Cryptographic Protocols

Spring 2021

MPC Part 5

Setting

- Information-theoretic security, active adversary, $t < n/3$.

Approach

- Values are Shamir-shared with degree $t \rightarrow$ no commitments!
- Reconstruction deals with faulty shares $\rightarrow$ error-correction codes
- Generating random double-sharings $\rightarrow$ hyper-invertible matrices 2.0
- Public reconstruction $\rightarrow$ new trick

Structure

1. Detectable MPC $\rightarrow$ security with abort (abort only in case of cheating)
2. Preprocessing phase $\rightarrow$ circuit randomization
3. Full security $\rightarrow$ player-elimination framework

Goal: Reconstruct sharing $[s]_d$ towards P_i. $(d = t$ or $d = 2t)$

Protocol

$t < n/3$

1. $\forall P_j$: send s_j to $\cancel{P_i}$ U. ← user
2. P_i: If $\exists\, g$ with $\deg(g) \leq d$ and $\left|\{j : s_j = g(\alpha_j)\}\right| \geq d+1+t$ then
   output $s = g(0)$
   else
   ABORT

Correctness: $d+1+t$ shares on $g \Rightarrow d+1$ "honest" shares $\Rightarrow$ correct g.

Robustness: Robust if at least $d+1+t$ honest parties, i.e., if $d < n-2t$.

$d+1+t \leqslant n-t$

Efficiency: Berlekamp-Welch decoder $\Rightarrow$ find g efficiently.

Active Adversaries – Public Reconstruction

Goal: Publicly reconstruct $k+1$ sharings $[s_0]_d, \ldots, [s_k]_d$.

u_1 u_2 u_n

High-Level Protocol

1. Expand $[s_0]_d, \ldots, [s_k]_d$ to $[u_1]_d, \ldots, [u_n]_d$, with redundancy.
2. $\forall P_i$: locally reconstruct $[u_i]_d$ to P_i, send u_i to $\forall P_j$ (might **ABORT**).
3. $\forall P_j$: shrink $u_1, \ldots, u_n$ to $s_0, \ldots, s_k$ (might **ABORT**).

Expansion

- Interpret $s_0, \ldots, s_k$ as coefficients of polynomial g of degree k.
- $u_i = g(\alpha_i) = s_0 + s_1\alpha_i + \ldots + s_k\alpha_i^k, \quad [u_i]_d = [s_0]_d + \ldots + [s_k]_d\alpha_i^k$.
- Shrinking: Find coefficients of g s.t. $|\{i : u_i = g(\alpha_i)\}| \geq k+1+t$.

Correctness: $k+1+t$ values u_i on $g \Rightarrow$ correct g.

Robustness: Robust if $d < n-2t$ **and** $k < n-2t$. e.g. $k = n-2t-1$ $\approx n/3$

Communication: $\mathcal{O}(n^2)$ fe for $k+1$ public reconstructions. ☺

$O(n)$ per public reconstruction

Generate Random Sharings

1. $\forall P_i$: chose random s_i, share s_i with degree $t \to [s_i]$.
2. All: $$2t \begin{bmatrix}[r_1]\\ \vdots \\ [r_n]\end{bmatrix} = \begin{bmatrix} & \text{HIM} & \end{bmatrix} \begin{bmatrix}[s_1]\\ \vdots \\ [s_n]\end{bmatrix}$$ ← n-t "good", right degree
   ← t bad known to adversary
3. For $j = 1, \ldots, 2t$:
   i) Reconstruct $[r_j]$ towards P_j.
   ii) P_j: check that *all* shares of $[r_j]$ lie on polynomial of degree t.
   Otherwise: **ABORT** no abort → all $[s_i]$ are good
4. Output $n - 2t$ sharings $[r_{2t+1}], \ldots, [r_n]$.

Correctness: $n-t$ good $[s_i]$, t checked $[r_j]$, others are linear combinations.

Secrecy: Adv. knows t $[s_i]$ plus t $[r_j]$, any $n-2t$ sharings are random.

Communication: $\mathcal{O}(n^2)$ for $n-2t$ sharings, i.e. $\mathcal{O}(n)$ per sharing. ☺

$\approx n/3$

Generate Random Double-Sharings

1. $\forall P_i$: chose random s_i, share s_i with degrees t and $2t \rightarrow [s_i]_{t,2t}$.
2. All: $$\begin{bmatrix} [r_1]_{t,2t} \\ \vdots \\ [r_n]_{t,2t} \end{bmatrix} = \begin{bmatrix} & & \\ & \text{HIM} & \\ & & \end{bmatrix} \begin{bmatrix} [s_1]_{t,2t} \\ \vdots \\ [s_n]_{t,2t} \end{bmatrix}$$
3. For $j = 1, \ldots, 2t$:
   i) Reconstruct $[r_j]_{t,2t}$ towards P_j.
   ii) P_j: check that *all* shares of $[r_j]_t$ lie on degree-t polynomial g,
   AND that *all* shares of $[r_j]_{2t}$ lie on degree-$2t$ polynomial g',
   AND that $g(0) = g'(0)$.
   Otherwise: **ABORT**
4. Output $n - 2t$ double-sharings $[r_{2t+1}]_{t,2t}, \ldots, [r_n]_{t,2t}$.

Observe: Linear combination of (correct) random double-sharings are (correct) random double-sharings!

$\rightarrow$ same analysis as for “normal” sharings.