Hyper-Invertible Matrices and Applications

Martin Hirt

ETH Zurich

Theory and Practice of MPC, Aarhus, June 2012

Outline

Hyper-Invertible Matrices

- Motivation
- Definition & Properties
- Construction
- Applications
- Conclusions

How can n parties generate random values?

Model

- n parties, t are bad
- aim for random *shared* values (sharing doesn't matter)

Approach 1

1. Every P_i shares random value x_i
2. $y = \sum_{i=1}^{n} x_i$

Only one good sharing from n sharings

Approach 2

1. Every P_i shares random value x_i
2. $y_1 = \sum_i \lambda_{1i} x_i, \qquad y_2 = \sum_i \lambda_{2i} x_i, \qquad \ldots$

How many good sharings from n sharings?

Best we can hope for: $n - t$

More Abstractly ...

Given: n values

$$x_1 \quad x_2 \quad x_3 \quad x_4 \quad x_5 \quad \dots \quad x_n$$

where

- $n - t$ values are good (e.g. uniformly random),
- t values are bad (e.g. chosen by adversary).

Goal: Find (the) $n - t$ good values

Goal': Find $y_1, \dots, y_{n-t}$ which are "as good as" $x_2, x_5, \dots, x_n$.

$$\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_{n-t} \\ y_{n-t+1} \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} \\ \\ \text{Hyper-Invertible} \\ \text{Matrix} \\ \\ \\ \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ \vdots \\ x_n \end{bmatrix}$$

Hyper-Invertible Matrix — The Definition

Def: M is *hyper-invertible* $:\Longleftrightarrow$ every square sub-matrix M_R^C is invertible.

$$\begin{bmatrix} \lambda_{11} & \lambda_{12} & \lambda_{13} & \cdots & \lambda_{1n} \\ \lambda_{21} & \lambda_{22} & \lambda_{23} & & \lambda_{2n} \\ \vdots & & & & \vdots \\ \lambda_{m1} & \lambda_{m2} & \lambda_{m3} & \cdots & \lambda_{mn} \end{bmatrix}$$

Note: Cf. Parity-check matrix of MDS-Codes, Cauchy matrices, . . .

Properties (1/2)

Property 1: Given some x_j-s and some y_i-s (in total n values), one can compute all other x_j-s and y_i-s .

$$\begin{bmatrix} y_1 \\ y_2 \\ \cdot \\ y_m \end{bmatrix} = \begin{bmatrix} & & \\ & M & \\ & & \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ x_n \end{bmatrix}$$

Lemma 1: Given HIM M, index sets $C \subseteq \{1 \ldots n\}$, $R \subseteq \{1 \ldots m\}$ with $|\overline{C}| = |R|$. Then given $\left(\vec{x}_C\,,\ \vec{y}_R\right)$ one can compute $\left(\vec{x}_{\overline{C}}\,,\ \vec{y}_{\overline{R}}\right)$.

Proof: 1. $\vec{y}_R = M_R\,\vec{x} = M_R^C \vec{x}_C + M_R^{\overline{C}} \vec{x}_{\overline{C}}$

2. $\vec{x}_{\overline{C}} = \left(M_R^{\overline{C}}\right)^{-1} \left(\vec{y}_R - M_R^C\,\vec{x}_C\right)$

Properties (1/2)

Property 1: Given some x_j-s and some y_i-s (in total n values), one can compute all other x_j-s and y_i-s .

$$\begin{bmatrix} y_1 \\ y_2 \\ \cdot \\ y_m \end{bmatrix} = \begin{bmatrix} & & \\ & M & \\ & & \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ x_n \end{bmatrix}$$

Lemma 2: Given matrix M. **If for all** $C \subseteq \{1 \ldots n\}$, $R \subseteq \{1 \ldots m\}$ with $|\overline{C}| = |R|$ one can compute $\vec{x}_{\overline{C}}$ from $(\vec{x}_C, \vec{y}_R)$, **then M is HIM.**

Proof: Invert $M_R^{\overline{C}}$ as follows:

1. Given $\vec{y}_R$. Let $\vec{x}_C = \vec{0}$
2. Can compute $\vec{x}_{\overline{C}} \rightarrow \left(M_R^{\overline{C}}\right)^{-1}$

Properties (2/2)

Property 2: Fix k values , then there is a bijection from any $n-k$ values to any other $n-k$ values .

$$\begin{bmatrix} y_1 \\ y_2 \\ \cdot \\ y_m \end{bmatrix} = \begin{bmatrix} & & \\ & M & \\ & & \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ x_n \end{bmatrix}$$

The Construction

Idea: Construct mapping $(x_1, .., x_n) \mapsto (y_1, .., y_m)$ with Property 1.

Construction

1. fix values $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m$ in $\mathcal{F}$
2. let polynomial $f(z)$ s.t. $f(\alpha_j) = x_j \quad \forall j$
3. compute $y_i = f(\beta_i) \quad \forall i$

Formally

- $f(z) = \sum_{j=1}^{n} \prod_{\substack{k=1 \\ k \neq j}}^{n} \frac{z - \alpha_k}{\alpha_j - \alpha_k} \; x_j$
- $y_i = f(\beta_i) = \sum_{j=1}^{n} \underbrace{\prod_{\substack{k=1 \\ k \neq j}}^{n} \frac{\beta_i - \alpha_k}{\alpha_j - \alpha_k}}_{\lambda_{i,j}} \; x_j = \sum_{j=1}^{n} \lambda_{i,j} \, x_j$
- $M := \left[\lambda_{i,j}\right]$

The Field

The Field Size

- Previous construction requires $|\mathcal{F}| \geq n + m$.
- Easy patch: $|\mathcal{F}| = n + m - 1$.

Lower Bounds (Conjecture)

- $|\mathcal{F}| = n + m - 1$ is optimal for $\mathcal{F} \neq \mathrm{GF}(2^k)$
- But: $\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$ is HIM over $\mathrm{GF}(4)$ (though $m + n - 1 = 5$)

Randomness Extraction – Passive Security

Model

- n parties, t are bad **(passive only)**
- aim for random *shared* values
- given $n \times n$ hyper-invertible matrix M

Protocol

1. Every P_i shares random value $x_i \to [x_i]$
2. $([y_1], \ldots, [y_n]) = M([x_1], \ldots, [x_n])$
3. Output $[y_1], \ldots, [y_{n-t}]$

Analysis

- Adversary $A \subseteq \{1, \ldots, n\}$, $|A| = t$, hence knows $\overrightarrow{[x]}_A$.
- Prop. 2: Fix A, $\overrightarrow{[x]}_A$, mapping $\overrightarrow{[x]}_{\overline{A}} \mapsto \overrightarrow{[y]}_{\{1,\ldots,n-t\}}$ is bijective.

Randomness Extraction – Active Security – Attempt #1

Model

- n parties, t are bad **(active)**

Protocol

- Every P_i **VSSes** random value $x_i \to [x_i]$
- $\ldots$

Analysis

- works, but complicated & inefficient

Randomness Extraction – Active Security – Attempt #2

Model

- n parties, t are bad **(active)**
- **detectable security** (cf player elimination / dispute control)

Protocol

1. Every P_i **passively** shares random $x_i \to [x_i]$
2. $([y_1], \ldots, [y_n]) = M([x_1], \ldots, [x_n])$
3. Reconstruct and **check degree** of $[y_1], \ldots, [y_t]$
4. Output $[y_{t+1}], \ldots, [y_{n-t}]$

Analysis

- Adversary $A \subseteq \{1, \ldots, n\}$, $|A| = t$; $H \subseteq \overline{A}$, $|H| = n - 2t$.
- Prop. 1: Degrees of $\overrightarrow{[x]}_{\overline{A}}$ and $\overrightarrow{[y]}_{\{1,\ldots,t\}}$ ok $\to$ all degrees ok.
- Prop. 2: Fix $A, \overrightarrow{[x]}_A, \overrightarrow{y}_{\{1,\ldots,t\}}$, bij. mapping $\overrightarrow{[x]}_H \mapsto \overrightarrow{[y]}_{\{t+1,\ldots,n-t\}}$.

Randomness Extraction – Active Security – Attempt #3

Protocol

1. Every P_i **passively** shares random $x_i \to [x_i]$
2. $([y_1], \ldots, [y_n]) = M([x_1], \ldots, [x_n])$
3. For $i = 1, \ldots, 2t$, have P_i check degree of $[y_i]$
4. Output $[y_{2t+1}], \ldots, [y_n]$

Analysis

- Adversary $A \subseteq \{1, \ldots, n\}$, $|A| = t$; $H \subseteq \overline{A}$, $|H| = n - 2t$.
- Prop. 1: Degrees of $\overrightarrow{[x]}_{\overline{A}}$ and $\overrightarrow{[y]}_{\{1,\ldots,2t\}\cap\overline{A}}$ ok $\to$ all degrees ok.
- Prop. 2: Fix $A, \overrightarrow{[x]}_A$, $\overrightarrow{[y]}_{\{1,\ldots,2t\}\cap A}$,

  mapping $\overrightarrow{[x]}_H \mapsto \overrightarrow{[y]}_{\{2t+1,\ldots,n\}}$ is bijective.

Efficiency

- n **passive** sharings $\to n - 2t$ good random sharings

Enhanced Checks

Example: Random Zero-Sharings [0]

1. Every P_i **passively** shares $x_i = 0 \to [x_i]$
2. $([y_1], \ldots, [y_n]) = M([x_1], \ldots, [x_n])$
3. For $i = 1, \ldots, 2t$, have P_i check degree of $[y_i]$ and $y_i \stackrel{?}{=} 0$.
4. Output $[y_{2t+1}], \ldots, [y_n]$

Analysis

- Adversary $A \subseteq \{1, \ldots, n\}$, $|A| = t$
- Prop. 1: If $\overrightarrow{[x]}_{\overline{A}}$ and $\overrightarrow{[y]}_{\{1,\ldots,2t\} \cap \overline{A}}$ have right degree and share 0
  $\Rightarrow$ all sharings have right degree and share 0.

Enhanced Checks – More Abstractly

Requirements

- "Goodness" must be linear: x_1 and x_2 good $\Rightarrow$ $x_1 + x_2$ good.
- Remember: $\left(\overrightarrow{[x]}_A\,,\ \ \overrightarrow{[y]}_{\{t+1,\ldots,n\}} \right) = \mathcal{L}\left(\overrightarrow{[x]}_{\overline{A}}\,,\ \ \overrightarrow{[y]}_{\{1,\ldots,t\}} \right)$
- "Badness" does not need to be linear.

Examples

- Sharings $[x_i]$ of degree $\leq t$
- Sharings $[x_i]$ of degree $\leq t$ and $x_i = 0$
- Shared random bits $[b_i]$ over $\mathrm{GF}(2^k)$.
- Double-sharings $[x_i], [y_i]$ of degrees $\leq t$, $\leq 2t$, resp., and $x_i = y_i$.
- …

Perfect MPC with Active Security

Model

- n parties, $t < n/3$ actively corrupted
- secure channels model (w/o broadcast)

Achievements

- $\mathcal{O}(n\kappa)$ bits for multiplying two κ-bit values

Tools

- Use HIM to generate random $[x], [y]$ of degree t,2t and $x = y$.
- Mult.: $\forall$ P_i compute $v_i = a_i b_i - y_i$, reconstruct v, use $[x] - v$ for $[ab]$.
- Beaver's circuit randomization + Player Elimination

Conclusions

Hyper-Invertible Matrices

- easy to construct
- very good diffusing properties
- perfect security, no probabilities

Applications

- extract randomness (propagate good properties)
- check consistency (concentrate bad properties)
- linear-complexity perfectly-secure MPC, very small overhead
- many more?