More Efficient (Almost) Tightly Secure Structure-Preserving Signatures

Romain Gay[1] Dennis Hofheinz[2] Lisa Kohl[2] Jiaxin Pan [2]

[1] ENS Paris, France
[2] Karlsruhe Institute of Technology, Germany

This talk

- A structure-preserving signature scheme with
  - Tighter security
  - (Significantly) shorter signatures: $25 \rightarrow 14$ elements
- The core technique can be presented in a simple, algebraic and modular way.

Signature

- $(pk, sk) \xleftarrow{\$} \mathsf{Gen}(\mathsf{par})$
- $\sigma \xleftarrow{\$} \mathsf{Sign}(sk, \mathsf{m})$
- $0/1 \leftarrow \mathsf{Ver}(pk, \mathsf{m}, \sigma)$

Structure-Preserving Signatures (SPS) [AFGHO10]

Pairing groups

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ cyclic groups of prime order q:

- $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ (Type III)

- $(pk, sk) \stackrel{\$}{\leftarrow} \mathsf{Gen}(\mathsf{par})$: $\boxed{pk \in \mathbb{G}_s}$ $(s \in \{1, 2, T\})$
- $\sigma \stackrel{\$}{\leftarrow} \mathsf{Sign}(sk, \mathsf{m})$: $\boxed{\mathsf{m} \in \mathbb{G}_s \text{ and } \sigma \in \mathbb{G}_s}$
- $0/1 \leftarrow \mathsf{Ver}(pk, \mathsf{m}, \sigma)$: $\boxed{\text{Only pairing product equations are allowed.}}$

Applications of SPS

- Composition with:
  - Groth-Sahai NIZK proofs, ElGamal Encryption, ...
- Efficient modular design for:
  - Group signatures, blind signatures, anonymous credentials, ...

Applications of SPS

- Composition with:
  - Groth-Sahai NIZK proofs, ElGamal Encryption, ...
- Efficient modular design for:
  - Group signatures, blind signatures, anonymous credentials, ...

Goal

Construct simple and efficient SPS under standard assumptions.

Applications of SPS

- Composition with:
  - Groth-Sahai NIZK proofs, ElGamal Encryption, ...
- Efficient modular design for:
  - Group signatures, blind signatures, anonymous credentials, ...

Goal

Construct simple and efficient SPS under standard assumptions.

Standard assumptions (e.g. DDH/SXDH, DLIN, k-LIN): non-interactive and static assumptions

Important measures of efficiency for SPS

- Size of public keys, $|pk|$
- Size of signatures, $|\sigma|$
- Number of pairing product equations, $\#$PPEs
- Tightness of security reductions

Important measures of efficiency for SPS

- Size of public keys, $|pk|$
- Size of signatures, $|\sigma|$
- Number of pairing product equations, $\#$PPEs
- Tightness of security reductions
  - Affects the key length recommendation

with success ratio

$\rho := \frac{\varepsilon}{t}$

with success ratio

$\rho' := \frac{\varepsilon'}{t'} = \rho / {\color{red}L}$

Tight security [BBM00,Coron00]

with success ratio $\rho := \frac{\varepsilon}{t}$

with success ratio $\rho' := \frac{\varepsilon'}{t'} = \rho / L$

- This work: $t' = O(t)$

Tight security [BBM00,Coron00]

with success ratio

$\rho := \frac{\varepsilon}{t}$

with success ratio

$\rho' := \frac{\varepsilon'}{t'} = \rho / L$

- This work: $t' = O(t)$
- Tight security: L = "small" (e.g. $L = O(\lambda)$, or $O(\log Q)$, or $O(1)$)
- Non-tight security: $L = \Omega(Q)$

- λ: security parameter
- $Q :=$ poly$(\lambda) < 2^\lambda \Rightarrow \log Q < \lambda$

Example: Why tightness?

with success ratio $\rho := \frac{\varepsilon}{t} < 2^{-80}$

with success ratio $\rho' := \frac{\varepsilon'}{t'} = \rho / L < 2^{-110}$

- Tight security: $L = 1$
- Non-tight security: for example, L = #signing queries = 2^{30}

State-of-the-Art: Tightness and Efficiency

	Schemes	Security loss	Signature size
Tight	[HJ12]	$O(1)$	$O(\lambda)$
	[AHNOP17]	$O(\lambda)$	25

Non-tight	[JR17]	$O(Q \log Q)$	6
	[KPW15]	$O(Q^2)$	7
	[LPY15]	$O(Q)$	11
	[ACDKNO12]	$O(Q)$	11
	⋮	⋮	⋮

State-of-the-Art: Tightness, and Efficiency

	Schemes	Security loss	Signature size
Tight	[HJ12]	$O(1)$	$O(\lambda)$
	[AHNOP17]	$O(\lambda)$	25
	[JOR18]	$O(\lambda)$	17
	This work	$O(\log Q)$	14
Non-tight	[JR17]	$O(Q \log Q)$	6
	[KPW15]	$O(Q^2)$	7
	[LPY15]	$O(Q)$	11
	[ACDKNO12]	$O(Q)$	11
	⋮	⋮	⋮

This Work

$$\text{Algebraic MAC} \longmapsto \text{SPS}$$

- The core component:

  an efficient tightly secure message authentication code (MAC)

This Work

Algebraic MAC $\longmapsto$ SPS

- The core component:

  an efficient tightly secure message authentication code (MAC)

- The resulting SPS has **better** performance:
  - **shorter** signatures
  - **shorter** public keys
  - **less** pairing product equations
  - **tighter** security

Our Technique

One-time MAC
(private-key, information-theoretically secure, SP)

↓ Motivated by the adaptive partioning technique ([Hof17], [GHK17])

Many-time MAC
(SP)

Our Technique

One-time MAC
(private-key, information-theoretically secure, SP)

↓

This talk

Many-time MAC
(SP)

↓

private-key ↦ public-key via pairings
(Similar to [BKP14,KPW15])

SPS

Signature vs. MAC

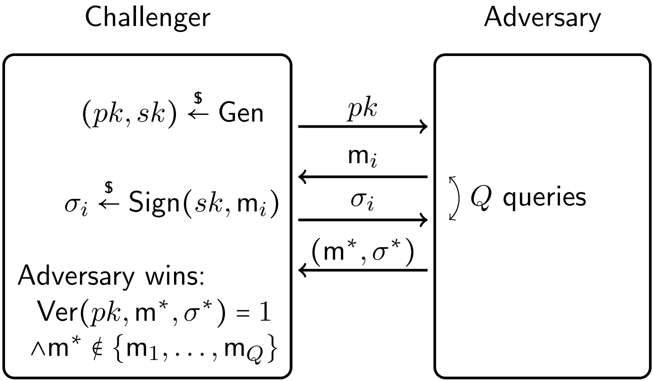
Signature

- $(pk, sk) \xleftarrow{\$} \mathsf{Gen}(\mathsf{par})$
- $\sigma \xleftarrow{\$} \mathsf{Sign}(sk, \mathsf{m})$
- $0/1 \leftarrow \mathsf{Ver}(pk, \mathsf{m}, \sigma)$

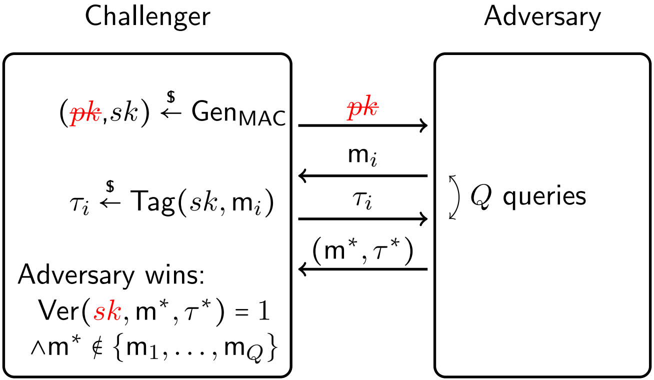
MAC

- $(\cancel{pk}, sk) \xleftarrow{\$} \mathsf{Gen}_{\mathsf{MAC}}(\mathsf{par})$
- $\tau \xleftarrow{\$} \mathsf{Tag}(sk, \mathsf{m})$
- $0/1 \leftarrow \mathsf{Ver}(\cancel{pk}, sk, \mathsf{m}, \tau)$

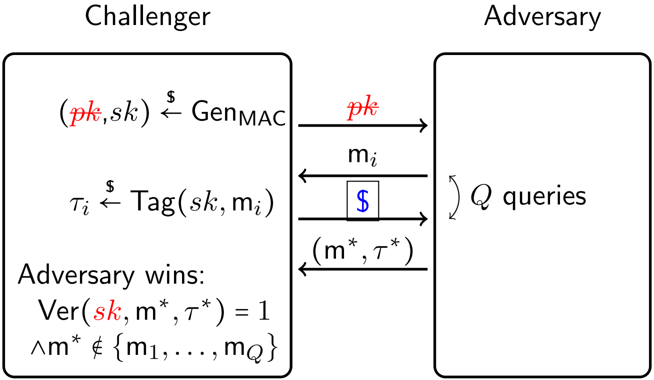
Security of Signature



Security of MAC



For our MAC



Challenger
Adversary
$(\cancel{pk}, sk) \xleftarrow{\$} \mathsf{Gen}_{\mathsf{MAC}}$
$\cancel{pk}$
m_i
$\tau_i \xleftarrow{\$} \mathsf{Tag}(sk, \mathsf{m}_i)$
$
Q queries
(m^*, τ^*)
Adversary wins:
$\mathsf{Ver}(sk, \mathsf{m}^*, \tau^*) = 1$
$\wedge \mathsf{m}^* \notin \{\mathsf{m}_1, \ldots, \mathsf{m}_Q\}$

Implicit Notation

- Let $a \in \mathbb{Z}_p$, $[a]_s := a\mathcal{P}_s \in \mathbb{G}_s$

Implicit Notation

- Let $a \in \mathbb{Z}_p$, $[a]_s := a\mathcal{P}_s \in \mathbb{G}_s$
- Let $\mathbf{A} = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ & \ddots & \\ a_{n1} & \dots & a_{nm} \end{pmatrix} \in \mathbb{Z}_p^{n\times m}$,

$$[\mathbf{A}]_s := \begin{pmatrix} a_{11}\mathcal{P}_s & \dots & a_{1m}\mathcal{P}_s \\ & \ddots & \\ a_{n1}\mathcal{P}_s & \dots & a_{nm}\mathcal{P}_s \end{pmatrix} \in \mathbb{G}_s^{n\times m},$$

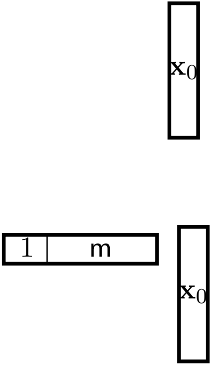
where $s \in \{1, 2, T\}$.

One-time MAC

- $\mathsf{Gen_{MAC}} : sk := \mathbf{x}_0 \xleftarrow{\$} \mathbb{Z}_p^{1+n}$

- $\mathsf{Tag}(sk, [\mathsf{m}]_1)$:

$$\tau := \underbrace{[(1, \mathsf{m}^\top)\mathbf{x}_0]_1}_{\text{2-wise independent hash}}$$



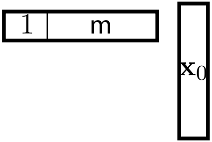
- $\mathsf{Ver}(sk, [\mathsf{m}]_1, \sigma) : \tau \stackrel{?}{=} [(1, \mathsf{m})]_1 \mathbf{x}_0$

One-time $\rightsquigarrow$ Many-time MAC

▸ $\mathsf{Gen}_{\mathsf{MAC}} : sk := (\mathbf{x}_0 \xleftarrow{\$} \mathbb{Z}_p^{1+n}, \mathbf{x} \xleftarrow{\$} \mathbb{Z}_p^{2k})$

▸ $\mathsf{Tag}(sk, [\mathsf{m}]_1)$:

$$\tau := \underbrace{[(1, \mathsf{m}^\top)\mathbf{x}_0]_1}_{\text{2-wise independent hash}} + \text{Random}$$



▸ $\mathsf{Ver}(sk, [\mathsf{m}]_1, \sigma) : \tau \stackrel{?}{=} [(1, \mathsf{m})]_1 \mathbf{x}_0$

The Core Idea (Simplified Version)

$$\mathbf{t} = \mathbf{A}_0 \mathbf{r}$$

$$u = \mathbf{t}^\top \mathbf{x}$$

where $\mathbf{A}_0 \in \mathbb{Z}_p^{2k \times k}$.

The Core Idea (Simplified Version)

$$\mathbf{t} = \mathbf{A}_0 \mathbf{r}$$

$$u = \mathbf{t}^\top \mathbf{x}$$

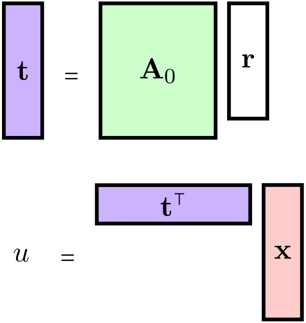
where $\mathbf{A}_0 \in \mathbb{Z}_p^{2k \times k}$.

$$([\mathbf{t}_0],[u_0]),\ldots,([\mathbf{t}_{Q-1}],[u_{Q-1}])$$

$$\approx_c$$

$$([\mathbf{t}_0],[\$_0]),\ldots,([\mathbf{t}_{Q-1}],[\$_{Q-1}]).$$

The Core Idea (Simplified Version)



where $\mathbf{A}_0 \in \mathbb{Z}_p^{2k\times k}$.

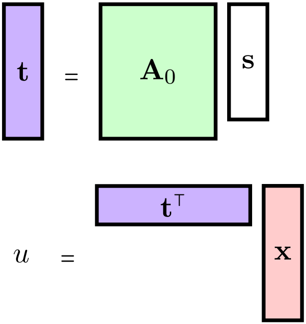
Real: $\{([\mathbf{t}_i],[\mathbf{t}_i^\top \mathbf{x}])\}_{1\le i\le Q}$

$\approx_c$

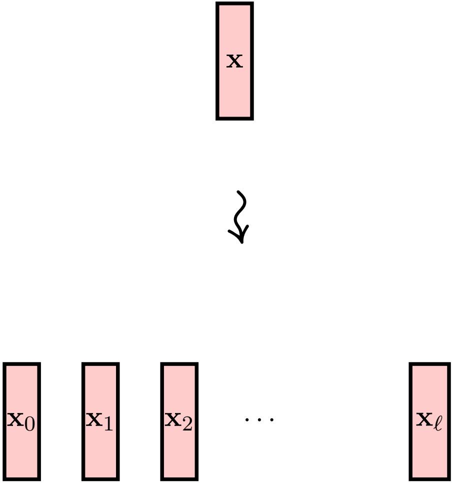
Rand: $\{([\mathbf{t}_i],[\mathbf{t}_i^\top \mathbf{x}_i])\}_{1\le i\le Q}$

where $\mathbf{x}_i \overset{\$}{\leftarrow} \mathbb{Z}_p^{2k}$.

The Core Idea (Simplified Version)



where $\mathbf{A}_0 \in \mathbb{Z}_p^{2k \times k}$.



$(\ell = Q - 1)$

In generation of $[u_i]$

$$\mathbf{x} \overset{\mathcal{C}}{\rightsquigarrow} \mathbf{x}_0 \;,\; \mathbf{x}_1$$

(Advanced) Simple Facts

Let $\mathbf{A}_0, \mathbf{A}_1 \xleftarrow{\$} \mathbb{Z}_p^{2k \times k}$, and $\mathbf{v}_0, \mathbf{v}_1 \xleftarrow{\$} \mathbb{Z}_p^{k}$

- Full-rank Kernel matrices, $\mathbf{A}_0^{\perp}, \mathbf{A}_1^{\perp} \in \mathbb{Z}_p^{2k \times k}$:

$$\mathbf{A}_0^{\top} \mathbf{A}_0^{\perp} = \mathbf{0} = \mathbf{A}_1^{\top} \mathbf{A}_1^{\perp}$$

- Fact 1:

$$\mathbf{v} = (\mathbf{A}_0^{\perp} | \mathbf{A}_1^{\perp}) \begin{pmatrix} \mathbf{v}_0 \\ \mathbf{v}_1 \end{pmatrix}$$

  is random.

- Fact 2: Let $\mathbf{t} \in \text{Span}(\mathbf{A}_0)$

$$\mathbf{t}^{\top}(\mathbf{x} + \mathbf{A}_0^{\perp} \mathbf{v}_0) = \mathbf{t}^{\top} \mathbf{x}$$

- Fact 3:

$$\{\text{Span}([\mathbf{A}_0])\} \approx_c \{\text{Span}([\mathbf{A}_1])\}$$

  by the Decisional Diffie-Hellman assumption.

Our Goal

$$\mathbf{x} \overset{\mathcal{C}}{\rightsquigarrow} \mathbf{x}_0 \; , \; \mathbf{x}_1$$

Intuition

- Switch $\mathbf{t}_i$ (Fact 3)
  - $i = 0\ldots$: $\mathbf{t}_i = \mathbf{A}_0\mathbf{r}$
  - $i = 1\ldots$: $\mathbf{t}_i = \mathbf{A}_1\mathbf{r}$

Intuition

- Switch $\mathbf{t}_i$ (Fact 3)
  - $i = 0 \ldots$: $\mathbf{t}_i = \mathbf{A}_0 \mathbf{r}$
  - $i = 1 \ldots$: $\mathbf{t}_i = \mathbf{A}_1 \mathbf{r}$
- Rewrite the vector $\mathbf{x}$ (Fact 1)

$$\mathbf{x} := (\mathbf{A}_0^{\perp} | \mathbf{A}_1^{\perp}) \begin{pmatrix} \mathbf{v}_0 \\ \mathbf{v}_1 \end{pmatrix}$$

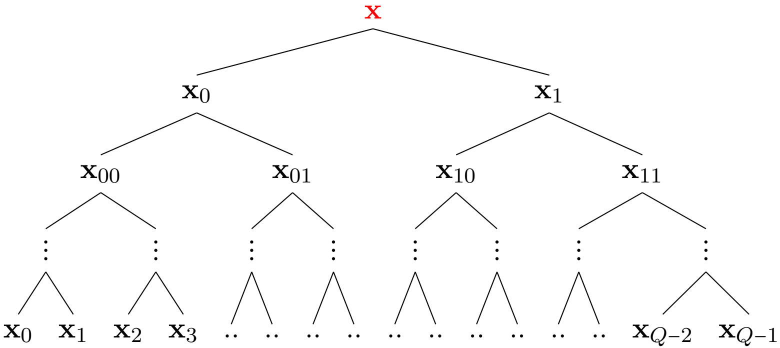
Intuition

- Switch $\mathbf{t}_i$ (Fact 3)
  - $i = 0 \ldots$: $\mathbf{t}_i = \mathbf{A}_0 \mathbf{r}$
  - $i = 1 \ldots$: $\mathbf{t}_i = \mathbf{A}_1 \mathbf{r}$
- Rewrite the vector $\mathbf{x}$ (Fact 1) $\mathbf{x} := (\mathbf{A}_0^{\perp} | \mathbf{A}_1^{\perp}) \begin{pmatrix} \mathbf{v}_0 \\ \mathbf{v}_1 \end{pmatrix}$
- Introduce new randomness (w/o change adversaries' view, by Fact 2)

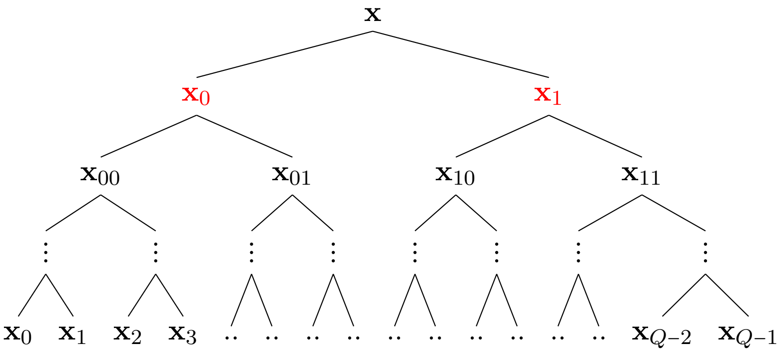
$$\mathbf{x}_0 := (\mathbf{A}_0^{\perp} | \mathbf{A}_1^{\perp}) \begin{pmatrix} \mathbf{r}_0 \\ \mathbf{v}_1 \end{pmatrix} \qquad \mathbf{x}_1 := (\mathbf{A}_0^{\perp} | \mathbf{A}_1^{\perp}) \begin{pmatrix} \mathbf{v}_0 \\ \mathbf{r}_1 \end{pmatrix}$$

  - $i = 0 \ldots$: $\mathbf{t}_i^{\top} \mathbf{x}_0 = \mathbf{t}_i^{\top} \mathbf{x}$
  - $i = 1 \ldots$: $\mathbf{t}_i^{\top} \mathbf{x}_1 = \mathbf{t}_i^{\top} \mathbf{x}$

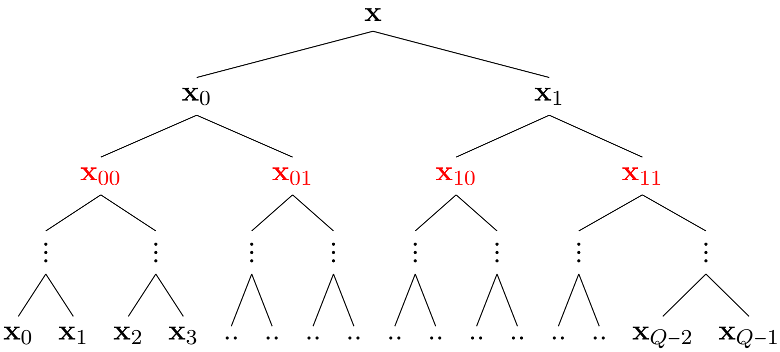
Overview of $\log Q$ Loops

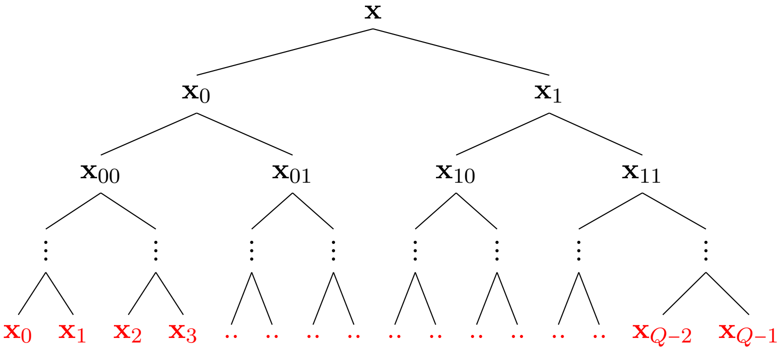


Overview of $\log Q$ Loops



Overview of $\log Q$ Loops





x
x0
x1
x00
x01
x10
x11
x0
x1
x2
x3
xQ−2
xQ−1

Our MAC

- $\mathsf{Gen}_{\mathsf{MAC}}(\mathsf{par})$
  - $\mathbf{A}_0, \mathbf{A}_1 \overset{\$}{\leftarrow} \mathcal{D}_{2k,k}$ // $\mathbf{A}_0, \mathbf{A}_1 \in \mathbb{Z}_p^{2k \times k}$
  - $\mathbf{x}_0 \overset{\$}{\leftarrow} \mathbb{Z}_p^{n+1}$, $\mathbf{x} \overset{\$}{\leftarrow} \mathbb{Z}_p^{2k}$
  - $crs \overset{\$}{\leftarrow} \mathsf{Gen}_{\mathsf{NIZK}}(\mathsf{par})$
  - Return $sk := ([\mathbf{A}_0], [\mathbf{A}_1], \mathbf{x}_0, \mathbf{x}, crs)$
- $\mathsf{Tag}(sk, [\mathsf{m}] \in \mathbb{G}^n)$: // i-th query $(1 \leq i \leq Q)$
  - $\mathbf{t} = \mathbf{A}_0\mathbf{s}$ for $\mathbf{s} \overset{\$}{\leftarrow} \mathbb{Z}_p$
  - $u = (1, \mathbf{m}^\top)\mathbf{x}_0 + \boxed{\mathbf{t}^\top \mathbf{x}}$
  - π proves that "$\mathbf{t} \in \mathsf{Span}(\mathbf{A}_0)$" *or* "$\mathbf{t} \in \mathsf{Span}(\mathbf{A}_1)$" // [Ráfols15]
  - Return $\tau := ([\mathbf{t}], [u], \pi)$
- $\mathsf{Ver}(sk, [\mathsf{m}^*], \tau^* := ([\mathbf{t}^*, u^*], \pi^*))$
  - $u^* \overset{?}{=} (1, \mathbf{m}^{*\top})\mathbf{x}_0 + \mathbf{t}^{*\top}\mathbf{x}$
  - Check π^*

Our SPS

- Gen(par)
  - $\mathbf{A}_0, \mathbf{A}_1 \xleftarrow{\$} \mathcal{D}_{2k,k}$, $\mathbf{B} \xleftarrow{\$} \mathcal{D}_{k+1,k}$ // $\mathbf{A}_0, \mathbf{A}_1 \in \mathbb{Z}_p^{2k \times k}, \mathbf{B} \in \mathbb{Z}_p^{(k+1)\times k}$
  - $\mathbf{X}_0 \xleftarrow{\$} \mathbb{Z}_p^{(n+1)\times(k+1)}$, $\mathbf{X} \xleftarrow{\$} \mathbb{Z}_p^{2k\times(k+1)}$
  - $crs \xleftarrow{\$} \mathsf{Gen}_{\mathsf{NIZK}}(\mathsf{par})$
  - $sk := (\mathbf{X}_0, \mathbf{X}, crs)$
  - $pk := ([\mathbf{A}_0]_1, [\mathbf{A}_1]_1, [\mathbf{B}]_2[\mathbf{X}_0\mathbf{B}]_2, [\mathbf{X}\mathbf{B}]_2, crs)$
  - Return (pk, sk)
- Sign$(sk, [\mathsf{m}]_1 \in \mathbb{G}_1^n)$: // i-th query $(1 \le i \le Q)$
  - $\mathbf{t} = \mathbf{A}_0\mathbf{s} \in \mathbb{Z}_p^{2k}$ for $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_p$
  - $\mathbf{u} = (1, \mathbf{m}^\top)\mathbf{X}_0 + \mathbf{t}^\top\mathbf{X} \in \mathbb{Z}_p^{1\times(k+1)}$
  - π proves that "$\mathbf{t} \in \mathsf{Span}(\mathbf{A}_0)$" *or* "$\mathbf{t} \in \mathsf{Span}(\mathbf{A}_1)$"
  - Return $\sigma := ([\mathbf{t}]_1, [\mathbf{u}]_1, \pi)$
- Ver$(pk, [\mathsf{m}^*]_1, \sigma^* := ([\mathbf{t}^*, \mathbf{u}^*]_1, \pi^*))$
  - $u^*\mathbf{B} \stackrel{?}{=} (1, \mathbf{m}^{*\top})\mathbf{X}_0\mathbf{B} + \mathbf{t}^{*\top}\mathbf{X}\mathbf{B}$ via pairings
  - Check π^*

Comparison

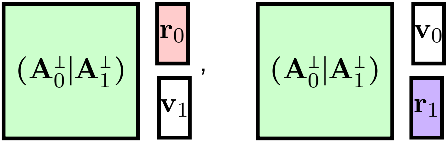
Scheme	$\lvert\sigma\rvert$	$\lvert pk\rvert$	#PPEs	Sec. loss	Assumption
ACDKNO12	11	$n_1 + 17$	4	Q	SXDH, XDLIN
LPY15	11	$2n_1 + 21$	5	$O(Q)$	SXDH, XDLIN
KPW15	7	$n_1 + 6$	3	$2Q^2$	SXDH
JR17	6	$n_1 + 6$	2	$Q \log Q$	SXDH
HJ12	$10\lambda + 6$	13	$O(\lambda)$	8	DLIN
AHNOP17	25	$n_1 + 29$	15	80λ	SXDH
JOR18	17	$n_1 + 23$	7	116λ	SXDH
Ours	14	$n_1 + 11$	6	$6 \log Q$	SXDH

Summary

- More efficient tightly secure SPS with
  - shorter $|\sigma|$ and $|pk|$
  - Less pairing product equations and security loss
- The core component:

structure-preserving, pseudorandom MAC

with tight security reductions.



Open problems

- Tightly secure SPS with shorter signature size?
- Tightly secure and compact IBE from our partially affine MAC?