Ramp hyper-invertible matrices and their applications to MPC protocols

Hongqing Liu[1], Chaoping Xing[1], Yanjiang Yang[2] and Chen Yuan[1]

Shanghai Jiao Tong University,China

Huawei International, Singapore

December 6, 2023

Hyper invertible matrix [BH08]

Hyper invertible matrix

An $m \times n$ matrix over $\mathbb{F}_q$ is called hyper invertible matrix(HIM) $\iff$ every square sub-matrix is invertible.

Hyper invertible function

A mapping f from n values $(x_1, \cdots, x_n)$ to m values $(y_1, \cdots, y_m)$ is called hyper invertible function(HIF) $\iff$ given any n values(inputs and outputs), one can compute other m values.

Relationship between HIM and HIF

If M is an HIM, then $f_M : (y_1, \cdots, y_m)^T = M(x_1, \cdots, x_n)^T$ is an HIF.

Construction of HIM

Construction of HIF: $(x_1, \cdots, x_n) \to (y_1, \cdots, y_m)$

1. Fix $n+m$ distinct values $\alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_m \in \mathbb{F}_q$
2. Choose a polynomial $f(z)$ such that $f(\alpha_i) = x_i$ for $i \in [n]$
3. Compute $y_i = f(\beta_i)$ for $i \in [m]$

Construction of HIM (polynomial interpolation)

$$M_{i,j} = \prod_{k \neq j} \frac{\beta_i - \alpha_k}{\alpha_j - \alpha_k}$$

Application of HIM: generating random sharing

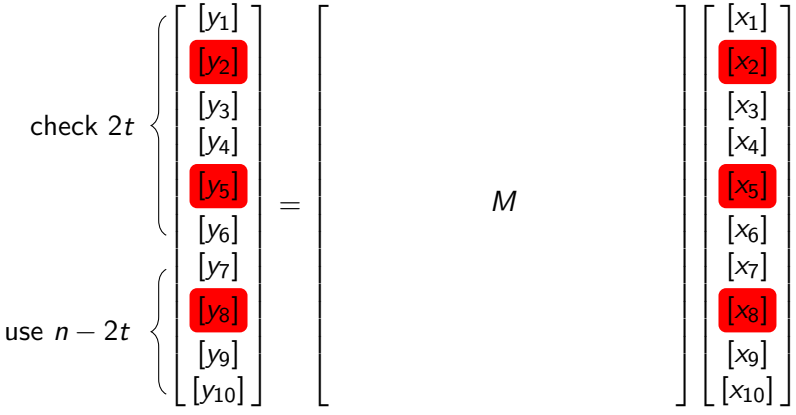
Model

- n parties, $t \leq n/3$ parties are corrupted by a malicious adversary
- Linear secret sharing scheme $[x]$
- An $n \times n$ hyper invertible matrix M

Generating random sharing

1. Every P_i distributes a random sharing $[x_i]$ to all parties
2. All parties locally compute $([y_1], \ldots, [y_n])^T = M([x_1], \cdots, [x_n])^T$
3. For $i \in [2t]$, all parties open $[y_i]$ to P_i and P_i checks the consistency
4. If no party complains, output remaining $n - 2t$ random sharings $[y_{2t+1}], \cdots, [y_n]$

Application of HIM: generating random sharing



Application of HIM: generating random sharing

Advantages of HIM in generating random sharings

- The verification is deterministic and error probability is zero.
- To generate $O(n)$ random sharings, the parties communicate $O(n^2)$ field elements, therefore amortized communication is $O(n)$.
- The MPC protocol realizes perfect security.

Functionality of HIM

- Extract randomness (**privacy**)
- Check consistency (**reconstruction**)

From HIM to ramp HIM

Restriction of HIM

An $n \times n$ HIM requires that there are $2n$ evaluation points in $\mathbb{F}_q$, which is equivalent to $q \geq 2n$.

Goal

Question: Can we construct HIM over constant-size fields?

Answer: We can construct a variant of HIM — ramp HIM over constant-size fields.

Ramp hyper invertible matrix

Ramp hyper invertible matrix

An $m \times n$ matrix M over $\mathbb{F}_q$ with $m \leq n$ is called $(n, m; r, p)_q$-ramp hyper invertible matrix if

1. For any integer s, t such that $0 \leq s \leq m, 0 \leq t \leq n$ and $s + t \geq r$, every $s \times (n - t)$ sub-matrix has full column rank
2. For any integer s, t such that $0 \leq s \leq m, 0 \leq t \leq n$ and $s + t \leq p$, every $s \times (n - t)$ sub-matrix has full row rank

Relationship between ramp HIM and HIM

An $(n, m; n, n)$-ramp HIM is actually an $m \times n$ HIM. Therefore, ramp HIM is the generalization of HIM.

Ramp hyper invertible function

Ramp hyper invertible function

An $\mathbb{F}_q$-linear mapping $f : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is called as $(n, m; r, p)_q$-ramp hyper invertible matrix if

1. Given any subset $I \subset [n]$ and $J \subset [m]$ with $|I| + |J| \geq r$, and $\boldsymbol{x} \in \mathbb{F}_q^n$ and $\boldsymbol{y} \in \mathbb{F}_q^m$ with $\boldsymbol{y} = f(\boldsymbol{x})$, $\boldsymbol{x}_I$ and $\boldsymbol{y}_J$ uniquely determine $\boldsymbol{x}_{\bar{I}}$.
2. Given any subset $I \subset [n]$ and $J \subset [m]$ with $|I| + |J| \leq p$ and vector $\boldsymbol{u}_I \in \mathbb{F}_q^{|I|}$, the composition map $\pi_J \circ f(\boldsymbol{u}_I, \boldsymbol{x}_{\bar{I}})$ is a surjective mapping from $\mathbb{F}_q^{|\bar{I}|}$ to $\mathbb{F}_q^{|J|}$

$$\mathbb{F}_q^{|\bar{I}|} \xrightarrow{f(\boldsymbol{u}_I, \boldsymbol{x}_{\bar{I}})} \mathbb{F}_q^m \xrightarrow{\pi_J} \mathbb{F}_q^{|J|}$$

where π_J is the projection mapping at index set J.

Construction of ramp HIM

Connection with linear codes

The following are equivalent

1. There exists an $[n, m; r, p]_q$-ramp HIM
2. There exists an $[n, m; r, p]_q$-ramp HIF
3. There exists an $[n + m, n, n + m - r + 1]$ linear code C over $\mathbb{F}_q$ with dual distance $p + 1$.

Goal

To construct a ramp HIM with **small reconstruction** r and **large privacy** p, we need a linear code with both large **distance** and **dual distance**.

Construction of ramp HIM

Algebraic geometry code

Let $\mathcal{X}/\mathbb{F}_q$ be an algebraic curve of genus g with at least $m+n+1$ pairwise distinct rational points. If $g-1 \leq m \leq n$, then there exists an $(n, m; r, p)_q$-ramp HIM with $r \leq n+g$ and $p \geq n-g$.

Conclusion

If $q = O(1/\epsilon^2)$ for $\epsilon \in (0,1)$, then there exists a family of $(n, n; (1+\epsilon)n, (1-\epsilon)n)_q$-ramp HIMs with $n \to \infty$. Furthermore, this family can be constructed in time $O(n^3)$.

Perfectly secure MPC over constant-size fields

Model

- Constant-size field $\mathbb{F}_q$ ($q = O(1/\epsilon^2)$)
- n parties, $t \leq \frac{1-\epsilon}{3}n$ parties are corrupted by a malicious adversary
- Arithmetic secret sharing $[x]$ over $\mathbb{F}_q$
- An $(n, n; (1+\epsilon)n, (1-\epsilon)n)_q$-ramp HIM M.

Obstacles

- Ramp HIM over constant-size fields (**Generating random sharing**)
- **Dynamic** arithmetic secret sharing over constant-size fields (**Player elimination**)
- Error correction over constant-size fields (**Public reconstruction**)

Perfectly secure MPC over constant-size fields

Arithmetic secret sharing

- secret space: $\mathbb{F}_q^{\frac{\epsilon}{6}n}$
- $\frac{1-\epsilon}{3}n$-privacy and $\frac{n}{3}$-reconstruction
- strongly multiplicative

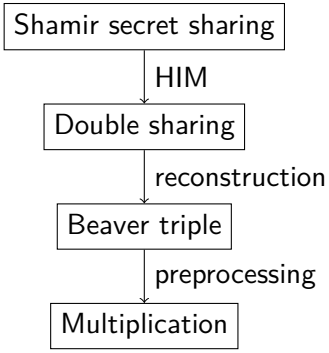
Generating random sharings

1. Every P_i distributes a random sharing $[x_i]$ to all parties
2. All parties locally compute $([y_1], \cdots, [y_n])^T = M([x_1], \cdots, [x_n])^T$
3. For $i \in [t+1, n]$, all parties open $[y_i]$ to P_i and P_i checks the consistency
4. If no party complains, output the remaining t random sharings $[y_1], \cdots, [y_t]$

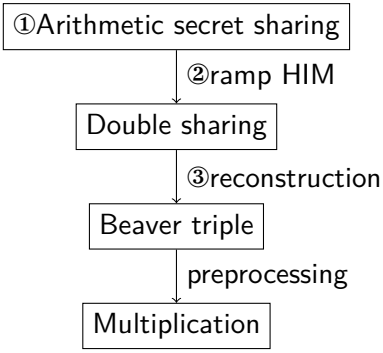
Perfectly secure MPC over constant-size fields

$$\begin{matrix} \text{use } t \\ \\ \\ \text{check } n-t \\ \\ \\ \\ \\ \\ \end{matrix} \left\{ \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix} \right. \begin{bmatrix} [y_1] \\ [y_2] \\ [y_3] \\ [y_4] \\ [y_5] \\ [y_6] \\ [y_7] \\ [y_8] \\ [y_9] \\ [y_{10}] \end{bmatrix} = \begin{bmatrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{bmatrix} M \begin{bmatrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{bmatrix} \begin{bmatrix} [x_1] \\ [x_2] \\ [x_3] \\ [x_4] \\ [x_5] \\ [x_6] \\ [x_7] \\ [x_8] \\ [x_9] \\ [x_{10}] \end{bmatrix}$$

Perfectly secure MPC over $\mathbb{F}_q$

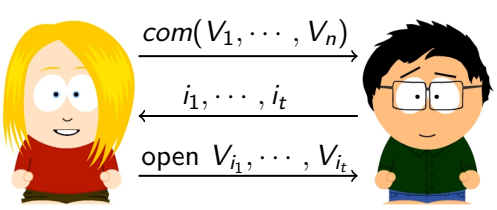


$q \geq 2n$

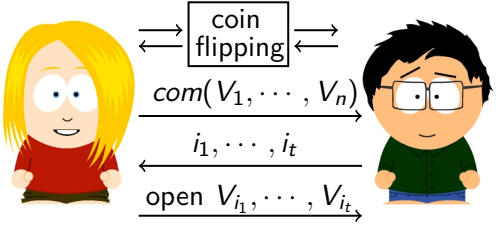


$q = O(1/\epsilon^2)$

MPC-in-the-head [Ish+07]



perfectly secure MPC



statistically secure MPC

MPC-in-the-head

Check consistency of randomness via ramp HIM

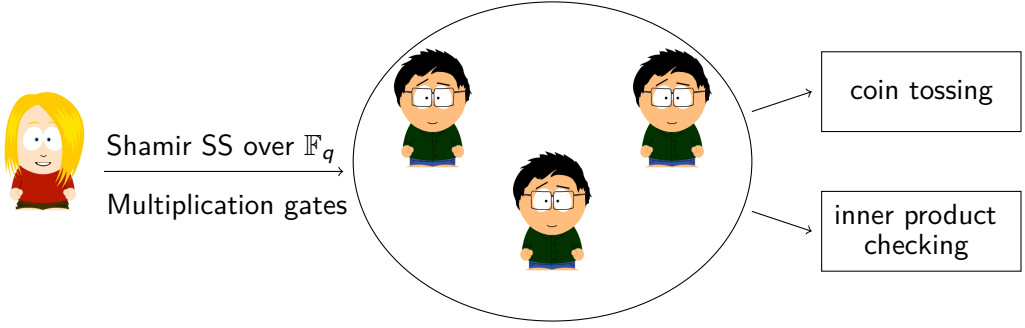
Setup: n imaginary parties $\{P_i\}_{i\in[n]}$ and an input client I
Private input: an $(n, n; (1+\epsilon)n, (1-\epsilon)n)$-ramp HIM
Private input: P_i obtains corresponding shares of $[\boldsymbol{r}_1]_d, \cdots, [\boldsymbol{r}_{2t}]_d$

- I randomly generates $[\boldsymbol{r}_{2t+1}]_d, \cdots, [\boldsymbol{r}_n]_d$ and distributes shares to $P_1, \cdots, P_n$
- Parties locally compute $([\boldsymbol{s}_1]_d, \cdots, [\boldsymbol{s}_n]_d)^T = M([\boldsymbol{r}_1]_d, \cdots, [\boldsymbol{r}_n]_d)^T$
- Party P_i receives all shares of $[\boldsymbol{s}_i]$ from other parties and checks the consistency.
- If no party complains, the parties conclude that $[\boldsymbol{r}_1]_d, \cdots, [\boldsymbol{r}_{2t}]_d$ are consistent.

Multi-Verifier Zero-Knowledge [YW22]

Model

- One prover, n verifiers.
- $t \leq n/2$ verifiers are corrupted by a malicious adversary.



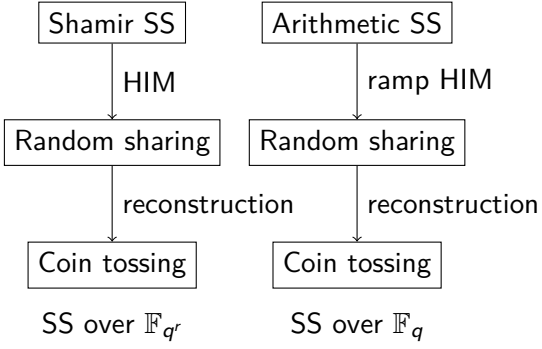
Multi-Verifier Zero-Knowledge

Coin tossing

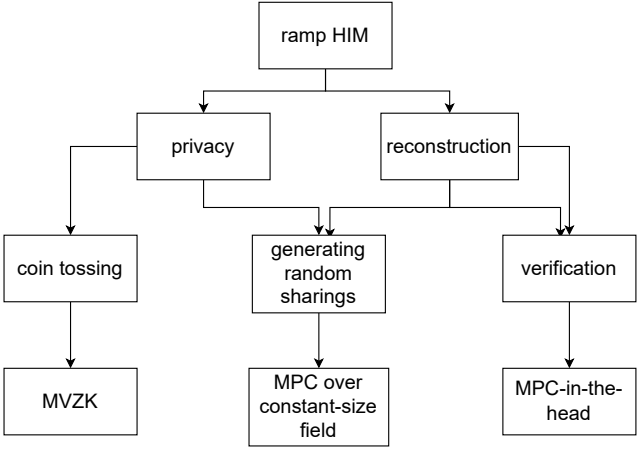
- n verifiers sample $\chi \leftarrow \mathbb{F}_{q^r}$ as challenge
- Soundness error: $\frac{|C|-1}{q^r} \leq 2^{-\lambda}$
- Comm: $O(n^2(\boldsymbol{\lambda} + \mathbf{log}\,|\boldsymbol{C}|))$

Coin tossing over constant fields

- $\epsilon = O(\frac{\lambda + \log|C|}{n})$
- $t = \frac{1-\epsilon}{2}n$
- Secret space: $\mathbb{F}_q^{\Omega(\epsilon n)} \simeq \mathbb{F}_{q^{\Omega}(\epsilon n)}$



Summary: Application of ramp HIM



References

[BH08] Zuzana Beerliová-Trubíniová and Martin Hirt. "Perfectly-Secure MPC with Linear Communication Complexity". In: *TCC*. Vol. 4948. Springer, 2008, pp. 213–230.

[Ish+07] Yuval Ishai et al. "Zero-knowledge from secure multiparty computation". In: *STOC*. ACM, 2007, pp. 21–30.

[YW22] Kang Yang and Xiao Wang. "Non-interactive Zero-Knowledge Proofs to Multiple Verifiers". In: *ASIACRYPT*. Vol. 13793. Springer, 2022, pp. 517–546.