Staircase Codes for Communication Efficient Secret Sharing

Rawad Bitar and Salim El Rouayheb

Secret Sharing

Secret sharing [?] 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.

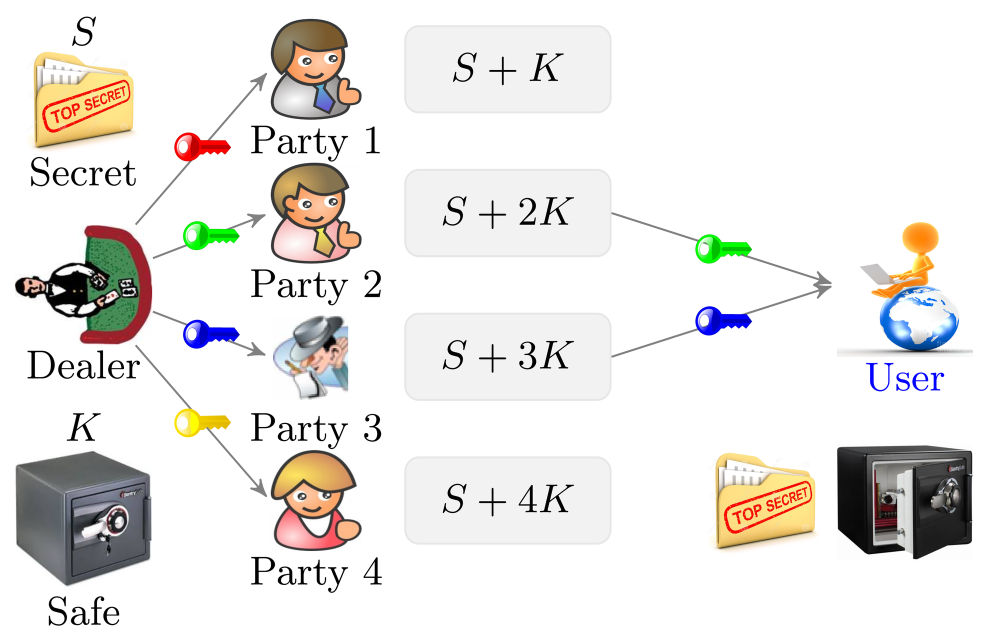
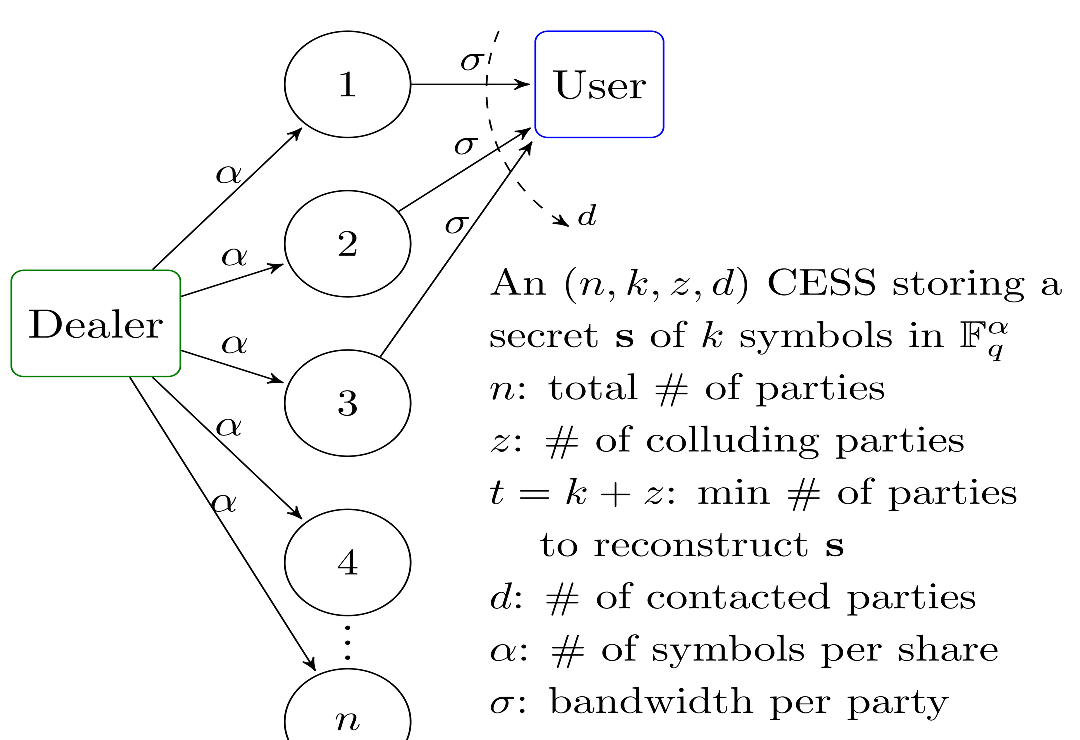


Figure 1: An $n=4$, $t=2$ and $z=1$ secret sharing.

Communication Efficient Secret Sharing



A communication efficient secret sharing (CESS) [?] 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.

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

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

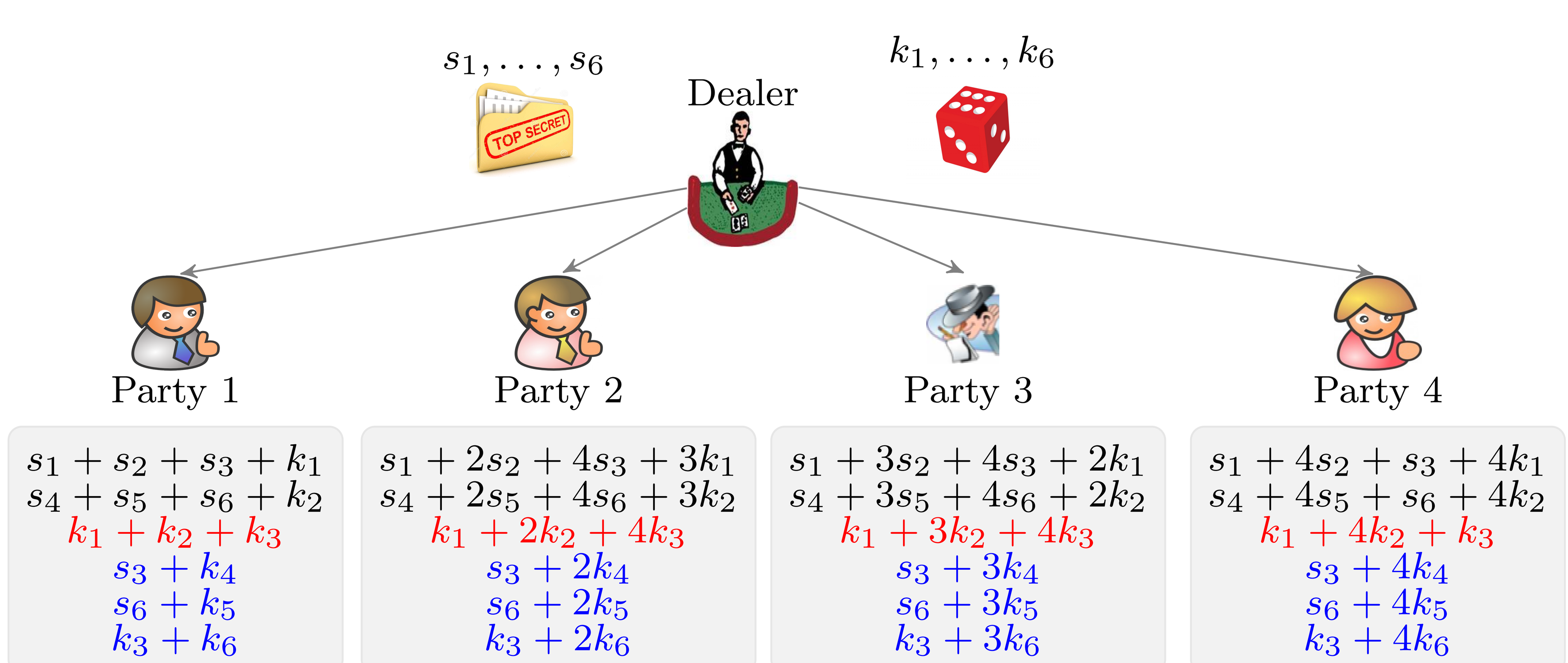
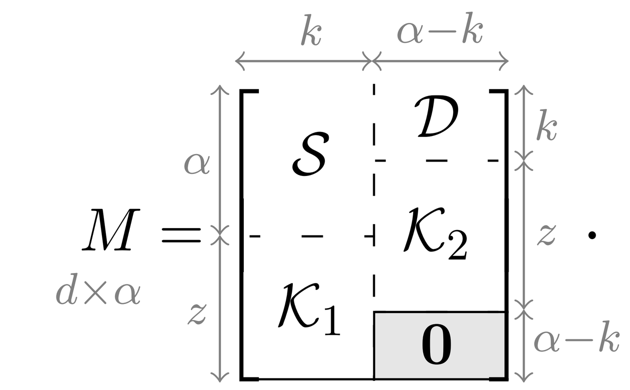


Figure 2: A universal $(n,k,z)=(4,1,1)$ CESS code.

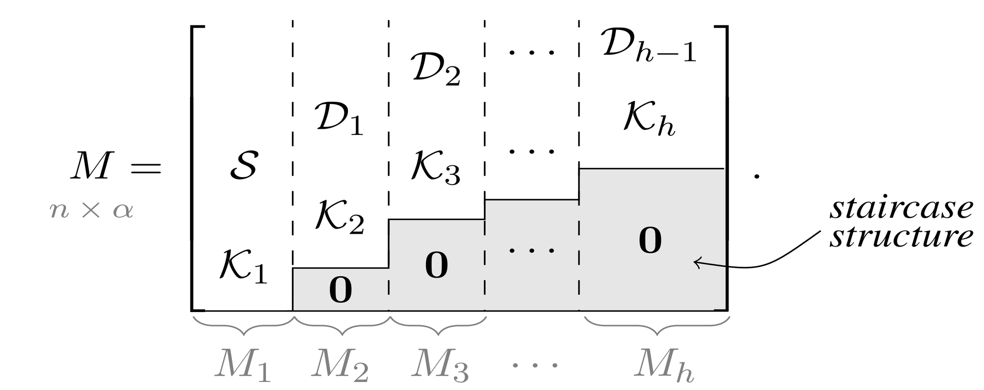
Problem: Explicit CESS code constructions achieving minimum CO and RO are restricted to the cases where $z = t-1$ and optimal for all d [?, ?] or $z < t$ and optimal for $d = n$ [?].

Results

Theorem 1 [?] *The (n,k,z,d) Staircase CESS code defined as the product of an $n \times d$ Vandermonde matrix by the matrix M defined below ($\alpha = d - z$) over $GF(q)$, $q > n$, satisfies the required MDS and perfect secrecy constraints, and achieves optimal communication and read overheads* $\mathrm{CO}(d)$ *and* $\mathrm{RO}(d)$ *for any given d, $d \in \{k+z,\dots,n\}$.*



Theorem 2 [?] *The (n,k,z) universal Staircase CESS code defined as the product of an $n \times n$ Vandermonde matrix by the matrix M defined below over $GF(q)$, $q > n$, satisfies the required MDS and perfect secrecy constraints, and achieves optimal communication and read overheads* $\mathrm{CO}(d)$ *and* $\mathrm{RO}(d)$ *simultaneously for all d, $k+z \leq d \leq n$.*



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 $k_1,\dots,k_6$ uniformly at random over $GF(5)$ and independently of s. Arrange the secret in a matrix $\mathcal{S} = \begin{bmatrix} s_1 & s_2 & s_3 \\ s_4 & s_5 & s_6 \end{bmatrix}^t$. Arrange the random symbols in three matrices as follows, $\mathcal{K}_1 = \begin{bmatrix} k_1 & k_2 \end{bmatrix}$, $\mathcal{K}_2 = \begin{bmatrix} k_3 \end{bmatrix}$ and $\mathcal{K}_3 = \begin{bmatrix} k_4 & k_5 & k_6 \end{bmatrix}$. Let $\mathcal{D}_1$ be the transpose of the last row of $M_1 \triangleq \begin{bmatrix} \mathcal{S} & \mathcal{K}_1 \end{bmatrix}^t$ and $\mathcal{D}_2$ be the second to last row of $\begin{bmatrix} M_1 & M_2 \end{bmatrix}$. Let V be an 4×4 Vandermonde matrix over $GF(5)$. Then, M and V can be expressed as

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

$$\qquad\quad \underbrace{}_{M_1}\ \underbrace{}_{M_2}\ \underbrace{}_{M_3}$$

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

References

[1] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[2] H. Wang and D. S. Wong, "On secret reconstruction in secret sharing schemes," *IEEE Transactions on Information Theory*, vol. 54, pp. 473–480, Jan 2008.

[3] Z. Zhang, Y. M. Chee, S. Ling, M. Liu, and H. Wang, "Threshold changeable secret sharing schemes revisited," *Theoretical Computer Science*, vol. 418, pp. 106–115, 2012.

[4] W. Huang, M. Langberg, J. Kliewer, and J. Bruck, "Communication efficient secret sharing," *arXiv preprint arXiv:1602.04496*, 2015.

[5] R. Bitar and S. El Rouayheb, "Staircase codes for secret sharing with optimal communication and read overheads," *IEEE International Symposium on Information Theory (ISIT)*, Barcelona, July 2016.