Secret Sharing

Secret sharing [1] consists of a dealer randomly encoding a secret $s$ into $n$ shares and distributing them to $n$ parties. Such that, a legitimate user downloading any set of at least $t$, $t < n$, shares can decode the secret and any set of at most $z$, $z < t$, parties cannot obtain any information about the secret.

Secret sharing is a building block of many cryptographic and distributed computing protocols. Its applications include access control, generalized oblivious transfer and secure multiparty computation.

Communication Efficient Secret Sharing

The extra amount of information (beyond the secret size) read and communicated to the user is termed as read overhead (RO) and communication overhead (CO).

A CESS code must satisfy:

**MDS property:** A user downloading any $t = k + z$ shares can decode the secret.

**Perfect secrecy constraint:** Any set of at most $z$ parties cannot obtain any information about the secret.

**Minimum CO and RO:** [4] A user contacting any $d$ parties, $t \leq d \leq n$, is able to decode the secret by reading and downloading exactly $k + CO(d)$ units of information in total from all the contacted parties, where

$$ CO(d) = \frac{kz}{d - z} \quad \text{and} \quad RO(d) = CO(d). $$

A communication efficient secret sharing (CESS) [2] is a secret sharing with the additional property that a user contacting more than $t$ parties can download less than $t$ shares and decode the secret.

Example

To construct the $(n, k, z) = (4, 1, 1)$ universal Staircase CESS code, divide the secret $s$ into 6 symbols over $GF(5)$. Choose 6 independent random symbols $k_1, \ldots, k_6$ uniformly at random over $GF(5)$ and independently of $s$. Arrange the secret in a matrix $S = \begin{bmatrix} k_1 & s_1 & s_2 & k_3 & s_4 & k_5 \end{bmatrix}$. Arrange the random symbols in three matrices as follows, $K_1 = \{k_1, k_2\}$, $K_2 = \{k_3, k_4\}$ and $K_3 = \{k_5, k_6\}$. Let $D_i$ be the transpose of the last row of $M_i \triangleq [S \mid K_i]$ and $D$ be the second to last row of $[M_1 \mid M_2]$. Let $V$ be an $4 \times 4$ Vandermonde matrix over $GF(5)$. Then, $M$ and $V$ can be expressed as

$$ M = \begin{bmatrix} s_1 & s_4 & k_1 & k_5 \\ s_2 & s_5 & k_2 & k_6 \\ s_3 & s_6 & k_3 & k_2 \\ s_4 & s_1 & k_4 & k_6 \\ s_5 & s_2 & k_5 & k_1 \\ s_6 & s_3 & k_6 & k_5 \\ \end{bmatrix}, \quad V = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \\ 1 & 3 & 4 & 2 \\ 0 & 0 & 0 & 0 \end{bmatrix}. $$

The encoding is given by $C = VM$, where the $i^{th}$ row of $C$ is given as a share to party $i$, $i = 1, \ldots, 4$.

References


