Subset Signatures with Controlled Context-Hiding

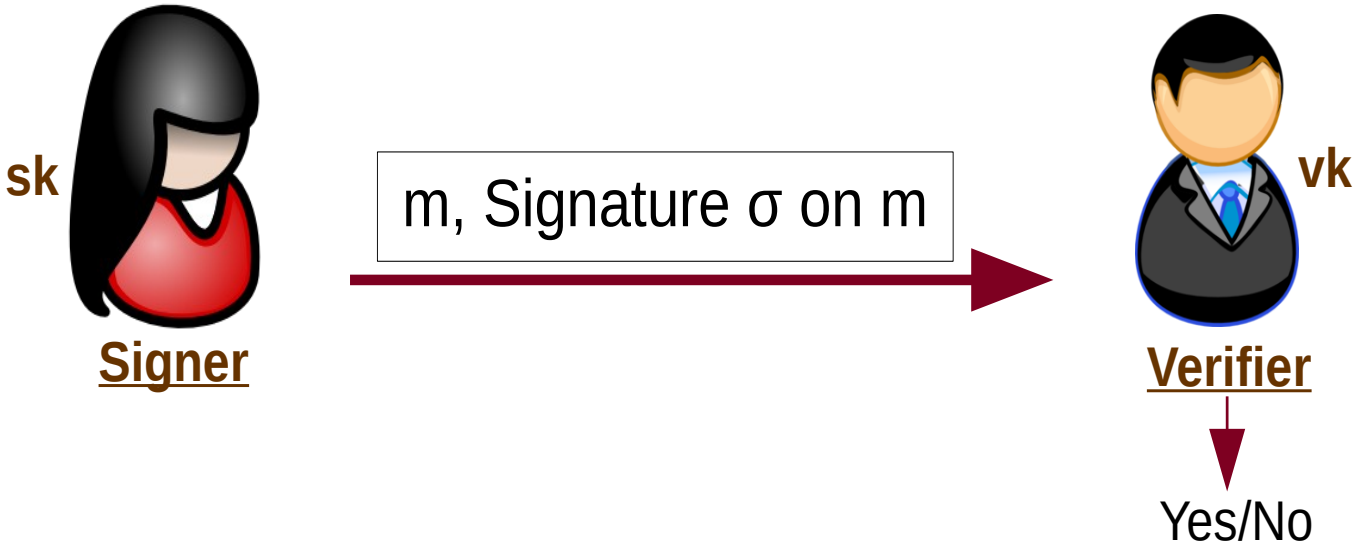
Essam Ghadafi

University of the West of England

IMA International Conference on Cryptography and Coding 2017

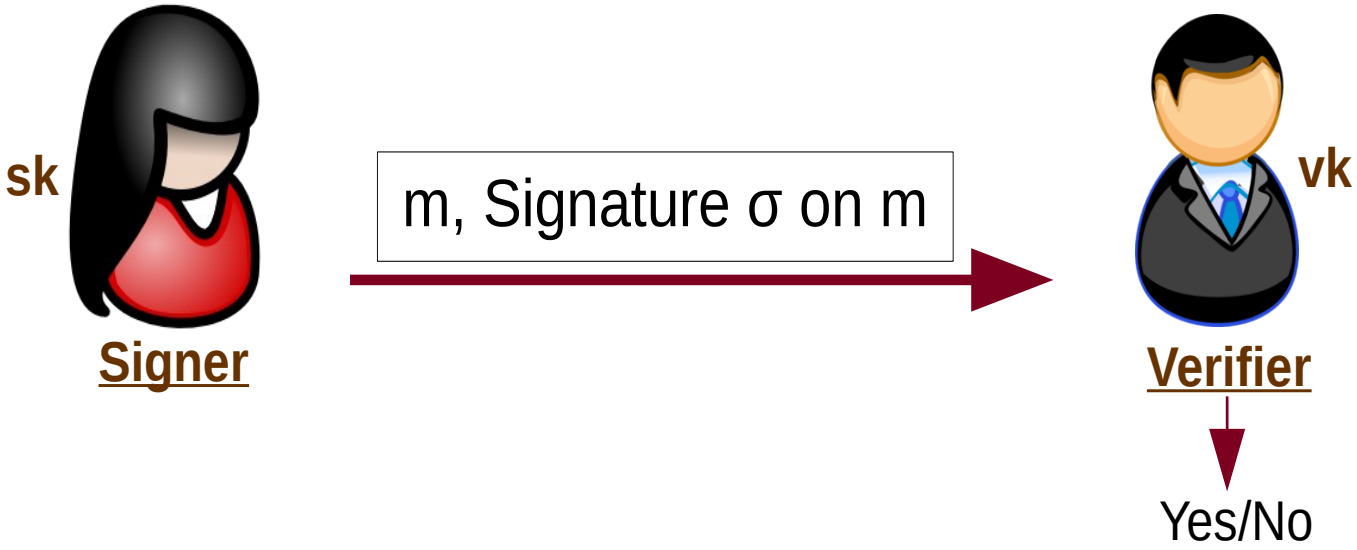
Outline

Digital Signatures



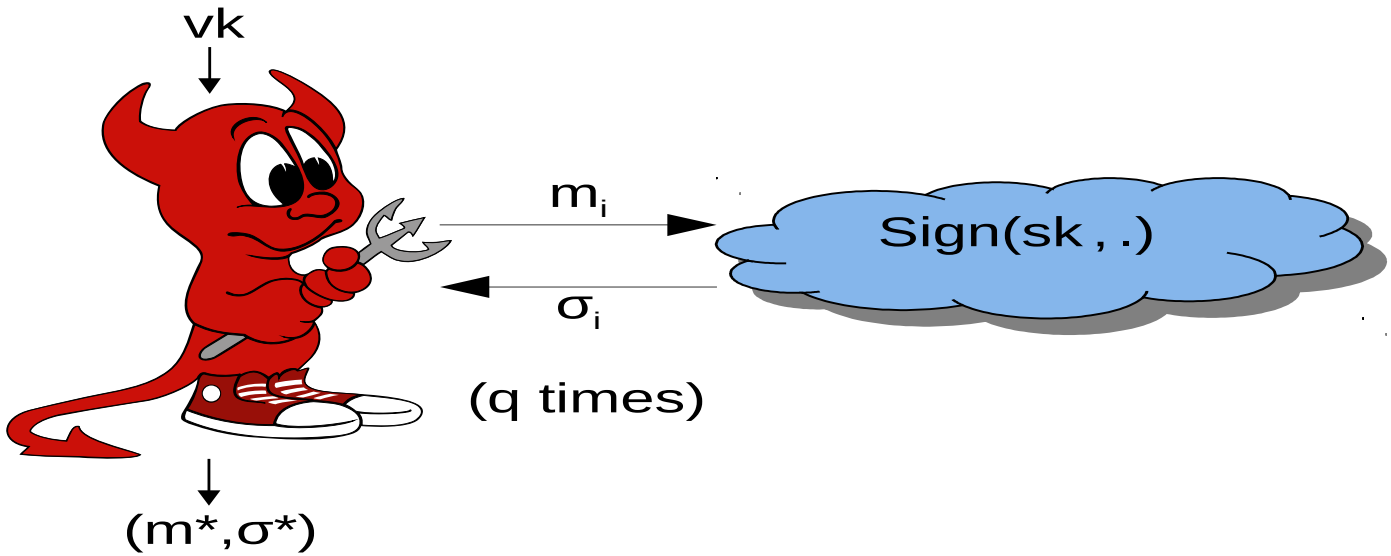
Unforgeabiltiy: You can only sign messages if you have the signing key

Digital Signatures



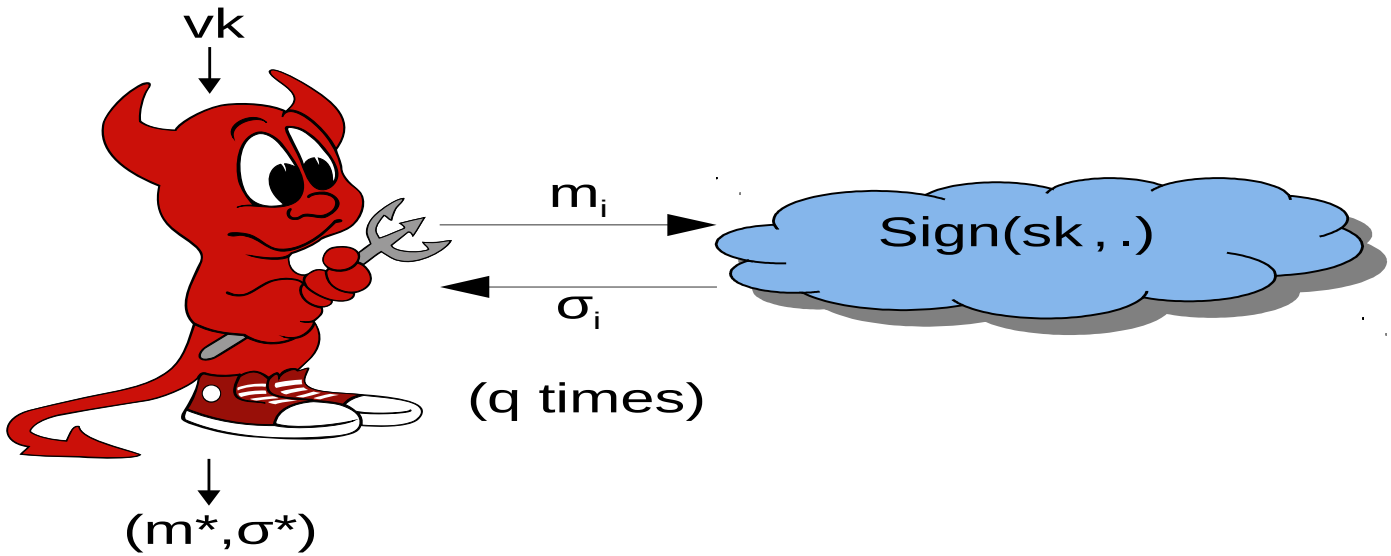
Unforgeabiltiy: You can only sign messages if you have the signing key

Existential Unforgeability



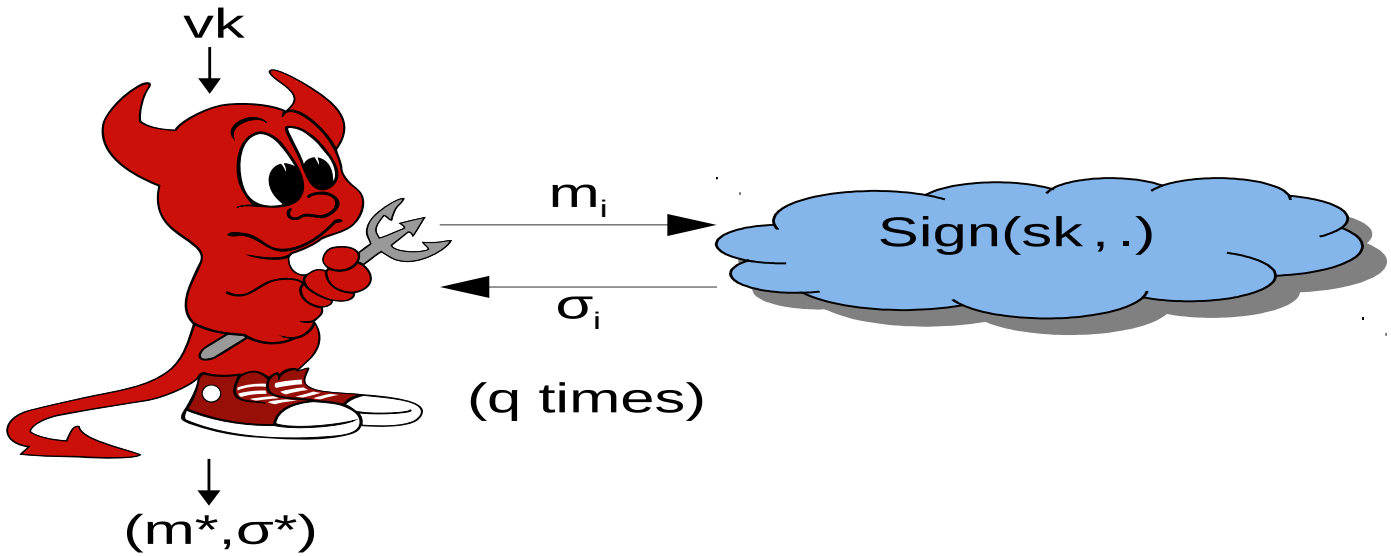
- EUF-CMA: Adversary wins if σ^* is valid on m^* & $m^* \notin \{m_i\}_{i=1}^{q}$
- Strong EUF-CMA (sEUF-CMA): Adversary wins if σ^* is valid on m^* & $(m^*, \sigma^*) \notin \{(m_i, \sigma_i)\}_{i=1}^{q}$

Existential Unforgeability



- EUF-CMA: Adversary wins if σ^* is valid on m^* & $m^* \notin \{m_i\}_{i=1}^{q}$
- Strong EUF-CMA (sEUF-CMA): Adversary wins if σ^* is valid on m^* & $(m^*, \sigma^*) \notin \{(m_i, \sigma_i)\}_{i=1}^{q}$

Existential Unforgeability



- EUF-CMA: Adversary wins if σ^* is valid on m^* & $m^* \notin \{m_i\}_{i=1}^{q}$
- Strong EUF-CMA (sEUF-CMA): Adversary wins if σ^* is valid on m^* & $(m^*, \sigma^*) \notin \{(m_i, \sigma_i)\}_{i=1}^{q}$

Malleable Signatures

Malleable/Homomorphic Signatures [Desmedt 1993, Johnson et al. 2002] allow useful controlled forms of forgeability:

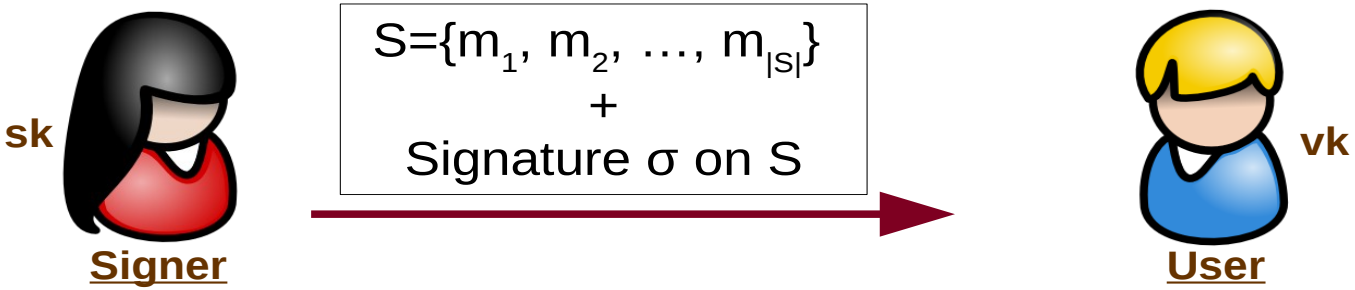
- Redactable Signatures
- Signatures for Arithmetic Circuits
- Transitive Signatures
- Append-Only Signatures
- Quoting Signatures
- Subset Signatures
- Linearly Homomorphic Signatures
- Sanitizable Signatures
- ...

Malleable Signatures

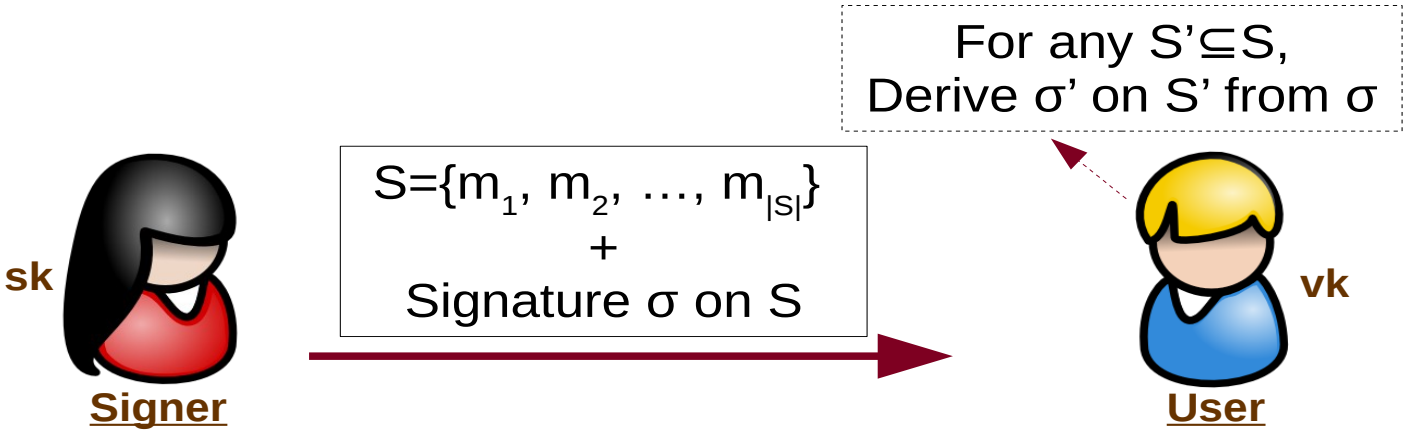
Malleable/Homomorphic Signatures [Desmedt 1993, Johnson et al. 2002] allow useful controlled forms of forgeability:

- Redactable Signatures
- Signatures for Arithmetic Circuits
- Transitive Signatures
- Append-Only Signatures
- Quoting Signatures
- Subset Signatures
- Linearly Homomorphic Signatures
- Sanitizable Signatures
- ...

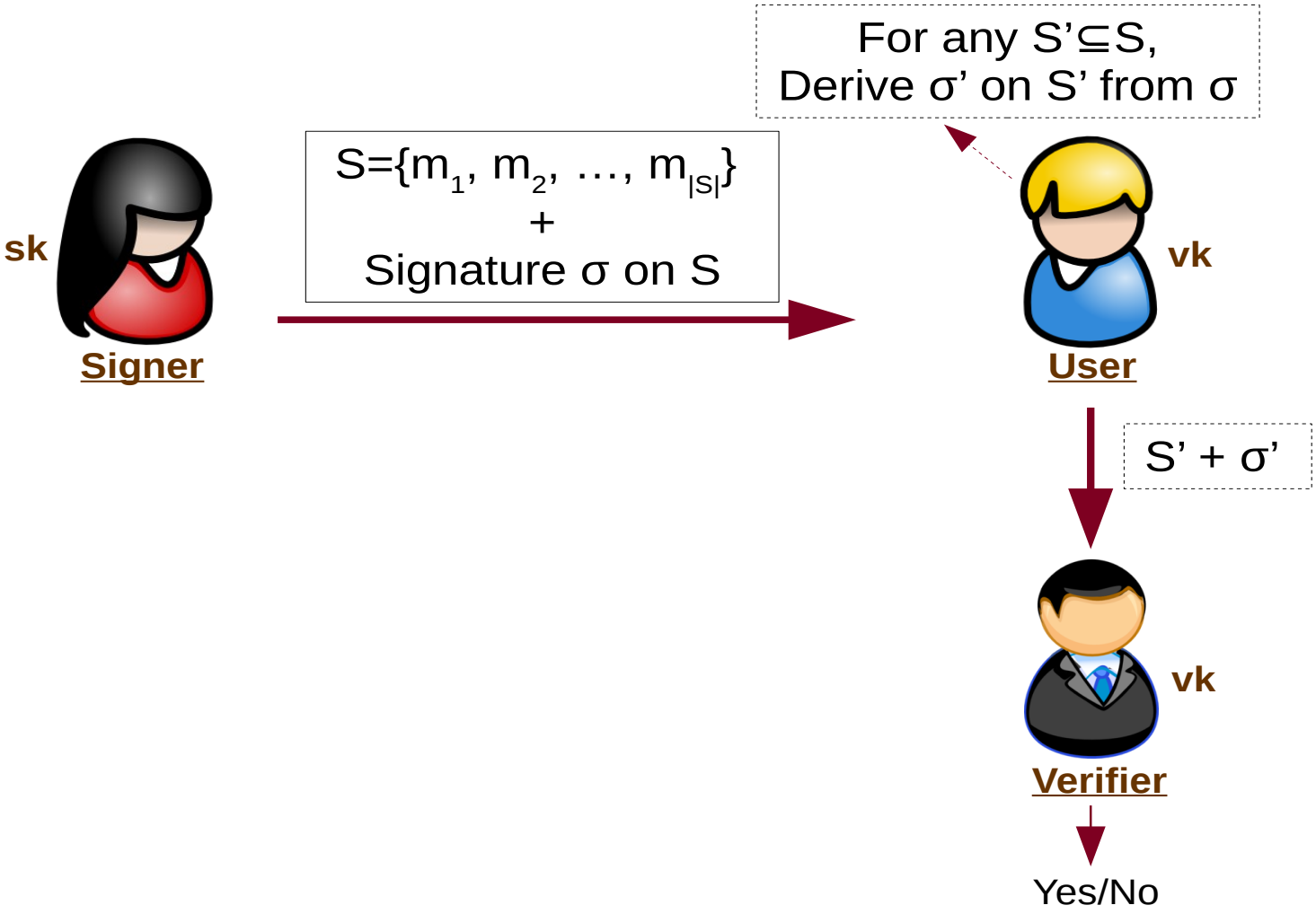
Subset Signatures



Subset Signatures

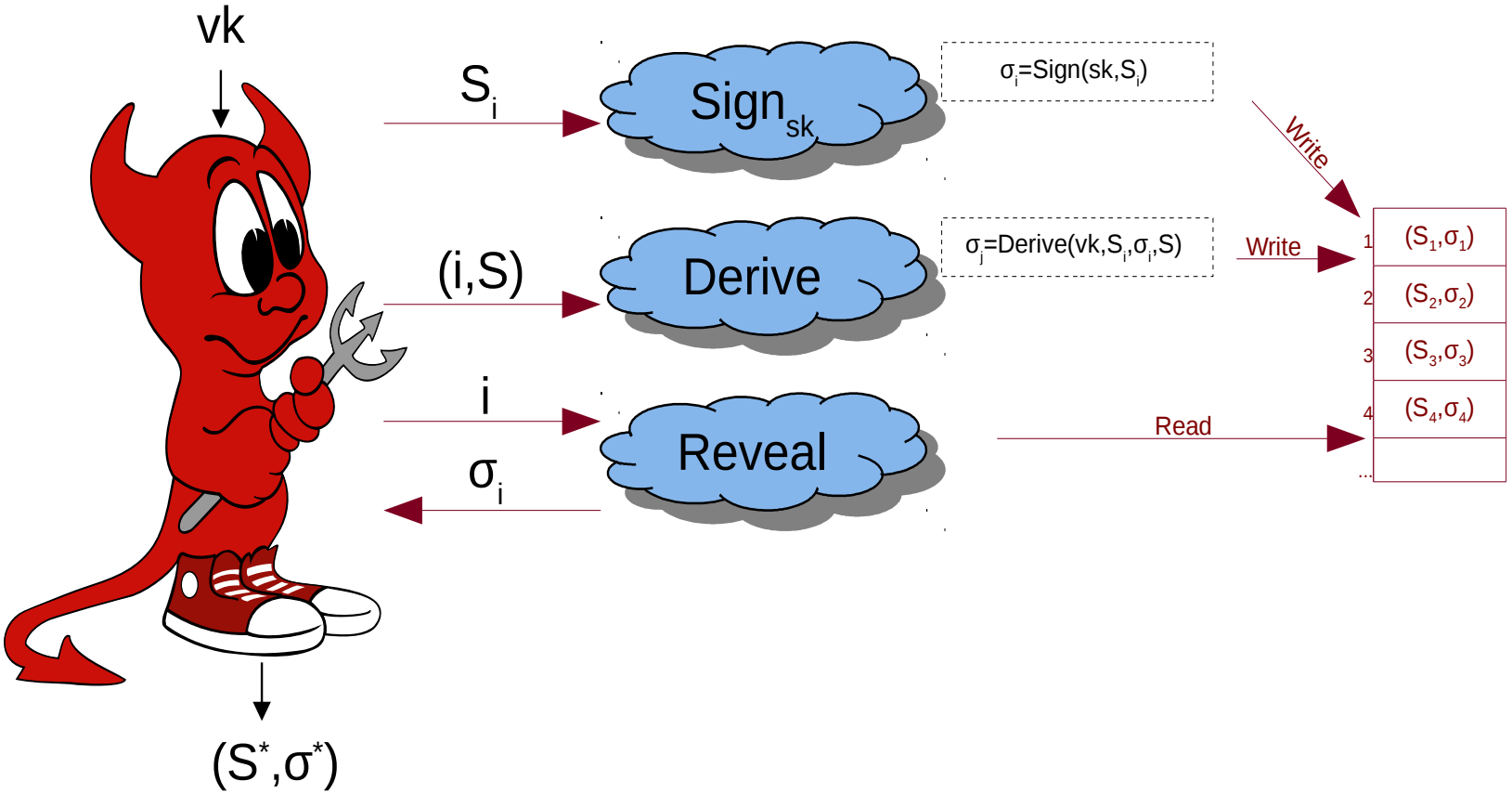


Subset Signatures

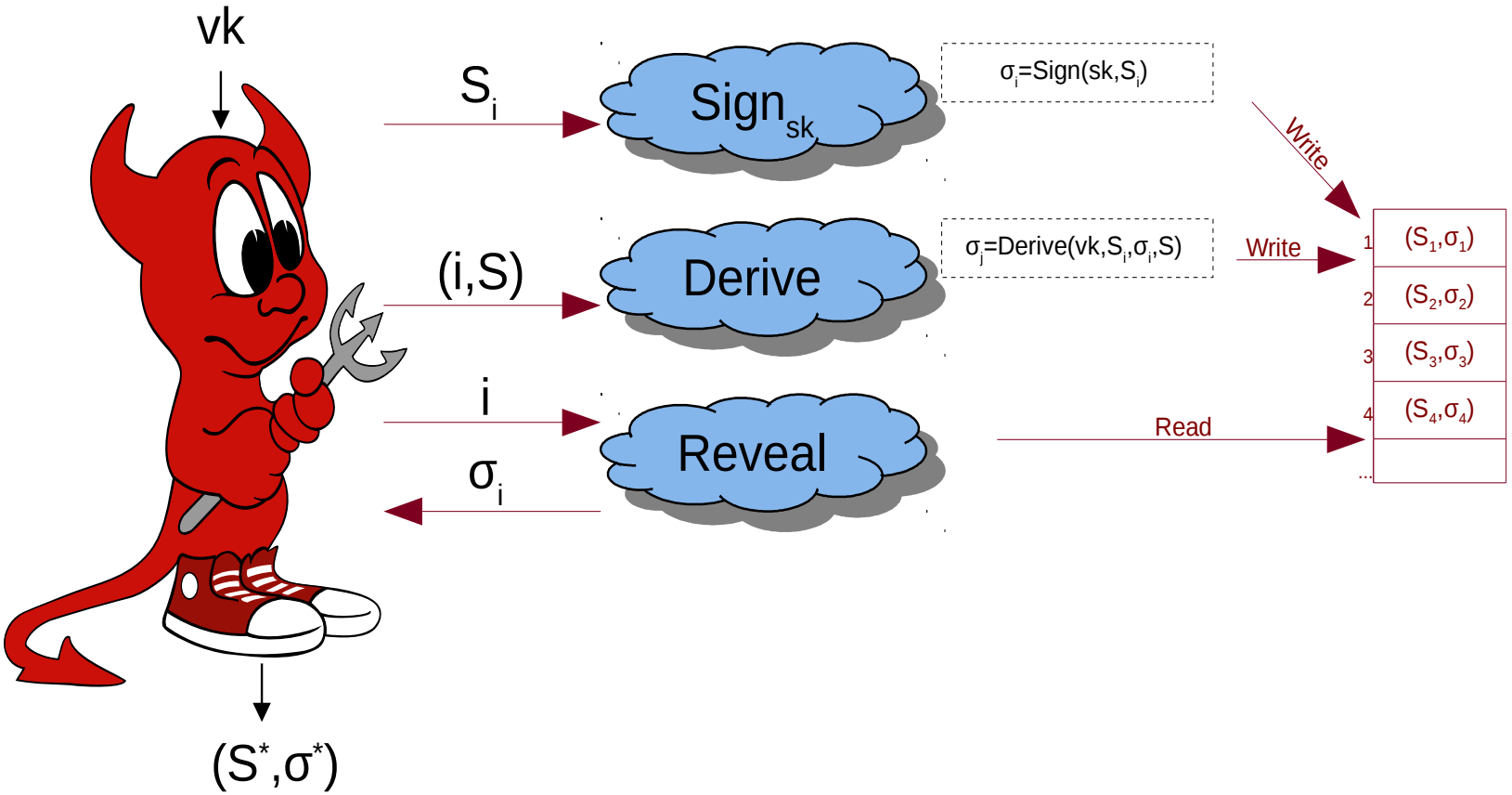


Unforgeability [Ahn et al. 2012]: Adversary cannot output a signature on a new set that is not a subset of any revealed signed set

Unforgeability [Ahn et al. 2012]: Adversary cannot output a signature on a new set that is not a subset of any revealed signed set



Unforgeability [Ahn et al. 2012]: Adversary cannot output a signature on a new set that is not a subset of any revealed signed set



- Adversary wins if σ^* is valid on S^* & she did not see a signature on any S s.t. $S^* \subseteq S$

Context-Hiding: Derived signatures are indistinguishable from fresh signatures on the same set

Different variants: (Strong) Adaptive Context-Hiding [Ahn et al. 2012, Attrapadung et al. 2012] & Complete Context-Hiding [Attrapadung et al. 2012].

Complete Context-Hiding:

$$\left\{\left(\mathsf{sk}, \mathsf{Sign}(\mathsf{sk}, S')\right)\right\}_{\{\mathsf{sk},S,S'\}} \approx_{\text{Statistically}} \left\{\left(\mathsf{sk}, \mathsf{Derive}(\mathsf{vk}, S, \sigma, S')\right)\right\}_{\{\mathsf{sk},S,S'\}}$$

Context-Hiding: Derived signatures are indistinguishable from fresh signatures on the same set

Different variants: (Strong) Adaptive Context-Hiding [Ahn et al. 2012, Attrapadung et al. 2012] & Complete Context-Hiding [Attrapadung et al. 2012].

Complete Context-Hiding:

$$\left\{\left(\mathsf{sk}, \mathsf{Sign}(\mathsf{sk}, S')\right)\right\}_{\{\mathsf{sk},S,S'\}} \approx_{\text{Statistically}} \left\{\left(\mathsf{sk}, \mathsf{Derive}(\mathsf{vk}, S, \sigma, S')\right)\right\}_{\{\mathsf{sk},S,S'\}}$$

Context-Hiding: Derived signatures are indistinguishable from fresh signatures on the same set

Different variants: (Strong) Adaptive Context-Hiding [Ahn et al. 2012, Attrapadung et al. 2012] & Complete Context-Hiding [Attrapadung et al. 2012].

Complete Context-Hiding:

$$\left\{\left(\mathsf{sk}, \mathsf{Sign}(\mathsf{sk}, S')\right)\right\}_{\{\mathsf{sk},S,S'\}} \approx_{\text{Statistically}} \left\{\left(\mathsf{sk}, \mathsf{Derive}(\mathsf{vk}, S, \sigma, S')\right)\right\}_{\{\mathsf{sk},S,S'\}}$$

(Prime-Order) Bilinear Groups

$\mathbb{G}, \tilde{\mathbb{G}}, \mathbb{T}$ are finite cyclic groups of prime order p s.t. $\mathbb{G} = \langle G \rangle$ and $\tilde{\mathbb{G}} = \langle \tilde{G} \rangle$.
$e : \mathbb{G} \times \tilde{\mathbb{G}} \longrightarrow \mathbb{T}$ is efficiently computable satisfying:

- $\forall P \in \mathbb{G}, \forall \tilde{Q} \in \tilde{\mathbb{G}}, \forall x, y \in \mathbb{Z}$: $e(P^x, \tilde{Q}^y) = e(P, \tilde{Q})^{xy}$
- $e(G, \tilde{G}) \neq 1$ generates $\mathbb{T}$

Type-3 [GPS 2008]: $\mathbb{G} \neq \tilde{\mathbb{G}}$ and no efficient homomorphisms
Note: The size of elements of $\tilde{\mathbb{G}}$ is twice that of elements of $\mathbb{G}$

(Prime-Order) Bilinear Groups

$\mathbb{G}, \tilde{\mathbb{G}}, \mathbb{T}$ are finite cyclic groups of prime order p s.t. $\mathbb{G} = \langle G \rangle$ and $\tilde{\mathbb{G}} = \langle \tilde{G} \rangle$.
$e : \mathbb{G} \times \tilde{\mathbb{G}} \longrightarrow \mathbb{T}$ is efficiently computable satisfying:

- $\forall P \in \mathbb{G}, \forall \tilde{Q} \in \tilde{\mathbb{G}}, \forall x, y \in \mathbb{Z}$: $e(P^x, \tilde{Q}^y) = e(P, \tilde{Q})^{xy}$
- $e(G, \tilde{G}) \neq 1$ generates $\mathbb{T}$

Type-3 [GPS 2008]: $\mathbb{G} \neq \tilde{\mathbb{G}}$ and no efficient homomorphisms
Note: The size of elements of $\tilde{\mathbb{G}}$ is twice that of elements of $\mathbb{G}$

(Prime-Order) Bilinear Groups

$\mathbb{G}, \tilde{\mathbb{G}}, \mathbb{T}$ are finite cyclic groups of prime order p s.t. $\mathbb{G} = \langle G \rangle$ and $\tilde{\mathbb{G}} = \langle \tilde{G} \rangle$.
$e : \mathbb{G} \times \tilde{\mathbb{G}} \longrightarrow \mathbb{T}$ is efficiently computable satisfying:

- $\forall P \in \mathbb{G}, \forall \tilde{Q} \in \tilde{\mathbb{G}}, \forall x, y \in \mathbb{Z}$: $e(P^x, \tilde{Q}^y) = e(P, \tilde{Q})^{xy}$
- $e(G, \tilde{G}) \neq 1$ generates $\mathbb{T}$

Type-3 [GPS 2008]: $\mathbb{G} \neq \tilde{\mathbb{G}}$ and no efficient homomorphisms
Note: The size of elements of $\tilde{\mathbb{G}}$ is twice that of elements of $\mathbb{G}$

Existing Constructions of Subset Signatures

- [Ahn et al. 2012]:
  - From Ciphertext-Policy Attribute-Based Encryption (CP-ABE)
- [Attrapadung et al. 2012]:
  - Uses [Abe et al. 2010] Structure-Preserving Signatures + Waters' Signatures + Groth-Sahai Proofs

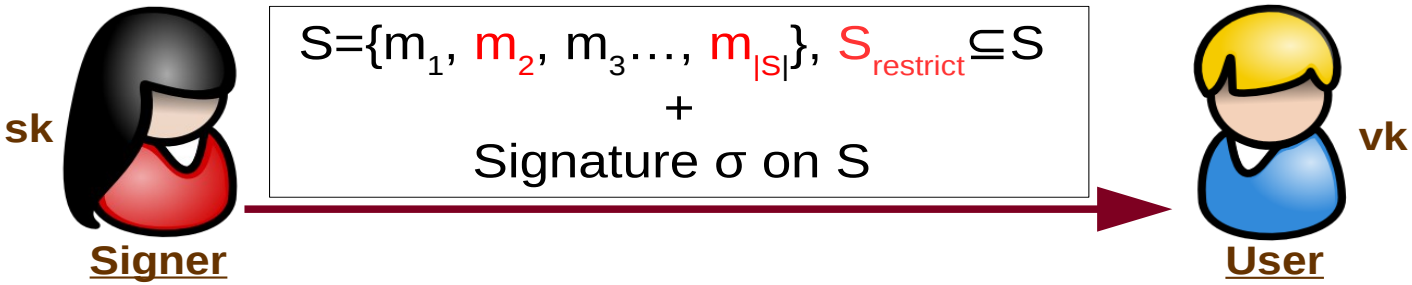
Existing Constructions of Subset Signatures

- [Ahn et al. 2012]:
  - From Ciphertext-Policy Attribute-Based Encryption (CP-ABE)

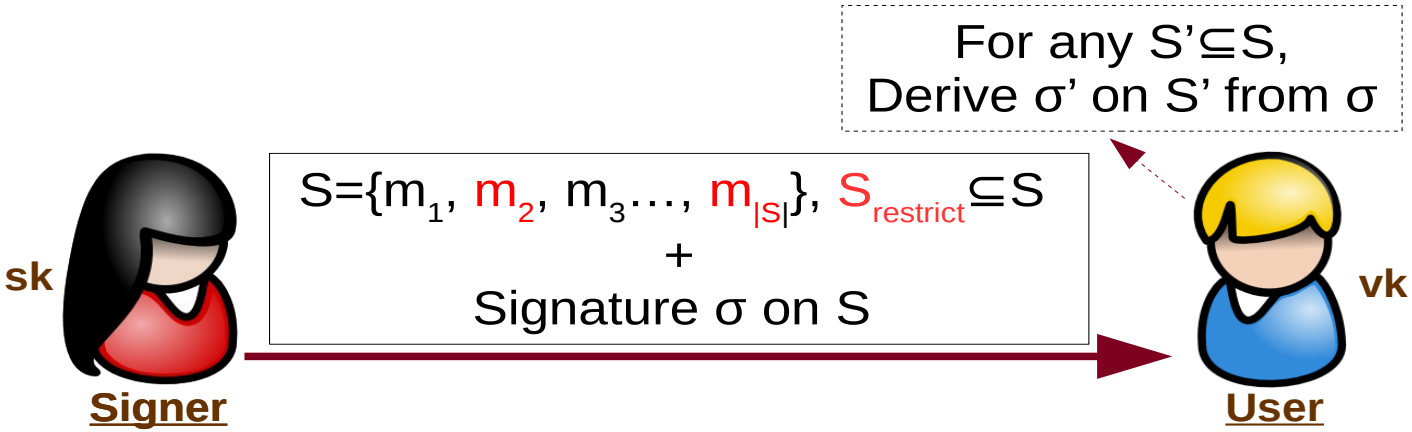
- [Attrapadung et al. 2012]:
  - Uses [Abe et al. 2010] Structure-Preserving Signatures + Waters' Signatures + Groth-Sahai Proofs

Our Contribution

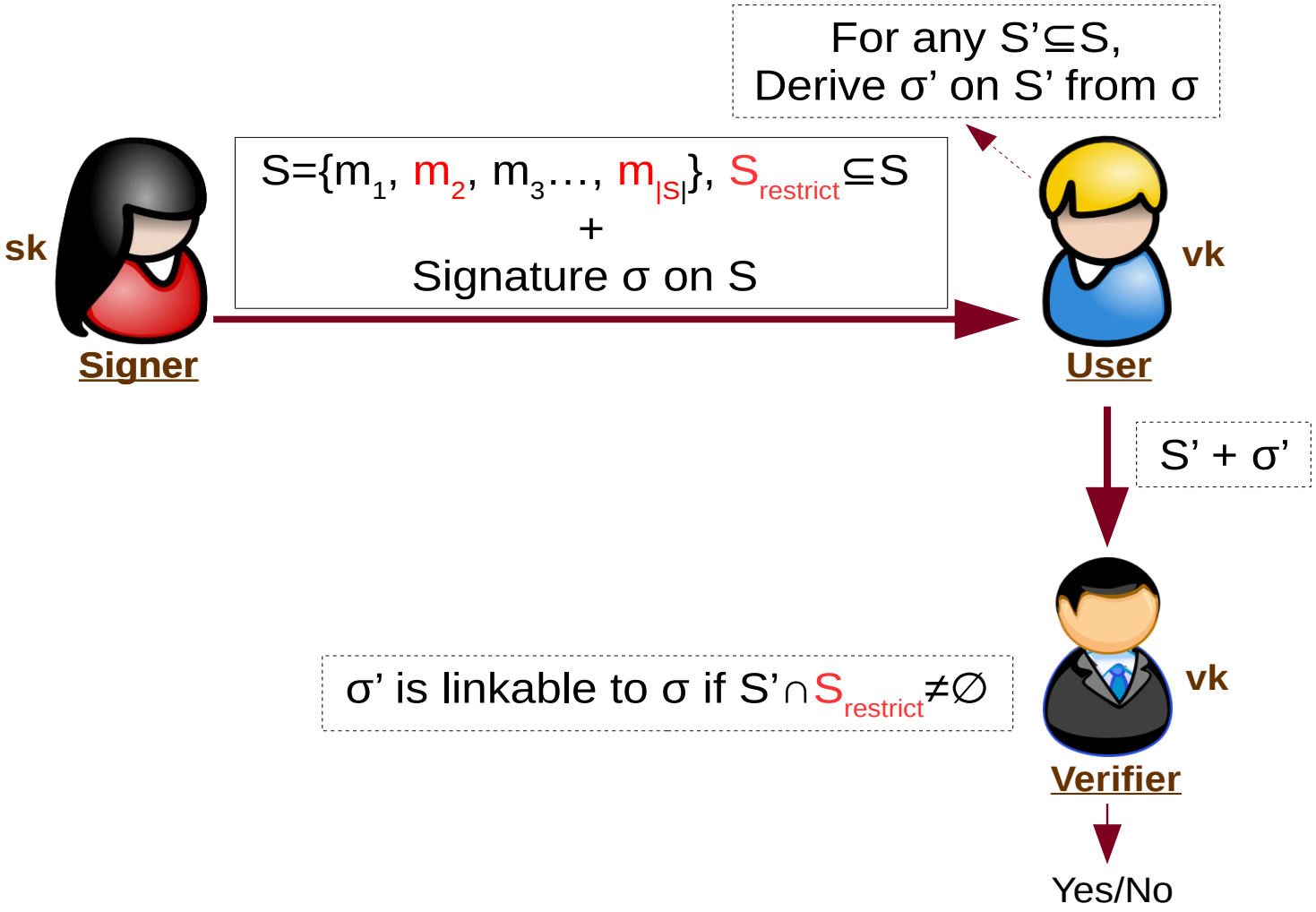
- More efficient constructions of subset signatures
- Adding controllability to the context-hiding property
- Efficient constructions of subset signatures with controlled context-hiding


sk
Signer
S={m1, m2, m3…, m|S|}, Srestrict⊆S
+
Signature σ on S
vk
User

Subset Signatures with controlled context-hiding



Subset Signatures with controlled context-hiding



Building Blocks

- Randomizable Non-Interactive Witness-Indistinguishable Proofs (RNIWI)
  - NIWI Proof System where proofs are publicly re-randomizable

⇒ Instantiation uses the SXDH-based instantiation of Groth-Sahai Proofs

  - The *Hiding setting* ⇒ Perfectly witness-indistinguishable proofs
    ⇒ We get complete context-hiding
  - The *Binding setting* ⇒ Perfectly sound proofs

- Randomizable Non-Interactive Witness-Indistinguishable Proofs (RNIWI)
  - NIWI Proof System where proofs are publicly re-randomizable

⇒ Instantiation uses the SXDH-based instantiation of Groth-Sahai Proofs

- The *Hiding setting* ⇒ Perfectly witness-indistinguishable proofs
  ⇒ We get complete context-hiding

- The *Binding setting* ⇒ Perfectly sound proofs

- Randomizable Non-Interactive Witness-Indistinguishable Proofs (RNIWI)
  - NIWI Proof System where proofs are publicly re-randomizable

⇒ Instantiation uses the SXDH-based instantiation of Groth-Sahai Proofs

- The *Hiding setting* ⇒ Perfectly witness-indistinguishable proofs
  ⇒ We get complete context-hiding
- The *Binding setting* ⇒ Perfectly sound proofs

Building Blocks

- Combined Tagged Signature Scheme (CTS)
  - Signs messages w.r.t. tags
  - 2 modes of signing [Groth 2015]: EUF-CMA and sEUF-CMA

$\Rightarrow$ Instantiation uses an extension of the additively randomizable SPS scheme [Chatterjee & Menezes 2015] to sign vectors of messages and provide combined unforgeability

  - Observation: Scheme combines nicely with Groth-Sahai proofs as can randomize both committed and public components of σ and associated Groth-Sahai proofs

- Combined Tagged Signature Scheme (CTS)
  - Signs messages w.r.t. tags
  - 2 modes of signing [Groth 2015]: EUF-CMA and sEUF-CMA

$\Rightarrow$ Instantiation uses an extension of the additively randomizable SPS scheme [Chatterjee & Menezes 2015] to sign vectors of messages and provide combined unforgeability

- Observation: Scheme combines nicely with Groth-Sahai proofs as can randomize both committed and public components of σ and associated Groth-Sahai proofs

- Combined Tagged Signature Scheme (CTS)
  - Signs messages w.r.t. tags
  - 2 modes of signing [Groth 2015]: EUF-CMA and sEUF-CMA

$\Rightarrow$ Instantiation uses an extension of the additively randomizable SPS scheme [Chatterjee & Menezes 2015] to sign vectors of messages and provide combined unforgeability

- Observation: Scheme combines nicely with Groth-Sahai proofs as can randomize both committed and public components of σ and associated Groth-Sahai proofs

SPS Scheme with Combined Unforgeability

- KeyGen:

  Choose $x_1, \ldots, x_n, y, z \leftarrow \mathbb{Z}_p$

  $\mathsf{sk} := (x_1, \ldots, x_n, y, z)$

  $\mathsf{vk} := (\tilde{X}_1 := \tilde{G}^x, \ldots, \tilde{X}_n := \tilde{G}^{x_n}, \tilde{Y} := \tilde{G}^y, \tilde{Z} := \tilde{G}^z) \in \tilde{\mathbb{G}}^{n+2}$

- Sign: To sign $(M_1, \ldots, M_n) \in \mathbb{G}^n$,
  - Choose $r \leftarrow \mathbb{Z}_p$,

    $\sigma := \left(R := G^r,\ S := \prod_{i=1}^n M_i^{x_i} \cdot G^{r^2+y+zrb},\ \tilde{R} := \tilde{G}^r\right) \in \mathbb{G}^2 \times \tilde{\mathbb{G}}$

    If $b = 0$, we get EUF-CMA, whereas if $b = 1$, we get sEUF-CMA
- Verify: Check that

$$e(G, \tilde{R}) = e(R, \tilde{G})$$

$$e(S, \tilde{G}) = \prod_{i=1}^{n} e(M_i, \tilde{X}_i) e(R, \tilde{R}) e(G, \tilde{Y}) e(R, \tilde{Z}^b)$$

- Randomize: Choose $r' \leftarrow \mathbb{Z}_p$, return

  $\sigma' := \left(R' := R \cdot G^{r'}, \tilde{R}' := \tilde{R} \cdot \tilde{G}^{r'},\ S' := S \cdot R^{2r'} \cdot G^{r'^2}\right)$

SPS Scheme with Combined Unforgeability

- KeyGen:
  Choose $x_1, \ldots, x_n, y, z \leftarrow \mathbb{Z}_p$
  $\mathsf{sk} := (x_1, \ldots, x_n, y, z)$
  $\mathsf{vk} := (\tilde{X}_1 := \tilde{G}^x, \ldots, \tilde{X}_n := \tilde{G}^{x_n}, \tilde{Y} := \tilde{G}^y, \tilde{Z} := \tilde{G}^z) \in \tilde{\mathbb{G}}^{n+2}$

- Sign: To sign $\left(M_1, \ldots, M_n\right) \in \mathbb{G}^n$,
  - Choose $r \leftarrow \mathbb{Z}_p$,
    $\sigma := \left(R := G^r,\ S := \prod_{i=1}^n M_i^{x_i} \cdot G^{r^2+y+zrb},\ \tilde{R} := \tilde{G}^r\right) \in \mathbb{G}^2 \times \tilde{\mathbb{G}}$
    If $b = 0$, we get EUF-CMA, whereas if $b = 1$, we get sEUF-CMA
- Verify: Check that

$$e(G, \tilde{R}) = e(R, \tilde{G})$$

$$e(S, \tilde{G}) = \prod_{i=1}^{n} e(M_i, \tilde{X}_i) e(R, \tilde{R}) e(G, \tilde{Y}) e(R, \tilde{Z}^b)$$

- Randomize: Choose $r' \leftarrow \mathbb{Z}_p$, return
  $\sigma' := \left(R' := R \cdot G^{r'}, \tilde{R}' := \tilde{R} \cdot \tilde{G}^{r'},\ S' := S \cdot R^{2r'} \cdot G^{r'^2}\right)$

SPS Scheme with Combined Unforgeability

- KeyGen:
  Choose $x_1, \ldots, x_n, y, z \leftarrow \mathbb{Z}_p$
  $\mathsf{sk} := (x_1, \ldots, x_n, y, z)$
  $\mathsf{vk} := (\tilde{X}_1 := \tilde{G}^x, \ldots, \tilde{X}_n := \tilde{G}^{x_n}, \tilde{Y} := \tilde{G}^y, \tilde{Z} := \tilde{G}^z) \in \tilde{\mathbb{G}}^{n+2}$

- Sign: To sign $(M_1, \ldots, M_n) \in \mathbb{G}^n$,
  - Choose $r \leftarrow \mathbb{Z}_p$,
    $\sigma := \left(R := G^r,\ S := \prod_{i=1}^n M_i^{x_i} \cdot G^{r^2+y+zrb},\ \tilde{R} := \tilde{G}^r\right) \in \mathbb{G}^2 \times \tilde{\mathbb{G}}$
    If $b = 0$, we get EUF-CMA, whereas if $b = 1$, we get sEUF-CMA

- Verify: Check that

$$e(G, \tilde{R}) = e(R, \tilde{G})$$

$$e(S, \tilde{G}) = \prod_{i=1}^{n} e(M_i, \tilde{X}_i) e(R, \tilde{R}) e(G, \tilde{Y}) e(R, \tilde{Z}^b)$$

- Randomize: Choose $r' \leftarrow \mathbb{Z}_p$, return
  $\sigma' := \left(R' := R \cdot G^{r'}, \tilde{R}' := \tilde{R} \cdot \tilde{G}^{r'},\ S' := S \cdot R^{2r'} \cdot G^{r'^2}\right)$

SPS Scheme with Combined Unforgeability

- KeyGen:
  Choose $x_1, \ldots, x_n, y, z \leftarrow \mathbb{Z}_p$
  $\mathsf{sk} := (x_1, \ldots, x_n, y, z)$
  $\mathsf{vk} := (\tilde{X}_1 := \tilde{G}^x, \ldots, \tilde{X}_n := \tilde{G}^{x_n}, \tilde{Y} := \tilde{G}^y, \tilde{Z} := \tilde{G}^z) \in \tilde{\mathbb{G}}^{n+2}$

- Sign: To sign $(M_1, \ldots, M_n) \in \mathbb{G}^n$,
  - Choose $r \leftarrow \mathbb{Z}_p$,
    $\sigma := \left(R := G^r,\ S := \prod_{i=1}^n M_i^{x_i} \cdot G^{r^2+y+zrb},\ \tilde{R} := \tilde{G}^r\right) \in \mathbb{G}^2 \times \tilde{\mathbb{G}}$
    If $b = 0$, we get EUF-CMA, whereas if $b = 1$, we get sEUF-CMA
- Verify: Check that

$$e(G, \tilde{R}) = e(R, \tilde{G})$$

$$e(S, \tilde{G}) = \prod_{i=1}^{n} e(M_i, \tilde{X}_i) e(R, \tilde{R}) e(G, \tilde{Y}) e(R, \tilde{Z}^b)$$

- Randomize: Choose $r' \leftarrow \mathbb{Z}_p$, return
  $\sigma' := \left(R' := R \cdot G^{r'}, \tilde{R}' := \tilde{R} \cdot \tilde{G}^{r'},\ S' := S \cdot R^{2r'} \cdot G^{r'^2}\right)$

- KeyGen(1^λ):
  - $\mathsf{crs} \leftarrow \mathsf{RNIWI} \cdot \mathsf{Setup}(1^\lambda)$
  - $(\mathsf{sk}, \mathsf{vk}) \leftarrow \mathsf{CTS} \cdot \mathsf{KeyGen}(1^\lambda)$
  - $\mathsf{sk} := \mathsf{sk}_{\mathsf{CTS}}$, $\mathsf{vk} := (\mathsf{crs}, \mathsf{vk}_{\mathsf{CTS}})$

- Sign: To sign $\left(S = \{\vec{m}_1, \ldots, \vec{m}_{|S|}\}, S_{\text{restrict}} \subseteq S\right)$,
  - Choose a random tag τ_S for CTS
  - Use $\mathsf{sk}_{\mathsf{CTS}}$ to sign elements of S w.r.t. τ_S:
    - Mode is sEUF-CMA for elements in S_{restrict}
    - Mode is EUF-CMA for elements in $S \setminus S_{\text{restrict}}$
  - Use RNIWI to prove knowledge of τ_S and the components $\{\hat{\sigma}_i\}_{i=1}^{|S|}$ of $\{\sigma_i\}_{i=1}^{|S|}$ which depend on τ_S
    - Elements $\{\check{\sigma}_i\}_{i=1}^{|S|} := \{\sigma_i\}_{i=1}^{|S|} \setminus \{\hat{\sigma}_i\}_{i=1}^{|S|}$ are part of the statement
  - $\Sigma := \left(\pi_{\text{sig}}, \{\check{\sigma}_i\}_{i=1}^{|S|}\right)$

- $\mathsf{KeyGen}(1^\lambda)$:
  - $\mathsf{crs} \leftarrow \mathsf{RNIWI} \cdot \mathsf{Setup}(1^\lambda)$
  - $(\mathsf{sk}, \mathsf{vk}) \leftarrow \mathsf{CTS} \cdot \mathsf{KeyGen}(1^\lambda)$
  - $\mathsf{sk} := \mathsf{sk}_{\mathsf{CTS}}$, $\mathsf{vk} := (\mathsf{crs}, \mathsf{vk}_{\mathsf{CTS}})$

- Sign: To sign $\left(S = \{\vec{m}_1, \ldots, \vec{m}_{|S|}\}, S_{\text{restrict}} \subseteq S\right)$,
  - Choose a random tag τ_S for CTS
  - Use $\mathsf{sk}_{\mathsf{CTS}}$ to sign elements of S w.r.t. τ_S:
    - Mode is sEUF-CMA for elements in S_{restrict}
    - Mode is EUF-CMA for elements in $S \setminus S_{\text{restrict}}$
  - Use RNIWI to prove knowledge of τ_S and the components $\{\hat{\sigma}_i\}_{i=1}^{|S|}$ of $\{\sigma_i\}_{i=1}^{|S|}$ which depend on τ_S
    - Elements $\{\check{\sigma}_i\}_{i=1}^{|S|} := \{\sigma_i\}_{i=1}^{|S|} \setminus \{\hat{\sigma}_i\}_{i=1}^{|S|}$ are part of the statement
  - $\Sigma := \left(\pi_{\text{sig}}, \{\check{\sigma}_i\}_{i=1}^{|S|}\right)$

- Derive: To derive a signature on $S' \subseteq S$ given (S, Σ) :
  - Remove the commitments and sub-proofs concerning σ_i corresponding to elements $\vec{m}_i \in S \setminus S'$
  - Randomize π_{sig} into π'_{sig}
  - Randomize $\{\check{\sigma}_i\}_{i=1}^{|S'|}$ accordingly
- Verify: To verify $\Sigma = \left(\pi_{\text{sig}}, \{\check{\sigma}_i\}_{i=1}^{|S|}\right)$ on $S = \{\vec{m}_1, \ldots, \vec{m}_{|S|}\}$:
  - Verify π_{sig} and return 0/1 accordingly
- Link: If Σ' on S' was derived from Σ on S where $S' \cap S_{\text{restrict}} \neq \emptyset$, Σ' and Σ will be linkable since signatures on elements of S_{restrict} cannot be re-randomized

Generic Construction

- Derive: To derive a signature on $S' \subseteq S$ given (S, Σ) :
  - Remove the commitments and sub-proofs concerning σ_i corresponding to elements $\vec{m}_i \in S \setminus S'$
  - Randomize π_{sig} into π'_{sig}
  - Randomize $\{\check{\sigma}_i\}_{i=1}^{|S'|}$ accordingly

- Verify: To verify $\Sigma = \left(\pi_{\text{sig}}, \{\check{\sigma}_i\}_{i=1}^{|S|}\right)$ on $S = \{\vec{m}_1, \ldots, \vec{m}_{|S|}\}$:
  - Verify π_{sig} and return 0/1 accordingly

- Link: If Σ' on S' was derived from Σ on S where $S' \cap S_{\text{restrict}} \neq \emptyset$, Σ' and Σ will be linkable since signatures on elements of S_{restrict} cannot be re-randomized

Generic Construction

- Derive: To derive a signature on $S' \subseteq S$ given (S, Σ) :
  - Remove the commitments and sub-proofs concerning σ_i corresponding to elements $\vec{m}_i \in S \setminus S'$
  - Randomize π_{sig} into π'_{sig}
  - Randomize $\{\check{\sigma}_i\}_{i=1}^{|S'|}$ accordingly
- Verify: To verify $\Sigma = \left(\pi_{\text{sig}}, \{\check{\sigma}_i\}_{i=1}^{|S|}\right)$ on $S = \{\vec{m}_1, \ldots, \vec{m}_{|S|}\}$:
  - Verify π_{sig} and return 0/1 accordingly
- Link: If Σ' on S' was derived from Σ on S where $S' \cap S_{\text{restrict}} \neq \emptyset$, Σ' and Σ will be linkable since signatures on elements of S_{restrict} cannot be re-randomized

- **Context-Hiding:**
  Complete Context-Hiding if:
  - RNIWI is perfectly witness-indistinguishable
  - RNIWI is perfectly randomizable
  - CTS is perfectly randomizable

  Or Adaptive Context-Hiding if any of the above hold computationally

- **Unforgeability:**
  - Soundness of RNIWI
  - Combined Existential Unforgeability of CTS

- **Linkability:**
  - Combined Existential Unforgeability of CTS

Security of the Construction

- **Context-Hiding:**
  Complete Context-Hiding if:
  - RNIWI is perfectly witness-indistinguishable
  - RNIWI is perfectly randomizable
  - CTS is perfectly randomizable

  Or Adaptive Context-Hiding if any of the above hold computationally

- **Unforgeability:**
  - Soundness of RNIWI
  - Combined Existential Unforgeability of CTS

- **Linkability:**
  - Combined Existential Unforgeability of CTS

Security of the Construction

- **Context-Hiding:**
  Complete Context-Hiding if:
  - RNIWI is perfectly witness-indistinguishable
  - RNIWI is perfectly randomizable
  - CTS is perfectly randomizable

  Or Adaptive Context-Hiding if any of the above hold computationally

- **Unforgeability:**
  - Soundness of RNIWI
  - Combined Existential Unforgeability of CTS

- **Linkability:**
  - Combined Existential Unforgeability of CTS

Efficiency Comparison of Subset Signatures

Scheme	$\lvert\Sigma\rvert$	$\lvert\mathsf{vk}\rvert$	$\lvert\mathsf{sk}\rvert$	**Assumptions**
[ALP12]	$(22 + 7\lvert S\rvert)\lvert\mathbb{G}\rvert$	$(\lvert\mathcal{M}\rvert + 16)\lvert\mathbb{G}\rvert + 2\lvert\mathbb{T}\rvert$	$6\lvert\mathbb{Z}_p\rvert$	CDH DLIN q-SFP
Ours	$(2 + 3\lvert S\rvert)\lvert\mathbb{G}\rvert + (3\lvert S\rvert)\lvert\tilde{\mathbb{G}}\rvert$	$4\lvert\mathbb{G}\rvert + 7\lvert\tilde{\mathbb{G}}\rvert$	$3\lvert\mathbb{Z}_p\rvert$	SXDH Interactive/GG

Summary

- More efficient schemes than existing subset schemes
- Adding controllability to the context-hiding requirement

Open Problems

- Efficient constructions based on standard static intractability assumptions

Summary

- More efficient schemes than existing subset schemes
- Adding controllability to the context-hiding requirement

Open Problems

- Efficient constructions based on standard static intractability assumptions

The End

☺

?