\}_{i\in\overline{\mathcal{I}}}$ are redacted, with $\overline{\mathcal{I}} = \{1,\ldots,n\} \setminus \mathcal{I}$

- Standard solution:
  - prove knowledge of redacted messages
  - reveal and/or prove relations about $\{m_i\}_{i\in\mathcal{I}}$

    $\Rightarrow$ inefficient

A First Attempt

- Verification of PS signatures:

$$e(g, \widetilde{\sigma}_2) \stackrel{?}{=} e(X \prod_{i=1}^{n} Y_i^{m_i}, \widetilde{\sigma}_1)$$

A First Attempt

- Verification of PS signatures:

$$e(g, \widetilde{\sigma}_2) \stackrel{?}{=} e(X \prod_{i=1}^{n} Y_i^{m_i}, \widetilde{\sigma}_1)$$
$$\stackrel{?}{=} e(X \prod_{i \in \overline{\mathcal{I}}} Y_i^{m_i} \prod_{i \in \mathcal{I}} Y_i^{m_i}, \widetilde{\sigma}_1)$$

A First Attempt

- Verification of PS signatures:

$$e(g, \widetilde{\sigma}_2) \stackrel{?}{=} e(X \prod_{i=1}^{n} Y_i^{m_i}, \widetilde{\sigma}_1)$$

$$\stackrel{?}{=} e(X \prod_{i \in \overline{\mathcal{I}}} Y_i^{m_i} \prod_{i \in \mathcal{I}} Y_i^{m_i}, \widetilde{\sigma}_1)$$

$$\stackrel{?}{=} e(X \sigma_1 \prod_{i \in \mathcal{I}} Y_i^{m_i}, \widetilde{\sigma}_1) \qquad \sigma_1 = \prod_{i \in \overline{\mathcal{I}}} Y_i^{m_i}$$

A First Attempt

- Verification of PS signatures:

$$
\begin{aligned}
e(g, \widetilde{\sigma}_2) &\stackrel{?}{=} e(X \prod_{i=1}^{n} Y_i^{m_i}, \widetilde{\sigma}_1) \\
&\stackrel{?}{=} e(X \prod_{i \in \overline{\mathcal{I}}} Y_i^{m_i} \prod_{i \in \mathcal{I}} Y_i^{m_i}, \widetilde{\sigma}_1) \\
&\stackrel{?}{=} e(X \sigma_1 \prod_{i \in \mathcal{I}} Y_i^{m_i}, \widetilde{\sigma}_1) \qquad\qquad \sigma_1 = \prod_{i \in \overline{\mathcal{I}}} Y_i^{m_i} \\
&\stackrel{?}{=} e(X \sigma_1 Y_{i_0}^{m_{i_0}} \prod_{i \in \mathcal{I} \setminus i_0} Y_i^{m_i}, \widetilde{\sigma}_1)
\end{aligned}
$$

- $(\sigma_1, \widetilde{\sigma}_1, \widetilde{\sigma}_2)$ is not a secure redactable signature on $\{m_i\}_{i \in \mathcal{I}}$:

A First Attempt

- Verification of PS signatures:

$$
\begin{aligned}
e(g, \widetilde{\sigma}_2) &\stackrel{?}{=} e(X \prod_{i=1}^{n} Y_i^{m_i}, \widetilde{\sigma}_1) \\
&\stackrel{?}{=} e(X \prod_{i \in \overline{\mathcal{I}}} Y_i^{m_i} \prod_{i \in \mathcal{I}} Y_i^{m_i}, \widetilde{\sigma}_1) \\
&\stackrel{?}{=} e(X \sigma_1 \prod_{i \in \mathcal{I}} Y_i^{m_i}, \widetilde{\sigma}_1) && \sigma_1 = \prod_{i \in \overline{\mathcal{I}}} Y_i^{m_i} \\
&\stackrel{?}{=} e(X \sigma_1 Y_{i_0}^{m_{i_0}} \prod_{i \in \mathcal{I} \setminus i_0} Y_i^{m_i}, \widetilde{\sigma}_1) \\
&\stackrel{?}{=} e(X \sigma_1' Y_{i_0}^{t} \prod_{i \in \mathcal{I} \setminus i_0} Y_i^{m_i}, \widetilde{\sigma}_1) && \sigma_1' = \sigma_1 Y_{i_0}^{m_{i_0} - t}
\end{aligned}
$$

- $(\sigma_1, \widetilde{\sigma}_1, \widetilde{\sigma}_2)$ is not a secure redactable signature on $\{m_i\}_{i \in \mathcal{I}}$:

  $(\sigma_1', \widetilde{\sigma}_1, \widetilde{\sigma}_2)$ is valid on t and $\{m_i\}_{i \in \mathcal{I} \setminus i_0}$

A Linkable Solution

Problem: elements $Y_i^{u_i}$, for $i \in \mathcal{I}$, can be aggregated in σ_1

- solution 1: prove that $\sigma_1 = \prod_{i \in \mathcal{I}} Y_i^{m_i}$
  - inefficient (back to square 1)
  - overkill: prove more that what we need

A Linkable Solution

Problem: elements $Y_i^{u_i}$, for $i \in \mathcal{I}$, can be aggregated in σ_1

- our solution: if σ_1 is honestly formed

$$e(\sigma_1, \prod_{i \in \mathcal{I}} \widetilde{g}^{y_i}) = e(g, \widetilde{g})^{f(y_1, \ldots, y_n)}$$

f only contains monomials $y_i \cdot y_j$, for $i \neq j$

A Linkable Solution

Problem: elements $Y_i^{u_i}$, for $i \in \mathcal{I}$, can be aggregated in σ_1

- our solution: if σ_1 is forged

$$e(\sigma_1, \prod_{i \in \mathcal{I}} \widetilde{g}^{y_i}) = e(g, \widetilde{g})^{f(y_1, \ldots, y_n)}$$

$$f \text{ contains monomials } y_i^2,\ i \in \mathcal{I}$$

- we add $\{g^{y_i y_j}\}_{i \neq j}$ in pk
  - sufficient to compute $\sigma_2 = g^{f(y_1, \ldots, y_n)}$ if σ_1 honestly formed
  - not sufficient to compute $\sigma_2 = g^{f(y_1, \ldots, y_n)}$ if σ_1 forged
  - "validity" of σ_1 can be checked: $e(\sigma_1, \prod_{i \in \mathcal{I}} \widetilde{g}^{y_i}) \stackrel{?}{=} e(\sigma_2, \widetilde{g})$

Achieving Unlinkability

- Our redactable signature $(\sigma_1, \sigma_2, \widetilde{\sigma}_1, \widetilde{\sigma}_2)$ is:
  - ✓ constant size (4 group elements)
  - ✓ $O(|\mathcal{I}|)$ complexity for verification
  - ✗ not unlinkable
- $(\widetilde{\sigma}_1, \widetilde{\sigma}_2)$ can be re-randomized but not (σ_1, σ_2)
- We use a different approach:
  - σ_2 only proves that σ_1 does not contain illicit elements $\{Y_{i_0}^{u_{i_0}}\}_{i_0 \in \mathcal{I}}$
  - we can aggregate anything else in σ_1

Achieving Unlinkability

- Step 1: aggregate $t \xleftarrow{\$} \mathbb{Z}_p$ under dummy public key 1
  - $\widetilde{\sigma}_2'' \leftarrow \widetilde{\sigma}_2 \cdot \widetilde{\sigma}_1^t$
  - re-randomize $(\widetilde{\sigma}_1', \widetilde{\sigma}_2') \leftarrow (\widetilde{\sigma}_1^r, (\widetilde{\sigma}_2'')^r)$, with $r \xleftarrow{\$} \mathbb{Z}_p$

$(\widetilde{\sigma}_1', \widetilde{\sigma}_2')$ is valid on $(m_1, \ldots, m_n, t)$

Achieving Unlinkability

- Step 1: aggregate $t \xleftarrow{\$} \mathbb{Z}_p$ under dummy public key 1
  - $\widetilde{\sigma}_2'' \leftarrow \widetilde{\sigma}_2 \cdot \widetilde{\sigma}_1^t$
  - re-randomize $(\widetilde{\sigma}_1', \widetilde{\sigma}_2') \leftarrow (\widetilde{\sigma}_1^r, (\widetilde{\sigma}_2'')^r)$, with $r \xleftarrow{\$} \mathbb{Z}_p$

    $(\widetilde{\sigma}_1', \widetilde{\sigma}_2')$ is valid on $(m_1, \ldots, m_n, t)$
- Step 2: redact $\{m_i\}_{i \in \overline{\mathcal{I}}}$ and t
  - $\sigma_1' = g^t \cdot \prod_{i \in \overline{\mathcal{I}}} Y_i^{m_i}$
  - $\sigma_2' \leftarrow (\prod_{i \in \mathcal{I}} Y_i)^t \prod_{i \in \mathcal{I}, j \in \overline{\mathcal{I}}} (g^{y_i y_j})^{m_j}$

Achieving Unlinkability

- Step 1: aggregate $t \xleftarrow{\$} \mathbb{Z}_p$ under dummy public key 1
  - $\widetilde{\sigma}_2'' \leftarrow \widetilde{\sigma}_2 \cdot \widetilde{\sigma}_1^t$
  - re-randomize $(\widetilde{\sigma}_1', \widetilde{\sigma}_2') \leftarrow (\widetilde{\sigma}_1^r, (\widetilde{\sigma}_2'')^r)$, with $r \xleftarrow{\$} \mathbb{Z}_p$

    $(\widetilde{\sigma}_1', \widetilde{\sigma}_2')$ is valid on $(m_1, \ldots, m_n, t)$
- Step 2: redact $\{m_i\}_{i \in \overline{\mathcal{I}}}$ and t
  - $\sigma_1' = g^t \cdot \prod_{i \in \overline{\mathcal{I}}} Y_i^{m_i}$
  - $\sigma_2' \leftarrow (\prod_{i \in \mathcal{I}} Y_i)^t \prod_{i \in \mathcal{I}, j \in \overline{\mathcal{I}}} (g^{y_i y_j})^{m_j}$
- Step 3: output $\sigma = (\sigma_1', \sigma_2', \widetilde{\sigma}_1', \widetilde{\sigma}_2')$
- t perfectly hides redacted messages:

  unlinkability holds unconditionnaly

Anonymous Credentials

- converting our scheme into anonymous credentials is straightforward
- a credential is a signature on user's secret key usk and $\{m_i\}_{i=1}^n$
- to show a credential on $\{m_i\}_{i \in \mathcal{I}}$
  - run `Derive` on usk and $\{m_i\}_{i \in \mathcal{I}}$ to get σ
  - prove knowledge of usk
- almost as efficient as our URS scheme
- security follows from the one of our URS scheme
- unlinkability holds under the DDH assumption

Conclusion

We have proposed a versatile and efficient URS scheme:

- signatures can be derived on any subset $\{m_i\}_{i\in\mathcal{I}}$ of signed messages
- derived signature contains 4 elements and can be verified with $O(|\mathcal{I}|)$ complexity
- derived signature are unlinkable
- possible to disclose $\{m_i\}_{i\in\mathcal{I}}$ or prove that they satisfy some relations
- derivation public key contains $O(n^2)$ elements

thank you