Silence Laboratories

1 Dynamic Secret Sharing

Lagrange coefficients. Let $P(\cdot)$ be a polynomial of degree t and let T be a set of $t+1$ points $(x_i, y_i)_{i\in T}$ then for every x we have $P(x) = \sum_{i\in T} y_i \cdot \ell(x)$, where $\ell_i(x) = \prod_{j\in T, j\neq i} \frac{j-x}{j-i}$.

For a set of $t+1$ points, T, we define $\lambda_{i,T} = \ell_i(0) = \prod_{j\in T, j\neq i} \frac{j}{j-i}$. Then, $P(0) = \sum_{i\in T} y_i \cdot \lambda_{i,T}$.

Problem statement. There are two sets of parties, the old group are the P_i's and new group are the P'_i's, as follows.

- Old group: There are n parties: P_i, $i \in \{1, \ldots, n\}$. The parties have a Shamir sharing of a secret x, namely, each P_i holds s_i such that there exists a degree-t polynomial P with $P(i) = s_i$ for all i, and $P(0) = x$.
- The group element $X = x \cdot G$ is public, as well as all X_i's, where $X_i = s_i \cdot G$. Let T be set of $t+1$ points, then $X = \sum \lambda_{i,T} \cdot X_i = (\sum \lambda_{i,T} \cdot s_i) \cdot G = x \cdot G$.
- New group: There are m parties P_i, $i \in \{1, \ldots, m\}$ who wish to obtain shares s'_i such that there exists a degree-t' polynomial Q with $Q(i) = s_i$ for all i, and $Q(0) = x$.

Generic solution with semi-honest parties

1. Choose a committee of $t+1$ parties from the old group. Without loss of generality, let them be $P_1, \ldots, P_{t+1}$.
2. Let λ^x_i, $i \in \{1, \ldots, t+1\}$, be the Lagrange coefficients for computing $P(x)$, that is, $P(x) = \sum_{i=1}^{t+1} \lambda^x_i \cdot s_i$.
3. Each party P_i, $i \in \{1, \ldots, t+1\}$, picks a random degree t' polynomial Q_i, such that $Q_i(0) = s_i$, and sends $s'^j_i = Q_i(j)$ to party P'_j, $j \in \{1, \ldots, m\}$.
4. Note that

$$\begin{aligned} x = P(0) = \sum_{i=1}^{t+1} \lambda^0_i \cdot s_i = \sum_{i=1}^{t+1} \lambda^0_i \cdot Q_i(0) &= \sum_{i=1}^{t+1} \lambda^0_i \cdot \left(\sum_{j\in M} \lambda^0_{j,M} \cdot s'^j_i \right) \\ &= \sum_{i=1}^{t+1} \sum_{j\in M} \lambda^0_i \cdot \lambda^0_{j,M} \cdot s'^j_i \\ &= \sum_{j\in M} \lambda^0_{j,M} \cdot \sum_{i=1}^{t+1} \lambda^0_i \cdot s'^j_i \end{aligned}$$

   where $M \subset \{1, \ldots, m\}$ is some set of size $t'+1$, and $\lambda^0_{j,M}$ is the Lagrange coefficient associated with P_j when evaluating $Q_i(0)$ using the points of parties in M.

Thus, since $s_i = Q_i(0)$ is linearly shared among $P'_1, \ldots, P'_m$, each party P'_j, $j \in \{1, \ldots, m\}$, computes its final share

$$s'_j = \sum_{i=1}^{t+1} \lambda_i^0 \cdot {s'}_i^j$$

The new shares s'_j are correct since for every subset $M \subset \{1, \ldots, m\}$ of size $t'+1$, the below equation holds:

$$\sum_{j \in M} \lambda_{j,M}^0 \cdot {s'}_j \quad = \quad \sum_{j \in M} \lambda_{j,M}^0 \cdot \left(\sum_{i=1}^{t+1} \lambda_i^0 \cdot {s'}_i^j \right)$$

Extending to malicious parties. This require each party $P_1, \ldots, P_{t+1}$ to generate Q_i as above (such that $Q_i(0) = s_i$) and secret share s_i in a publicly verifiable manner. See here for PVSS: eprint.iacr.org/2004/201.pdf.

(2/3) to (3/5) Parties Threshold Modification

1. Let the parties be. $\{P_1, P_2, P_3\}$. Let x coordinates of $\{P_1, P_2, P_3\}$ be x_1, x_2, x_3
2. Let the modified quorum for (3/5) be $\{P_1, P_2, P_3, P_4, P_5\}$ parties. Let x coordinates of $\{P_1, P_2, P_3, P_4, P_5\}$ be x_1, x_2, x_3, x_4, x_5. Here n=5 and t'=3
3. Choose a committee of 2 parties from the old group. Let them be $\Delta = \{P_1, P_2\}$.
4. Let x coordinates of P_1 and P_2 be x_1 and x_2 respectively
5. Each player P_1 AND P_2 does the following:

   Selects a random polynomial $g_1(x)$ and $g_2(x)$ respectively of degree at most 2 (t' -1) such that $g_1(0)=f(x_1)$ $g_2(0) = f(x_2)$

   [i] P_1 generates shares on $g_1(x)$ for P_1 : $g_{1,1} = g_1(x_1)$

   [ii] P_1 generates shares on $g_1(x)$ for P_2 : $g_{1,2} = g_1(x_2)$ and communicates $g_{1,2}$ to P_2. P_1 generates shares on $g_1(x)$ for P_3 : $g_{1,3} = g_1(x_3)$ and communicates $g_{1,3}$ to P_3 and so on it generates $g_{1,4}$ for P_4 and $g_{1,5}$ for P_5

   [iii] P_2 generates shares on $g_2(x)$ for P_2 : $g_{2,2} = g_2(x_2)$

   [iv] P_2 generates shares on $g_2(x)$ for P_1 : $g_{1,2} = g_1(x_1)$ and communicates $g_{2,1}$ to P_1. P_3 generates shares on $g_2(x)$ for P_3 : $g_{2,3} = g_1(x_3)$ and communicates $g_{2,3}$ to P_3 and so on it generates $g_{2,4}$ for P_4 and $g_{2,5}$ for P_5
6. Each player P_1 , P_2 does the following:

   [i] Generates public constants γ_1^Δ and γ_2^Δ for P_1 and P_2 respectively:

$$\gamma_1^\Delta = \frac{x_2}{x_2 - x_1}$$

$$\gamma_2^\Delta = \frac{x_1}{x_1 - x_2}$$

7. Each player P_1 , P_2 and P_3 does the following:

[i] Erases their old shares

[ii] P_1 computes his new shares

$$\Phi_1 = \gamma_1^{\Delta} \times g_{1,1} + \gamma_2^{\Delta} \times g_{2,1}$$

[iii] P_2 computes his shares:

$$\Phi_2 = \gamma_1^{\Delta} \times g_{2,2} + \gamma_2^{\Delta} \times g_{1,2}$$

[iv] P_3 computes his new share

$$\Phi_3 = \gamma_1^{\Delta} \times g_{1,3} + \gamma_2^{\Delta} \times g_{2,3}$$

[iv] P_4 computes his new share

$$\Phi_3 = \gamma_1^{\Delta} \times g_{1,4} + \gamma_2^{\Delta} \times g_{2,4}$$

[v] P_5 computes his new share

$$\Phi_3 = \gamma_1^{\Delta} \times g_{1,5} + \gamma_2^{\Delta} \times g_{2,5}$$

(2/3) Parties Secret Recovery

1. The set Δ' contains at least t' members . P_1 $P_2$and P_3 recover the secret using Lagrange interpolation method

$$secret = (\gamma_1^{\Delta'} \times \Phi_1) + (\gamma_2^{\Delta'} \times \Phi_2) + (\gamma_3^{\Delta'} \times \Phi_3)$$

Extending to malicious parties. This require each party $P_1, \ldots, P_{t+1}$ to generate Q_i as above (such that $Q_i(0) = s_i$) and secret share s_i in a publicly verifiable manner. See here for PVSS: eprint.iacr.org/2004/201.pdf.

2 Weighted Threshold SS

Setting. There are N parties: P_i, $i \in \{1, \ldots, N\}$. Each party is associated with a weight; party P_i is associated with weight $w^i \in \mathbb{N}$. There is a threshold weight $W \in \mathbb{N}$ and we assume that $w^i < W$ for all $i \in \{1, \ldots, N\}$. The threshold weight W can be represented by an ℓ-bit integer: $W = W_{\ell-1}W_{\ell-2}\ldots W_0$. Similarly, the i-th party's weight can be represented by an ℓ-bit integer $w^i = w^i_{\ell-1}w^i_{\ell-2}w^i_0$.

Let $B = \{i \in \{\ell - 1, \ldots, 0\} \mid W_i = 1\}$ be the set of indices for which the threshold weight W's bit representation is 1, and let $|B|$ be this set's size.

Let $C_j = \left\{i \in \{1, \ldots, N\} \mid w^i_j = 1\right\}$ be the set of indices of parties P_i, $i \in \{1, \ldots, N\}$ whose weight's j-th bit is 1, and let $|C_j|$ be this set's size.

Direction. Let $x \in \mathbb{F}$ be the secret, the dealer do as follows:

1. pick random $x_i \in \mathbb{F}$ for all $i \in B$ and set $x_i = 0$ such that $\sum_{i=0}^{\ell-1} x_i = x$. That is, this is a $|B|$-out-of-$|B|$ sharing of x.
2. pick a random $y_i \in \mathbb{F}$ for every $i \in \{1, \ldots, \ell - 1\}$
3. deal y_1 using a 2-out-of-$|C_0|$ secret sharing and hand a share to each party P_i where $i \in C_0$ (recall that C_0 represent the set of parties who hold a weight with the 0-bit equal 1).
4. for $i \in \{2, \ldots, \ell - 1\}$, generate a degree-1 polynomial, by interpolating points $(\alpha_i, y_i), (\beta_i, y_{i-1})$, deal y_i using a 2-out-of-$|C_{i-1}|$ sharing, and hand a share to each party P_i where $i \in C_{i-1}$.