CMSC 858K — Introduction to Secure Computation	November 13, 2013
Lecture 29	
Lecturer: Jonathan Katz	*Scribe(s): Xiong Fan*

1 BGW Protocol

BGW protocol is an information-theoretic (in fact, perfect) secure multiparty computation protocol against $t \leq \frac{n}{3}$ corrupted parties:

- In point-to-point model, even broadcast is possible for $t \geq \frac{n}{3}$.
- In broadcast mode, it can achieve its security for $t \leq \frac{n}{2}$.

Below, we recall the BGW protocol in semi-honest case:

Invariant : Parties hold shares of the values on each wire of the circuit.

Multi-Gate : If parties had shares $(a_i), (b_i)$ of value a, b, then each party locally computes $c_i = a_i b_i$. Share c_i with all other parties, then all parties use Lagrange interpolation to get shares $c_1, ..., c_n$ of c.

For BGW protocol in malicious setting:

- Invariant will remain the same.
- Consider output wires:
  1. Say each party P_i holds a valid share a_i of value a, i.e., $a_i = f(i)$ for some f with $f(0) = a$.
  2. During reconstruction, corrupted parties might send a_i.
  3. View shares as codeword in an error-correcting code (ECC). We want an ECC of length n that can recover from t errors.

In fact, shares already gives you a codeword in a Reed-Solomon (RS) code. RS code encodes a polynomial f of degree $deg(f) \leq t$ in n symbols $f(1), ..., f(n)$. Consider two different polynomials f, g:

$\Rightarrow$ f and g can agree on at most t points (if f, g agree on $t+1$ points, then $f - g$ is a non-zero polynomial of degree $deg(f-g) \leq t$ with $t+1$ zeros).

$\Rightarrow$ Min distance is $n - t$.

$\Rightarrow$ Can only hope to recover from less than $\frac{n-t}{2}$ errors.

$\Rightarrow$ $t < \frac{n-t}{2} \Rightarrow t < \frac{n}{3}$ and efficient decoding is possible.

2 Verifiable Secret Sharing (VSS)

Functionality $F_{vss}(q(n))$ (where $q(n)$ is from some designated dealer):

$$F_{vss}(q(x)) = (q(1), q(2), ..., q(n))$$

for q of degree $deg(g) \leq t$.

A bivariate polynomial with degree $deg \leq t$ is $S(x, y) = \sum_{i=0}^{t} \sum_{j=0}^{t} s_{i,j} x^i y^j$. It is uniquely defined by its values on $(1, ..., t+1) \times (1, ..., t+1)$.

For univariate, let δ_i be a degree-t polynomial, such that:

$$\delta_j = \begin{cases} 1, & \text{If } j = i \\ 0, & \text{Otherwise} \end{cases}$$

Given values $y_1, ..., y_{t+1}$ of some polynomial f, recover f as:

$$f(x) = \sum_{i=1}^{t+1} y_i \delta_i(x)$$

For bivariate, given values $z_{1,1}, ..., z_{t+1,t+1}$, recover S as:

$$S(x, y) = \sum_{i=1}^{t+1} \sum_{i=1}^{t+1} z_{i,j} \delta_i(x) \delta_j(x)$$

The protocol for $F_{vss}(q(x))$ is the following:

Phase 1 : Dealer (D) chooses $S(x, y)$ such that $S(0, y) = q(y)$. Define

$$f_i(x) = S(x, i), g_i(y) = S(i, y)$$

Send $(f_i(x), g_i(y))$ to P_i.

Phase 2 : Each P_i sends $(f_i(j), g_i(j))$ to P_j.

Phase 3 : Each P_i: Let (u_j, v_j) be the value received from P_j. If $u_j \neq g_i(j)$ or $v_j \neq f_i(j)$, then broadcast complaint $(i, j f_i(j), g_i(j))$.

Phase 4 : For each complaint (i, j, u, v):

- If $u = S(j, i)$ and $v = S(i, j)$, then do nothing.
- Otherwise, broadcast reveal $(i, f_i(x), g_i(y))$.

Phase 5 : If P_i sees two messages complaint (j, k, u, v) and complaint (kmj, u', v') with $u \neq v'$ or $v \neq u'$. Check that D broadcast approximate reveal messages. If not, go to Phase 6. For each reveal $(j, f_j(x), g_j(y))$:

- If $j = i$, then use f_j, g_j and go to Phase 6.
- If $j \neq i$, check that $f_j(i) = g_i(j)$ and $g_j(i) = f_i(j)$. If not, go to Phase 6.

Broadcast 'good'.

Phase 6 : If more than ($\geq$) $n - t$ parties broadcast 'good', then output $f_i(0)$.

Say D is honest:

- We can check the protocol to see that every honest party will broadcast 'good' (so more than ($\geq$) $n - t$ do so).
- Every honest party output $f_i(0) = S(0, i) = q(i)$.
- Corrupted parties do not learn $q(0)$ from $\{f_i(x), g_i(x)\}_{i \in I}$, where I is the set of corrupted parties.

Say D is malicious. If more than ($\geq$) $n - t$ parties broadcast 'good':

- More than ($\geq$) $n - 2t$ honest parties broadcast 'good'.
- At least $t + 1$ honest parties broadcast 'good'.