Building MPCitH-based Signatures from MQ, MinRank, Rank SD and PKP

Thibault Feneuil[1,2]

1. CryptoExperts, Paris, France

2. Sorbonne Université, CNRS, INRIA, Institut de Mathématiques de Jussieu-Paris Rive Gauche, Ouragan, Paris, France

INRIA. *November 21, 2022.*

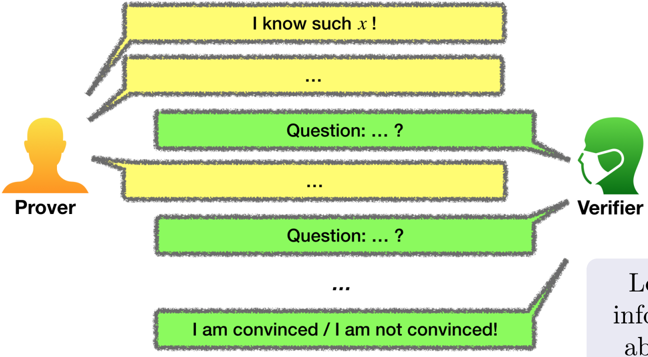
Table of Contents

Zero-Knowledge Proofs of Knowledge

Let have a circuit C and an output y.
Problem: find x such that $C(x) = y$.

Zero-Knowledge Proofs of Knowledge

Let have a circuit C and an output y.
Problem: find x such that $C(x) = y$.



Learn no information about the secret x.

MPC-in-the-Head Paradigm

MPC-in-the-Head Paradigm

- Generic technique to build *zero-knowledge protocols* using *multi-party computation*.
- Introduced in 2007 by:

  [IKOS07] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. *Zero-knowledge from secure multiparty computation.* STOC 2007.

- Popularized in 2016 by *Picnic*, a former candidate of the NIST Post-Quantum Cryptography Standardization.

Sharing of the secret

The secret x satisfies

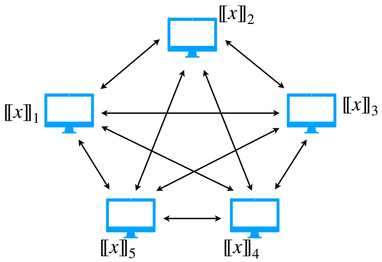
$$y = C(x).$$

We share it in N parts:

$$x = [\![x]\!]_1 + [\![x]\!]_2 + \ldots + [\![x]\!]_{N-1} + [\![x]\!]_N.$$

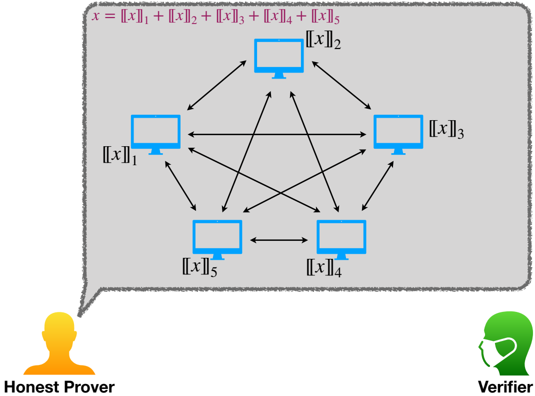
MPC-in-the-Head Paradigm

$x = [\![x]\!]_1 + [\![x]\!]_2 + [\![x]\!]_3 + [\![x]\!]_4 + [\![x]\!]_5$

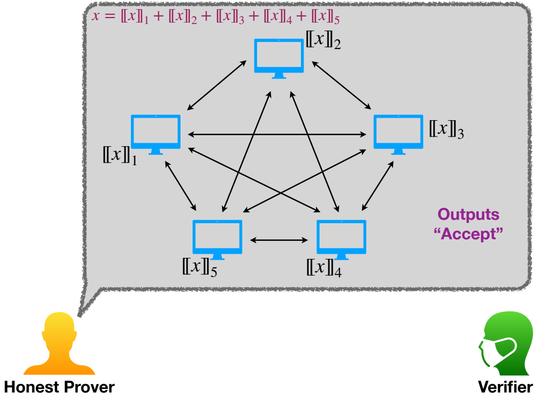


The multi-party computation outputs
- *Accept* if x satisfies $y = C(x)$,
- *Reject* otherwise.

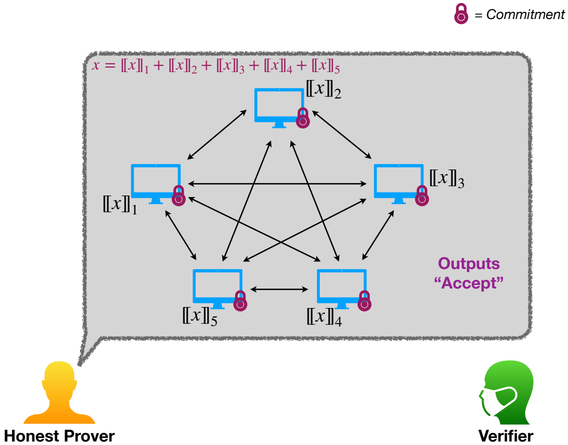
MPC-in-the-Head Paradigm



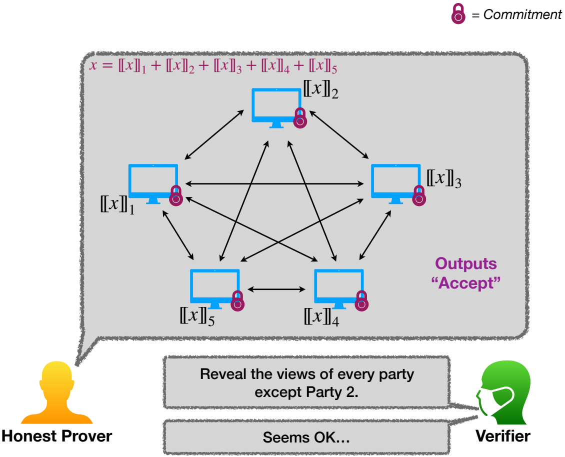
MPC-in-the-Head Paradigm



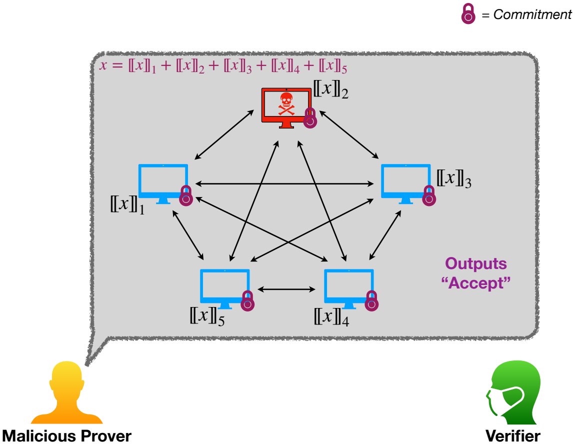
MPC-in-the-Head Paradigm



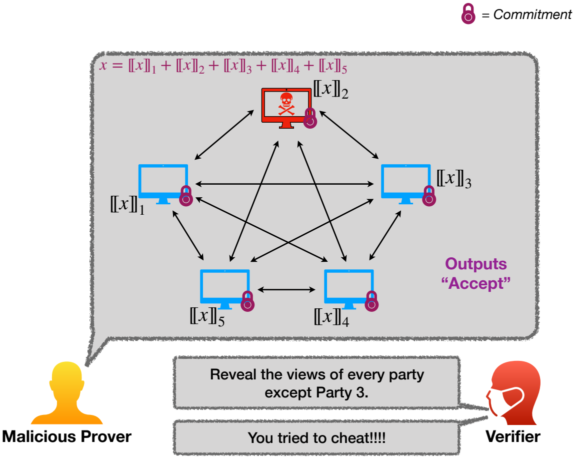
MPC-in-the-Head Paradigm



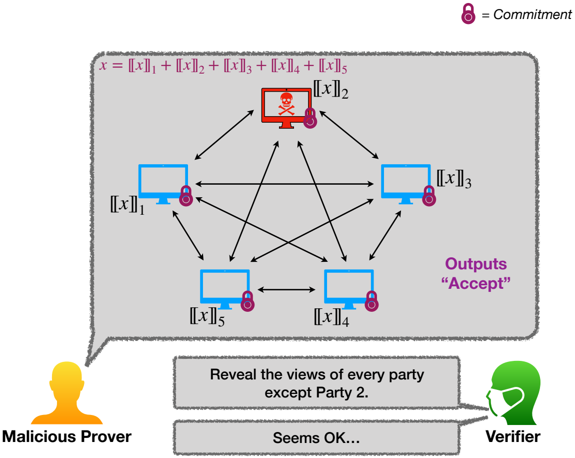
MPC-in-the-Head Paradigm



MPC-in-the-Head Paradigm



MPC-in-the-Head Paradigm



MPC-in-the-Head Paradigm

Soundness error:

$$\frac{1}{N}$$

Proof size: depends on the multi-party computation protocol

Two possible trade-offs:

- Repeat the protocol many times:

  fast proofs, but large proofs

- Take a larger N:

  short proofs, but slow proofs

Syndrome Decoding in the Head

Syndrome Decoding Problem

From (H, y), find $x \in \mathbb{F}^m$ such that

$$y = Hx \quad \text{and} \quad \mathrm{wt}_H(x) \leq w.$$

The multi-party computation must check that the vector x satisfies

$$\underbrace{y = Hx}_{\text{linear, easy to check}} \qquad \text{and} \qquad \underbrace{\mathrm{wt}_H(x) \leq w}_{\text{non-linear, hard to check}}$$

[FJR22] Thibauld Feneuil, Antoine Joux and Matthieu Rivain. *Syndrome Decoding in the Head: Shorter Signatures from Zero-Knowledge Proofs*. Crypto 2022.

Syndrome Decoding in the Head

Syndrome Decoding Problem

From (H, y), find $x \in \mathbb{F}^m$ such that

$$y = Hx \quad \text{and} \quad \mathrm{wt}_H(x) \le w.$$

The multi-party computation must check that the vector x satisfies

$$y = Hx$$

and

$$\exists\ Q, P \text{ two polynomials} : SQ = PF \text{ and } \deg Q = w$$

where

S is defined by interpolation such that $\forall i,\ S(\gamma_i) = x_i$,

$F := \prod_{i=1}^{m} (X - \gamma_i)$.

Syndrome Decoding in the Head - MPC Protocol

The MPC protocol π checks that x describes a solution of the SD instance (H, y).

	Output of π	
	ACCEPT	REJECT
A good witness	1	0
Not a good witness	p	$1-p$

where

$$p = \underbrace{\frac{m+w-1}{|\mathbb{F}_{\text{points}}|}}_{\substack{\text{false positive}\\\text{from Schwartz-Zippel}}} + \left(1 - \frac{m+w-1}{|\mathbb{F}_{\text{points}}|}\right) \cdot \underbrace{\frac{1}{|\mathbb{F}_{\text{points}}|}}_{\substack{\text{false positive}\\\text{from [BN20]}}}$$

Zero-Knowledge Protocol

Soundness error:

$$p + (1 - p) \cdot \frac{1}{N}$$

Zero-Knowledge Protocol

Soundness error:

$$p + (1-p) \cdot \frac{1}{N}$$

Proof size:

- Inputs of $N-1$ parties:

$$\begin{array}{ccccccccccc}
 & & \mathcal{P}_1 & & \mathcal{P}_2 & & \dots & & \mathcal{P}_{N-1} & & \mathcal{P}_N \\
x_A & = & [\![x]\!]_1 & + & [\![x]\!]_2 & + & \dots & + & [\![x]\!]_{N-1} & + & [\![x]\!]_N \\
Q & = & [\![Q]\!]_1 & + & [\![Q]\!]_2 & + & \dots & + & [\![Q]\!]_{N-1} & + & [\![Q]\!]_N \\
P & = & [\![P]\!]_1 & + & [\![P]\!]_2 & + & \dots & + & [\![P]\!]_{N-1} & + & [\![P]\!]_N \\
 & & \uparrow & & \uparrow & & & & \uparrow & & \\
 & & \mathsf{seed}_1 & & \mathsf{seed}_2 & & & & \mathsf{seed}_{N-1} & &
\end{array}$$

Zero-Knowledge Protocol

Soundness error:

$$p + (1-p) \cdot \frac{1}{N}$$

Proof size:

- Inputs of $N-1$ parties:
  - Party $i < N$: a seed of λ bits
  - Last party: uncompressed shares $[\![x]\!]_N, [\![Q]\!]_N, [\![P]\!]_N$

Zero-Knowledge Protocol

Soundness error:

$$p + (1-p) \cdot \frac{1}{N}$$

Proof size:

- Inputs of $N-1$ parties:
  - Party $i < N$: a seed of λ bits
  - Last party: uncompressed shares $[\![x]\!]_N, [\![Q]\!]_N, [\![P]\!]_N$
- Broadcast communication between parties.

Zero-Knowledge Protocol

Soundness error:

$$p + (1-p) \cdot \frac{1}{N}$$

Proof size:

- Inputs of $N-1$ parties:
  - Party $i < N$: a seed of λ bits
  - Last party: uncompressed shares $[\![x]\!]_N, [\![Q]\!]_N, [\![P]\!]_N$
- Broadcast communication between parties.

Signature: Fiat-Shamir Transform

Syndrome Decoding in the Head - Performances

Scheme Name	$\vert\mathsf{sgn}\vert$	$\vert\mathsf{pk}\vert$	t_{sgn}	t_{verif}
FJR22 - $\mathbb{F}_2$ (fast)	15.6 KB	0.09 KB	-	-
FJR22 - $\mathbb{F}_2$ (short)	10.9 KB	0.09 KB	-	-
FJR22 - $\mathbb{F}_2$ (fast)	17.0 KB	0.09 KB	13 ms	13 ms
FJR22 - $\mathbb{F}_2$ (short)	11.8 KB	0.09 KB	64 ms	61 ms
FJR22 - $\mathbb{F}_{256}$ (fast)	11.5 KB	0.14 KB	6 ms	6 ms
FJR22 - $\mathbb{F}_{256}$ (short)	8.26 KB	0.14 KB	30 ms	27 ms

Table of Contents

MPC protocol to check that $x \cdot y = z$ [BN20]

Inputs: (x, y, z), plus $(a, c := x \cdot a)$.

1. The parties get a random $\varepsilon \in \mathbb{F}$.
2. The parties locally set $\alpha = \varepsilon \cdot y + a$.
3. The parties broadcast α to obtain α.
4. The parties locally set $v = \alpha \cdot x - c - \varepsilon \cdot z$.
5. The parties broadcast v to obtain v.
6. The parties output Accept if $v = 0$, and Reject otherwise.

Computation:

$$v = \varepsilon \cdot (x \cdot y - z) + (a \cdot x - c)$$

If $x \cdot y \neq x$, then v is zero only with probability $1/|\mathbb{F}|$.

MPC protocol to check that $XY = Z$

Check that $XY = Z$, where $X \in \mathbb{F}_q^{m \times p}$, $Y \in \mathbb{F}_q^{p \times n}$, $Z \in \mathbb{F}_q^{m \times n}$.

Inputs: (X, Y, Z), plus $(A, C := X \cdot A)$.

1. The parties get a random $\Sigma \in \mathbb{F}_q^{n \times \eta}$.
2. The parties locally set $D = Y\Sigma + A$.
3. The parties broadcast D to obtain $D \in \mathbb{F}_q^{p \times \eta}$.
4. The parties locally set $V = XD - C - Z\Sigma$.
5. The parties broadcast V to obtain $V \in \mathbb{F}_q^{m \times \eta}$.
6. The parties output Accept if $V = 0$, and Reject otherwise.

If $XY \neq Z$, then v is zero only with probability $1/|\mathbb{F}|^\eta$.

Multivariate Quadratic Problem

Multivariate Quadratic Problem

From $(A_1, \dots, A_m, b_1, \dots b_m, y_1, \dots, y_m)$, find $x \in \mathbb{F}_q^n$ such that

$$\forall i \le m,\ y_i = x^T A_i x + b_i^T x.$$

The multi-party computation must check that the vector x satisfies

$$\begin{aligned} y_1 &= x^T A_1 x + b_1^T x \\ y_2 &= x^T A_2 x + b_2^T x \\ &\vdots \\ y_m &= x^T A_m x + b_m^T x \end{aligned}$$

Multivariate Quadratic Problem

Multivariate Quadratic Problem

From $(A_1, \ldots, A_m, b_1, \ldots b_m, y_1, \ldots, y_m)$, find $x \in \mathbb{F}^n$ such that

$$\forall i \leq m,\ \ y_i = x^T A_i x + b_i^T x.$$

The multi-party computation must check that the vector x satisfies

$$\sum_{i=1}^{m} \gamma_i \cdot (y_i - x^T A_i x - b_i^T x) = 0.$$

where $\gamma_1, \ldots, \gamma_m \in \mathbb{F}_{\mathrm{EXT}}$ chosen by the verifier.

False positive rate:

$$\frac{1}{|\mathbb{F}_{\mathrm{EXT}}|}$$

Multivariate Quadratic Problem

Multivariate Quadratic Problem

From $(A_1, \ldots, A_m, b_1, \ldots b_m, y_1, \ldots, y_m)$, find $x \in \mathbb{F}^n$ such that

$$\forall i \leq m,\ y_i = x^T A_i x + b_i^T x.$$

The multi-party computation must check that the vector x satisfies

$$\underbrace{\sum_{i=1}^{m} \gamma_i \cdot (y_i - b_i^T x)}_{\text{linear, easy to compute}} = \langle x, \underbrace{\left(\sum_{i=1}^{m} \gamma_i \cdot A_i\right) x}_{\text{linear, easy to compute}} \rangle.$$

where $\gamma_1, \ldots, \gamma_m \in \mathbb{F}_{\text{EXT}}$ chosen by the verifier.

False positive rate:

$$\frac{1}{|\mathbb{F}_{\text{EXT}}|}$$

Multivariate Quadratic Problem - MPC Protocol

Inputs: x.

1. Get random coefficients $\gamma_1, \ldots, \gamma_m$ from $\mathbb{F}_{\text{EXT}}$.
2. Compute $z := \sum_{i=1}^{m} \gamma_i \cdot (y_i - b_i^T x)$.
3. Compute $w := \left(\sum_{i=1}^{m} \gamma_i \cdot A_i\right) x$.
4. Check that $z = \langle x, w \rangle$.

Multivariate Quadratic Problem - ZKPoK

Soundness error:

$$\frac{1}{N} + \left(1 - \frac{1}{N}\right) \cdot p$$

where

$$p = \underbrace{\frac{1}{|\mathbb{F}_{\text{EXT}}|}}_{\substack{\text{false positive}\\\text{from batching}}} + \left(1 - \frac{1}{|\mathbb{F}_{\text{EXT}}|}\right) \cdot \underbrace{\frac{1}{|\mathbb{F}_{\text{EXT}}|}}_{\substack{\text{false positive}\\\text{from } \Pi_{\text{MM}}}}$$

Proof size:

$$4\lambda + \tau \cdot \left(\underbrace{n \cdot \log_2(q)}_{x} + \underbrace{(n+1) \cdot \eta \cdot \log_2(q)}_{\text{from } \Pi_{\text{MM}}} + \underbrace{\lambda \cdot \log_2 N + 2\lambda}_{\text{MPCitH}}\right)$$

Multivariate Quadratic Problem - Performances

Instance	Protocol Name	Variant	Parameters N	M	τ	Sig. Size
$q=4$, $m=88$, $n=88$	MudFish	-	4	191	68	14 640 B
	Mesquite	Fast	8	187	49	9 578 B
		Short	32	389	28	**8 609 B**
	Our scheme	Fast	32	-	40	10 764 B
		Short	256	-	25	9 064 B
$q=256$, $m=40$, $n=40$	MudFish	Fast	8	176	51	15 958 B
		Short	16	250	36	13 910 B
	Mesquite	Fast	8	187	49	11 339 B
		Short	32	389	28	9 615 B
	Our scheme	Fast	32	-	36	8 488 B
		Short	256	-	25	**7 114 B**

Permuted Kernel Problem

Permuted Kernel Problem

From (H, y, v), find a permutation σ such that

$$y = H\sigma(v).$$

The multi-party computation must check that the permutation σ satisfies

$$y = H\sigma(v).$$

Permuted Kernel Problem

Permuted Kernel Problem

From (H, y, v), find a permutation σ such that

$$y = H\sigma(v).$$

The multi-party computation must check that the vector x satisfies

$$y = Hx \quad \text{such that} \quad \exists\sigma : x = \sigma(v).$$

Permuted Kernel Problem

Permuted Kernel Problem

From (H, y, v), find a permutation σ such that

$$y = H\sigma(v).$$

The multi-party computation must check that the vector x satisfies

$$y = Hx$$

such that

$$\underbrace{(X - x_1)\dots(X - x_n)}_{P(X)} = \underbrace{(X - v_1)\dots(X - v_n)}_{Q(X)}.$$

Permuted Kernel Problem - MPC Protocol

Inputs: x.

1. Check that $y = Hx$.
2. Check that

$$\underbrace{(X - x_1)\dots(X - x_n)}_{P(X)} \text{ is equal to } \underbrace{(X - v_1)\dots(X - v_n)}_{Q(X)}.$$

Permuted Kernel Problem - MPC Protocol

Inputs: x.

1. Check that $y = Hx$.
2. Get a random ξ from $\mathbb{F}_{\text{EXT}}$.
2. Check that

$$\underbrace{(\xi - x_1)\dots(\xi - x_n)}_{P(\xi)} \text{ is equal to } \underbrace{(\xi - v_1)\dots(\xi - v_n)}_{Q(\xi)}.$$

Permuted Kernel Problem - Performances

Instance	Protocol Name	Variant	Parameters N	Parameters M	Parameters τ	Sig. Size
$q = 997$, $n = 61$, $m = 38$	Stern	-	-	-	219	23 848 B
	Véron	-	-	-	219	21 272 B
	SushyFish	Fast	4	191	68	18 448 B
		Short	128	916	20	12 145 B
	FJR21	Fast	8	187	49	15 420 B
		Short	32	389	28	11 947 B
	BG22	Fast	32	-	42	9 896 B
		Short	256	-	31	**8 813 B**
	Our scheme	Fast	32	-	41	16 373 B
		Short	256	-	24	12 816 B

Hard Problems with Rank Constraint

MinRank Problem

From $(M_0, M_1, \ldots, M_k)$, find $x \in \mathbb{F}_q^k$ such that

$$\mathrm{rank}(M_0 + \sum_{i=1}^{k} x_i M_i) \leq r.$$

Hard Problems with Rank Constraint

MinRank Problem

From $(M_0, M_1, \dots, M_k)$, find $x \in \mathbb{F}_q^k$ such that

$$\mathrm{rank}(M_0 + \sum_{i=1}^{k} x_i M_i) \leq r.$$

Rank Syndrome Decoding Problem

From (H, y), find $x \in \mathbb{F}_{q^m}^n$ such that

$$y = Hx \quad \text{and} \quad \mathrm{rank}(x) \leq r.$$

MPC protocol (RD)

The multi-party computation must check that a matrix $M \in \mathbb{F}_q^{m \times n}$ has a rank of at most r.

MPC protocol (RD)

The multi-party computation must check that a matrix $M \in \mathbb{F}_q^{m \times n}$ has a rank of at most r.

Rank Decomposition:

$$\text{A matrix } M \in \mathbb{F}_q^{n \times m} \text{ has a rank of at most } r$$
$$\textit{iff} \text{ there exists } T \in \mathbb{F}_q^{n \times r} \text{ and } R \in \mathbb{F}_q^{r \times m} \text{ such that } M = TR.$$

MPC protocol (RD)

The multi-party computation must check that a matrix $M \in \mathbb{F}_q^{m\times n}$ has a rank of at most r.

Rank Decomposition:

$$\text{A matrix } M \in \mathbb{F}_q^{n\times m} \text{ has a rank of at most } r$$
$$\textit{iff} \text{ there exists } T \in \mathbb{F}_q^{n\times r} \text{ and } R \in \mathbb{F}_q^{r\times m} \text{ such that } M = TR.$$

Inputs: M, T, R.

1. Check that $M = TR$.

MinRank Problem - Performances

Instance	Protocol Name	Variant	Parameters N	M	τ	Sig. Size
$q = 16$, $m = 16$, $n = 16$, $k = 142$, $r = 4$	Cou01	-	-	-	219	52 430 B
		Optimized	-	-	219	28 575 B
	SINY22	-	-	-	128	50 640 B
		Optimized	-	-	128	28 128 B
	BESV22	-	-	256	128	26 405 B
	BG22	Fast	8	187	49	13 644 B
		Short	32	389	28	10 937 B
	ARZV22	Fast	32	-	28	10 116 B
		Short	256	-	18	7 422 B
	Our scheme (RD)	Fast	32	-	33	9 288 B
		Short	256	-	19	7 122 B

Rank Syndrome Decoding Problem - Performances

Instance	Protocol Name	Variant	Parameters N	M	τ	Sig. Size
$q=2$, $m=31$, $n=30$, $k=15$, $r=9$	Stern	-	-	-	219	31 358 B
	Véron	-	-	-	219	27 115 B
	FJR21	Fast	8	187	49	19 328 B
		Short	32	389	28	14 181 B
	BG22	Fast	8	187	49	15 982 B
		Short	32	389	28	12 274 B
	Our scheme (RD)	Fast	32	-	33	11 000 B
		Short	256	-	21	8 543 B
Ideal RSL	BG22	Fast	32	-	27	9 392 B
		Short	256	-	17	6 754 B

Cost Decomposition

Component	**MinRank**	**Rank SD**
Seeds	2432 (35%)	2688 (31%)
Secret x	1349 (19%)	1221 (14%)
Decomposition T, R	1216 (17%)	1441 (17%)
Π_{MM}	1453 (20%)	2457 (29%)
Commitments	672 (9%)	736 (9%)
Total	7122 B	8543 B

MPC protocol (LP)

The multi-party computation must check that a matrix $M \in \mathbb{F}_q^{m\times n}$ has a rank of at most r. Rewrite M as $(x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$.

MPC protocol (LP)

The multi-party computation must check that a matrix $M \in \mathbb{F}_q^{m \times n}$ has a rank of at most r. Rewrite M as $(x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$.

A matrix $M \in \mathbb{F}_q^{n \times m}$ has a rank of at most r
$\Leftrightarrow$ there exists a linear subspace U of $\mathbb{F}_{q^m}$ of dimension r
such that $\{x_1, \ldots, x_n\} \subset U$.

MPC protocol (LP)

The multi-party computation must check that a matrix $M \in \mathbb{F}_q^{m \times n}$ has a rank of at most r. Rewrite M as $(x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$.

A matrix $M \in \mathbb{F}_q^{n \times m}$ has a rank of at most r
$\Leftrightarrow$ there exists a linear subspace U of $\mathbb{F}_{q^m}$ of dimension r
such that $\{x_1, \ldots, x_n\} \subset U$.

Let us define

$$L_U := \prod_{u \in U} (X - u) = X^{q^r} + \sum_{i=0}^{r-1} \beta_i X^{q^i}$$

MPC + Frobenius endomorphism

Let have

$$v = [\![v]\!]_1 + [\![v]\!]_2 + \ldots + [\![v]\!]_N.$$

We get

$$\begin{aligned} v^q &= ([\![v]\!]_1 + [\![v]\!]_2 + \ldots + [\![v]\!]_N)^q \\ &= [\![v]\!]_1^q + [\![v]\!]_2^q + \ldots + [\![v]\!]_N^q. \end{aligned}$$

Computing $[\![v^q]\!]$ from $[\![v]\!]$ is <u>free</u>.

MPC protocol (LP)

The multi-party computation must check that a matrix $M \in \mathbb{F}_q^{m\times n}$ has a rank of at most r. Rewrite M as $(x_1, \dots, x_n) \in \mathbb{F}_{q^m}^n$.

$$\begin{gathered}\text{A matrix } M \in \mathbb{F}_q^{n\times m} \text{ has a rank of at most } r \\ \Leftrightarrow \text{ there exists a linear subspace } U \text{ of } \mathbb{F}_{q^m} \text{ of dimension } r \\ \text{such that } \{x_1, \dots, x_n\} \subset U. \\ \Rightarrow \text{ there exists a } \underline{\text{monic } q\text{-polynomial}}\ L_U \text{ of degree } q^r \\ \text{such that } x_1, \dots, x_n \text{ are roots of } L_U.\end{gathered}$$

MPC protocol (LP)

The multi-party computation must check that a matrix $M \in \mathbb{F}_q^{m \times n}$ has a rank of at most r. Rewrite M as $(x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$.

A matrix $M \in \mathbb{F}_q^{n \times m}$ has a rank of at most r
$\Leftrightarrow$ there exists a linear subspace U of $\mathbb{F}_{q^m}$ of dimension r
such that $\{x_1, \ldots, x_n\} \subset U$.
$\Leftrightarrow$ there exists a <u>monic q-polynomial</u> L_U of degree q^r
such that $x_1, \ldots, x_n$ are roots of L_U.

MPC protocol (LP)

We have

$$L_U := \prod_{u \in U} (X - u) = X^{q^r} + \sum_{i=0}^{r-1} \beta_i X^{q^i}$$

We will check that

$$L_U(x_1) = \ldots = L_U(x_n) = 0.$$

MPC protocol (LP)

We have

$$L_U := \prod_{u \in U} (X - u) = X^{q^r} + \sum_{i=0}^{r-1} \beta_i X^{q^i}$$

We will check that

$$0 = \sum_{j=1}^{n} \gamma_j \cdot L_U(x_j).$$

MPC protocol (LP)

We have

$$L_U := \prod_{u \in U} (X - u) = X^{q^r} + \sum_{i=0}^{r-1} \beta_i X^{q^i}$$

We will check that

$$\begin{aligned} 0 &= \sum_{j=1}^{n} \gamma_j \cdot L_U(x_j) \\ &= \sum_{j=1}^{n} \gamma_j \cdot \left(x_j^{q^r} + \sum_{i=0}^{r-1} \beta_i x_j^{q^i} \right) \\ &= \underbrace{\sum_{j=1}^{n} \gamma_j \cdot x_j^{q^r}}_{-z} + \sum_{i=0}^{r-1} \beta_i \underbrace{\sum_{j=1}^{n} \gamma_j \cdot x_j^{q^i}}_{w_i} \end{aligned}$$

MPC protocol (LP)

Inputs: x and $L_U := \prod_{u \in U}(X - u) = X^{q^r} + \sum_{i=0}^{r-1} \beta_i X^{q^i}$.

1. Get random coefficients $\gamma_1, \ldots, \gamma_n$ from $\mathbb{F}_{\text{EXT}}$.
2. Compute $z = -\sum_{j=1}^{n} \gamma_j \cdot x_j^{q^r}$.
3. Compute $w_i = \sum_{j=1}^{n} \gamma_j \cdot x_j^{q^i}$ for $i \in \{0, \ldots, r-1\}$.
4. Check that $z = \langle \beta, w \rangle$.

MinRank Problem

Instance	Protocol Name	Variant	Parameters N	M	τ	Sig. Size
$q = 16$ $m = 16$ $n = 16$ $k = 142$ $r = 4$	Cou01	-	-	-	219	52 430 B
		Optimized	-	-	219	28 575 B
	SINY22	-	-	-	128	50 640 B
		Optimized	-	-	128	28 128 B
	BESV22	-	-	256	128	26 405 B
	BG22	Fast	8	187	49	13 644 B
		Short	32	389	28	10 937 B
	ARZV22	Fast	32	-	28	10 116 B
		Short	256	-	18	7 422 B
	Our scheme (RD)	Fast	32	-	33	9 288 B
		Short	256	-	19	7 122 B
	Our scheme (LP)	Fast	32	-	28	7 204 B
		Short	256	-	18	**5 518 B**

Rank Syndrome Decoding Problem

Instance	Protocol Name	Variant	Parameters N	M	τ	Sig. Size
$q=2$, $m=31$, $n=30$, $k=15$, $r=9$	Stern	-	-	-	219	31 358 B
	Véron	-	-	-	219	27 115 B
	FJR21	Fast	8	187	49	19 328 B
		Short	32	389	28	14 181 B
	BG22	Fast	8	187	49	15 982 B
		Short	32	389	28	12 274 B
	Our scheme (RD)	Fast	32	-	33	11 000 B
		Short	256	-	21	8 543 B
	Our scheme (LP)	Fast	32	-	30	7 376 B
		Short	256	-	20	**5 899 B**
Ideal RSL	BG22	Fast	32	-	27	9 392 B
		Short	256	-	17	6 754 B

Cost Decomposition

For the Rank Syndrome Decoding Problem:

Component	RD	LP
Seeds	2688 (31%)	2560 (43%)
Secret x	1221 (14%)	1162 (20%)
Auxiliary	1441 (17%)	697 (12%)
Π_{MM}	2457 (29%)	775 (13%)
Commitments	736 (9%)	704 (12%)
Total	8543 B	5899 B

where the auxiliary values are

- the rank decomposition T, R in the first case, and
- the q-polynomial L_U in the second case.

Summary

Hard Problem	Best scheme	Achieved sizes
Multivariate Quadratic	Over $\mathbb{F}_4$, [Wan22] Over $\mathbb{F}_{256}$, this work	8.4 – 9.4 KB 6.9 – 8.3 KB
Min Rank	This work	5.4 – 7.0 KB
Permuted Kernel	[BG22]	8.6 – 9.7 KB
Subset Sum	[FMRV22]	21.1 – 33.2 KB
SD *(Hamming)*	[FJR22]	($\mathbb{F}_2$) 10.9 – 15.6 KB ($\mathbb{F}_{256}$) 8.3 – 11.5 KB
SD *(Rank)*	This work	5.8 – 7.2 KB

Summary

Hard Problem	Best scheme	Achieved sizes
Multivariate Quadratic	Over $\mathbb{F}_4$, [Wan22] Over $\mathbb{F}_{256}$, this work	8.4 – 9.4 KB 6.9 – 8.3 KB
Min Rank	This work	5.4 – 7.0 KB
Permuted Kernel	[BG22]	8.6 – 9.7 KB
Subset Sum	[FMRV22]	21.1 – 33.2 KB
SD *(Hamming)*	[FJR22]	($\mathbb{F}_2$) 10.9 – 15.6 KB ($\mathbb{F}_{256}$) 8.3 – 11.5 KB
SD *(Rank)*	This work	5.8 – 7.2 KB

Future Work.

- ☞ Implement some of the schemes proposed in this work.
- ☞ Search parameter sets that provide better performances.

Table of Contents

MPC-in-the-Head Paradigm

MPC-in-the-Head Paradigm

- Generic technique to build *zero-knowledge protocols* using *multi-party computation.*
- Introduced in 2007 by:

[IKOS07] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. *Zero-knowledge from secure multiparty computation.* STOC 2007.

MPC-in-the-Head Paradigm

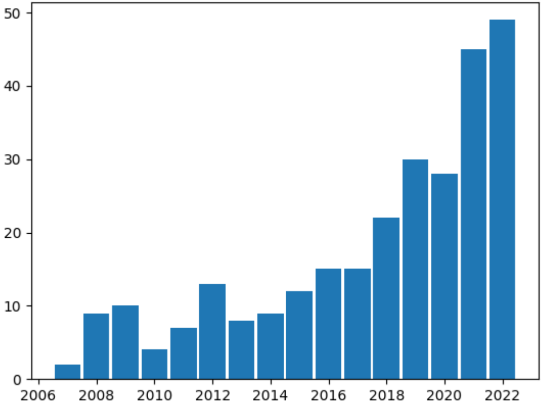


Figure: Number of citations of [IKOS07] (source: *Semantic Scholar*)

MPC-in-the-Head Paradigm

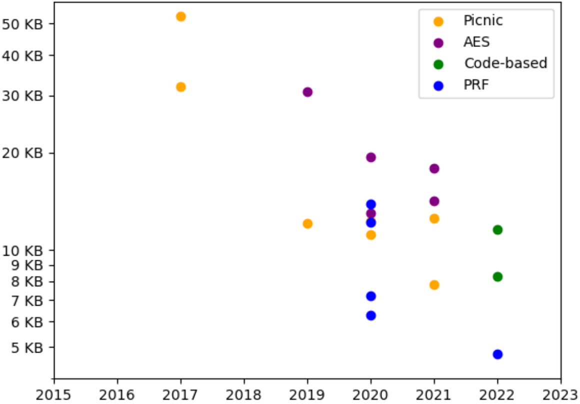


Figure: Evolution of the signature sizes (figure **not up-to-date**)

MPC-in-the-Head History

2007. MPCitH has been introduced [IKOS07].

2016. First practical MPCitH-based scheme [GMO16].

2018. The current form of the MPCitH schemes [KKW18].

End 2021. MPCitH + Hard Problems (SD, MQ, ...)

Limitations of the MPCitH paradigm (size)

- N-additive sharing + MPC protocol
- Reveal $(N-1)$ parties' inputs: a seed of λ bits per party
- Per iteration: $\log_2 N$ seeds, soundess error of $1/N$.
- Incompressible cost:

$$\underbrace{\frac{\lambda}{\log_2 N}}_{\text{Nb iterations}} \cdot \underbrace{(\lambda \cdot \log_2 N)}_{\text{All opened seeds}} = \lambda^2$$

Numerical Application:

128-bit	2 KB
192-bit	4.5 KB
256-bit	8 KB

Limitations of the MPCitH paradigm (size)

For 128-bit security and using 256 parties:

- ☞ Well-known symmetric primitives: ≈ 10 KB (AES)
- ☞ MPC-friendly primitives: ≈ 5 KB (Rain, ...)
- ☞ Well-known hard problems: ≤ 6 KB (MinRank, RSD)

2023. Stabilization of the MPCitH?

My guess: $4-5$ *KB when using 256 parties.*

Limitations of the MPCitH paradigm (running times)

- N-additive sharing + MPC protocol
- The Signer emulates N parties by iteration

$$\underbrace{\frac{\lambda}{\log_2 N}}_{\text{Nb iterations}} \times N = \lambda \cdot \frac{N}{\log_2 N}$$

- The Verifier emulates $N-1$ parties by iteration

$$\underbrace{\frac{\lambda}{\log_2 N}}_{\text{Nb iterations}} \times (N-1) = \lambda \cdot \frac{N-1}{\log_2 N}$$

Limitations of the MPCitH paradigm (running times)

For 256 parties:

	Signer	Verifier
128-bit	4096	4080
192-bit	6144	6120
256-bit	8192	8160

$\rightarrow$ 4-30 ms

Limitations of the MPCitH paradigm (running times)

For 256 parties:

	Signer	Verifier
128-bit	4096	4080
192-bit	6144	6120
256-bit	8192	8160

$\rightarrow$ 4-30 ms

Signing time $\approx$ Verification time

Limitations of the MPCitH paradigm (running times)

For 256 parties:

	Signer	Verifier
128-bit	4096	4080
192-bit	6144	6120
256-bit	8192	8160

$\rightarrow$ 4-30 ms

#Matrix Mult.:
- Stern94: 219
- SDitH (fast): 864
- SDitH (short): 4352

Signing time $\approx$ Verification time

Some challenges for the MPCitH paradigm

MPCitH-based Signatures:

- ☞ Fast verification timing (≤ 1 ms)
- ☞ Fast signing timing (≤ 1 ms)
- ☞ Exploit problem structures
- ☞ Decrease the communication cost

Some challenges for the MPCitH paradigm

MPCitH-based Signatures:

- ☞ Fast verification timing (≤ 1 ms)
- ☞ Fast signing timing (≤ 1 ms)
- ☞ Exploit problem structures
- ☞ Decrease the communication cost

MPCitH-based Proof Systems:

- ☞ Fast verification timing (≤ 1 ms)
- ☞ Fast proving timing (≤ 1 ms)
- ☞ Achieve sublinear communication

Many directions to optimize

- ☞ The proved statement,
- ☞ The used MPC protocol,
- ☞ The used sharing scheme.

Changing the sharing scheme...

[FMRV22] Thibauld Feneuil, Jules Maire, Matthieu Rivain and Damien Vergnaud. *Zero-Knowledge Protocols for the Subset Sum Problem from MPC-in-the-Head with Rejection.* Asiacrypt 2022.

- ☞ Decrease cost when using large modulus.

[FR22] Thibauld Feneuil and Matthieu Rivain. *Threshold Linear Secret Sharing to the Rescue of MPC-in-the-Head.* Eprint 2022/1407.

- ☞ New trade-offs.
- ☞ Fast verification timing.

Scheme Name	$\lvert\mathsf{sgn}\rvert$	$\lvert\mathsf{pk}\rvert$	t_{sgn}	t_{verif}
FJR22 - $\mathbb{F}_{256}$ (fast)	11.5 KB	0.14 KB	6 ms	6 ms
FJR22 - $\mathbb{F}_{256}$ (short)	8.26 KB	0.14 KB	30 ms	27 ms
FJR22 - $\mathbb{F}_{256}$ (SSS)	9.97 KB	0.14 KB	2.2 ms	0.38 ms

Changing the sharing scheme...

[FMRV22] Thibauld Feneuil, Jules Maire, Matthie
Vergnaud. *Zero-Knowledge Protocols for the Subs*
MPC-in-the-Head with Rejection. Asiacrypt 2022.

- Decrease cost when using large mo

#Matrix Mult.:
- Stern94: 219
- SDitH (fast): 864
- SDitH (short): 4352
- SDitH (SSS): 24

[FR22] Thibauld Feneuil and Matthieu Rivain. *Threshold Linear Secret Sharing to the Rescue of MPC-in-the-Head.* Eprint 2022/1407.

- New trade-offs.
- Fast verification timing.

Scheme Name	|sgn|	|pk|	t_{sgn}	t_{verif}
FJR22 - $\mathbb{F}_{256}$ (fast)	11.5 KB	0.14 KB	6 ms	6 ms
FJR22 - $\mathbb{F}_{256}$ (short)	8.26 KB	0.14 KB	30 ms	27 ms
FJR22 - $\mathbb{F}_{256}$ (SSS)	9.97 KB	0.14 KB	2.2 ms	0.38 ms

Conclusion

2007. MPCitH has been introduced [IKOS07].

2016. First practical MPCitH-based scheme [GMO16].

2018. The current form of the MPCitH schemes [KKW18].

End 2021. MPCitH + Hard Problems (SD, MQ, ...)

My guess:

2023-...

- Optimizations of the current MPCitH form,
- Development of new MPCitH techniques,
- Advanced functionalities.