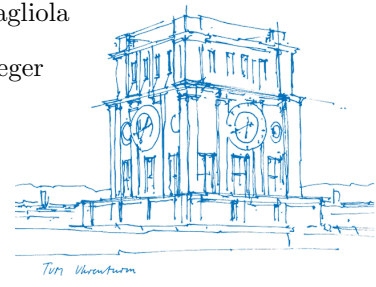
TCitH- & VOLEitH-based Signatures from Restricted Decoding

Sebastian Bitzer Michele Battagliola

Antonia Wachter-Zeh Violetta Weger

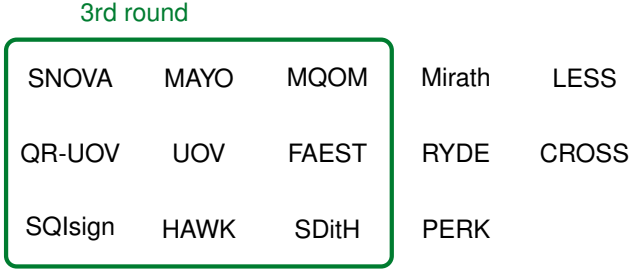
ISIT'26



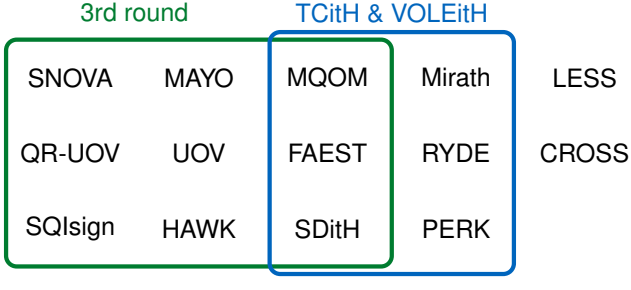
NIST's Additional Signatures: Round 2 and 3

SNOVA	MAYO	MQOM	Mirath	LESS
QR-UOV	UOV	FAEST	RYDE	CROSS
SQIsign	HAWK	SDitH	PERK	

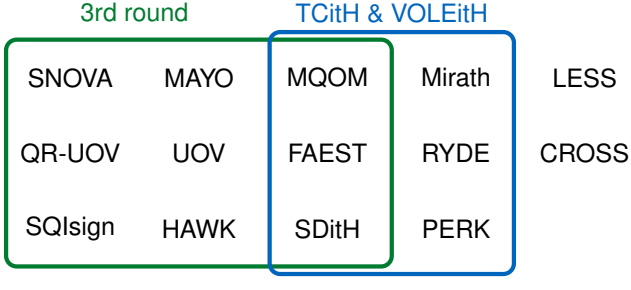
NIST's Additional Signatures: Round 2 and 3



NIST's Additional Signatures: Round 2 and 3



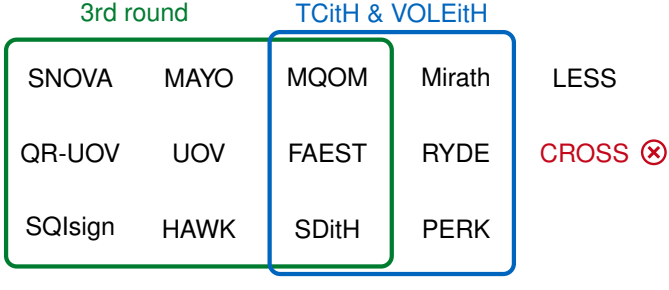
NIST's Additional Signatures: Round 2 and 3



Introduction to TCitH & VOLEitH

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

NIST's Additional Signatures: Round 2 and 3



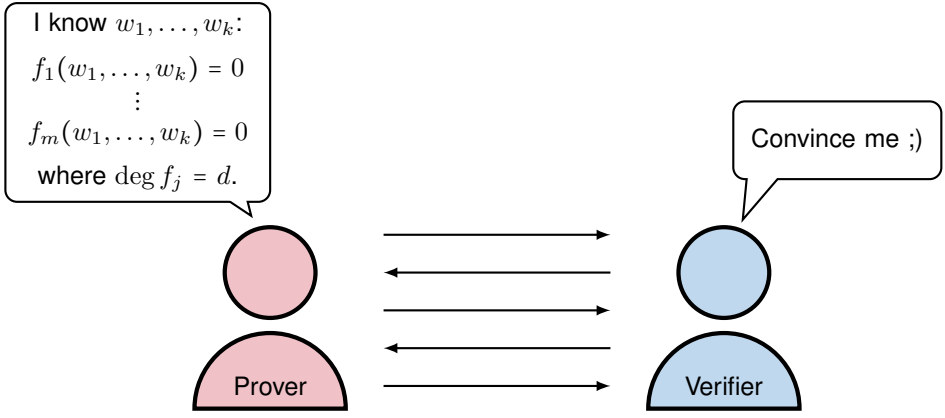
Introduction to TCitH & VOLEitH

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

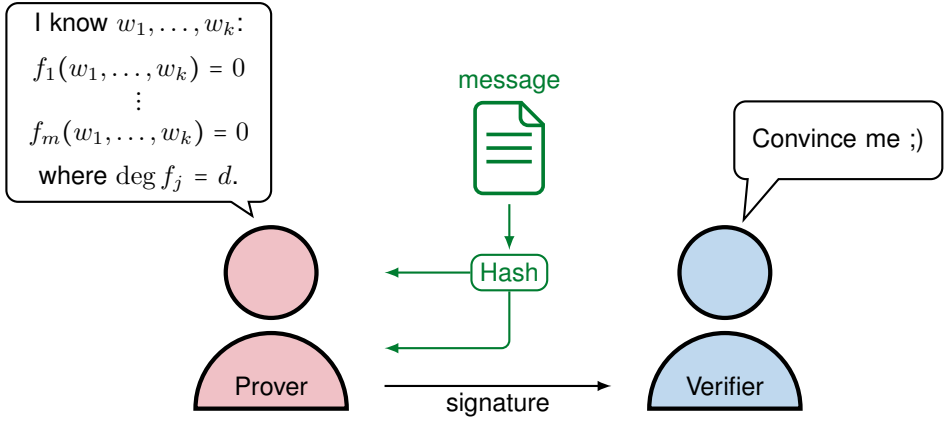
$\mathcal{E}$-SDP-based signatures

- ⊗ Simple polynomial modeling
- ⊗ Competitive sizes

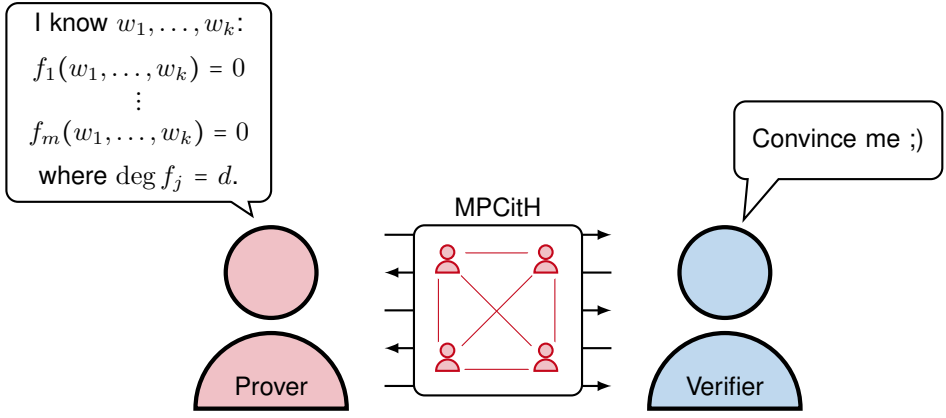
Signatures from Identification Schemes



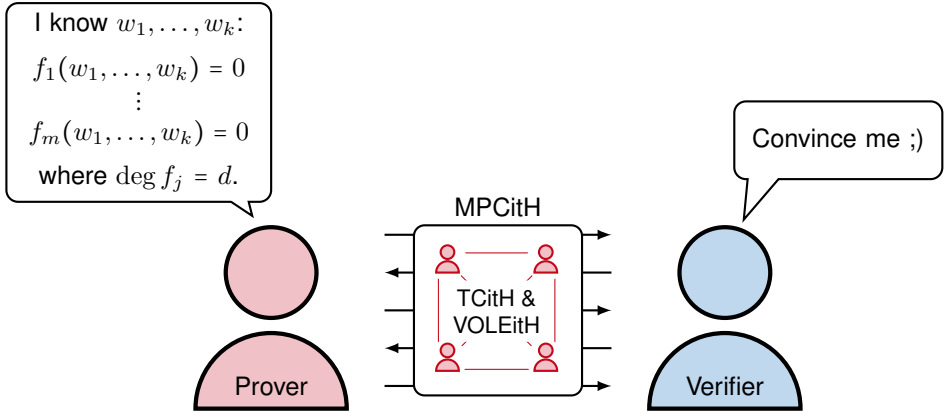
Signatures from Identification Schemes



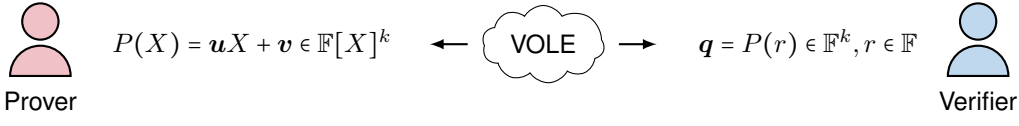
Signatures from Identification Schemes



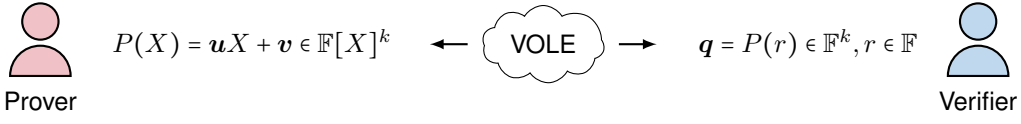
Signatures from Identification Schemes



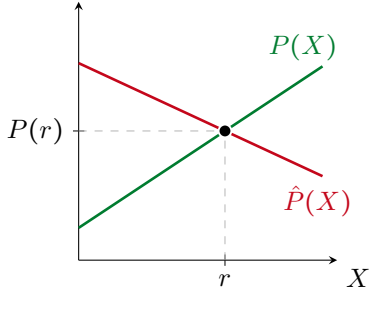
Vector Oblivious Linear Evaluation



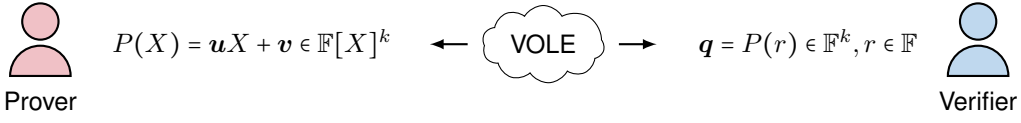
Vector Oblivious Linear Evaluation



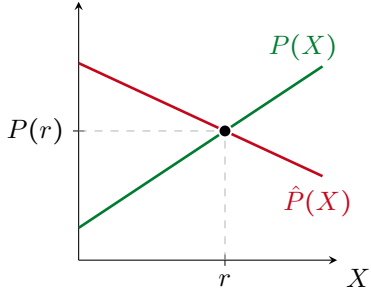
➔ Hiding & binding commitment to $\boldsymbol{u}$



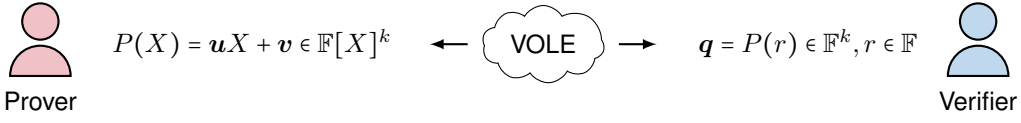
Vector Oblivious Linear Evaluation



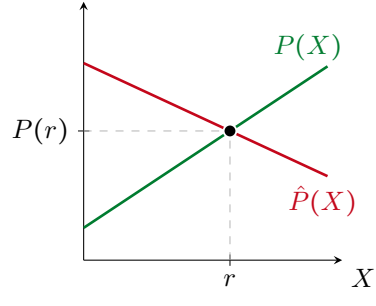
- Hiding & binding commitment to $\boldsymbol{u}$
- Add: $(P_1 + P_2)(r) = q_1 + q_2$



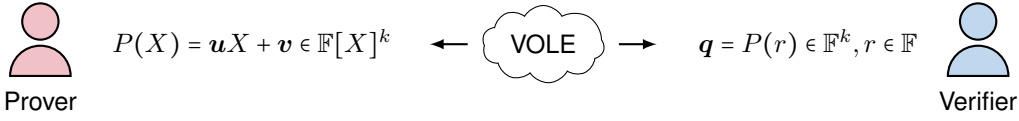
Vector Oblivious Linear Evaluation



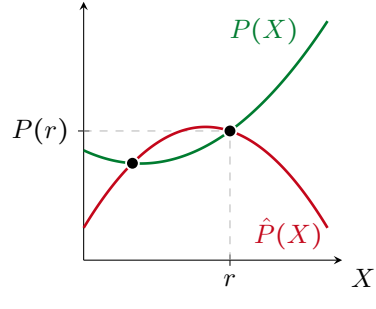
- Hiding & binding commitment to $\boldsymbol{u}$
- Add: $(P_1 + P_2)(r) = q_1 + q_2$
- Multiply: $(P_1 \cdot P_2)(r) = q_1 \cdot q_2$



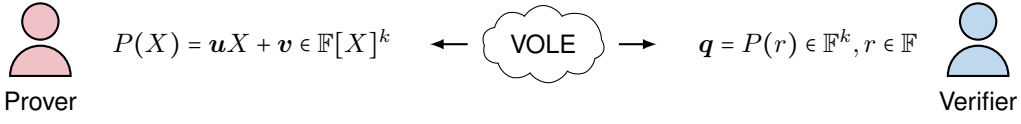
Vector Oblivious Linear Evaluation



- Hiding & binding commitment to $\boldsymbol{u}$
- Add: $(P_1 + P_2)(r) = q_1 + q_2$
- Multiply: $(P_1 \cdot P_2)(r) = q_1 \cdot q_2$

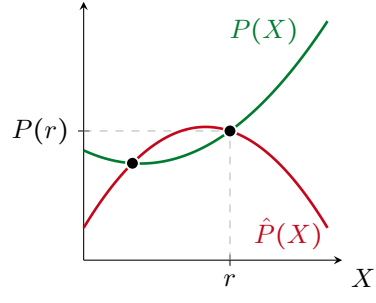


Vector Oblivious Linear Evaluation



- Hiding & binding commitment to $\boldsymbol{u}$
- Add: $(P_1 + P_2)(r) = q_1 + q_2$
- Multiply: $(P_1 \cdot P_2)(r) = q_1 \cdot q_2$

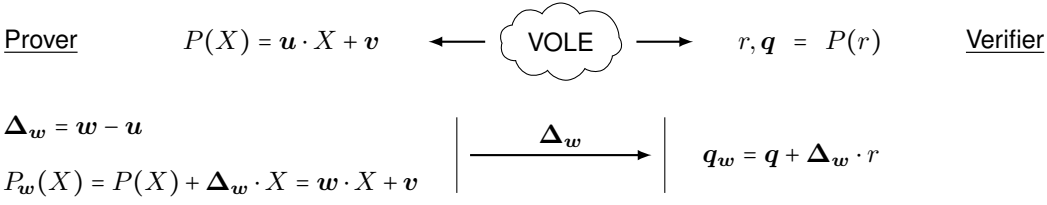
} evaluate $f_1, \ldots, f_m$



TCitH & VOLEitH Frameworks



TCitH & VOLEitH Frameworks



TCitH & VOLEitH Frameworks



$\boldsymbol{\Delta_w} = \boldsymbol{w} - \boldsymbol{u}$

$P_{\boldsymbol{w}}(X) = P(X) + \boldsymbol{\Delta_w} \cdot X = \boldsymbol{w} \cdot X + \boldsymbol{v}$

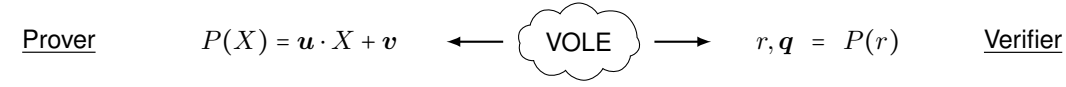
$Q_j(X) = \mathsf{eval}(f_j; P_{\boldsymbol{w}}(X)) \ \forall j \in [m]$

$\boldsymbol{\Delta_w}$ →

$\boldsymbol{q_w} = \boldsymbol{q} + \boldsymbol{\Delta_w} \cdot r$

$Q_1, \ldots, Q_m$ →

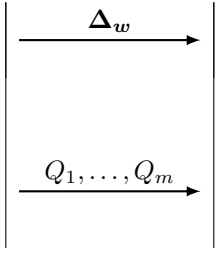
TCitH & VOLEitH Frameworks



$\boldsymbol{\Delta_w} = \boldsymbol{w} - \boldsymbol{u}$

$P_{\boldsymbol{w}}(X) = P(X) + \boldsymbol{\Delta_w} \cdot X = \boldsymbol{w} \cdot X + \boldsymbol{v}$

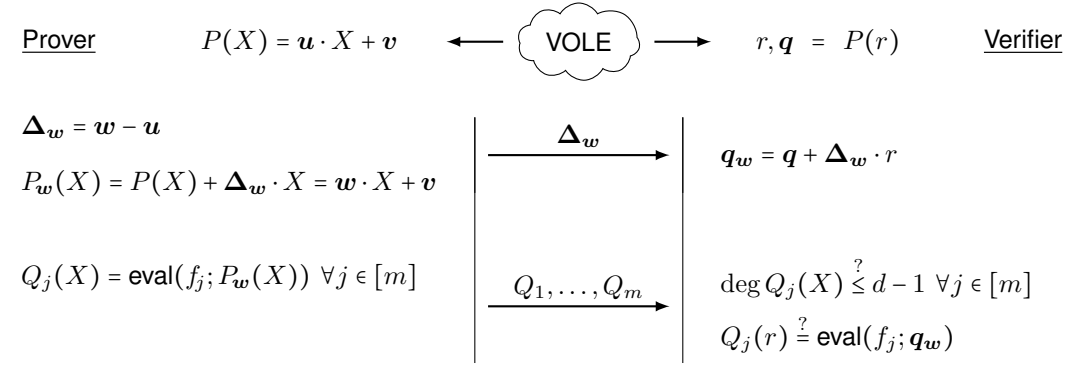
$Q_j(X) = \mathsf{eval}(f_j; P_{\boldsymbol{w}}(X)) \ \forall j \in [m]$



$\boldsymbol{q_w} = \boldsymbol{q} + \boldsymbol{\Delta_w} \cdot r$

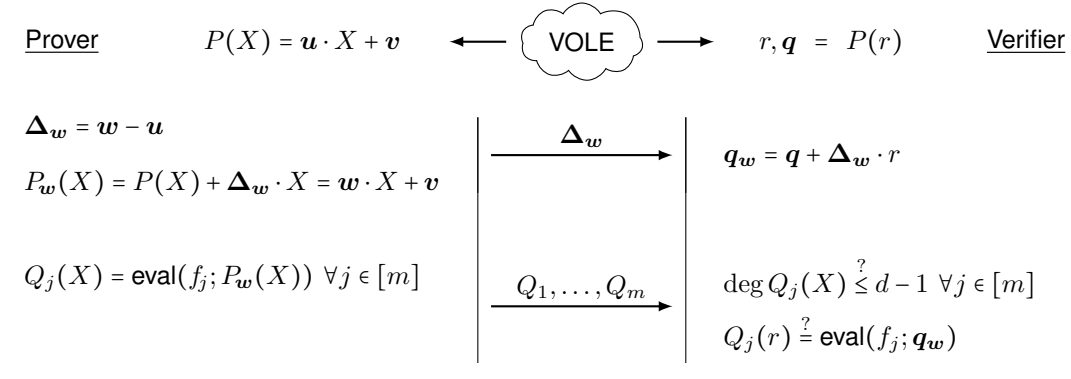
$$Q_j(X) = \underbrace{f_j(\boldsymbol{w})}_{=0} X^d + \ldots$$

TCitH & VOLEitH Frameworks



$$Q_j(X) = \underbrace{f_j(\boldsymbol{w})}_{=0} X^d + \ldots$$

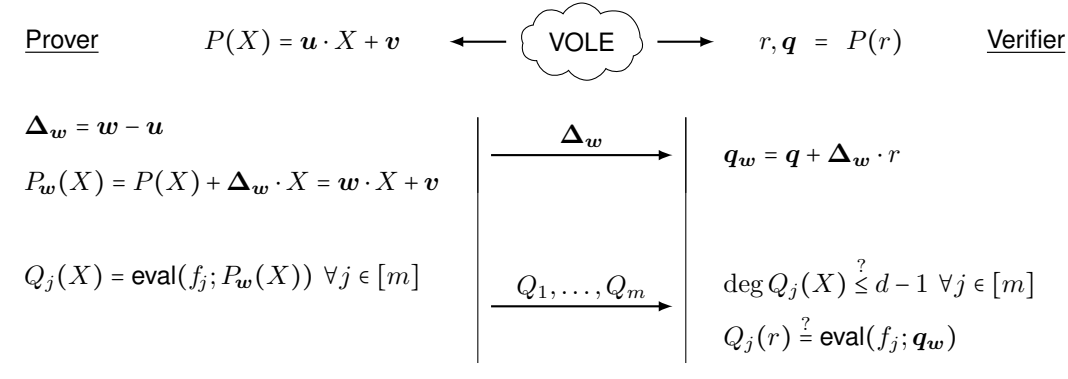
TCitH & VOLEitH Frameworks



Correctness

$$Q_j(X) = \underbrace{f_j(\boldsymbol{w})}_{=0} X^d + \ldots$$

TCitH & VOLEitH Frameworks



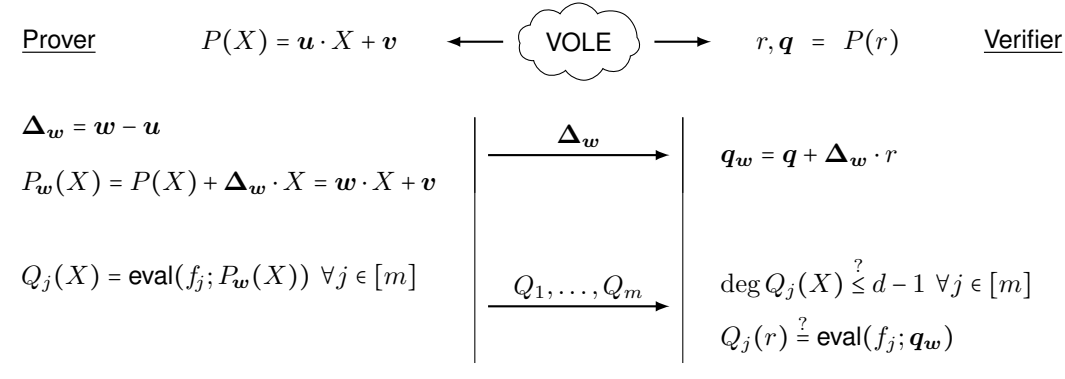
Correctness

$$Q_j(X) = \underbrace{f_j(\boldsymbol{w})}_{=0} X^d + \ldots$$

Soundness

?

TCitH & VOLEitH Frameworks



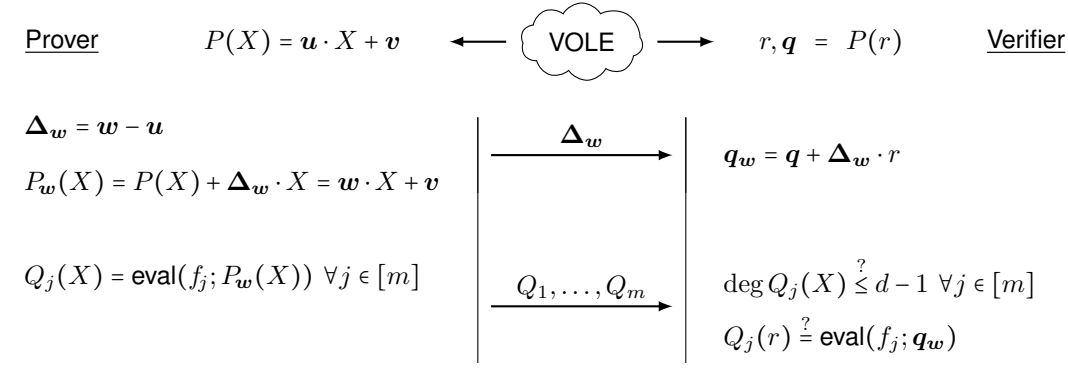
Correctness

$$Q_j(X) = \underbrace{f_j(\boldsymbol{w})}_{=0} X^d + \ldots$$

Soundness

$$\Pr[\hat{Q}_j(r) = Q_j(r)] \leq \frac{d}{|\mathbb{F}|}$$

TCitH & VOLEitH Frameworks



Correctness

$$Q_j(X) = \underbrace{f_j(\boldsymbol{w})}_{=0} X^d + \ldots$$

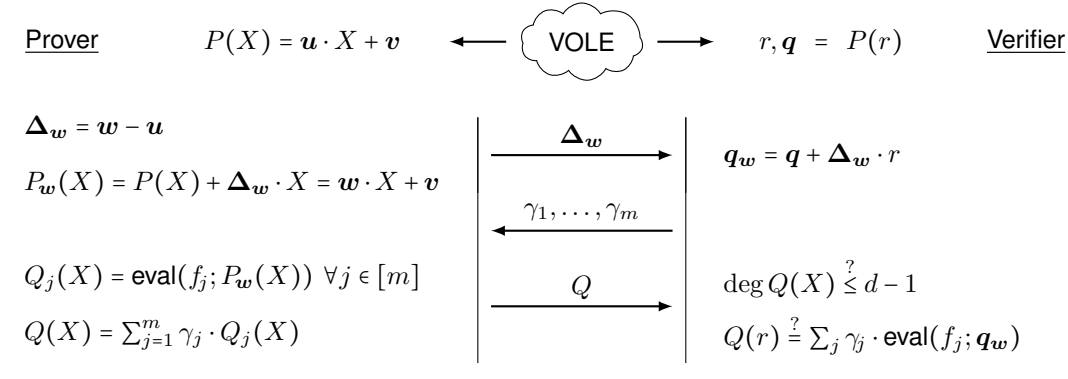
Soundness

$$\Pr[\hat{Q}_j(r) = Q_j(r)] \leq \frac{d}{|\mathbb{F}|}$$

Size

?

TCitH & VOLEitH Frameworks



Correctness

$$Q_j(X) = \underbrace{f_j(\boldsymbol{w})}_{=0} X^d + \ldots$$

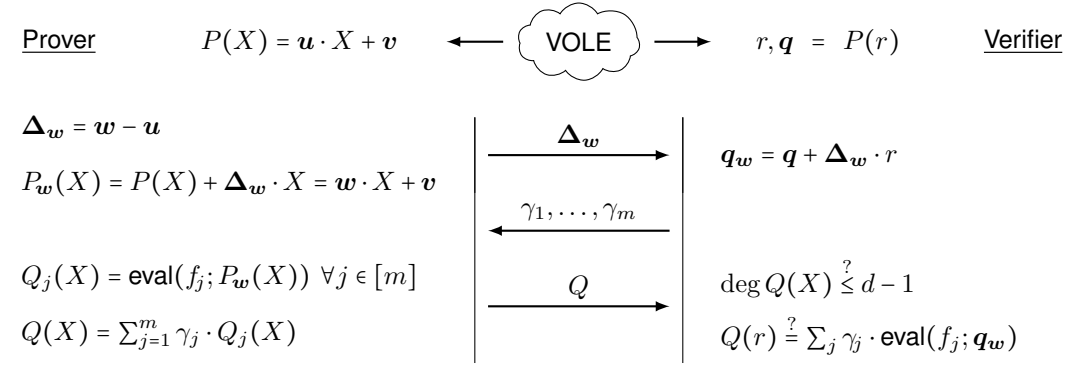
Soundness

$$\Pr[\hat{Q}_j(r) = Q_j(r)] \leq \tfrac{d}{|\mathbb{F}|}$$

Size

?

TCitH & VOLEitH Frameworks



Correctness

$$Q_j(X) = \underbrace{f_j(\boldsymbol{w})}_{=0} X^d + \ldots$$

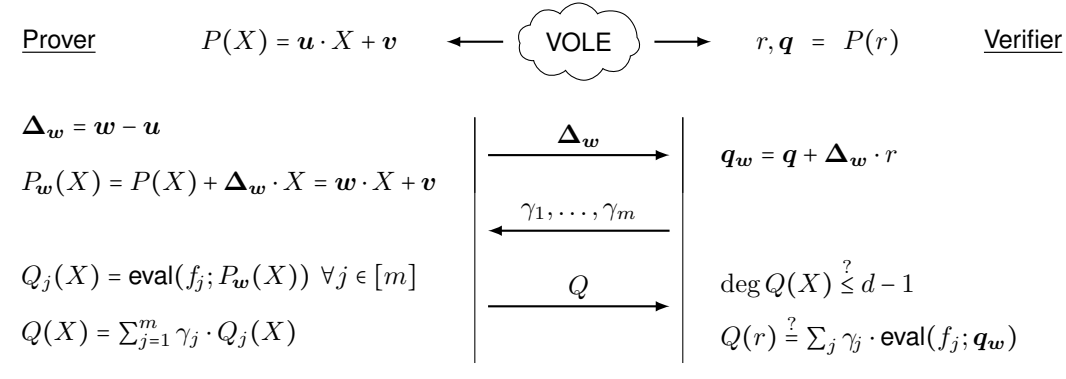
Soundness

$$\Pr[\hat{Q}_j(r) = Q_j(r)] \leq \tfrac{d}{|\mathbb{F}|}$$

Size

Witness size + degree

TCitH & VOLEitH Frameworks



Correctness

$Q_j(X) = \underbrace{f_j(\boldsymbol{w})}_{=0} X^d + \ldots$

Soundness

$\Pr[\hat{Q}_j(r) = Q_j(r)] \leq \frac{d}{|\mathbb{F}|}$

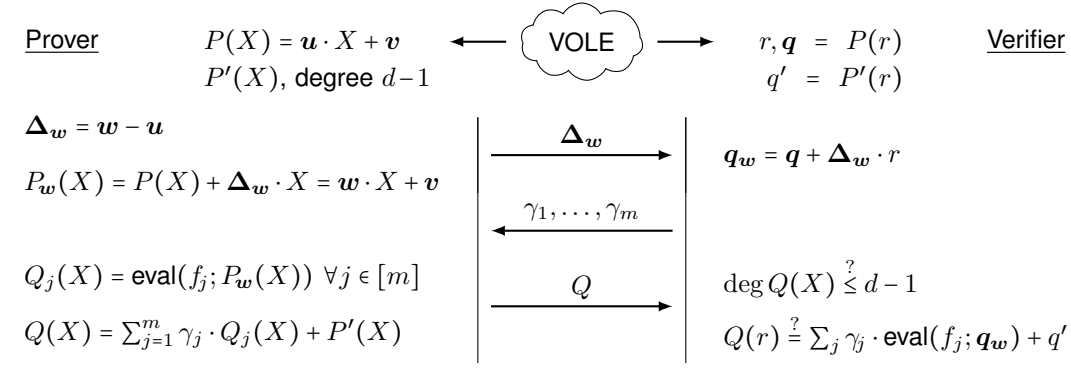
Size

Witness size + degree

Zero-Knowledge

?

TCitH & VOLEitH Frameworks



Correctness

$Q_j(X) = \underbrace{f_j(\boldsymbol{w})}_{=0} X^d + \ldots$

Soundness

$\Pr[\hat{Q}_j(r) = Q_j(r)] \leq \frac{d}{|\mathbb{F}|}$

Size

Witness size + degree

Zero-Knowledge

Mask via $P'(X)$

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

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

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

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

← 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 $w_1, \ldots, w_k$ s.t.:

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

← 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 $w_1, \ldots, w_k$ s.t.:

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

← equivalent →

Solving a hard problem

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



Restricted SDP ($\mathcal{E}$-SDP)

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

$\mathcal{E}$-SDPs and Where to Find Them

Restricted SDP ($\mathcal{E}$-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. $\boldsymbol{e}\boldsymbol{H}^\top = \boldsymbol{s}$

$\mathcal{E}$-SDPs and Where to Find Them

Restricted SDP ($\mathcal{E}$-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:

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

$\mathcal{E}$-SDPs and Where to Find Them

Restricted SDP ($\mathcal{E}$-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:

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

WAVE-like:

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

$\mathcal{E}$-SDPs and Where to Find Them

Restricted SDP ($\mathcal{E}$-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

$\mathcal{E}$-SDPs and Where to Find Them

Restricted SDP ($\mathcal{E}$-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,
until now ;)

Modeling $\mathcal{E}$-SDP

Restricted SDP ($\mathcal{E}$-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 $\mathcal{E}$-SDP

Restricted SDP ($\mathcal{E}$-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 $\mathcal{E}$-SDP

Restricted SDP ($\mathcal{E}$-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:

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

witness size n,
degree $|\mathcal{E}|$

Modeling $\mathcal{E}$-SDP

Restricted SDP ($\mathcal{E}$-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:

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

Parity checks:

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

witness size n,
degree $|\mathcal{E}|$

Modeling $\mathcal{E}$-SDP

Restricted SDP ($\mathcal{E}$-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. $\boldsymbol{e}'' = \boldsymbol{s} - \boldsymbol{e}'\boldsymbol{A}^\top \in \mathcal{E}^{n-k}$

Restriction:

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

Parity checks:

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

witness size n,
degree $|\mathcal{E}|$

Modeling $\mathcal{E}$-SDP

Restricted SDP ($\mathcal{E}$-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. $\boldsymbol{e}'' = \boldsymbol{s} - \boldsymbol{e}'\boldsymbol{A}^\top \in \mathcal{E}^{n-k}$

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:

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

witness size n,
degree $|\mathcal{E}|$

Modeling $\mathcal{E}$-SDP

Restricted SDP ($\mathcal{E}$-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. $\boldsymbol{e}'' = \boldsymbol{s} - \boldsymbol{e}'\boldsymbol{A}^\top \in \mathcal{E}^{n-k}$

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:

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

witness size n, degree $|\mathcal{E}|$ → witness size k, degree $|\mathcal{E}|$

Comparison with NIST Candidates

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

	parameters				size [kB]	
	n	k	p	$\lvert\mathcal{E}\rvert$	TCitH	VOLEitH
CROSS-like	127	76	127	7	5.5	4.4
WAVE-like	518	191	3	2	3.1	3.0

Comparison with NIST Candidates

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

	parameters				size [kB]	
	n	k	p	$\lvert\mathcal{E}\rvert$	TCitH	VOLEitH
CROSS-like	127	76	127	7	5.5	4.4
WAVE-like	518	191	3	2	3.1	3.0

	CROSS
size [kB]	9.0

Comparison with NIST Candidates

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

	parameters				size [kB]	
	n	k	p	$\lvert\mathcal{E}\rvert$	TCitH	VOLEitH
CROSS-like	127	76	127	7	5.5	4.4
WAVE-like	518	191	3	2	3.1	3.0

	CROSS	SDitH	PERK	RYDE	MQOM
size [kB]	9.0	3.7	3.5	3.1	2.8

Conclusion

TCitH- & VOLEitH-based signatures from $\mathcal{E}$-SDP

- ☺ Recap of TCitH & VOLEitH
- ☺ Simple modeling of $\mathcal{E}$-SDP
- ☺ Competitive signature sizes

Conclusion

TCitH- & VOLEitH-based signatures from $\mathcal{E}$-SDP

- ☺ Recap of TCitH & VOLEitH
- ☺ Simple modeling of $\mathcal{E}$-SDP
- ☺ Competitive signature sizes

Research question:

- ? Study concrete hardness of $\mathcal{E}$-SDP

Conclusion

TCitH- & VOLEitH-based signatures from $\mathcal{E}$-SDP

- ☺ Recap of TCitH & VOLEitH
- ☺ Simple modeling of $\mathcal{E}$-SDP
- ☺ Competitive signature sizes

Research question:

- ? Study concrete hardness of $\mathcal{E}$-SDP

Thank you!

Questions?

