How Low Can You Go? Short Structure-Preserving Signatures for Diffie-Hellman Vectors

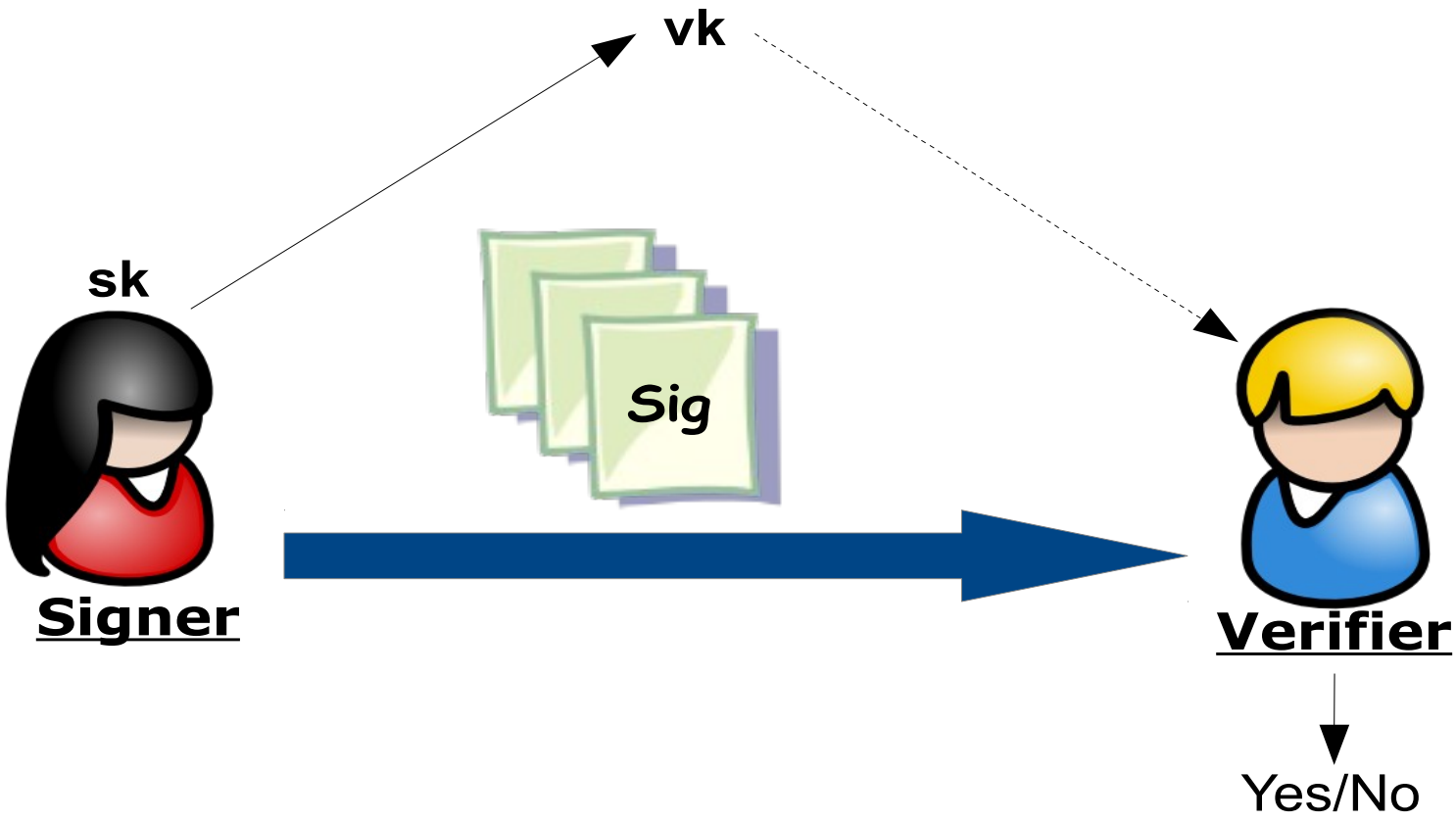
Essam Ghadafi

University of the West of England

IMA International Conference on Cryptography and Coding 2017

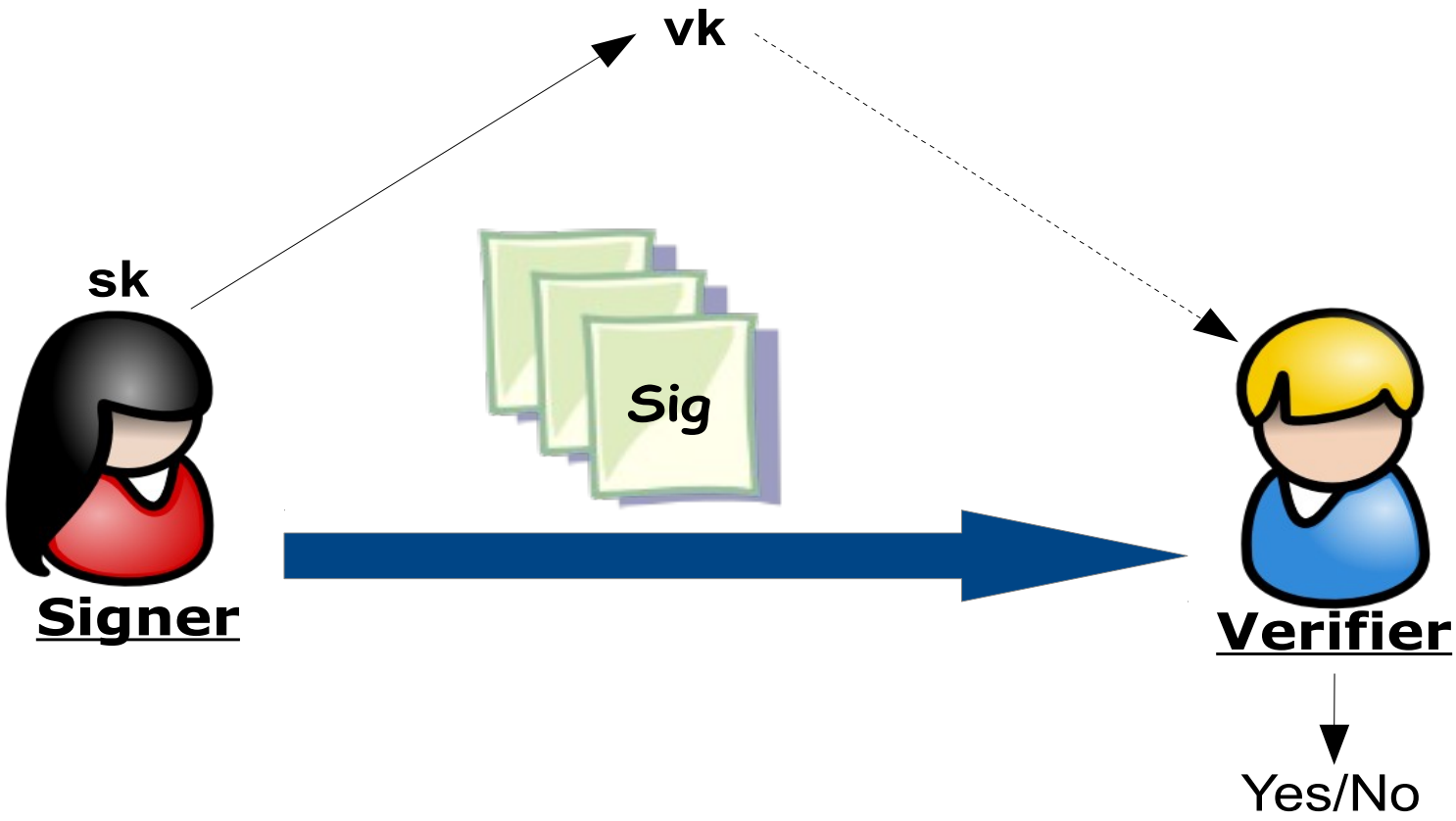
Outline

Digital Signatures



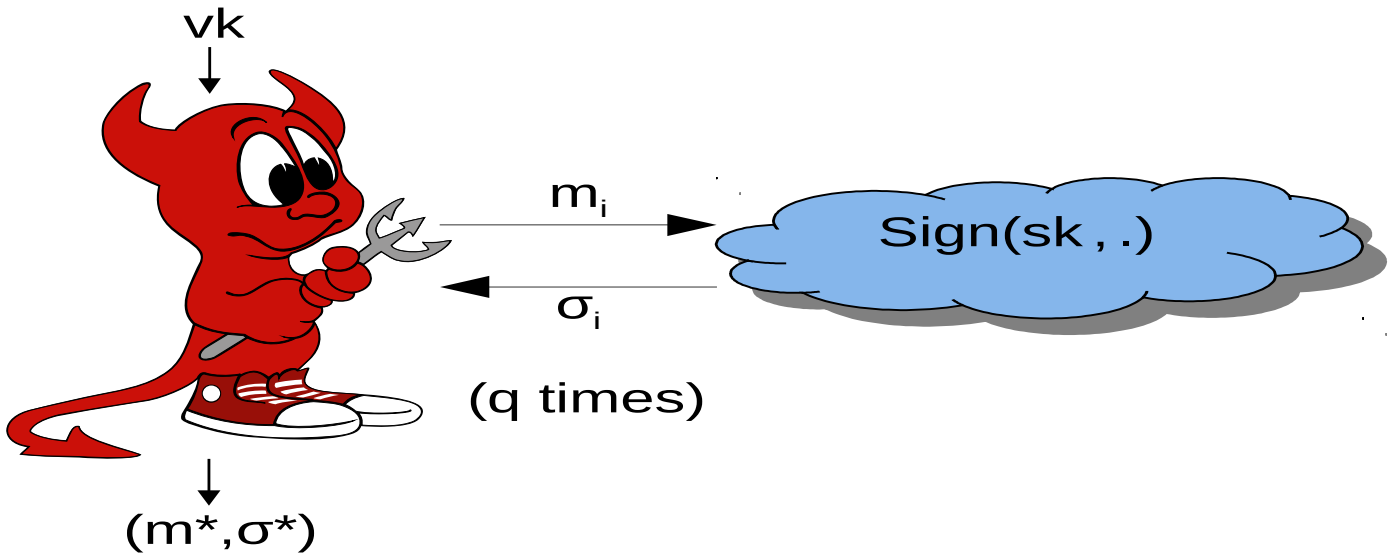
Unforgeabiltiy: You can only sign messages if you have the signing key

Digital Signatures



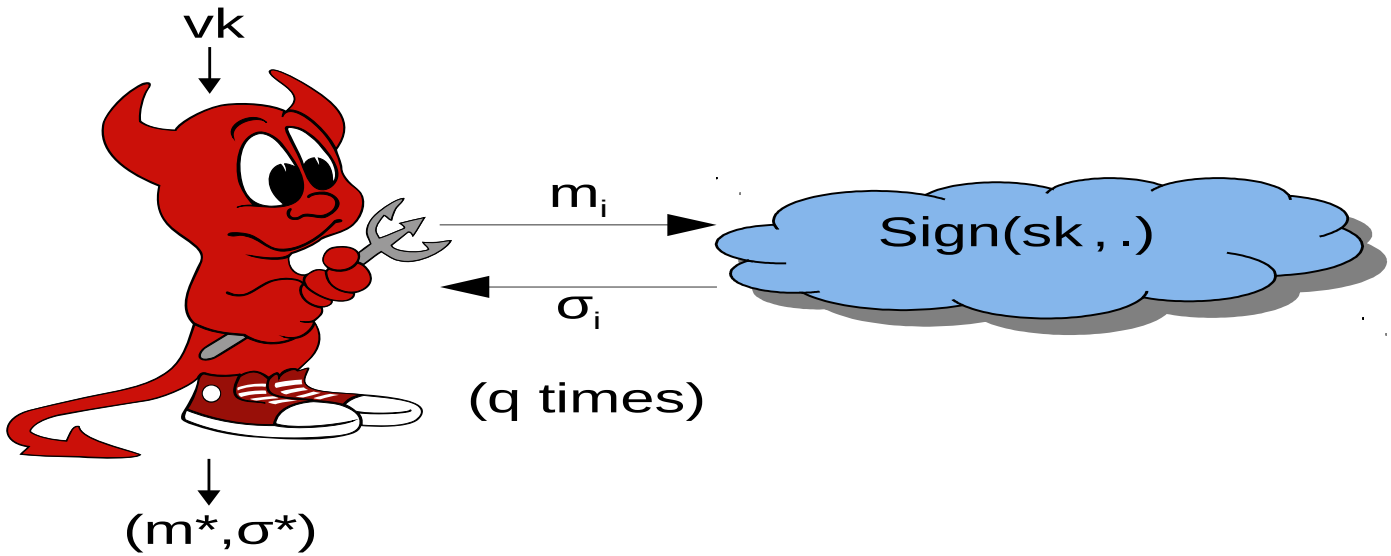
Unforgeabiltiy: You can only sign messages if you have the signing key

Existential Unforgeability



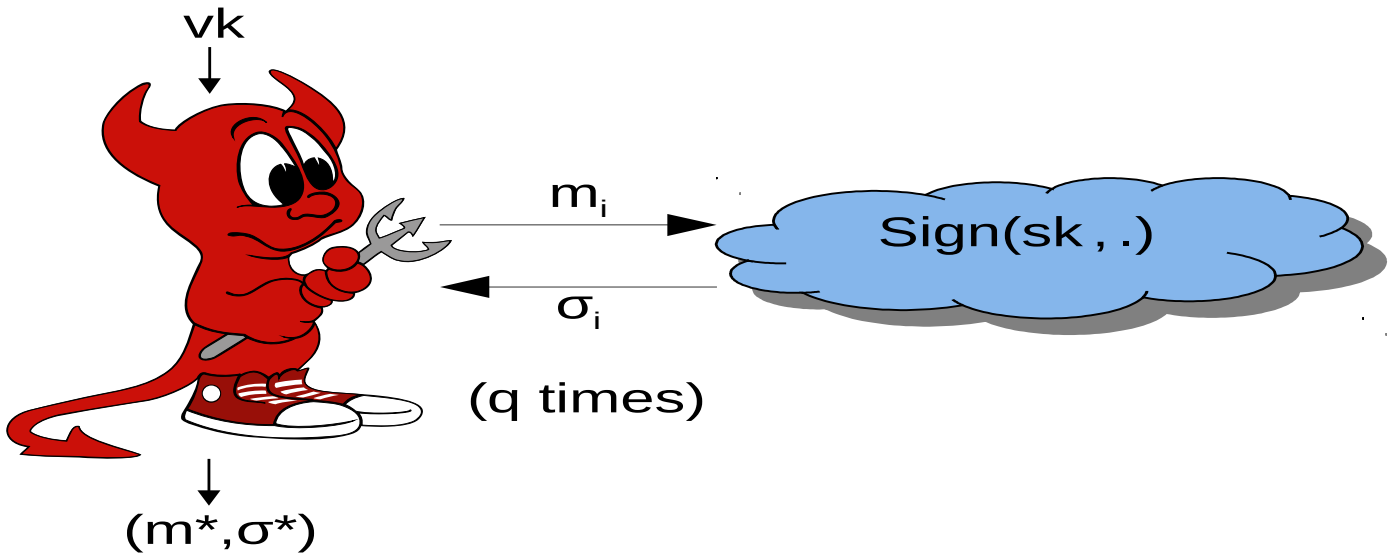
- EUF-CMA: Adversary wins if σ^* is valid on m^* & $m^* \notin \{m_i\}_{i=1}^{q}$
- Strong EUF-CMA (sEUF-CMA): Adversary wins if σ^* is valid on m^* & $(m^*, \sigma^*) \notin \{(m_i, \sigma_i)\}_{i=1}^{q}$

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^* & $(m^*, \sigma^*) \notin \{(m_i, \sigma_i)\}_{i=1}^{q}$

(Prime-Order) Bilinear Groups

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

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

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

Diffie-Hellman (DH) Pairs [Abe et al. 2010]:

- The set $\widehat{\mathbb{GH}} = \{(M, \tilde{N}) | (M, \tilde{N}) \in \mathbb{G} \times \mathbb{H}, e(M, \tilde{H}) = e(G, \tilde{N})\}$

(Prime-Order) Bilinear Groups

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

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

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

Diffie-Hellman (DH) Pairs [Abe et al. 2010]:

- The set $\widehat{\mathbb{GH}} = \{(M, \tilde{N}) | (M, \tilde{N}) \in \mathbb{G} \times \mathbb{H}, e(M, \tilde{H}) = e(G, \tilde{N})\}$

(Prime-Order) Bilinear Groups

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

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

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

Diffie-Hellman (DH) Pairs [Abe et al. 2010]:

- The set $\widehat{\mathbb{GH}} = \{(M, \tilde{N}) | (M, \tilde{N}) \in \mathbb{G} \times \mathbb{H}, e(M, \tilde{H}) = e(G, \tilde{N})\}$

(Prime-Order) Bilinear Groups

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

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

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

Diffie-Hellman (DH) Pairs [Abe et al. 2010]:

- The set $\widehat{\mathbb{GH}} = \{(M, \tilde{N}) | (M, \tilde{N}) \in \mathbb{G} \times \mathbb{H}, e(M, \tilde{H}) = e(G, \tilde{N})\}$

Structure-Preserving Cryptography (SPC)

- Works over bilinear groups
  - $\Rightarrow$ Communication consists of elements from $\mathbb{G}$ and $\mathbb{H}$
- Uses generic group operations (Group operation, membership testing, pairing)
- Preserves the structure of elements
  - $\Rightarrow$ No hashing

Why SPC?

Allow modular design of protocols

- Structure-preserving blocks are easy to combine

Structure-Preserving Cryptography (SPC)

- Works over bilinear groups
  - $\Rightarrow$ Communication consists of elements from $\mathbb{G}$ and $\mathbb{H}$
- Uses generic group operations (Group operation, membership testing, pairing)
- Preserves the structure of elements
  - $\Rightarrow$ No hashing

Why SPC?

Allow modular design of protocols

- Structure-preserving blocks are easy to combine

Structure-Preserving Cryptography (SPC)

- Works over bilinear groups
  - $\Rightarrow$ Communication consists of elements from $\mathbb{G}$ and $\mathbb{H}$
- Uses generic group operations (Group operation, membership testing, pairing)
- Preserves the structure of elements
  - $\Rightarrow$ No hashing

Why SPC?

Allow modular design of protocols

- Structure-preserving blocks are easy to combine

Structure-Preserving Signatures

- m, vk and σ only contain elements from $\mathbb{G}$ and/or $\mathbb{H}$
- Verification requires deciding group membership and evaluating pairing-product equations (PPEs):

$$\prod_i \prod_j e(A_i, \tilde{B}_j)^{c_{i,j}} = Z,$$

where $A_i \in \mathbb{G}$, $\tilde{B}_j \in \mathbb{H}$ and $Z \in \mathbb{T}$ are elements appearing in $\mathcal{P}, m, \mathsf{vk}, \sigma$, whereas $c_{i,j} \in \mathbb{Z}_p$ are constants

- m, vk and σ only contain elements from $\mathbb{G}$ and/or $\mathbb{H}$
- Verification requires deciding group membership and evaluating pairing-product equations (PPEs):

$$\prod_i \prod_j e(A_i, \tilde{B}_j)^{c_{i,j}} = Z,$$

where $A_i \in \mathbb{G}$, $\tilde{B}_j \in \mathbb{H}$ and $Z \in \mathbb{T}$ are elements appearing in $\mathcal{P}, m, \mathsf{vk}, \sigma$, whereas $c_{i,j} \in \mathbb{Z}_p$ are constants

History of Structure-Preserving Signatures

- The term was coined by Abe et al. 2010 but earlier constructions include Groth 2006 and Green & Hohenberger 2008
- Many constructions in the 3 main settings of bilinear groups
- Optimal type-3 constructions are the most efficient

Applications of Structure-Preserving Signatures

- Blind signatures
- Group signatures
- Malleable signatures
- Attribute-based signatures
- Direct anonymous attestation
- Tightly secure encryption schemes
- Anonymous credentials
- Oblivious transfer
- Network coding
- . . .

Current State-of-the-Art

- $|\sigma| = 2|\mathbb{G}| + |\mathbb{H}|$ & 2 PPEs for optimal schemes for unilateral $\vec{m}$ [Abe et al. 2011 & 2014, Chatterjee & Menezes 2015, etc.]
- $|\sigma| = 2|\mathbb{G}|$ & 1 PPE (excl. DH verification cost) for a single DH pair (and $\vec{u} \in \mathbb{Z}_p^k$) [Ghadafi 2017]
  - ☹ Techniques used do not seem to generalize to DH vectors

Can we do better for vectors of group elements?

Current State-of-the-Art

- $|\sigma| = 2|\mathbb{G}| + |\mathbb{H}|$ & 2 PPEs for optimal schemes for unilateral $\vec{m}$ [Abe et al. 2011 & 2014, Chatterjee & Menezes 2015, etc.]

- $|\sigma| = 2|\mathbb{G}|$ & 1 PPE (excl. DH verification cost) for a single DH pair (and $\vec{u} \in \mathbb{Z}_p^k$) [Ghadafi 2017]
  - ☹ Techniques used do not seem to generalize to DH vectors

Can we do better for vectors of group elements?

Current State-of-the-Art

- $|\sigma| = 2|\mathbb{G}| + |\mathbb{H}|$ & 2 PPEs for optimal schemes for unilateral $\vec{m}$ [Abe et al. 2011 & 2014, Chatterjee & Menezes 2015, etc.]

- $|\sigma| = 2|\mathbb{G}|$ & 1 PPE (excl. DH verification cost) for a single DH pair (and $\vec{u} \in \mathbb{Z}_p^k$) [Ghadafi 2017]
  - ☹ Techniques used do not seem to generalize to DH vectors

Can we do better for vectors of group elements?

Current State-of-the-Art

- $|\sigma| = 2|\mathbb{G}| + |\mathbb{H}|$ & 2 PPEs for optimal schemes for unilateral $\vec{m}$ [Abe et al. 2011 & 2014, Chatterjee & Menezes 2015, etc.]

- $|\sigma| = 2|\mathbb{G}|$ & 1 PPE (excl. DH verification cost) for a single DH pair (and $\vec{u} \in \mathbb{Z}_p^k$) [Ghadafi 2017]
  - ☹ Techniques used do not seem to generalize to DH vectors

Can we do better for vectors of group elements?

Our Contribution

- 2 Type-3 EUF-CMA Schemes
  - $|\sigma| = |\mathbb{G}| + |\mathbb{H}|$ & 1 PPE (excl. DH verification cost)
  - Message space is a vector of DH pairs

- Type-3 EUF-CMA Scheme
  - $|\sigma| = 3|\mathbb{G}|$ & 1 PPE (excl. DH verification cost)
  - Message space is 2 DH pairs

Observation

To get *Unilateral Structure-Preserving Signatures on a DH Pair (USPSDH) where* $|\sigma| = 2|\mathbb{G}|$, [Ghadafi 2017] approach was:

- Unilateral σ & vk
  - Use $\frac{r}{y}$ in the exponent of a component of σ depending on m and the other component of σ is G^r.
- m is a DH pair
- Prevent forgeries of the form $r = 0$

Does not work for a vector of group elements ☹

Observation

To get *Unilateral Structure-Preserving Signatures on a DH Pair (USPSDH) where* $|\sigma| = 2|\mathbb{G}|$, [Ghadafi 2017] approach was:

- Unilateral σ & vk
  - Use $\frac{r}{y}$ in the exponent of a component of σ depending on m and the other component of σ is G^r.
- m is a DH pair
- Prevent forgeries of the form $r = 0$

Does not work for a vector of group elements ☹

Our Approach

- Transpose one of σ components to the apposite group
- Instead of $\frac{r}{y}$ use $\frac{1}{r}$ in the exponent of the $\vec{m}$-dependent component of σ
  - This allows to "commit" to messages in σ as $\prod_{i=1}^{\ell} M_i^{x_i}$ . . . where $x_i \in \mathsf{sk}$
- Messages are still DH pairs

SCHEME I

- KeyGen:
  Choose $x_1, \ldots, x_\ell, y \leftarrow \mathbb{Z}_p$
  $\mathsf{sk} := (x_1, \ldots, x_\ell, y)$
  $\mathsf{vk} := (X_1 := G^x, \ldots, X_\ell := G^{x_\ell}, \tilde{Y} := \tilde{H}^y) \in \mathbb{G}^\ell \times \mathbb{H}$

- Sign: To sign $\left((M, \tilde{N})_1, \ldots, (M, \tilde{N})_\ell\right) \in \widehat{\mathbb{G}\mathbb{H}}^\ell$,
  - Choose $r \leftarrow \mathbb{Z}_p^\times$,

$$\sigma := \left(R := G^r,\ \tilde{S} := \left(\prod_{i=1}^{\ell} \tilde{N}_i^{x_i} \cdot \tilde{Y}^{x_1} \cdot \tilde{H}\right)^{\frac{1}{r}}\right) \in \mathbb{G} \times \mathbb{H}$$

- Verify: Check that $(M, \tilde{N})_i \in \widehat{\mathbb{G}\mathbb{H}}$ and

$$e(R, \tilde{S}) = \prod_{i=1}^{\ell} e(X_i, \tilde{N}_i) e(X_1, \tilde{Y}) e(G, \tilde{H})$$

- Randomize: Choose $r' \leftarrow \mathbb{Z}_p^\times$, return $\sigma' := \left(R' := R^{r'},\ S' := S^{\frac{1}{r'}}\right)$

SCHEME I

- KeyGen:
  Choose $x_1, \ldots, x_\ell, y \leftarrow \mathbb{Z}_p$
  $\mathsf{sk} := (x_1, \ldots, x_\ell, y)$
  $\mathsf{vk} := (X_1 := G^x, \ldots, X_\ell := G^{x_\ell}, \tilde{Y} := \tilde{H}^y) \in \mathbb{G}^\ell \times \mathbb{H}$

- Sign: To sign $\left((M, \tilde{N})_1, \ldots, (M, \tilde{N})_\ell\right) \in \widehat{\mathbb{GH}}^\ell$,
  - Choose $r \leftarrow \mathbb{Z}_p^\times$,
    $\sigma := \left(R := G^r,\ \tilde{S} := \left(\prod_{i=1}^{\ell} \tilde{N}_i^{x_i} \cdot \tilde{Y}^{x_1} \cdot \tilde{H}\right)^{\frac{1}{r}}\right) \in \mathbb{G} \times \mathbb{H}$

- Verify: Check that $(M, \tilde{N})_i \in \widehat{\mathbb{GH}}$ and

$$e(R, \tilde{S}) = \prod_{i=1}^{\ell} e(X_i, \tilde{N}_i) e(X_1, \tilde{Y}) e(G, \tilde{H})$$

- Randomize: Choose $r' \leftarrow \mathbb{Z}_p^\times$, return $\sigma' := \left(R' := R^{r'},\ S' := S^{\frac{1}{r'}}\right)$

SCHEME I

- KeyGen:
  Choose $x_1, \ldots, x_\ell, y \leftarrow \mathbb{Z}_p$
  $\mathsf{sk} := (x_1, \ldots, x_\ell, y)$
  $\mathsf{vk} := (X_1 := G^x, \ldots, X_\ell := G^{x_\ell}, \tilde{Y} := \tilde{H}^y) \in \mathbb{G}^\ell \times \mathbb{H}$

- Sign: To sign $\left((M, \tilde{N})_1, \ldots, (M, \tilde{N})_\ell\right) \in \widehat{\mathbb{GH}}^\ell$,
  - Choose $r \leftarrow \mathbb{Z}_p^\times$,
    $\sigma := \left(R := G^r,\ \tilde{S} := \left(\prod_{i=1}^{\ell} \tilde{N}_i^{x_i} \cdot \tilde{Y}^{x_1} \cdot \tilde{H}\right)^{\frac{1}{r}}\right) \in \mathbb{G} \times \mathbb{H}$

- Verify: Check that $(M, \tilde{N})_i \in \widehat{\mathbb{GH}}$ and

$$e(R, \tilde{S}) = \prod_{i=1}^{\ell} e(X_i, \tilde{N}_i) e(X_1, \tilde{Y}) e(G, \tilde{H})$$

- Randomize: Choose $r' \leftarrow \mathbb{Z}_p^\times$, return $\sigma' := \left(R' := R^{r'},\ S' := S^{\frac{1}{r'}}\right)$

SCHEME I

- KeyGen:
  Choose $x_1, \ldots, x_\ell, y \leftarrow \mathbb{Z}_p$
  $\mathsf{sk} := (x_1, \ldots, x_\ell, y)$
  $\mathsf{vk} := (X_1 := G^x, \ldots, X_\ell := G^{x_\ell}, \tilde{Y} := \tilde{H}^y) \in \mathbb{G}^\ell \times \mathbb{H}$

- Sign: To sign $\left((M, \tilde{N})_1, \ldots, (M, \tilde{N})_\ell\right) \in \widehat{\mathbb{GH}}^\ell$,
  - Choose $r \leftarrow \mathbb{Z}_p^\times$,
    $$\sigma := \left(R := G^r,\ \tilde{S} := \left(\prod_{i=1}^{\ell} \tilde{N}_i^{x_i} \cdot \tilde{Y}^{x_1} \cdot \tilde{H}\right)^{\frac{1}{r}}\right) \in \mathbb{G} \times \mathbb{H}$$

- Verify: Check that $(M, \tilde{N})_i \in \widehat{\mathbb{GH}}$ and
  $$e(R, \tilde{S}) = \prod_{i=1}^{\ell} e(X_i, \tilde{N}_i) e(X_1, \tilde{Y}) e(G, \tilde{H})$$

- Randomize: Choose $r' \leftarrow \mathbb{Z}_p^\times$, return $\sigma' := \left(R' := R^{r'},\ S' := S^{\frac{1}{r'}}\right)$

Properties of Scheme I

- The scheme is secure in the generic group model
  - $\Rightarrow$ alternatively can be based on an interactive assumption
- Only $\tilde{N}$ part of the message is needed for signing
- σ' is perfectly indistinguishable from a fresh signature on the same message vector

Properties of Scheme I

- The scheme is secure in the generic group model
  - $\Rightarrow$ alternatively can be based on an interactive assumption
- Only $\tilde{N}$ part of the message is needed for signing
- σ' is perfectly indistinguishable from a fresh signature on the same message vector

Properties of Scheme I

- The scheme is secure in the generic group model
  - $\Rightarrow$ alternatively can be based on an interactive assumption
- Only $\tilde{N}$ part of the message is needed for signing
- σ' is perfectly indistinguishable from a fresh signature on the same message vector

SCHEME II

- KeyGen: Same as Scheme I
- Sign: To sign $\left((M,\tilde{N})_1,\ldots,(M,\tilde{N})_\ell\right) \in \widehat{\mathbb{GH}}^\ell$,
  - Choose $r \leftarrow \mathbb{Z}_p^\times$, $\sigma := \left(\tilde{R} := \tilde{H}^r,\ S := \left(\prod_{i=1}^{\ell} M_i^{x_i} \cdot X_1^y \cdot G\right)^{\frac{1}{r}}\right) \in \mathbb{H} \times \mathbb{G}$
- Verify: Same as Scheme I
- Randomize: Same as Scheme I

SCHEME II

- KeyGen: Same as Scheme I
- Sign: To sign $\left((M,\tilde{N})_1,\ldots,(M,\tilde{N})_\ell\right) \in \widehat{\mathbb{GH}}^\ell$,
  - Choose $r \leftarrow \mathbb{Z}_p^\times$, $\sigma := \left(\tilde{R} := \tilde{H}^r,\ S := \left(\prod_{i=1}^{\ell} M_i^{x_i} \cdot X_1^y \cdot G\right)^{\frac{1}{r}}\right) \in \mathbb{H} \times \mathbb{G}$
- Verify: Same as Scheme I
- Randomize: Same as Scheme I

SCHEME II

- KeyGen: Same as Scheme I
- Sign: To sign $\left((M,\tilde{N})_1,\ldots,(M,\tilde{N})_\ell\right) \in \widehat{\mathbb{GH}}^\ell$,
  - Choose $r \leftarrow \mathbb{Z}_p^\times$, $\sigma := \left(\tilde{R} := \tilde{H}^r,\ S := \left(\prod_{i=1}^{\ell} M_i^{x_i} \cdot X_1^y \cdot G\right)^{\frac{1}{r}}\right) \in \mathbb{H} \times \mathbb{G}$
- Verify: Same as Scheme I
- Randomize: Same as Scheme I

SCHEME II

- KeyGen: Same as Scheme I
- Sign: To sign $\left((M,\tilde{N})_1,\ldots,(M,\tilde{N})_\ell\right) \in \widehat{\mathbb{GH}}^\ell$,
  - Choose $r \leftarrow \mathbb{Z}_p^\times$, $\sigma := \left(\tilde{R} := \tilde{H}^r,\ S := \left(\prod_{i=1}^{\ell} M_i^{x_i} \cdot X_1^y \cdot G\right)^{\frac{1}{r}}\right) \in \mathbb{H} \times \mathbb{G}$
- Verify: Same as Scheme I
- Randomize: Same as Scheme I

Properties of Scheme II

- The scheme is secure in the generic group model
  - $\Rightarrow$ alternatively can be based on an interactive assumption
- Only M part of the message is needed for signing
- σ' is perfectly indistinguishable from a fresh signature on the same message vector

Properties of Scheme II

- The scheme is secure in the generic group model
  - $\Rightarrow$ alternatively can be based on an interactive assumption
- Only M part of the message is needed for signing
- σ' is perfectly indistinguishable from a fresh signature on the same message vector

Properties of Scheme II

- The scheme is secure in the generic group model
  - $\Rightarrow$ alternatively can be based on an interactive assumption
- Only M part of the message is needed for signing
- σ' is perfectly indistinguishable from a fresh signature on the same message vector

Efficiency Comparison

Work	σ		$\mathsf{vk}+\mathcal{P}$		$\mathcal{M}$	Randomize	Verifying n Signatures on $\vec{m}$	
	$\mathbb{G}$	$\mathbb{H}$	$\mathbb{G}$	$\mathbb{H}$			PPE	Pairing
[AFGHO10] I	5	2	$8+2\ell$	4	$\mathbb{G}^{\ell}$	Partially	$2n$	$6n+2\ell+4^{\dagger}$
[AFGHO10] II	2	5	$8+2\ell$	4	$\mathbb{H}^{\ell}$	Partially	$2n$	$6n+2\ell+4^{\dagger}$
[AGHO11]	2	1	ℓ	1	$\mathbb{H}^{\ell}$	Yes	$2n$	$3n+\ell+1^{\dagger}$
[Gro15] I	1	2	ℓ	1	$\mathbb{H}^{\ell}$	Yes	$2n$	$2n+\ell+3^{\dagger}$
[Gro15] II	1	2	ℓ	1	$\mathbb{H}^{\ell}$	No	$2n$	$3n+\ell+3^{\dagger}$
Ours I	1	1	ℓ	1	$\widehat{\mathbb{GH}}^{\ell}$	Yes	$n+\ell^{*}$ $n+1^{*}$	$n+\ell+1^{\dagger}+2\ell^{*}$ $n+\ell+1^{\dagger}+2^{*}$
Ours II	1	1	ℓ	1	$\widehat{\mathbb{GH}}^{\ell}$	Yes	$n+\ell^{*}$ $n+1^{*}$	$n+\ell+1^{\dagger}+2\ell^{*}$ $n+\ell+1^{\dagger}+2^{*}$

$*$: Cost for verifying DH

$\dagger$: Can be precomputed

SCHEME III

- KeyGen:
  Choose $x_1, x_2, y \leftarrow \mathbb{Z}_p$
  $\mathsf{sk} := (x_1, x_2, y)$
  $\mathsf{vk} := (\tilde{X}_1 := \tilde{H}^{x_1}, \tilde{X}_2 := \tilde{H}^{x_2}, \tilde{Y} := \tilde{H}^{y}) \in \mathbb{H}^3$

- Sign: To sign $\left((M, \tilde{N})_1, (M, \tilde{N})_2\right) \in \widehat{\mathbb{GH}}^2$,
  - Choose $r_1, r_2 \leftarrow \mathbb{Z}_p$,
    $\sigma := \left(R_1 := G^{r_1}, R_2 := G^{r_2}, \tilde{S} := \left(G^{x_1} \cdot M_1\right)^{\frac{r_1}{y}} \cdot \left(G^{x_2} \cdot M_2\right)^{\frac{r_2}{y}}\right) \in \mathbb{G}^3$

- Verify: Check that $(M, \tilde{N})_i \in \widehat{\mathbb{GH}}$ and

$$e(S, \tilde{Y}) = e(R_1, \tilde{X}_1 \cdot \tilde{N}_1) e(R_2, \tilde{X}_2 \cdot \tilde{N}_2)$$

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

SCHEME III

- KeyGen:
  Choose $x_1, x_2, y \leftarrow \mathbb{Z}_p$
  $\mathsf{sk} := (x_1, x_2, y)$
  $\mathsf{vk} := (\tilde{X}_1 := \tilde{H}^{x_1}, \tilde{X}_2 := \tilde{H}^{x_2}, \tilde{Y} := \tilde{H}^{y}) \in \mathbb{H}^3$

- Sign: To sign $\left((M, \tilde{N})_1, (M, \tilde{N})_2\right) \in \widehat{\mathbb{GH}}^2$,
  - Choose $r_1, r_2 \leftarrow \mathbb{Z}_p$,
    $\sigma := \left(R_1 := G^{r_1}, R_2 := G^{r_2}, \tilde{S} := \left(G^{x_1} \cdot M_1\right)^{\frac{r_1}{y}} \cdot \left(G^{x_2} \cdot M_2\right)^{\frac{r_2}{y}}\right) \in \mathbb{G}^3$

- Verify: Check that $(M, \tilde{N})_i \in \widehat{\mathbb{GH}}$ and

$$e(S, \tilde{Y}) = e(R_1, \tilde{X}_1 \cdot \tilde{N}_1) e(R_2, \tilde{X}_2 \cdot \tilde{N}_2)$$

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

SCHEME III

- KeyGen:
  Choose $x_1, x_2, y \leftarrow \mathbb{Z}_p$
  $\mathsf{sk} := (x_1, x_2, y)$
  $\mathsf{vk} := (\tilde{X}_1 := \tilde{H}^{x_1}, \tilde{X}_2 := \tilde{H}^{x_2}, \tilde{Y} := \tilde{H}^{y}) \in \mathbb{H}^3$

- Sign: To sign $\left((M, \tilde{N})_1, (M, \tilde{N})_2\right) \in \widehat{\mathbb{GH}}^2$,
  - Choose $r_1, r_2 \leftarrow \mathbb{Z}_p$,
    $\sigma := \left(R_1 := G^{r_1}, R_2 := G^{r_2}, \tilde{S} := \left(G^{x_1} \cdot M_1\right)^{\frac{r_1}{y}} \cdot \left(G^{x_2} \cdot M_2\right)^{\frac{r_2}{y}}\right) \in \mathbb{G}^3$

- Verify: Check that $(M, \tilde{N})_i \in \widehat{\mathbb{GH}}$ and

$$e(S, \tilde{Y}) = e(R_1, \tilde{X}_1 \cdot \tilde{N}_1) e(R_2, \tilde{X}_2 \cdot \tilde{N}_2)$$

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

SCHEME III

- KeyGen:
  Choose $x_1, x_2, y \leftarrow \mathbb{Z}_p$
  $\mathsf{sk} := (x_1, x_2, y)$
  $\mathsf{vk} := (\tilde{X}_1 := \tilde{H}^{x_1}, \tilde{X}_2 := \tilde{H}^{x_2}, \tilde{Y} := \tilde{H}^{y}) \in \mathbb{H}^3$

- Sign: To sign $\left((M, \tilde{N})_1, (M, \tilde{N})_2\right) \in \widehat{\mathbb{GH}}^2$,
  - Choose $r_1, r_2 \leftarrow \mathbb{Z}_p$,
    $\sigma := \left(R_1 := G^{r_1}, R_2 := G^{r_2}, \tilde{S} := \left(G^{x_1} \cdot M_1\right)^{\frac{r_1}{y}} \cdot \left(G^{x_2} \cdot M_2\right)^{\frac{r_2}{y}}\right) \in \mathbb{G}^3$

- Verify: Check that $(M, \tilde{N})_i \in \widehat{\mathbb{GH}}$ and

$$e(S, \tilde{Y}) = e(R_1, \tilde{X}_1 \cdot \tilde{N}_1) e(R_2, \tilde{X}_2 \cdot \tilde{N}_2)$$

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

Properties of Scheme III

- The scheme is secure in the generic group model
  - $\Rightarrow$ alternatively can be based on an interactive assumption
- Only M part of the message is needed for signing
- σ' is NOT indistinguishable from a fresh signature on the same message vector
  - The original signer can link σ' (randomized signature) to σ (original signature)

Properties of Scheme III

- The scheme is secure in the generic group model
  - $\Rightarrow$ alternatively can be based on an interactive assumption
- Only M part of the message is needed for signing
- σ' is NOT indistinguishable from a fresh signature on the same message vector
  - The original signer can link σ' (randomized signature) to σ (original signature)

Properties of Scheme III

- The scheme is secure in the generic group model
  - $\Rightarrow$ alternatively can be based on an interactive assumption
- Only M part of the message is needed for signing
- σ' is NOT indistinguishable from a fresh signature on the same message vector
  - The original signer can link σ' (randomized signature) to σ (original signature)

Summary

- More efficient schemes than optimal Type-3 schemes
  - Shorter signatures and less verification overhead ☺
  - Larger messages & messages have to be in a special form ☹
    - Batch verification can speed up DH verification ☺

Open Problems

- Applying similar techniques to standard-assumption constructions?

Summary

- More efficient schemes than optimal Type-3 schemes
  - Shorter signatures and less verification overhead ☺
  - Larger messages & messages have to be in a special form ☹
    - Batch verification can speed up DH verification ☺

Open Problems

- Applying similar techniques to standard-assumption constructions?

The End

☺

?