Homework 1

Advanced Tools From Modern Cryptography
CS 758 : Autumn 2023

Released: August 11 Friday
Due: August 28 Monday

Secret-Sharing [Total 100 pts]

1. **Linear Secret-Sharing** [20 points]

   Recall that a linear secret-sharing scheme over a field is defined using a matrix W and for each privileged set T, a reconstruction vector R_T with non-zero values only at the coordinates indexed by T.

   (a) Write down the sharing matrix and the reconstruction vector of $(3,3)$ additive secret-sharing, viewed as a linear secret-sharing scheme (over an arbitrary field).

   (b) Write down the sharing matrix and the reconstruction matrix for $(3,3)$ Shamir secret-sharing scheme over the field $GF(5)$ (i.e., integers modulo 5).

   (c) Write down the sharing matrix for $(3,2)$ Shamir secret-sharing scheme over $GF(5)$. Also give the reconstruction vectors for $T=\{1,2\}$ and $T=\{2,3\}$ (where the share of party $i \in \{1,2,3\}$ is obtained by evaluation of a polynomial at the field element i).

   (d) In class we described a secret-sharing scheme for the threshold tree access structure obtained using secret-sharing schemes for threshold access structures recursively. Consider the threshold tree consisting of a root node and its three children, all four nodes being $(3,2)$ threshold nodes. Write down the matrix corresponding to the scheme for this access structure, over $GF(5)$.

2. **Optimizing Shamir's Secret-Sharing** [25 points]

   In (n,t) Shamir secret-sharing where the secret is set to be the constant coefficient of the polynomial used to define the shares (as described in class), the field has to be of size at least $n+1$.

   (a) Prove that by setting the secret to be the coefficient of the largest degree term, the field needs to have only n elements.

   (b) Give the sharing matrix for a $(3,2)$ secret-sharing scheme over $GF(3)$.

3. **Blakely's Secret-Sharing** [35 points]

   Consider the following idea for a 2-out-of-n secret-sharing scheme. The message-space is a field $\mathbb{F}$ and the share-space is $\mathbb{F}^2$. The idea is that to share a secret $s \in \mathbb{F}$, the dealer will pick another field element $t \in \mathbb{F}$ and let the shares be lines passing through the point $(s,t) \in \mathbb{F}^2$. More formally, for each $i \in [n]$, the dealer picks $\alpha_i \in \mathbb{F}$, and sets the i^{th} share to be $\sigma_i := (\alpha_i, \beta_i)$, where $\beta_i = s - \alpha_i \cdot t$. (The line corresponds to $x = \alpha_i \cdot y + \beta_i$.)

   (a) Given two shares σ_i, σ_j for $i \neq j$, how can you reconstruct the secret? Is there any constraint on how t, α_i, α_j are chosen, for your reconstruction to succeed? [8 points]

   (b) Prove that this is a perfectly secure 2-out-of-n secret-sharing scheme if t and α_i are chosen from an appropriate distribution. (Be sure to precisely state the mathematical statement that you are proving.) [15 points]

   (c) Extend the scheme to a 3-out-of-n secret-sharing scheme, where the shares of $s \in \mathbb{F}$ correspond to planes passing through a point $(s,t,u) \in \mathbb{F}^3$. Clearly describe the distribution of all the random variables used. [12 points]

4. **Share Switching** [20 points]

   Suppose Σ_1 and Σ_2 are two n-party linear secret-sharing schemes for messages in a set $\mathcal{M}$, with access structures $\mathcal{A}_1$ and $\mathcal{A}_2$ respectively.

   Recall the protocol from the lectures for share-switching: Each party P_i is given w_i as input, where $(w_1, \ldots, w_m) \leftarrow \Sigma_1.\mathsf{share}(m)$. Then, each P_i sets $(\sigma_{i,1}, \ldots, \sigma_{i,n}) \leftarrow \Sigma_2.\mathsf{share}(w_i)$, and sends $\sigma_{i,j}$ to P_j. Finally, each P_i computes and outputs $z_i = \Sigma.\mathsf{recon}(\sigma_{1,i}, \ldots, \sigma_{n,i})$.

   (Here recon denotes the deterministic reconstruction algorithm and share denotes the randomized sharing algorithm, for a secret-sharing scheme.)

   Consider any set $T \notin \mathcal{A}_1 \cup \mathcal{A}_2$. Prove that the view of the set of parties $\{P_i \mid i \in T\}$ in the above protocol, is distributed identically for all messages m.