Dual Support Decomposition in the Head: Shorter Signatures from Rank SD and MinRank

Loïc Bidoux, Thibauld Feneuil, Philippe Gaborit, **Romaric Neveu**, Matthieu Rivain

10th December 2024

Comparison with former schemes

RSD Parameters	Scheme	N	M	τ	η	ρ	Signature Size
$q = 2$, $m = 31$, $n = 33$, $k = 15$, $r = 10$	[Ste93]	-	-	219	-	-	33 886 B
	[Vér97]	-	-	219	-	-	28 794 B
	[FJR22a]	32	389	28	-	-	14 792 B
	[BG23]	32	389	28	-	-	12 816 B
	[Fen24] RD	256	-	21	24	-	8 990 B
	[Fen24] LP and [ABB+23b]	256	-	20	1	-	5 956 B
$q = 2, m = 53, n = 53$, $k = 45, r = 4$	**Our scheme (TCitH)**	2 048	-	12	-	3	**2 937 B**
	Our scheme (VOLEitH)	2 048	-	11	-	128	**2 851 B**

Table: Comparison of the signatures relying on RSD

Comparison with former schemes

MinRank Parameters	Scheme	N	M	τ	η	ρ	Signature Size
$q = 16$ $m = 16$ $n = 16$ $k = 142$ $r = 4$	[Cou01]	-	-	219	-	-	28 575 B
	[SINY22]	-	-	128	-	-	28 128 B
	[BESV22]	-	256	128	-	-	26 405 B
	[BG23]	32	389	28	-	-	10 937 B
	[ARZV23]	256	-	18	-	-	7 422 B
	[Fen24] RD	256	-	19	9	-	7 122 B
$q = 16, m = 16, n = 16$ $k = 120, r = 5$	[Fen24] LP and [ABB+23c]	256	-	18	1	-	5 640 B
$q = 16, m = 15, n = 15$ $k = 78, r = 6$	MiRitH [ABB+23a]	256	-	19	9	-	5 673 B
$q = 2, m = 43, n = 43$ $k = 1520, r = 4$	**Our scheme (TCitH)**	2048	-	12	-	130	**2 896 B**
	Our scheme (VOLEitH)	2048	-	11	-	128	**2 813 B**

Table: Comparison of the signatures relying on MinRank

Rank Metric Background

Rank Metric Background

The Hard Problems

Syndrome decoding problem

Given a random matrix $\boldsymbol{H} \in \mathbb{F}_q^{(n-k)\times n}$ and a vector $\boldsymbol{y} = \boldsymbol{H}\boldsymbol{x}^\top \in \mathbb{F}_q^{(n-k)}$, recover $\boldsymbol{x} \in \mathbb{F}_q^n$.

This problem is easy to solve (simple linear algebra).

To turn it into a difficult problem: $\boldsymbol{x}$ of small weight for a particular metric:

- Euclidean $\rightarrow$ lattices;
- Hamming metric;
- **Rank metric**.

Rank metric

Let $\boldsymbol{x} = (x_1, ..., x_n) \in \mathbb{F}_{q^m}^n$, and $\mathcal{B} = (b_1, ..., b_m)$ an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$.

$$x_i = \sum_{j=1}^{m} x_{i,j} b_j$$

We can define the matrix: $\boldsymbol{M}(\boldsymbol{x}) = \begin{pmatrix} x_{1,1} & x_{2,1} & \cdots & x_{n,1} \\ x_{1,2} & x_{2,2} & \cdots & x_{n,2} \\ \vdots & \vdots & \ddots & \vdots \\ x_{1,m} & x_{2,m} & \cdots & x_{n,m} \end{pmatrix}$.

Rank weight: $w_R(\boldsymbol{x}) = \mathsf{rank}(\boldsymbol{M}(\boldsymbol{x}))$.

Rank Syndrome Decoding

Given $(\boldsymbol{H} \in \mathbb{F}_{q^m}^{n-k \times n}, \boldsymbol{y} \in \mathbb{F}_{q^m}^{n-k})$, find a vector $\boldsymbol{x} \in \mathbb{F}_{q^m}^{n}$ such that $\boldsymbol{H}\boldsymbol{x}^\top = \boldsymbol{y}^\top$ and $w_R(\boldsymbol{x}) = r$.

Rank Syndrome Decoding

Given $(\boldsymbol{H} \in \mathbb{F}_{q^m}^{n-k \times n}, \boldsymbol{y} \in \mathbb{F}_{q^m}^{n-k})$, find a vector $\boldsymbol{x} \in \mathbb{F}_{q^m}^{n}$ such that $\boldsymbol{H}\boldsymbol{x}^\top = \boldsymbol{y}^\top$ and $w_R(\boldsymbol{x}) = r$.

MinRank

Given $\boldsymbol{M}, \boldsymbol{M}_1, \ldots, \boldsymbol{M}_k \in \mathbb{F}_q^{m \times n}$, find $\boldsymbol{x} \in \mathbb{F}_q^k$ such that $\boldsymbol{E} := \boldsymbol{M} + \sum_{i=1}^{k} \boldsymbol{M}_i x_i$ and $\mathsf{rank}(\boldsymbol{E}) \leq r$.

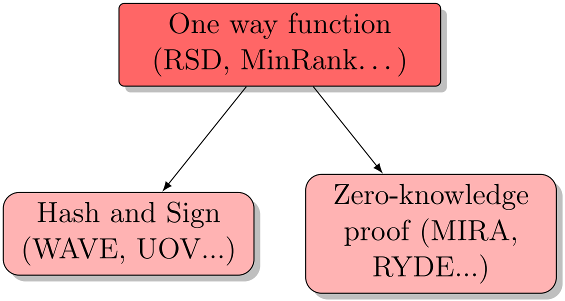
- Studied for several decades, used in many cryptosystems.
- Parameters taken on Gilbert-Varshamov bound, hardest instances.

MPC-in-the-Head Background

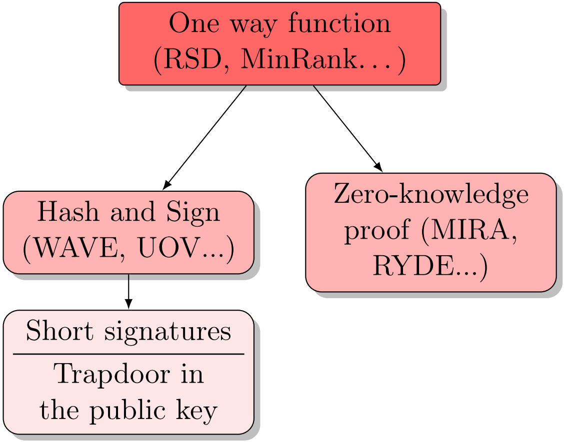
MPC-in-the-Head Background

The MPC-in-the-Head paradigm

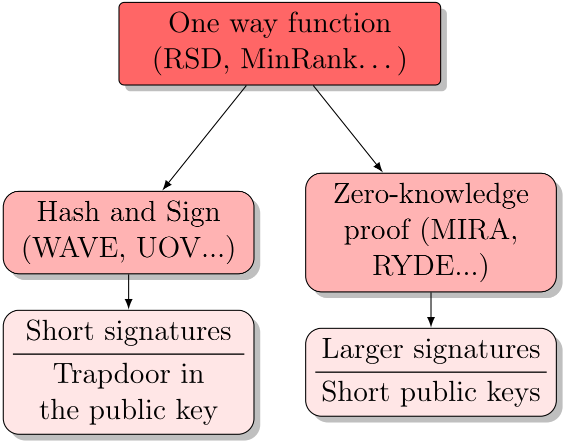
How to build signatures



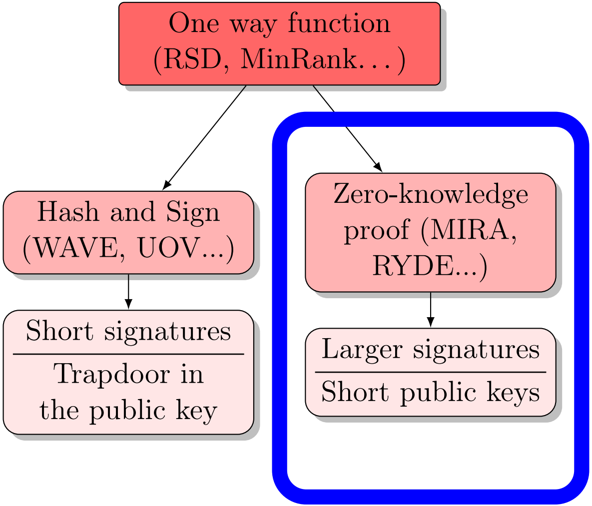
How to build signatures



How to build signatures



How to build signatures



- Many evolutions of zero-knowledge proofs in codes:
  - Stern protocol soundness error of $\frac{2}{3}$, uses permutations [Ste93];

- Many evolutions of zero-knowledge proofs in codes:
  - Stern protocol soundness error of $\frac{2}{3}$, uses permutations [Ste93];
  - AGS protocol improvement of Stern, $\frac{1}{2}$ [AMGS11];

- Many evolutions of zero-knowledge proofs in codes:
  - Stern protocol soundness error of $\frac{2}{3}$, uses permutations [Ste93];
  - AGS protocol improvement of Stern, $\frac{1}{2}$ [AMGS11];
  - Shared Permutation, protocol with helper: soundness error down to $\frac{1}{N}$ $\rightarrow$ now depends of a chosen parameter [FJR22a];

Evolutions of ZKP

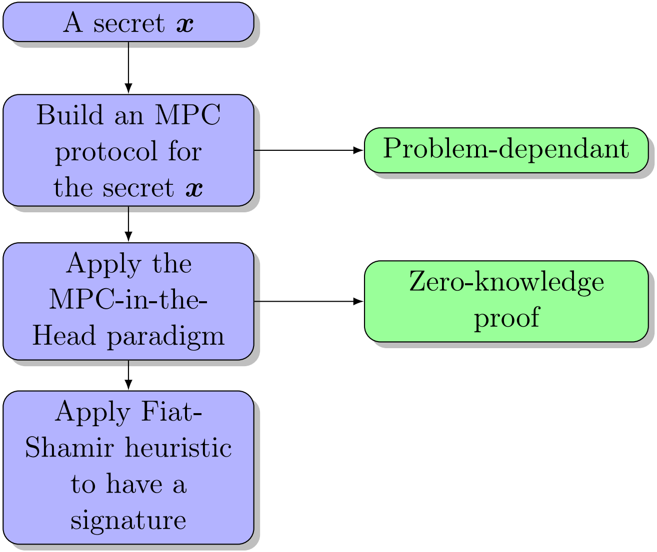
- Many evolutions of zero-knowledge proofs in codes:
  - Stern protocol soundness error of $\frac{2}{3}$, uses permutations [Ste93];
  - AGS protocol improvement of Stern, $\frac{1}{2}$ [AMGS11];
  - Shared Permutation, protocol with helper: soundness error down to $\frac{1}{N}$ $\rightarrow$ now depends of a chosen parameter [FJR22a];
  - Protocol without helper: $\frac{1}{N}$, more efficient [BG23];

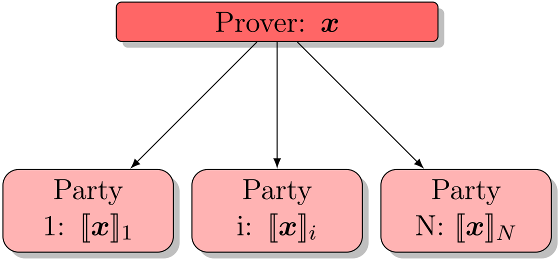
- Many evolutions of zero-knowledge proofs in codes:
  - Stern protocol soundness error of $\frac{2}{3}$, uses permutations [Ste93];
  - AGS protocol improvement of Stern, $\frac{1}{2}$ [AMGS11];
  - Shared Permutation, protocol with helper: soundness error down to $\frac{1}{N}$ $\rightarrow$ now depends of a chosen parameter [FJR22a];
  - Protocol without helper: $\frac{1}{N}$, more efficient [BG23];
  - MPC-in-the-Head: Additive secret sharing, $\frac{1}{N}$ too but more efficient [FJR22b];

Evolutions of ZKP

- Many evolutions of zero-knowledge proofs in codes:
  - Stern protocol soundness error of $\frac{2}{3}$, uses permutations [Ste93];
  - AGS protocol improvement of Stern, $\frac{1}{2}$ [AMGS11];
  - Shared Permutation, protocol with helper: soundness error down to $\frac{1}{N}$ $\rightarrow$ now depends of a chosen parameter [FJR22a];
  - Protocol without helper: $\frac{1}{N}$, more efficient [BG23];
  - MPC-in-the-Head: Additive secret sharing, $\frac{1}{N}$ too but more efficient [FJR22b];
  - Threshold-Computation-in-the-Head and VOLE-in-the-Head: Shamir secret sharings, $\frac{1}{N}$ much more efficient [FR23a], [BBdSG^{+}23].

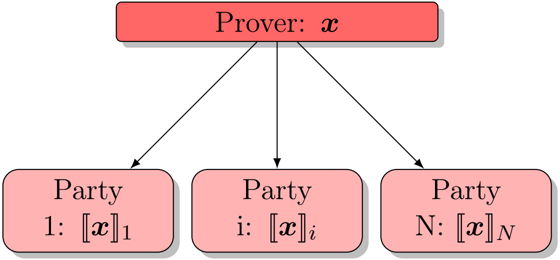
Construction of an MPC-in-the-Head protocol





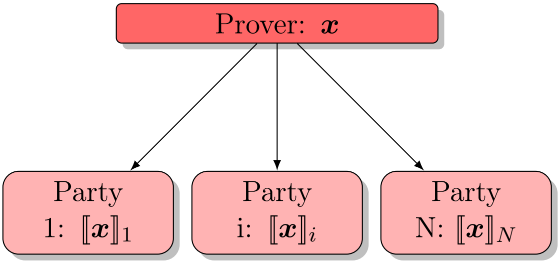
- Additive sharing:

$\boldsymbol{x} = [\![\boldsymbol{x}]\!]_1 + [\![\boldsymbol{x}]\!]_2 + \cdots + [\![\boldsymbol{x}]\!]_N.$



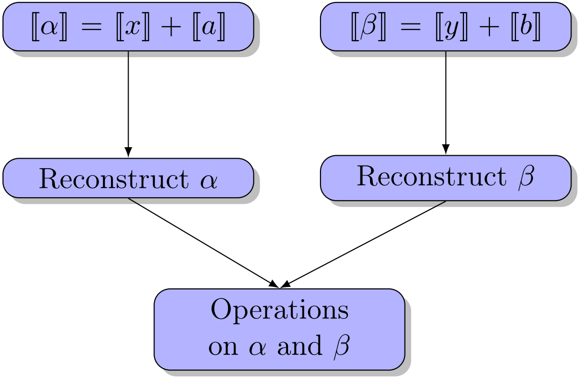
- Additive sharing: $\boldsymbol{x} = [\![\boldsymbol{x}]\!]_1 + [\![\boldsymbol{x}]\!]_2 + \cdots + [\![\boldsymbol{x}]\!]_N$.
- Linear operations: easy. But non-linear?

MPC model



- Additive sharing: $\boldsymbol{x} = [\![\boldsymbol{x}]\!]_1 + [\![\boldsymbol{x}]\!]_2 + \cdots + [\![\boldsymbol{x}]\!]_N$.
- Linear operations: easy. But non-linear?

- Beaver triples: how to get $[\![xy]\!]$ from $[\![x]\!]$ and $[\![y]\!]$?

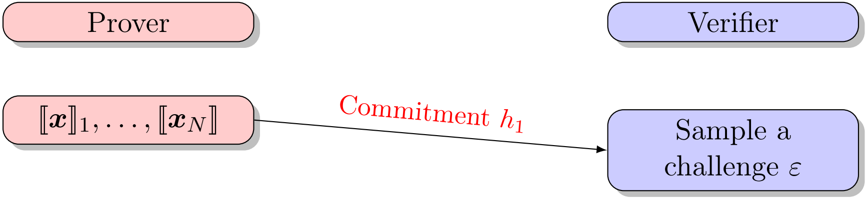


Blueprint of MPC-in-the-Head

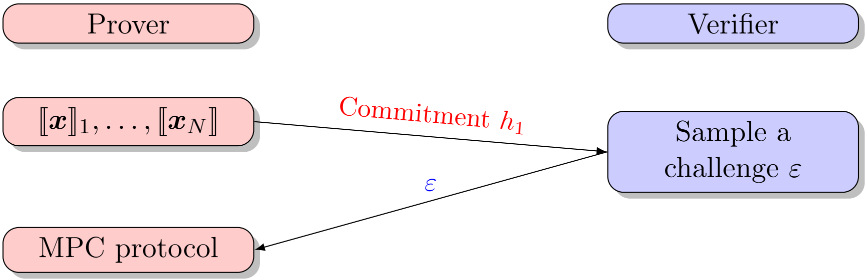
Prover

Verifier

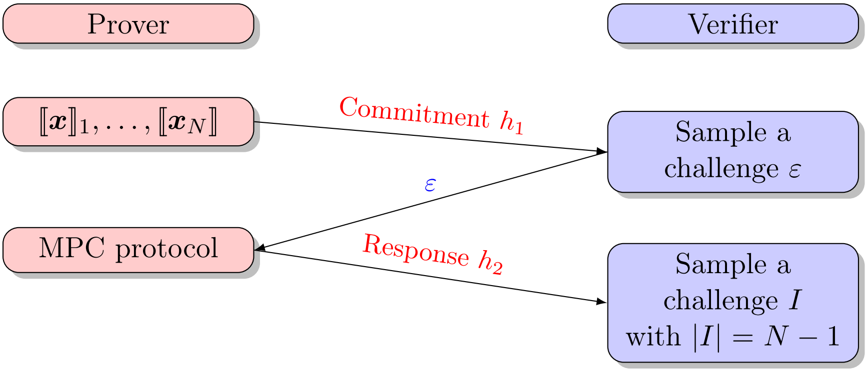
Blueprint of MPC-in-the-Head



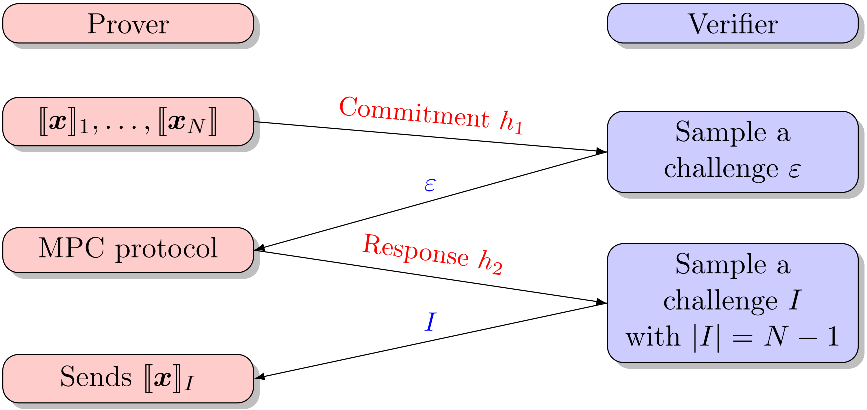
Blueprint of MPC-in-the-Head



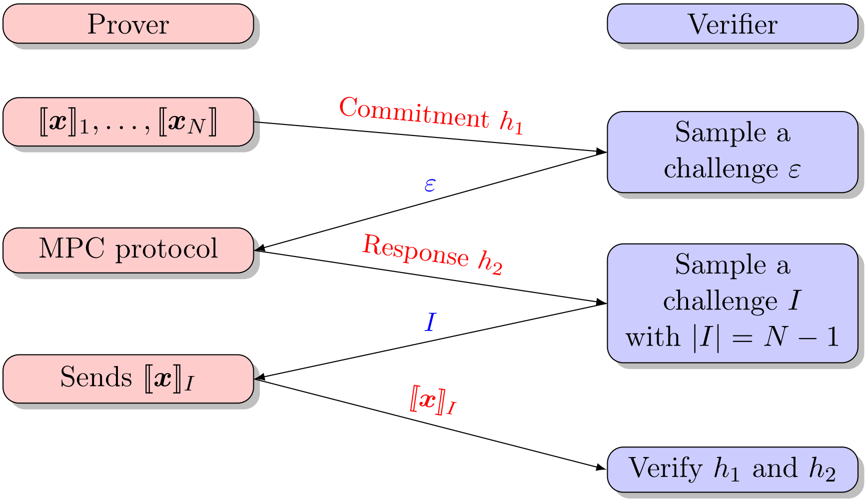
Blueprint of MPC-in-the-Head



Blueprint of MPC-in-the-Head



Blueprint of MPC-in-the-Head



MPC-in-the-Head Background

Threshold-Computation-in-the-Head and VOLE-in-the-Head

The TCitH framework

- Introduced in 2023 in [FR23b], improved later in [FR23a].

The TCitH framework

- Introduced in 2023 in [FR23b], improved later in [FR23a].
- Uses threshold linear secret sharing → Shamir's secret sharing: $P_\omega(X) = rX + \omega$ → hides ω.

The TCitH framework

- Introduced in 2023 in [FR23b], improved later in [FR23a].
- Uses threshold linear secret sharing → Shamir's secret sharing: $P_\omega(X) = rX + \omega$ → hides ω.
- Allows non-linear computations → avoid Beaver triples AND easier to model the problems.

The TCitH framework

- Introduced in 2023 in [FR23b], improved later in [FR23a].
- Uses threshold linear secret sharing $\rightarrow$ Shamir's secret sharing: $P_\omega(X) = rX + \omega$ $\rightarrow$ hides ω.
- Allows non-linear computations $\rightarrow$ avoid Beaver triples AND easier to model the problems.
- Faster: perform the MPC protocol τ times for only one party $\rightarrow$ bigger values of N.

The TCitH framework

- Introduced in 2023 in [FR23b], improved later in [FR23a].
- Uses threshold linear secret sharing → Shamir's secret sharing: $P_\omega(X) = rX + \omega$ → hides ω.
- Allows non-linear computations → avoid Beaver triples AND easier to model the problems.
- Faster: perform the MPC protocol τ times for only one party → bigger values of N.
- Polynomial constraints checking protocol → efficient protocol: false-positive probability and communication cost.

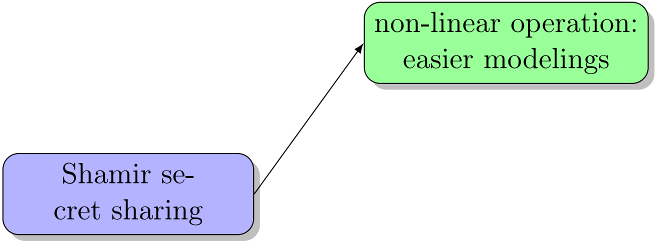
- How to check that we know ω such that $f_1(\omega) = \cdots = f_m(\omega) = 0$?

1. Evaluate $f_i([\![\omega]\!])$ for $i \in \{1, \ldots, m\}$;
2. Receive m random coefficients $\gamma_1, \ldots, \gamma_m$;
3. Compute $[\![\alpha]\!] = [\![0]\!] + \sum_{i=1}^{m} \gamma_i f_i([\![\omega]\!])$.

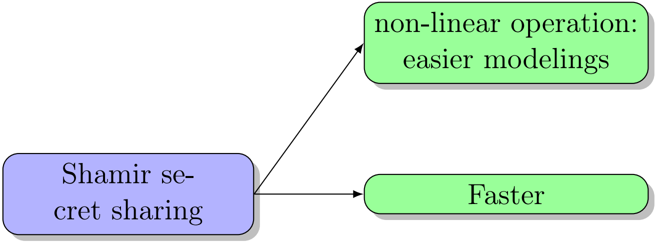
The Polynomial Checking protocol

- How to check that we know ω such that $f_1(\omega) = \cdots = f_m(\omega) = 0$?
  1. Evaluate $f_i([\![\omega]\!])$ for $i \in \{1, \ldots, m\}$;
  2. Receive m random coefficients $\gamma_1, \ldots, \gamma_m$;
  3. Compute $[\![\alpha]\!] = [\![0]\!] + \sum_{i=1}^{m} \gamma_i f_i([\![\omega]\!])$.
- If ω is a root of all f_i then $\alpha = 0$.
- No Beaver triples $\rightarrow$ efficient protocol.

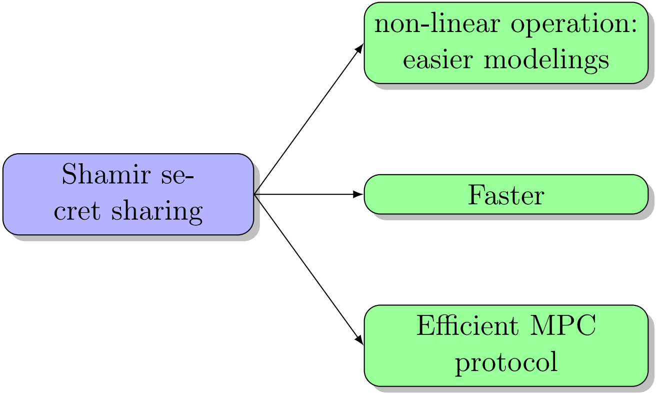
To sum up


non-linear operation: easier modelings
Shamir secret sharing

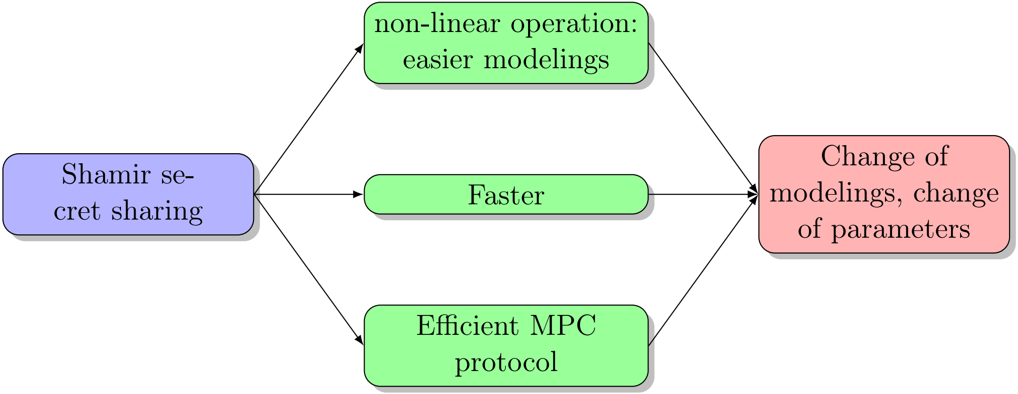
To sum up


Shamir se-
cret sharing
non-linear operation:
easier modelings
Faster

To sum up


Shamir secret sharing
non-linear operation: easier modelings
Faster
Efficient MPC protocol

To sum up



Shamir secret sharing
non-linear operation: easier modelings
Faster
Efficient MPC protocol
Change of modelings, change of parameters

- Introduced independently from TCitH, but can be expressed with the same syntax:
  - Uses Shamir's Secret Sharing with threshold $\ell = 1 \rightarrow$ hides the secret w with $P(X) = wX + r$;
  - Large field embedding: use the isomorphism ϕ between $\mathbb{F}_q^\tau$ and $\mathbb{F}_{q^\tau}$.

MinRank and RSD Modelings

MinRank and RSD Modelings

Existing Modelings

What to consider?

- Interaction between the base technique and the modelings: additive sharing or Shamir's $\rightarrow$ changes the best modeling, changes the parameters.

What to consider?

- Interaction between the base technique and the modelings: additive sharing or Shamir's $\rightarrow$ changes the best modeling, changes the parameters.
- For additive sharing schemes:
  - Size of the witness;
  - Communication between parties (Size of $\boldsymbol{\alpha}$);
  - False-positive probability.

What to consider?

- Interaction between the base technique and the modelings: additive sharing or Shamir's $\rightarrow$ changes the best modeling, changes the parameters.
- For additive sharing schemes:
  - Size of the witness;
  - Communication between parties (Size of $\boldsymbol{\alpha}$);
  - False-positive probability.
- With Shamir's secret sharing (TCitH and VOLEitH): only Size of the witness matters.

Several modelings

- Rank decomposition;
- Kipnis-Shamir modeling;
- q-polynomials;
- New modeling: dual support decomposition.

- Degree 2 modeling $\rightarrow$ optimal signature sizes.

- For MinRank: prove that $\boldsymbol{E} = \boldsymbol{M} + \sum_{i=1}^{k} x_i \boldsymbol{M}_i$ is of rank $\leq r$.
- To prove that a matrix $\boldsymbol{X}$ is of rank r: sends the right-kernel $\boldsymbol{K}$ of rank $n - r$ and compute $\boldsymbol{X}\boldsymbol{K}$.
  - For RSD: send $\boldsymbol{x}_B \in \mathbb{F}_{q^m}^k$, $\boldsymbol{A} \in \mathbb{F}_q^{r \times (n-r)}$;
  - For MinRank: send $\boldsymbol{x} \in \mathbb{F}_q^k$, $\boldsymbol{A} \in \mathbb{F}_q^{r \times (n-r)}$.
- Witness is of size $k + r \cdot (n - r)$.

q-polynomial

A q-polynomial of q-degree r is a polynomial in $\mathbb{F}_{q^m}[X]$ of the form:

$$P(X) = X^{q^r} + \sum_{i=0}^{r-1} p_i \cdot X^{q^i} \qquad \text{with } p_i \in \mathbb{F}_{q^m}.$$

q-polynomials modeling

q-polynomial

A q-polynomial of q-degree r is a polynomial in $\mathbb{F}_{q^m}[X]$ of the form:

$$P(X) = X^{q^r} + \sum_{i=0}^{r-1} p_i \cdot X^{q^i} \qquad \text{with } p_i \in \mathbb{F}_{q^m}.$$

- To prove that $\boldsymbol{E} = \boldsymbol{M} + \sum_{i=1}^{k} x_i \boldsymbol{M}_i$ is of rank $\leq r$: give the polynomial $P_{\boldsymbol{E}}$ and check $\forall i$, $P_{\boldsymbol{E}}(e_i) = 0$.
  - For RSD: send $\boldsymbol{x}_B \in \mathbb{F}_{q^m}^k$, $P_{\boldsymbol{x}} \rightarrow \mathbb{F}_{q^m}^r$;
  - For MinRank: send $\boldsymbol{x} \in \mathbb{F}_q^k$, $P_{\boldsymbol{E}} \rightarrow \mathbb{F}_{q^m}^r$.
- Witness: $k + rm$, but lower false-positive probability.

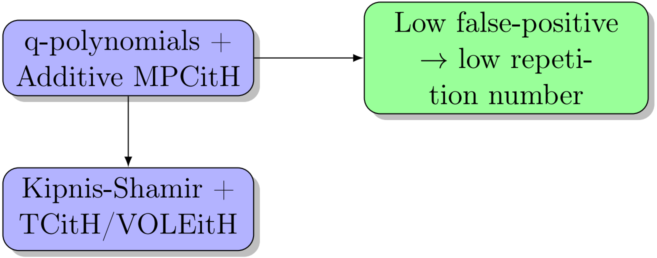
A change of efficiency

- Most efficient signatures:

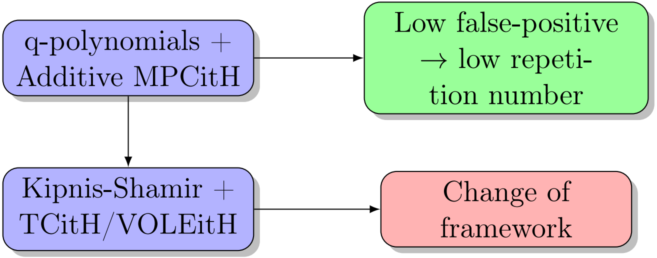
q-polynomials + Additive MPCitH $\longrightarrow$ Low false-positive $\rightarrow$ low repetition number

A change of efficiency

- Most efficient signatures:

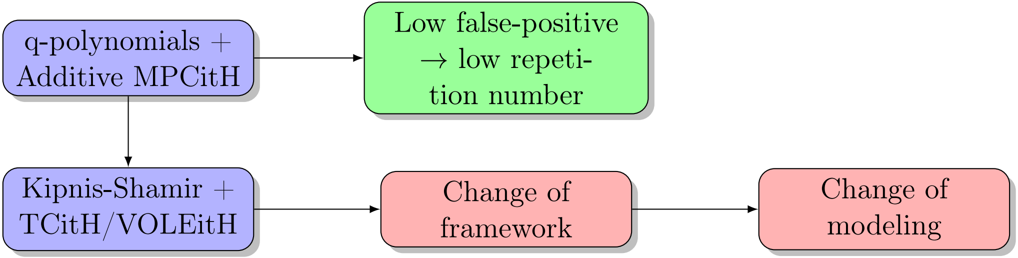


- Most efficient signatures:



A change of efficiency

- Most efficient signatures:



MinRank and RSD Modelings

New Modeling: Dual Support Decomposition

Dual support decomposition

- New modeling to achieve smaller signature sizes.

- For RSD: improvement of the Rank Decomposition modeling, Shamir's secret sharing $\rightarrow$ easier multiplications.

Dual support decomposition

- New modeling to achieve smaller signature sizes.
- For RSD: improvement of the Rank Decomposition modeling, Shamir's secret sharing $\rightarrow$ easier multiplications.
- Check that $\boldsymbol{H}\boldsymbol{x}^\top = \boldsymbol{y}^\top$ with $\boldsymbol{x}$ of weight $\leq r$.
- $\boldsymbol{x}$ of small weight $\rightarrow$ $\boldsymbol{x} = (x_1, \ldots, x_r) \cdot \boldsymbol{C}$ with $\boldsymbol{C} \in \mathbb{F}_q^{r \times n}$.

Dual support decomposition

- New modeling to achieve smaller signature sizes.
- For RSD: improvement of the Rank Decomposition modeling, Shamir's secret sharing $\rightarrow$ easier multiplications.
- Check that $\boldsymbol{H}\boldsymbol{x}^\top = \boldsymbol{y}^\top$ with $\boldsymbol{x}$ of weight $\leq r$.
- $\boldsymbol{x}$ of small weight $\rightarrow$ $\boldsymbol{x} = (x_1, \ldots, x_r) \cdot \boldsymbol{C}$ with $\boldsymbol{C} \in \mathbb{F}_q^{r \times n}$.
- Inputs:
  - $\mathsf{Supp}(\boldsymbol{x}) = \langle 1, x_2, \ldots, x_r \rangle$;
  - $\boldsymbol{C} \in \mathbb{F}_q^{r \times (n-r)}$ such that $(1, x_2, \ldots, x_r) \cdot \begin{pmatrix} \boldsymbol{I_r} & \boldsymbol{C} \end{pmatrix} = (1, x_2, \ldots, x_n) = \boldsymbol{x}$.

Dual support decomposition

- New modeling to achieve smaller signature sizes.
- For RSD: improvement of the Rank Decomposition modeling, Shamir's secret sharing $\rightarrow$ easier multiplications.
- Check that $\boldsymbol{H}\boldsymbol{x}^\top = \boldsymbol{y}^\top$ with $\boldsymbol{x}$ of weight $\leq r$.
- $\boldsymbol{x}$ of small weight $\rightarrow$ $\boldsymbol{x} = (x_1, \ldots, x_r) \cdot \boldsymbol{C}$ with $\boldsymbol{C} \in \mathbb{F}_q^{r \times n}$.
- Inputs:
  - $\mathsf{Supp}(\boldsymbol{x}) = \langle 1, x_2, \ldots, x_r \rangle$;
  - $\boldsymbol{C} \in \mathbb{F}_q^{r \times (n-r)}$ such that $(1, x_2, \ldots, x_r) \cdot \begin{pmatrix} \boldsymbol{I_r} & \boldsymbol{C} \end{pmatrix} = (1, x_2, \ldots, x_n) = \boldsymbol{x}$.
- Just compute $\boldsymbol{H} \cdot \boldsymbol{C}^\top \cdot (1, x_2, \ldots, x_r)^\top$: witness size is $(r-1)m + r(n-r)$.

- For MinRank, more work to adapt: How to avoid sending $\boldsymbol{x}$? $\rightarrow$ simple solution, but not used in this context before.

• For MinRank, more work to adapt: How to avoid sending $\boldsymbol{x}$? $\rightarrow$ simple solution, but not used in this context before.

$$
\begin{array}{rccc}
\rho : & \mathbb{F}_q^{m \times n} & \rightarrow & \mathbb{F}_q^{mn} \\
& \begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{m,1} & \dots & a_{m,n} \end{pmatrix} & \mapsto & \begin{pmatrix} a_{1,1}, \dots, a_{1,n}, \dots, a_{m,1}, \dots, a_{m,n} \end{pmatrix} .
\end{array}
$$

• For MinRank, more work to adapt: How to avoid sending $\boldsymbol{x}$? $\rightarrow$ simple solution, but not used in this context before.

$$\begin{array}{rccc} \rho : & \mathbb{F}_q^{m\times n} & \rightarrow & \mathbb{F}_q^{mn} \\ & \begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{m,1} & \dots & a_{m,n} \end{pmatrix} & \mapsto & \left(a_{1,1},\dots,a_{1,n},\dots,a_{m,1},\dots,a_{m,n}\right) . \end{array}$$

• Given the MinRank instance, build $\boldsymbol{G} = \begin{pmatrix} \rho(\boldsymbol{M}_1) \\ \vdots \\ \rho(\boldsymbol{M}_k) \end{pmatrix}$.

• For MinRank, more work to adapt: How to avoid sending $\boldsymbol{x}$? $\rightarrow$ simple solution, but not used in this context before.

$$\begin{array}{rccc} \rho : & \mathbb{F}_q^{m\times n} & \rightarrow & \mathbb{F}_q^{mn} \\ & \begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{m,1} & \dots & a_{m,n} \end{pmatrix} & \mapsto & \left(a_{1,1}, \dots, a_{1,n}, \dots, a_{m,1}, \dots, a_{m,n}\right) \end{array} .$$

• Given the MinRank instance, build $\boldsymbol{G} = \begin{pmatrix} \rho(\boldsymbol{M}_1) \\ \vdots \\ \rho(\boldsymbol{M}_k) \end{pmatrix}$.

• We have the relation $\rho(\boldsymbol{M}) = -\boldsymbol{x}\boldsymbol{G} + \rho(\boldsymbol{E}) \rightarrow$ Apply the dual.

MinRank Syndrome

Given $\boldsymbol{H} := \begin{bmatrix} \boldsymbol{I_{mn-k}} & \boldsymbol{H'} \end{bmatrix} \in \mathbb{F}_q^{(mn-k)\times mn}$ where $\boldsymbol{H'} \in \mathbb{F}_q^{(mn-k)\times k}$ and $\boldsymbol{y} \in \mathbb{F}_q^{mn-k}$, find $\boldsymbol{E}$ such that $\rho(\boldsymbol{E})\boldsymbol{H}^\top = \boldsymbol{y}$ and $\mathsf{rank}(\boldsymbol{E}) \leq r$.

MinRank Syndrome

Given $\boldsymbol{H} := \begin{bmatrix} \boldsymbol{I_{mn-k}} & \boldsymbol{H'} \end{bmatrix} \in \mathbb{F}_q^{(mn-k)\times mn}$ where $\boldsymbol{H'} \in \mathbb{F}_q^{(mn-k)\times k}$ and $\boldsymbol{y} \in \mathbb{F}_q^{mn-k}$, find $\boldsymbol{E}$ such that $\rho(\boldsymbol{E})\boldsymbol{H}^\top = \boldsymbol{y}$ and $\mathsf{rank}(\boldsymbol{E}) \leq r$.

- For the dual support, inputs are: $\boldsymbol{S} \in \mathbb{F}_q^{m\times r}$ and $\boldsymbol{C} \in \mathbb{F}_q^{r\times n}$
- The protocol: $\rho(\boldsymbol{SC})\boldsymbol{H}^\top = \boldsymbol{y} \quad$ with $\boldsymbol{S} = \begin{bmatrix} \boldsymbol{I_r} \\ \boldsymbol{S'} \end{bmatrix}$.

MinRank Syndrome

Given $\boldsymbol{H} := \begin{bmatrix} \boldsymbol{I_{mn-k}} & \boldsymbol{H'} \end{bmatrix} \in \mathbb{F}_q^{(mn-k)\times mn}$ where $\boldsymbol{H'} \in \mathbb{F}_q^{(mn-k)\times k}$ and $\boldsymbol{y} \in \mathbb{F}_q^{mn-k}$, find $\boldsymbol{E}$ such that $\rho(\boldsymbol{E})\boldsymbol{H}^\top = \boldsymbol{y}$ and $\mathsf{rank}(\boldsymbol{E}) \leq r$.

- For the dual support, inputs are: $\boldsymbol{S} \in \mathbb{F}_q^{m\times r}$ and $\boldsymbol{C} \in \mathbb{F}_q^{r\times n}$
- The protocol: $\rho(\boldsymbol{SC})\boldsymbol{H}^\top = \boldsymbol{y} \quad$ with $\boldsymbol{S} = \begin{bmatrix} \boldsymbol{I_r} \\ \boldsymbol{S'} \end{bmatrix}$.
- Important to note: size does not depend on k $\rightarrow$ explore other areas of parameters.
- Open doors for new cryptosystems based on MinRank (Niederreiter types of schemes for instance).

Comparison of the modelings

Modeling	Witness size	Parameters for $\lambda = 128$	
		(q, m, n, k, r)	Size
Rank Decomposition	$[\,km + (r-1)m + r(n-r)\,] \cdot \log_2(q)$	$(2, 31, 33, 15, 10)$	122 B
q-polynomial	$[\,km + (r-1)m\,] \cdot \log_2(q)$	$(2, 31, 33, 15, 10)$	93 B
Kipnis-Shamir	$[\,km + (r-1)(n-r)\,] \cdot \log_2(q)$	$(2, 31, 33, 15, 10)$	86 B
Dual Support Decomp.	$[\,(r-1)m + r(n-r)\,] \cdot \log_2(q)$	$(2, 53, 53, 45, 4)$	45 B

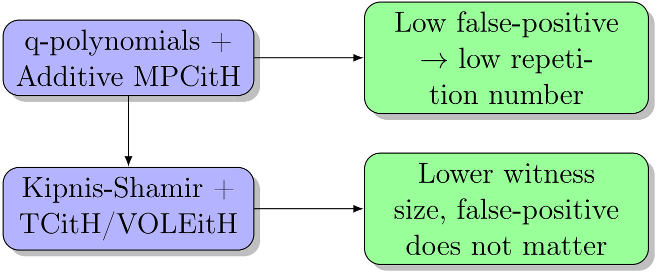
Table: Witness size for the RSD problem.

Modeling	Witness size	Parameters for $\lambda = 128$	
		(q, m, n, k, r)	Size
Rank Decomposition	$[\,k + r(m-r) + rn\,] \cdot \log_2(q)$	$(16, 15, 15, 78, 6)$	111 B
q-polynomial	$[\,k + rm\,] \cdot \log_2(q)$	$(16, 15, 15, 78, 6)$	76 B
Kipnis-Shamir	$[\,k + r(n-r)\,] \cdot \log_2(q)$	$(16, 15, 15, 78, 6)$	66 B
Dual Support Decomp.	$[\,r(m-r) + rn\,] \cdot \log_2(q)$	$(2, 43, 43, 1520, 4)$	41 B

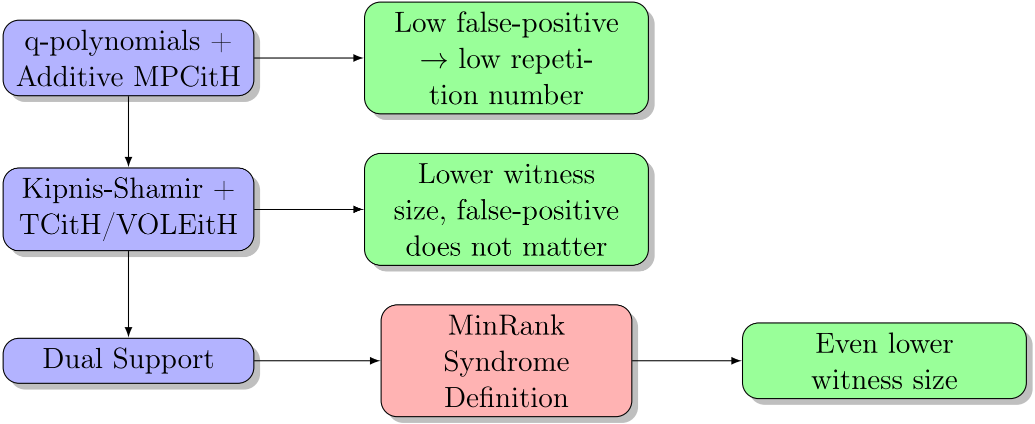
Table: Witness size for MinRank

Summary

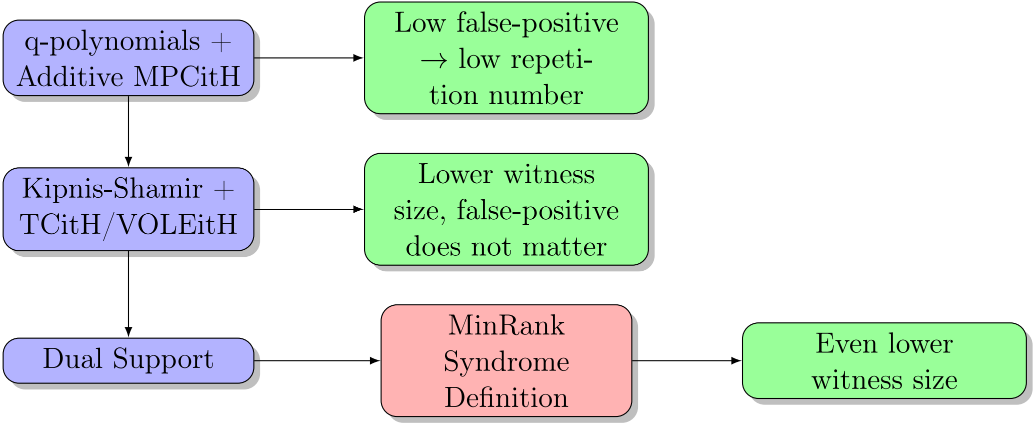
q-polynomials + Additive MPCitH $\longrightarrow$ Low false-positive $\rightarrow$ low repetition number


q-polynomials + Additive MPCitH
Low false-positive → low repetition number
Kipnis-Shamir + TCitH/VOLEitH
Lower witness size, false-positive does not matter

Summary


q-polynomials + Additive MPCitH
Low false-positive → low repetition number
Kipnis-Shamir + TCitH/VOLEitH
Lower witness size, false-positive does not matter
Dual Support
MinRank Syndrome Definition
Even lower witness size

Summary



- Parameters on GV bound → hardest instances.
- Resiliancy: more secure parameters for MinRank and RSD → not much bigger signatures.

Parameters and performances

Security	Trade-off	Framework	τ	Signature	Estimated time (MCycles)
NIST I	Short	TCitH	12	2 937 B	16.0
		VOLEitH	11	2 851 B	14.9
	Fast	TCitH	20	3 708 B	5.0
		VOLEitH	16	3 450 B	2.7
NIST III	Short	TCitH	18	6 713 B	54.3
		VOLEitH	16	6 566 B	40.6
	Fast	TCitH	30	8 454 B	33.3
		VOLEitH	24	8 207 B	8.0
NIST V	Short	TCitH	25	12 371 B	79.8
		VOLEitH	22	12 682 B	50.1
	Fast	TCitH	39	14 926 B	60.8
		VOLEitH	32	14 768 B	11.8

Table: Parameters and performance - RSD

- Will be used for RYDE - 2nd round.

Parameters and performances

Security	Trade-off	Framework	τ	Signature	Estimated time (MCycles)
NIST I	Short	TCitH	12	2 896 B	35.7
		VOLEitH	11	2 813 B	72.9
	Fast	TCitH	20	3 640 B	12.5
		VOLEitH	16	3 396 B	60.7
NIST III	Short	TCitH	18	6 584 B	111.0
		VOLEitH	16	6 452 B	270.5
	Fast	TCitH	30	8 240 B	42.8
		VOLEitH	24	8 036 B	237.9
NIST V	Short	TCitH	25	12 149 B	220.9
		VOLEitH	22	12 486 B	763.2
	Fast	TCitH	39	14 579 B	93.4
		VOLEitH	32	14 484 B	734.9

Table: Parameters and performance - MinRank

- Will be used for Mirath - 2nd round.

Thank you for your attention

Gora Adj, Stefano Barbero, Emanuele Bellini, Andre Esser, Luis Rivera-Zamarripa, Carlo Sanna, Javier Verbel, and Floyd Zweydinger.
MiRitH.
NIST's Post-Quantum Cryptography Standardization of Additional Digital Signature Schemes Project (Round 1), `https://pqc-mirith.org/`, 2023.

Nicolas Aragon, Magali Bardet, Loïc Bidoux, Jesús-Javier Chi-Domínguez, Victor Dyseryn, Thibauld Feneuil, Philippe Gaborit, Antoine Joux, Matthieu Rivain, Jean-Pierre Tillich, and Adrien Vincotte.
RYDE.
NIST's Post-Quantum Cryptography Standardization of Additional Digital Signature Schemes Project (Round 1), `https://pqc-ryde.org/`, 2023.

Nicolas Aragon, Magali Bardet, Loïc Bidoux, Jesús-Javier Chi-Domínguez, Victor Dyseryn, Thibauld Feneuil, Philippe Gaborit, Romaric Neveu, Matthieu Rivain, and Jean-Pierre Tillich.
MIRA.
NIST's Post-Quantum Cryptography Standardization of Additional Digital Signature Schemes Project (Round 1), `https://pqc-mira.org/`, 2023.

Carlos Aguilar-Melchor, Philippe Gaborit, and Julien Schrek.

A new zero-knowledge code based identification scheme with reduced communication.

2011 IEEE Information Theory Workshop, pages 648–652, 2011.

Gora Adj, Luis Rivera-Zamarripa, and Javier Verbel.

Minrank in the head.

In Nadia El Mrabet, Luca De Feo, and Sylvain Duquesne, editors, *Progress in Cryptology - AFRICACRYPT 2023*, pages 3–27, Cham, 2023. Springer Nature Switzerland.

Carsten Baum, Lennart Braun, Cyprien Delpech de Saint Guilhem, Michael Klooß, Emmanuela Orsini, Lawrence Roy, and Peter Scholl.

Publicly verifiable zero-knowledge and post-quantum signatures from vole-in-the-head.

In Helena Handschuh and Anna Lysyanskaya, editors, *Advances in Cryptology – CRYPTO 2023*, pages 581–615, Cham, 2023. Springer Nature Switzerland.

Emanuele Bellini, Andre Esser, Carlo Sanna, and Javier Verbel.

Mr-dss – smaller minrank-based (ring-)signatures.

In *Post-Quantum Cryptography: 13th International Workshop, PQCrypto 2022, Virtual Event, September 28–30, 2022, Proceedings*, page 144–169, Berlin, Heidelberg, 2022. Springer-Verlag.

Loïc Bidoux and Philippe Gaborit.

Compact Post-quantum Signatures from Proofs of Knowledge Leveraging Structure for the PKP, SD and RSD Problems.
In *Codes, Cryptology and Information Security (C2SI)*, 2023.

Nicolas T. Courtois.
Efficient zero-knowledge authentication based on a linear algebra problem minrank.
In Colin Boyd, editor, *Advances in Cryptology — ASIACRYPT 2001*, pages 402–421, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

Thibauld Feneuil.
Building MPCitH-based signatures from MQ, MinRank, Rank SD and PKP.
In *International Conference on Applied Cryptography and Network Security (ACNS)*, 2024.

Thibauld Feneuil, Antoine Joux, and Matthieu Rivain.
Shared permutation for syndrome decoding: new zero-knowledge protocol and code-based signature.
Designs, Codes and Cryptography, 91:563–608, 2022.

Thibauld Feneuil, Antoine Joux, and Matthieu Rivain.
Syndrome Decoding in the Head: Shorter Signatures from Zero-Knowledge Proofs.
In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology – CRYPTO 2022*, pages 541–572, Cham, 2022. Springer Nature Switzerland.

Thibauld Feneuil and Matthieu Rivain.
Threshold Computation in the Head: Improved Framework for Post-Quantum Signatures and Zero-Knowledge Arguments.
Cryptology ePrint Archive, Report 2023/1573, 2023.

Thibauld Feneuil and Matthieu Rivain.
Threshold Linear Secret Sharing to the Rescue of MPC-in-the-Head.
In *International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt)*, 2023.

Bagus Santoso, Yasuhiko Ikematsu, Shuhei Nakamura, and Takanori Yasuda.
Three-pass identification scheme based on minrank problem with half cheating probability, 2022.

Jacques Stern.
A new identification scheme based on syndrome decoding.
In *International Cryptology Conference (CRYPTO)*, 1993.

Pascal Véron.
Improved Identification Schemes Based on Error-Correcting Codes.
Applicable Algebra in Engineering, Communication and Computing, 8(1), January 1997.