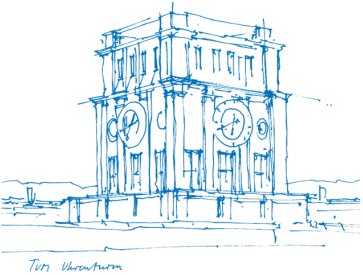
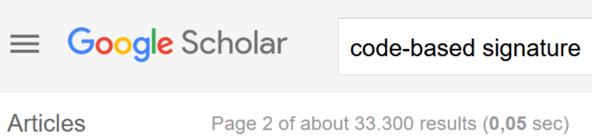
VOLEitH-based Signatures from Restricted Decoding Problems

Sebastian Bitzer Violetta Weger

CBC25

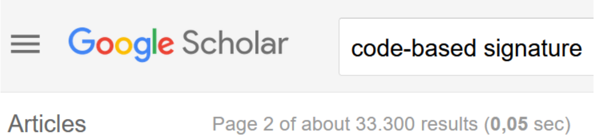


Code-based Signatures


code-based signature

Page 2 of about 33.300 results (**0,05** sec)

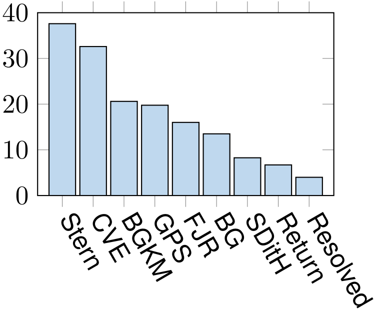
Code-based Signatures



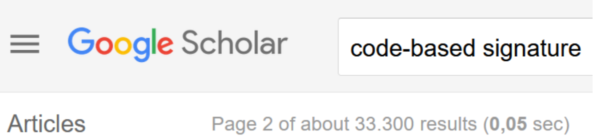
code-based signature

Articles

Page 2 of about 33.300 results (**0,05** sec)



Code-based Signatures

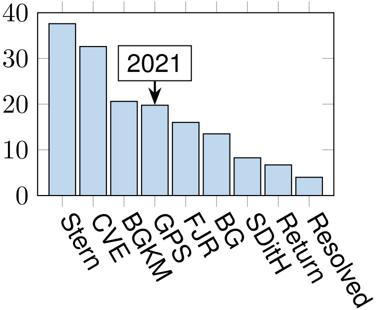


Google Scholar

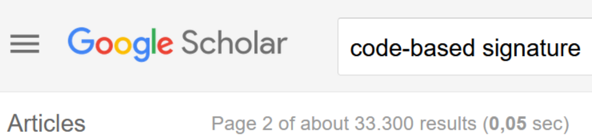
code-based signature

Articles

Page 2 of about 33.300 results (**0,05** sec)



Code-based Signatures

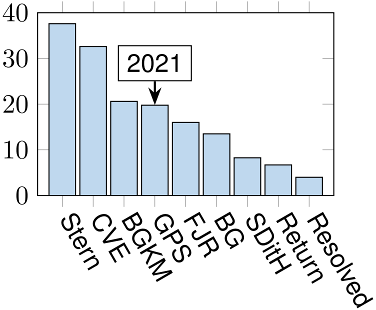


Google Scholar

code-based signature

Articles

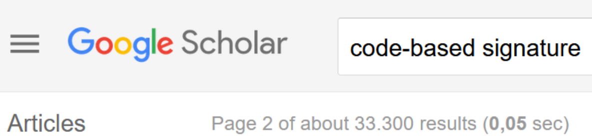
Page 2 of about 33.300 results (**0,05** sec)



Introduction to VOLE(itH)

- Thibauld Feneuil, Polynomial-IOP Vision of MPCitH
- Carsten Baum, VOLE-in-the-head and FAEST

Code-based Signatures

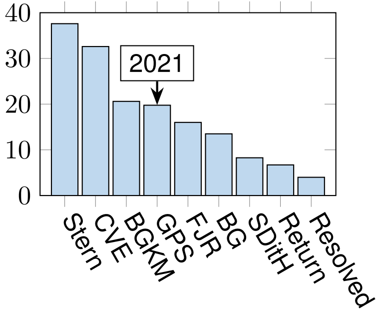


Google Scholar

code-based signature

Articles

Page 2 of about 33.300 results (**0,05** sec)



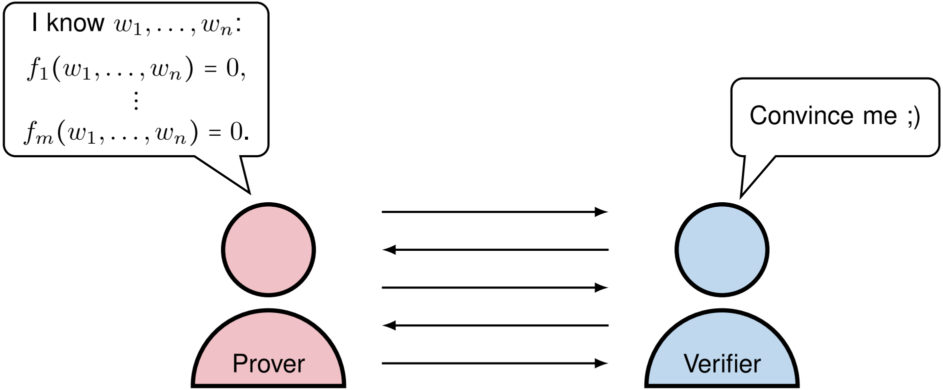
Introduction to VOLE(itH)

- Thibauld Feneuil, Polynomial-IOP Vision of MPCitH
- Carsten Baum, VOLE-in-the-head and FAEST

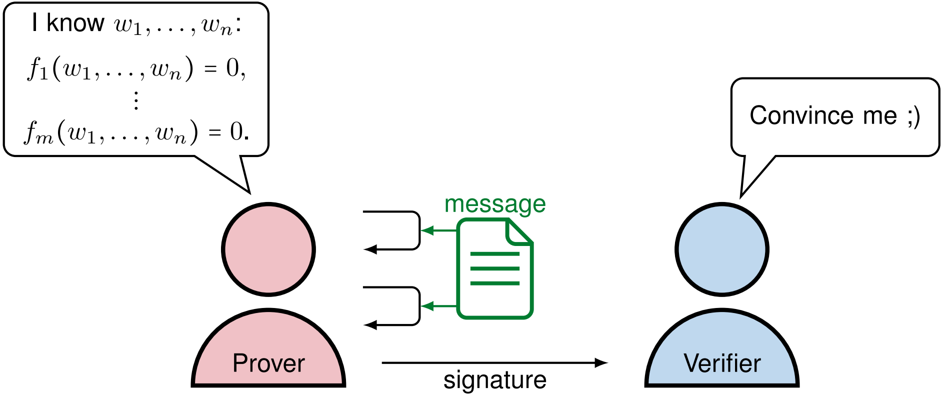
R-SDP signatures

- ⓧ Simple VOLEitH modeling
- ⓧ Competitive performance

Signatures from Identification Schemes



Signatures from Identification Schemes

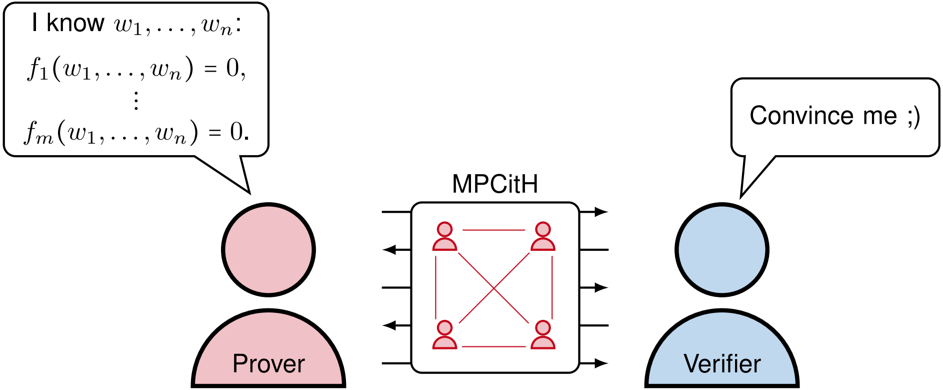


I know $w_1, \ldots, w_n$:

$$f_1(w_1, \ldots, w_n) = 0,$$
$$\vdots$$
$$f_m(w_1, \ldots, w_n) = 0.$$

Convince me ;)

Signatures from Identification Schemes

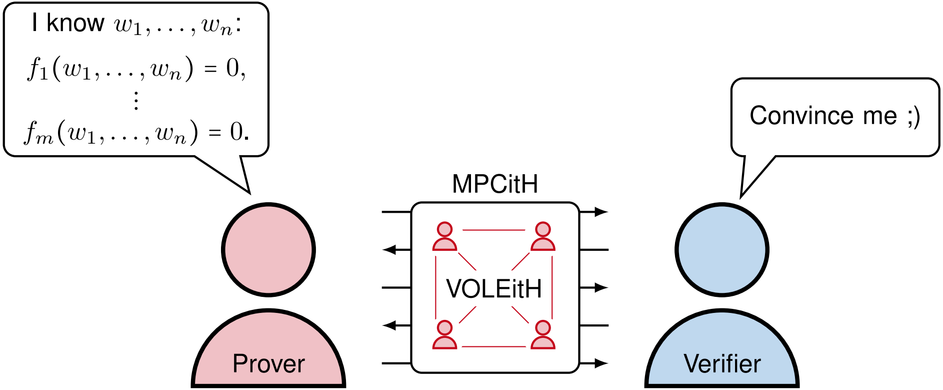


I know $w_1, \ldots, w_n$:

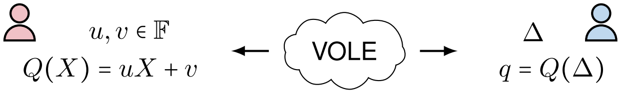
$$f_1(w_1, \ldots, w_n) = 0,$$
$$\vdots$$
$$f_m(w_1, \ldots, w_n) = 0.$$

Convince me ;)

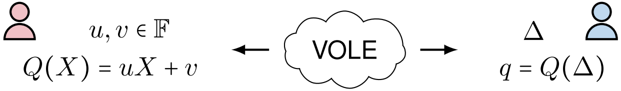
Signatures from Identification Schemes



Vector Oblivious Linear Evaluation



Vector Oblivious Linear Evaluation

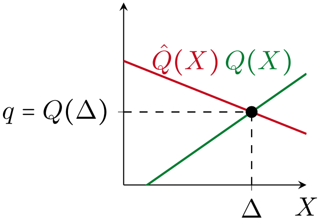


$u, v \in \mathbb{F}$

$Q(X) = uX + v$

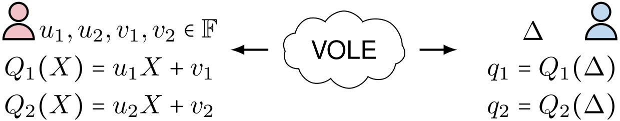
Δ

$q = Q(\Delta)$



→ Hiding & binding commitment to u

Vector Oblivious Linear Evaluation



$u_1, u_2, v_1, v_2 \in \mathbb{F}$

$Q_1(X) = u_1 X + v_1$

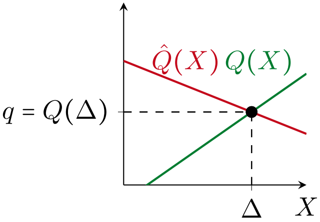
$Q_2(X) = u_2 X + v_2$

$\longleftarrow$ VOLE $\longrightarrow$

Δ

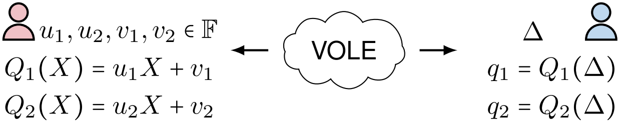
$q_1 = Q_1(\Delta)$

$q_2 = Q_2(\Delta)$



- ➔ Hiding & binding commitment to u
- ➔ Add: $Q_1 + Q_2 = (u_1 + u_2)X + \dots \quad (Q_1 + Q_2)(\Delta) = q_1 + q_2$

Vector Oblivious Linear Evaluation



$u_1, u_2, v_1, v_2 \in \mathbb{F}$

$Q_1(X) = u_1 X + v_1$

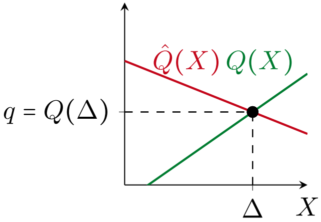
$Q_2(X) = u_2 X + v_2$

$\longleftarrow$ VOLE $\longrightarrow$

Δ

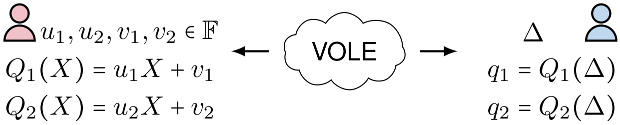
$q_1 = Q_1(\Delta)$

$q_2 = Q_2(\Delta)$



- ➔ Hiding & binding commitment to u
- ➔ Add: $Q_1 + Q_2 = (u_1 + u_2)X + \dots$ $(Q_1 + Q_2)(\Delta) = q_1 + q_2$
- ➔ Multiply: $Q_1 \cdot Q_2 = (u_1 \cdot u_2)X^2 + \dots$ $(Q_1 \cdot Q_2)(\Delta) = q_1 \cdot q_2$

Vector Oblivious Linear Evaluation



$u_1, u_2, v_1, v_2 \in \mathbb{F}$

$Q_1(X) = u_1 X + v_1$

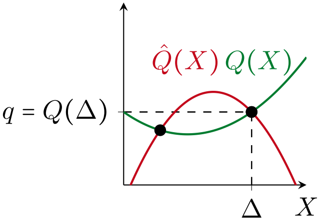
$Q_2(X) = u_2 X + v_2$

VOLE

Δ

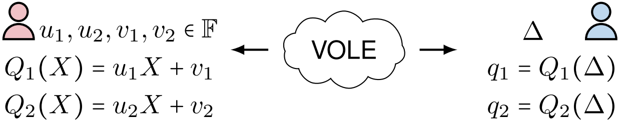
$q_1 = Q_1(\Delta)$

$q_2 = Q_2(\Delta)$



- Hiding & binding commitment to u
- Add: $Q_1 + Q_2 = (u_1 + u_2)X + \dots \quad (Q_1 + Q_2)(\Delta) = q_1 + q_2$
- Multiply: $Q_1 \cdot Q_2 = (u_1 \cdot u_2)X^2 + \dots \quad (Q_1 \cdot Q_2)(\Delta) = q_1 \cdot q_2$

Vector Oblivious Linear Evaluation



$u_1, u_2, v_1, v_2 \in \mathbb{F}$

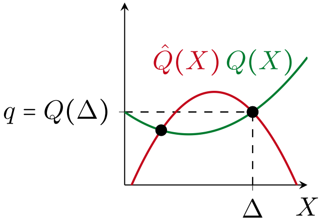
$Q_1(X) = u_1 X + v_1$

$Q_2(X) = u_2 X + v_2$

Δ

$q_1 = Q_1(\Delta)$

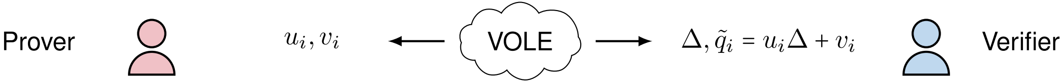
$q_2 = Q_2(\Delta)$



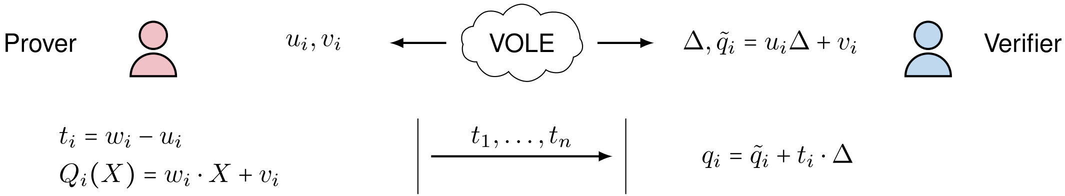
- Hiding & binding commitment to u

$$\left.\begin{array}{lll} \text{Add:} & Q_1 + Q_2 = (u_1 + u_2)X + \dots & (Q_1 + Q_2)(\Delta) = q_1 + q_2 \\ \text{Multiply:} & Q_1 \cdot Q_2 = (u_1 \cdot u_2)X^2 + \dots & (Q_1 \cdot Q_2)(\Delta) = q_1 \cdot q_2 \end{array}\right\} \text{evaluate } f_1, \dots, f_m$$

VOLEitH à la Thibauld



VOLEitH à la Thibauld



Prover

$u_i, v_i \longleftarrow$ VOLE $\longrightarrow \Delta, \tilde{q}_i = u_i \Delta + v_i$

Verifier

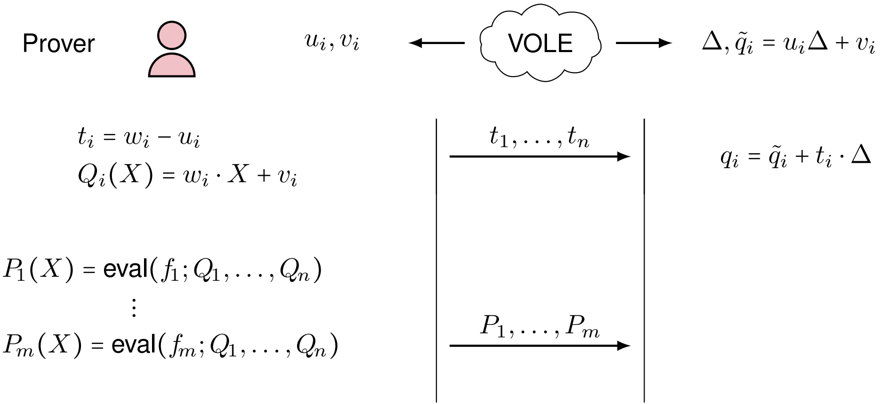
$t_i = w_i - u_i$

$Q_i(X) = w_i \cdot X + v_i$

$$\xrightarrow{t_1, \ldots, t_n}$$

$q_i = \tilde{q}_i + t_i \cdot \Delta$

VOLEitH à la Thibauld



Prover

u_i, v_i

VOLE

$\Delta, \tilde{q}_i = u_i \Delta + v_i$

Verifier

$t_i = w_i - u_i$

$Q_i(X) = w_i \cdot X + v_i$

$t_1, \ldots, t_n$

$q_i = \tilde{q}_i + t_i \cdot \Delta$

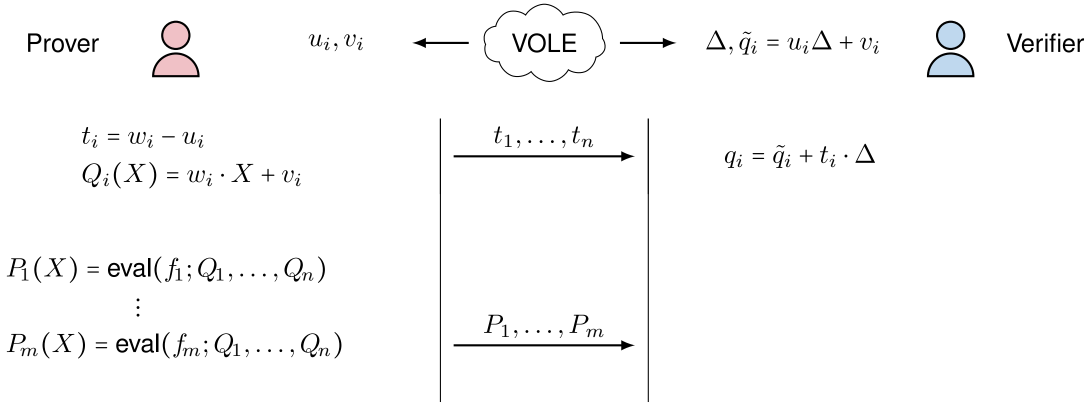
$P_1(X) = \mathsf{eval}(f_1; Q_1, \ldots, Q_n)$

$\vdots$

$P_m(X) = \mathsf{eval}(f_m; Q_1, \ldots, Q_n)$

$P_1, \ldots, P_m$

VOLEitH à la Thibauld



Prover

$u_i, v_i \longleftarrow$ VOLE $\longrightarrow \Delta, \tilde{q}_i = u_i\Delta + v_i$

Verifier

$t_i = w_i - u_i$

$Q_i(X) = w_i \cdot X + v_i$

$\xrightarrow{t_1, \ldots, t_n}$

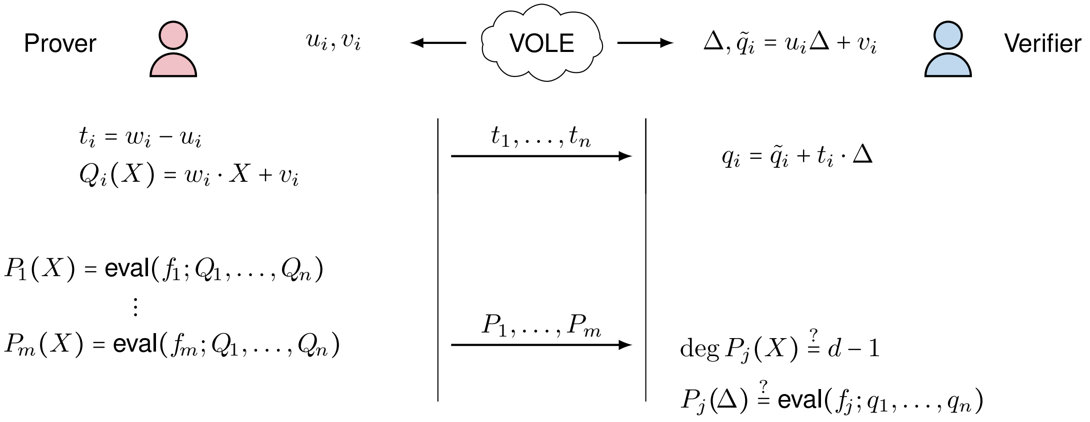
$q_i = \tilde{q}_i + t_i \cdot \Delta$

$$P_1(X) = \text{eval}(f_1; Q_1, \ldots, Q_n)$$
$$\vdots$$
$$P_m(X) = \text{eval}(f_m; Q_1, \ldots, Q_n)$$

$\xrightarrow{P_1, \ldots, P_m}$

$$\boxed{P_j(X) = \underbrace{f_j(w_1, \ldots, w_n)}_{=0} X^d + \ldots}$$

VOLEitH à la Thibauld



Prover u_i, v_i ← VOLE → $\Delta, \tilde{q}_i = u_i\Delta + v_i$ **Verifier**

$$t_i = w_i - u_i$$
$$Q_i(X) = w_i \cdot X + v_i$$

$\xrightarrow{t_1, \ldots, t_n}$

$$q_i = \tilde{q}_i + t_i \cdot \Delta$$

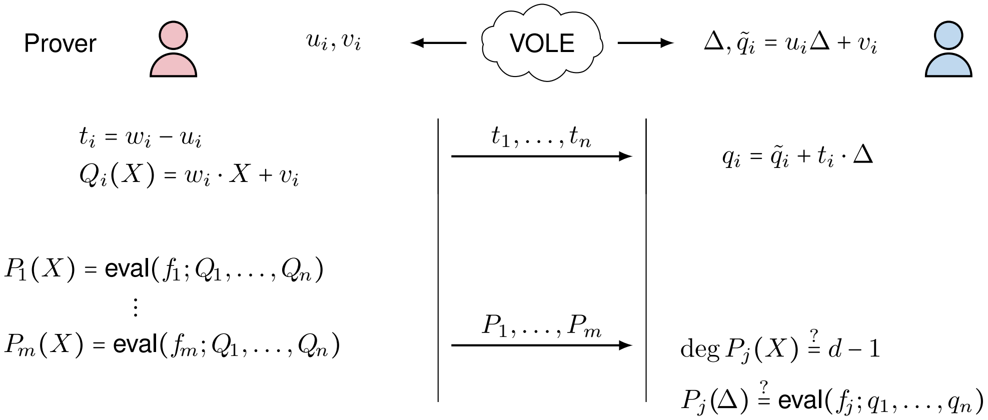
$$P_1(X) = \text{eval}(f_1; Q_1, \ldots, Q_n)$$
$$\vdots$$
$$P_m(X) = \text{eval}(f_m; Q_1, \ldots, Q_n)$$

$\xrightarrow{P_1, \ldots, P_m}$

$$\deg P_j(X) \overset{?}{=} d - 1$$
$$P_j(\Delta) \overset{?}{=} \text{eval}(f_j; q_1, \ldots, q_n)$$

$$\boxed{P_j(X) = \underbrace{f_j(w_1, \ldots, w_n)}_{=0} X^d + \ldots}$$

VOLEitH à la Thibauld



Prover

u_i, v_i

VOLE

$\Delta, \tilde{q}_i = u_i \Delta + v_i$

Verifier

$t_i = w_i - u_i$

$Q_i(X) = w_i \cdot X + v_i$

$t_1, \dots, t_n$

$q_i = \tilde{q}_i + t_i \cdot \Delta$

$P_1(X) = \mathsf{eval}(f_1; Q_1, \dots, Q_n)$

$\vdots$

$P_m(X) = \mathsf{eval}(f_m; Q_1, \dots, Q_n)$

$P_1, \dots, P_m$

$\deg P_j(X) \overset{?}{=} d - 1$

$P_j(\Delta) \overset{?}{=} \mathsf{eval}(f_j; q_1, \dots, q_n)$

Correctness

$$P_j(X) = \underbrace{f_j(w_1, ..., w_n)}_{=0} X^d + \dots$$

VOLEitH à la Thibauld

Prover $u_i, v_i \longleftarrow$ VOLE $\longrightarrow \Delta, \tilde{q}_i = u_i\Delta + v_i$ Verifier

$$t_i = w_i - u_i$$

$$Q_i(X) = w_i \cdot X + v_i$$

$$\xrightarrow{t_1, \ldots, t_n}$$

$$q_i = \tilde{q}_i + t_i \cdot \Delta$$

$$P_1(X) = \mathsf{eval}(f_1; Q_1, \ldots, Q_n)$$

$$\vdots$$

$$P_m(X) = \mathsf{eval}(f_m; Q_1, \ldots, Q_n)$$

$$\xrightarrow{P_1, \ldots, P_m}$$

$$\deg P_j(X) \overset{?}{=} d - 1$$

$$P_j(\Delta) \overset{?}{=} \mathsf{eval}(f_j; q_1, \ldots, q_n)$$

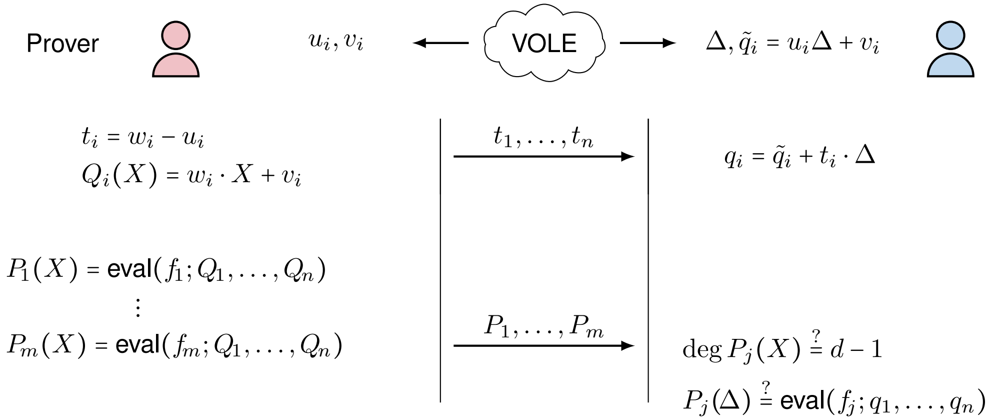
Correctness

$$P_j(X) = \underbrace{f_j(w_1, \ldots, w_n)}_{=0} X^d + \ldots$$

Soundness

?

VOLEitH à la Thibauld



Prover

$u_i, v_i \longleftarrow$ VOLE $\longrightarrow \Delta, \tilde{q}_i = u_i \Delta + v_i$

Verifier

$$t_i = w_i - u_i$$
$$Q_i(X) = w_i \cdot X + v_i$$

$$\xrightarrow{t_1, \dots, t_n}$$

$$q_i = \tilde{q}_i + t_i \cdot \Delta$$

$$P_1(X) = \mathsf{eval}(f_1; Q_1, \dots, Q_n)$$
$$\vdots$$
$$P_m(X) = \mathsf{eval}(f_m; Q_1, \dots, Q_n)$$

$$\xrightarrow{P_1, \dots, P_m}$$

$$\deg P_j(X) \overset{?}{=} d - 1$$
$$P_j(\Delta) \overset{?}{=} \mathsf{eval}(f_j; q_1, \dots, q_n)$$

Correctness

$$P_j(X) = \underbrace{f_j(w_1, ..., w_n)}_{=0} X^d + ...$$

Soundness

$$\Pr[P_j'(\Delta) = P_j(\Delta)] \leq \frac{d}{|\mathbb{F}|}$$

VOLEitH à la Thibauld

Prover $u_i, v_i \xleftarrow{} \text{VOLE} \xrightarrow{} \Delta, \tilde{q}_i = u_i\Delta + v_i$ **Verifier**

$$t_i = w_i - u_i$$
$$Q_i(X) = w_i \cdot X + v_i$$

$$\xrightarrow{t_1, \dots, t_n}$$

$$q_i = \tilde{q}_i + t_i \cdot \Delta$$

$$P_1(X) = \text{eval}(f_1; Q_1, \dots, Q_n)$$
$$\vdots$$
$$P_m(X) = \text{eval}(f_m; Q_1, \dots, Q_n)$$

$$\xrightarrow{P_1, \dots, P_m}$$

$$\deg P_j(X) \overset{?}{=} d - 1$$
$$P_j(\Delta) \overset{?}{=} \text{eval}(f_j; q_1, \dots, q_n)$$

Correctness

$$P_j(X) = \underbrace{f_j(w_1, \dots, w_n)}_{=0} X^d + \dots$$

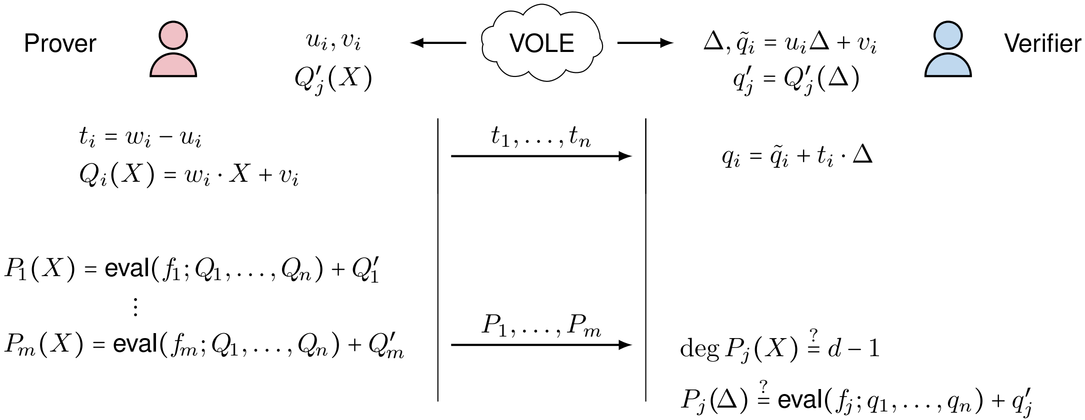
Soundness

$$\Pr[P_j'(\Delta) = P_j(\Delta)] \leq \frac{d}{|\mathbb{F}|}$$

ZKnowledge

?

VOLEitH à la Thibauld



Prover

u_i, v_i

$Q'_j(X)$

$\xleftarrow{\quad}$ VOLE $\xrightarrow{\quad}$

$\Delta, \tilde{q}_i = u_i \Delta + v_i$

$q'_j = Q'_j(\Delta)$

Verifier

$t_i = w_i - u_i$

$Q_i(X) = w_i \cdot X + v_i$

$\xrightarrow{t_1, \ldots, t_n}$

$q_i = \tilde{q}_i + t_i \cdot \Delta$

$P_1(X) = \mathsf{eval}(f_1; Q_1, \ldots, Q_n) + Q'_1$

$\vdots$

$P_m(X) = \mathsf{eval}(f_m; Q_1, \ldots, Q_n) + Q'_m$

$\xrightarrow{P_1, \ldots, P_m}$

$\deg P_j(X) \overset{?}{=} d - 1$

$P_j(\Delta) \overset{?}{=} \mathsf{eval}(f_j; q_1, \ldots, q_n) + q'_j$

Correctness

$$P_j(X) = \underbrace{f_j(w_1, \ldots, w_n)}_{=0} X^d + \ldots$$

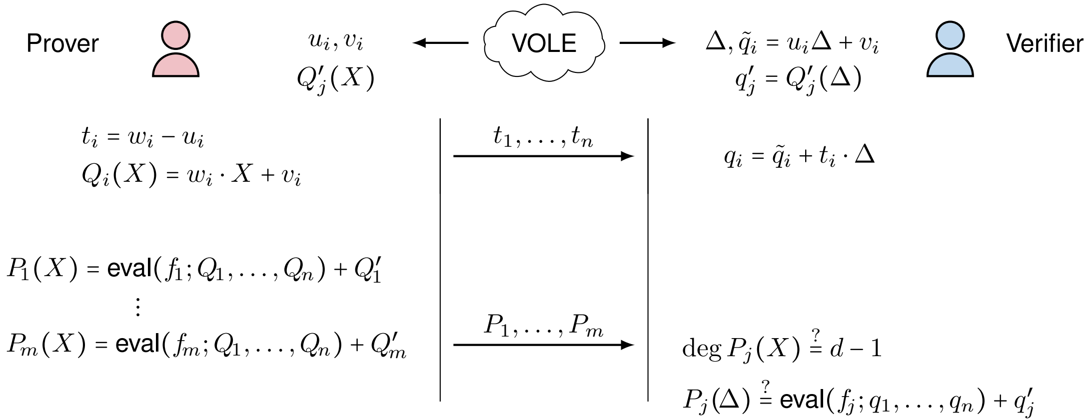
Soundness

$$\Pr[P'_j(\Delta) = P_j(\Delta)] \leq \frac{d}{|\mathbb{F}|}$$

ZKnowledge

Mask via $Q'_j(X)$

VOLEitH à la Thibauld



Prover u_i, v_i $Q'_j(X)$ $\longleftarrow$ VOLE $\longrightarrow$ $\Delta, \tilde{q}_i = u_i \Delta + v_i$ $q'_j = Q'_j(\Delta)$ **Verifier**

$$t_i = w_i - u_i$$
$$Q_i(X) = w_i \cdot X + v_i$$

$$\xrightarrow{t_1, \dots, t_n}$$

$$q_i = \tilde{q}_i + t_i \cdot \Delta$$

$$P_1(X) = \mathsf{eval}(f_1; Q_1, \dots, Q_n) + Q'_1$$
$$\vdots$$
$$P_m(X) = \mathsf{eval}(f_m; Q_1, \dots, Q_n) + Q'_m$$

$$\xrightarrow{P_1, \dots, P_m}$$

$$\deg P_j(X) \overset{?}{=} d - 1$$
$$P_j(\Delta) \overset{?}{=} \mathsf{eval}(f_j; q_1, \dots, q_n) + q'_j$$

Correctness

$$P_j(X) = \underbrace{f_j(w_1, \dots, w_n)}_{=0} X^d + \dots$$

Soundness

$$\Pr[P'_j(\Delta) = P_j(\Delta)] \le \frac{d}{|\mathbb{F}|}$$

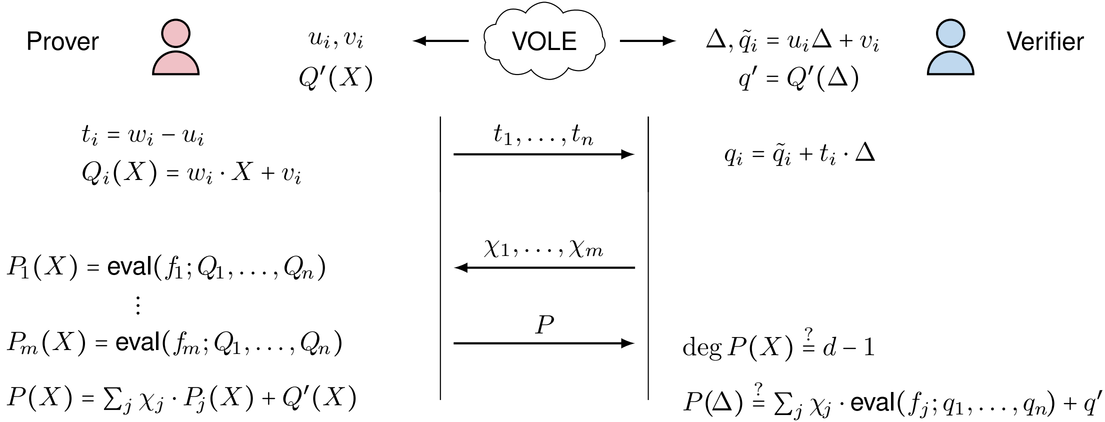
ZKnowledge

Mask via $Q'_j(X)$

Size

?

VOLEitH à la Thibauld



Prover

u_i, v_i

$Q'(X)$

VOLE

$\Delta, \tilde{q}_i = u_i \Delta + v_i$

$q' = Q'(\Delta)$

Verifier

$t_i = w_i - u_i$

$Q_i(X) = w_i \cdot X + v_i$

$\xrightarrow{t_1, \ldots, t_n}$

$q_i = \tilde{q}_i + t_i \cdot \Delta$

$\xleftarrow{\chi_1, \ldots, \chi_m}$

$P_1(X) = \mathsf{eval}(f_1; Q_1, \ldots, Q_n)$

$\vdots$

$P_m(X) = \mathsf{eval}(f_m; Q_1, \ldots, Q_n)$

$P(X) = \sum_j \chi_j \cdot P_j(X) + Q'(X)$

$\xrightarrow{P}$

$\deg P(X) \overset{?}{=} d - 1$

$P(\Delta) \overset{?}{=} \sum_j \chi_j \cdot \mathsf{eval}(f_j; q_1, \ldots, q_n) + q'$

Correctness

$P_j(X) = \underbrace{f_j(w_1, \ldots, w_n)}_{=0} X^d + \ldots$

Soundness

$\Pr[P'_j(\Delta) = P_j(\Delta)] \leq \frac{d}{|\mathbb{F}|}$

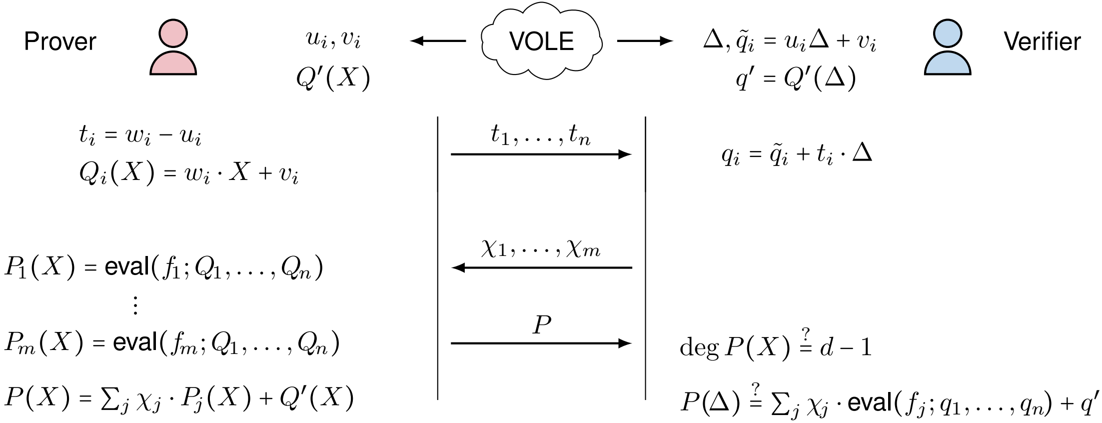
ZKnowledge

Mask via $Q'_j(X)$

Size

?

VOLEitH à la Thibauld



u_i, v_i

$Q'(X)$

$\Delta, \tilde{q}_i = u_i \Delta + v_i$

$q' = Q'(\Delta)$

$t_i = w_i - u_i$

$Q_i(X) = w_i \cdot X + v_i$

$\xrightarrow{t_1, \dots, t_n}$

$q_i = \tilde{q}_i + t_i \cdot \Delta$

$\xleftarrow{\chi_1, \dots, \chi_m}$

$P_1(X) = \text{eval}(f_1; Q_1, \dots, Q_n)$

$\vdots$

$P_m(X) = \text{eval}(f_m; Q_1, \dots, Q_n)$

$\xrightarrow{P}$

$P(X) = \sum_j \chi_j \cdot P_j(X) + Q'(X)$

$\deg P(X) \overset{?}{=} d - 1$

$P(\Delta) \overset{?}{=} \sum_j \chi_j \cdot \text{eval}(f_j; q_1, \dots, q_n) + q'$

Correctness

$P_j(X) = \underbrace{f_j(w_1, ..., w_n)}_{=0} X^d + \dots$

Soundness

$\Pr[P_j'(\Delta) = P_j(\Delta)] \leq \frac{d}{|\mathbb{F}|}$

ZKnowledge

Mask via $Q_j'(X)$

Size

Witness size
+ degree

Polynomial, I Choose You

$f_1, \ldots, f_m$: small witness, low degree

Polynomial, I Choose You

$f_1, \ldots, f_m$: small witness, low degree & hard to invert

Polynomial, I Choose You

$f_1, \dots, f_m$: small witness, low degree & hard to invert

Finding $w_1, \dots, w_n$ s.t.:

$$f_1(w_1, \dots, w_n) = 0$$
$$\vdots$$
$$f_m(w_1, \dots, w_n) = 0$$

← equivalent →

Solving a hard problem

- → Breaking AES
- → Multivariate quadratic

Polynomial, I Choose You

$f_1, \ldots, f_m$: small witness, low degree & hard to invert

Finding $w_1, \ldots, w_n$ s.t.:

$$\begin{aligned} f_1(w_1, \ldots, w_n) &= 0 \\ &\vdots \\ f_m(w_1, \ldots, w_n) &= 0 \end{aligned}$$

← equivalent →

Solving a hard problem

→ Breaking AES
→ Multivariate quadratic
→ Hamming-metric SDP

Polynomial, I Choose You

$f_1, \ldots, f_m$: small witness, low degree & hard to invert

Finding $w_1, \ldots, w_n$ s.t.:

$$\begin{aligned} f_1(w_1, \ldots, w_n) &= 0 \\ &\vdots \\ f_m(w_1, \ldots, w_n) &= 0 \end{aligned}$$

← equivalent →

Solving a hard problem

- → Breaking AES
- → Multivariate quadratic
- → Hamming-metric SDP
- → Restricted SDP

R-SDPs and Where to Find Them

Restricted SDP (R-SDP)

Given: $\mathcal{E} \subset \mathbb{F}$, $\boldsymbol{s} \in \mathbb{F}^{n-k}$ and $\boldsymbol{H} \in \mathbb{F}^{(n-k)\times n}$

R-SDPs and Where to Find Them

Restricted SDP (R-SDP)

Given: $\mathcal{E} \subset \mathbb{F}$, $\boldsymbol{s} \in \mathbb{F}^{n-k}$ and $\boldsymbol{H} \in \mathbb{F}^{(n-k)\times n}$

Find: $\boldsymbol{e} \in \mathcal{E}^n$ s.t. $\boldsymbol{e}\boldsymbol{H}^\top = \boldsymbol{s}$

R-SDPs and Where to Find Them

Restricted SDP (R-SDP)

Given: $\mathcal{E} \subset \mathbb{F}$, $\boldsymbol{s} \in \mathbb{F}^{n-k}$ and $\boldsymbol{H} \in \mathbb{F}^{(n-k)\times n}$

Find: $\boldsymbol{e} \in \mathcal{E}^n$ s.t. $\boldsymbol{e}\boldsymbol{H}^\top = \boldsymbol{s}$

CROSS:

→ $\mathbb{F}_{127}, \mathcal{E} = \{1, 2, 4, \dots, 64\}$

R-SDPs and Where to Find Them

Restricted SDP (R-SDP)

Given: $\mathcal{E} \subset \mathbb{F}$, $\boldsymbol{s} \in \mathbb{F}^{n-k}$ and $\boldsymbol{H} \in \mathbb{F}^{(n-k)\times n}$

Find: $\boldsymbol{e} \in \mathcal{E}^n$ s.t. $\boldsymbol{e}\boldsymbol{H}^\top = \boldsymbol{s}$

CROSS:

→ $\mathbb{F}_{127}$, $\mathcal{E} = \{1, 2, 4, \dots, 64\}$

WAVE-like:

→ $\mathbb{F}_3$, $\mathcal{E} = \{1, 2\}$

R-SDPs and Where to Find Them

Restricted SDP (R-SDP)

Given: $\mathcal{E} \subset \mathbb{F}$, $\boldsymbol{s} \in \mathbb{F}^{n-k}$ and $\boldsymbol{H} \in \mathbb{F}^{(n-k)\times n}$

Find: $\boldsymbol{e} \in \mathcal{E}^n$ s.t. $\boldsymbol{e}\boldsymbol{H}^\top = \boldsymbol{s}$

CROSS:

- ➔ $\mathbb{F}_{127}$, $\mathcal{E} = \{1, 2, 4, \ldots, 64\}$
- ➔ CVE-like ID protocol

WAVE-like:

- ➔ $\mathbb{F}_3$, $\mathcal{E} = \{1, 2\}$
- ➔ hash-&-sign

no MPCitH

R-SDPs and Where to Find Them

Restricted SDP (R-SDP)

Given: $\mathcal{E} \subset \mathbb{F}$, $\boldsymbol{s} \in \mathbb{F}^{n-k}$ and $\boldsymbol{H} \in \mathbb{F}^{(n-k)\times n}$

Find: $\boldsymbol{e} \in \mathcal{E}^n$ s.t. $\boldsymbol{e}\boldsymbol{H}^\top = \boldsymbol{s}$

CROSS:

- → $\mathbb{F}_{127}$, $\mathcal{E} = \{1, 2, 4, \dots, 64\}$
- → CVE-like ID protocol

WAVE-like:

- → $\mathbb{F}_3$, $\mathcal{E} = \{1, 2\}$
- → hash-&-sign

no MPCitH,
until now ;)

Modeling R-SDP

Restricted SDP (R-SDP)

Given: $\mathcal{E} \subset \mathbb{F}$, $\boldsymbol{s} \in \mathbb{F}^{n-k}$ and $\boldsymbol{H} \in \mathbb{F}^{(n-k)\times n}$

Find: $\boldsymbol{e} \in \mathcal{E}^n$ s.t. $\boldsymbol{e}\boldsymbol{H}^\top = \boldsymbol{s}$

Modeling R-SDP

Restricted SDP (R-SDP)

Given: $\mathcal{E} \subset \mathbb{F}$, $\boldsymbol{s} \in \mathbb{F}^{n-k}$ and $\boldsymbol{H} \in \mathbb{F}^{(n-k)\times n}$

Find: $\boldsymbol{e} \in \mathcal{E}^n$ s.t. $\boldsymbol{e}\boldsymbol{H}^\top = \boldsymbol{s}$

Restriction:

$$f_i = \prod_{\alpha\in\mathcal{E}}(x_i - \alpha),\ i \in [n]$$

Parity checks:

$$f_{n+i} = s_i - \langle(x_1,\ldots,x_n),\boldsymbol{h}_i\rangle,\ i \in [n-k]$$

Modeling R-SDP

Restricted SDP (R-SDP)

Given: $\mathcal{E} \subset \mathbb{F}$, $\boldsymbol{s} \in \mathbb{F}^{n-k}$ and $\boldsymbol{H} \in \mathbb{F}^{(n-k)\times n}$

Find: $\boldsymbol{e} \in \mathcal{E}^n$ s.t. $\boldsymbol{e}\boldsymbol{H}^\top = \boldsymbol{s}$

Restriction:

$$f_i = \prod_{\alpha\in\mathcal{E}}(x_i - \alpha),\ i \in [n]$$

Parity checks:

$$f_{n+i} = s_i - \langle (x_1, \dots, x_n), \boldsymbol{h}_i \rangle,\ i \in [n-k]$$

length n,
degree $|\mathcal{E}|$

Modeling R-SDP

Restricted SDP (R-SDP)

Given: $\mathcal{E} \subset \mathbb{F}$, $\boldsymbol{s} \in \mathbb{F}^{n-k}$ and $\boldsymbol{A} \in \mathbb{F}^{(n-k)\times k}$

Find: $\boldsymbol{e} \in \mathcal{E}^n$ s.t. $\boldsymbol{e}(\boldsymbol{A} \mid \boldsymbol{1})^\top = \boldsymbol{s}$

Restriction:

$$f_i = \textstyle\prod_{\alpha\in\mathcal{E}}(x_i - \alpha),\ i \in [n]$$

Parity checks:

$$f_{n+i} = s_i - \langle (x_1, \ldots, x_n), \boldsymbol{h}_i \rangle,\ i \in [n-k]$$

length n,
degree $|\mathcal{E}|$

Modeling R-SDP

Restricted SDP (R-SDP)

Given: $\mathcal{E} \subset \mathbb{F}$, $\boldsymbol{s} \in \mathbb{F}^{n-k}$ and $\boldsymbol{A} \in \mathbb{F}^{(n-k)\times k}$

Find: $\boldsymbol{e}' \in \mathcal{E}^k$ s.t. $\boldsymbol{s} - \boldsymbol{e}'\boldsymbol{A}^\top \in \mathcal{E}^{n-k}$

Restriction:

$$f_i = \prod_{\alpha\in\mathcal{E}}(x_i - \alpha),\ i \in [n]$$

Parity checks:

$$f_{n+i} = s_i - \langle(x_1, \dots, x_n), \boldsymbol{h}_i\rangle,\ i \in [n-k]$$

length n,
degree $|\mathcal{E}|$

Modeling R-SDP

Restricted SDP (R-SDP)

Given: $\mathcal{E} \subset \mathbb{F}$, $\boldsymbol{s} \in \mathbb{F}^{n-k}$ and $\boldsymbol{A} \in \mathbb{F}^{(n-k)\times k}$

Find: $\boldsymbol{e}' \in \mathcal{E}^k$ s.t. $\boldsymbol{s} - \boldsymbol{e}'\boldsymbol{A}^\top \in \mathcal{E}^{n-k}$

Restriction:

$$f_i = \prod_{\alpha\in\mathcal{E}}(x_i - \alpha),\ i \in [k]$$
$$f_{k+i} = \prod_{\alpha\in\mathcal{E}}(x_i' - \alpha),\ i \in [n-k]$$

Parity checks:

$$f_{n+i} = s_i - \langle(x_1,\dots,x_n),\boldsymbol{h}_i\rangle,\ i \in [n-k]$$
$$x_i' = s_i - \langle(x_1,\dots,x_k),\boldsymbol{a}_i\rangle,\ i \in [n-k]$$

length n,
degree $|\mathcal{E}|$

Modeling R-SDP

Restricted SDP (R-SDP)

Given: $\mathcal{E} \subset \mathbb{F}$, $\boldsymbol{s} \in \mathbb{F}^{n-k}$ and $\boldsymbol{A} \in \mathbb{F}^{(n-k)\times k}$

Find: $\boldsymbol{e}' \in \mathcal{E}^k$ s.t. $\boldsymbol{s} - \boldsymbol{e}'\boldsymbol{A}^\top \in \mathcal{E}^{n-k}$

Restriction:

$$\begin{aligned} f_i &= \textstyle\prod_{\alpha\in\mathcal{E}}(x_i - \alpha),\ i \in [k] \\ f_{k+i} &= \textstyle\prod_{\alpha\in\mathcal{E}}(x_i' - \alpha),\ i \in [n-k] \end{aligned}$$

Parity checks:

$$\begin{aligned} f_{n+i} &= s_i - \langle (x_1, \ldots, x_n), \boldsymbol{h}_i \rangle,\ i \in [n-k] \\ x_i' &= s_i - \langle (x_1, \ldots, x_k), \boldsymbol{a}_i \rangle,\ i \in [n-k] \end{aligned}$$

length k,
degree $|\mathcal{E}|$

Modeling R-SDP

Restricted SDP (R-SDP)

Given: $\mathcal{E} \subset \mathbb{F}$, $\boldsymbol{s} \in \mathbb{F}^{n-k}$ and $\boldsymbol{A} \in \mathbb{F}^{(n-k)\times k}$

Find: $\boldsymbol{e}' \in \mathcal{E}^k$ s.t. $\boldsymbol{s} - \boldsymbol{e}'\boldsymbol{A}^\top \in \mathcal{E}^{n-k}$

Restriction:

$$\begin{aligned} f_i &= \textstyle\prod_{\alpha\in\mathcal{E}}(x_i - \alpha),\ i \in [k] \\ f_{k+i} &= \textstyle\prod_{\alpha\in\mathcal{E}}(x_i' - \alpha),\ i \in [n-k] \end{aligned}$$

Parity checks:

$$\begin{aligned} f_{n+i} &= s_i - \langle (x_1, \dots, x_n), \boldsymbol{h}_i \rangle,\ i \in [n-k] \\ x_i' &= s_i - \langle (x_1, \dots, x_k), \boldsymbol{a}_i \rangle,\ i \in [n-k] \end{aligned}$$

length $k+n$,
degree $|\mathcal{E}|/2$

↔

length k,
degree $|\mathcal{E}|$

Modeling R-SDP

Restricted SDP (R-SDP)

Given: $\mathcal{E} \subset \mathbb{F}$, $\boldsymbol{s} \in \mathbb{F}^{n-k}$ and $\boldsymbol{A} \in \mathbb{F}^{(n-k)\times k}$

Find: $\boldsymbol{e}' \in \mathcal{E}^k$ s.t. $\boldsymbol{s} - \boldsymbol{e}'\boldsymbol{A}^\top \in \mathcal{E}^{n-k}$

Restriction:

$$\begin{aligned} f_i &= \textstyle\prod_{\alpha\in\mathcal{E}}(x_i - \alpha),\ i \in [k] \\ f_{k+i} &= \textstyle\prod_{\alpha\in\mathcal{E}}(x_i' - \alpha),\ i \in [n-k] \end{aligned}$$

Parity checks:

$$\begin{aligned} f_{n+i} &= s_i - \langle (x_1, \ldots, x_n), \boldsymbol{h}_i \rangle,\ i \in [n-k] \\ x_i' &= s_i - \langle (x_1, \ldots, x_k), \boldsymbol{a}_i \rangle,\ i \in [n-k] \end{aligned}$$

length $k+n$, degree $|\mathcal{E}|/2$ ↔ length k, degree $|\mathcal{E}|$ ↔ length $n/2$, degree $|\mathcal{E}|^2$

Numbers Don't Lie

Assumption	R-SDP parameters				Size [kB]
	n	k	p	$\lvert\mathcal{E}\rvert$	
WAVE-like	518	191	3	2	~2.9
CROSS	127	76	127	7	~4.9

- Rémi Bricout et al., Ternary Syndrome Decoding with Large Weight
- Marco Baldi et al., CROSS: Codes and Restricted Objects Signature Scheme

Numbers Don’t Lie

Assumption	R-SDP parameters				Size [kB]
	n	k	p	$\vert\mathcal{E}\vert$	
WAVE-like	518	191	3	2	~2.9
CROSS	127	76	127	7	~4.9

- Rémi Bricout et al., Ternary Syndrome Decoding with Large Weight
- Marco Baldi et al., CROSS: Codes and Restricted Objects Signature Scheme
- Vu Nguyen et al., A BKW-Style Solver for the Restricted Decoding Problem

Numbers Don’t Lie

Assumption	R-SDP parameters				Size [kB]
	n	k	p	$\vert\mathcal{E}\vert$	
WAVE-like	518	191	3	2	~2.9
CROSS	127	76	127	7	~4.9
Regular SDP					~3.7
Rank-SDP					~2.9
PKP					~3.9

- Rémi Bricout et al., Ternary Syndrome Decoding with Large Weight
- Marco Baldi et al., CROSS: Codes and Restricted Objects Signature Scheme
- Vu Nguyen et al., A BKW-Style Solver for the Restricted Decoding Problem

Conclusion

VOLEitH-based Signatures from R-SDP

- ☺ Recap of VOLEitH & R-SDP
- ☺ Simple Modeling of R-SDP
- ☺ Competitive performance

Conclusion

VOLEitH-based Signatures from R-SDP

- ☺ Recap of VOLEitH & R-SDP
- ☺ Simple Modeling of R-SDP
- ☺ Competitive performance

Research questions:

- ? TCitH Merkle trees or other optimizations?
- ? Concrete hardness of generic R-SDP

Conclusion

VOLEitH-based Signatures from R-SDP

- ☺ Recap of VOLEitH & R-SDP
- ☺ Simple Modeling of R-SDP
- ☺ Competitive performance

Research questions:

- ? TCitH Merkle trees or other optimizations?
- ? Concrete hardness of generic R-SDP

Thank you!

Questions?