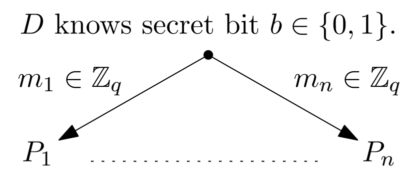
Threshold Secret Sharing Requires a Linear Size Alphabet

Andrej Bogdanov, Siyao Guo, Ilan Komargodski

Secret Bit Sharing



- Access structure $\mathcal{A} = (\mathcal{S}, \mathcal{R})$.
  - $\mathcal{R} \subseteq 2^n$ – qualified, closed to supersets.
  - $\mathcal{S} \subseteq 2^n$ – unqualified, closed to subsets.
- Scheme (formally) – pairs of distributions p_0 and p_1 over Σ_n.
- **Reconstruction:** Every set of parties from $\mathcal{R}$ can reconstruct the secret bit b.
  - For every $R \in \mathcal{R}$ the marginal distributions of p_0 and p_1 on the set R are disjoint.
- **Secrecy:** Every set of parties from $\mathcal{S}$ can not reveal any information about b.
  - For every $S \in \mathcal{S}$ the marginal distributions of p_0 and p_1 on the set S are identical.

Access Structure

- *Total access structure*: $\mathcal{A} = (\mathcal{R}, \mathcal{S})$ is a partition of 2^n, $A \in \mathcal{A}$ if $A \in \mathcal{R}, B \notin \mathcal{A}$ if $B \in \mathcal{S}$.
- *Threshold structure* $\mathsf{Thr}_t^n = \Big(\mathcal{R} = \big\{R \subseteq [n] : |R| \geq t\big\}, \mathcal{S} = \big\{S \subseteq [n] : |S| \leq t\big\}\Big)$.
- *Ramp structure* $\mathsf{Ramp}_{r,s}^n = \Big(\mathcal{R} = \big\{R \subseteq [n] : |R| \geq r\big\}, \mathcal{S} = \big\{S \subseteq [n] : |S| \leq s\big\}\Big)$.

Shamir's Secret Sharing

- Field $\mathbb{Z}_q$, secret $x \in \mathbb{Z}_q$, $a_1, \ldots, a_{t-1}, \in_r \mathbb{Z}_q, a_0 = x$.
- $p(x) = \sum_{i=0}^{t-1} a_i x^i, m_i = p(i)$.
- **Recovery**: Each t parties can reconstruct $t-1$ degree polynomial p and $p(0) = x$.
- **Secrecy**: For each $t-1$ parties the probability of each value of $p(0)$ is the same.

Alternative Formulation

- For $x \in \mathbb{Z}_q^n$: $[x]_{\neq 0} = \big\{j \in [n] : x_j \neq 0\big\}, [x]_{=0} = \big\{j \in [n] : x_j = 0\big\}$.
- A function $g_S : \mathbb{Z}_q^n \to \mathbb{C}$ is an S-junta if the value $g_S(x_1, \ldots, x_n)$ is determined by the inputs $x_j : j \in S$.

Lemma 1. *A secret sharing scheme of a 1-bit secret for a partial access structure $\mathcal{A} = (\mathcal{S}, \mathcal{R})$ over an alphabet Z_q exists if and only if there exists a function $f : \mathbb{Z}_q^n \to \mathbb{R}$ that is not identically zero satisfying the following properties:*

- **Reconstruction:** *For all $x, z \in \mathbb{Z}_q^n$ such that $[z]_{=0} \in \mathcal{R}$, $f(x)f(x-z) \geq 0$.*
- **Secrecy:** *For every $S \in \mathcal{S}$ and every S-junta $g_S : \mathbb{Z}_q^n \to \mathbb{C}$, $\mathbb{E}_x[f(x)g_S(x)] = 0$.*

Results

Theorem 2 (Main Theorem)**.** *For every $n \in \mathbb{N}$ and $1 \leq s < r < n$, any secret bit sharing scheme for $\mathsf{Ramp}_{r,s}^n$ requires shares of at least $\log\big((r+1)/(r-s)\big)$ bits.*

Corollary 3. *For every $n \in \mathbb{N}$ and $1 < t < n$, any secret bit sharing scheme for Thr_t^n requires shares of at least $\log\big(t+1\big)$ bits.*

Theorem 4 (Kilian, Nisan, '90)**.** *For every $n \in \mathbb{N}$ and $1 < t < n$, any secret bit sharing scheme for Thr_t^n requires shares of at least $\log\big(n-t+2\big)$ bits.*

Game $\mathcal{G}(\mathcal{A}, \theta)$

- $\mathcal{A}$ is an access structure $(\mathcal{R}, \mathcal{S})$, $\theta \in \mathbb{R}$ and $\theta > 0$.
- Alice picks $A \notin \mathcal{S}$, Bob picks $B \in \mathcal{R}$.
- Payoff: $(-\theta)^{|A \setminus B|}$, Alice wins if payoff is non-negative.

Lemma 5. *If there exists a secret sharing scheme for $\mathcal{A}$ with alphabet size $q \in \mathbb{N}$, then Alice wins in the game $\mathcal{G}\big(\mathcal{A}, 1/(q-1)\big)$.*

Lemma 6. *Bob wins in the game $\mathcal{G}(\mathsf{Ramp}_{r,s}^n, \theta)$ for any $\theta > (r-1)/(s+1)$.*

Limitation of the Game Approach

Theorem 7. *For all $1 < t < n$ and $0 < \theta \leq 1/t$, Alice wins in the game $\mathcal{G}(\mathsf{Thr}_t^n, \theta)$.*

- $\min \mathcal{A} = \{A \in \mathcal{A} : \forall B \in \mathcal{A} \not\subset A\}$.

Theorem 8. *For every access structure A and every $0 < \theta \leq 1/\big(|min\mathcal{A}| - 1\big)$ Alice wins in the game $\mathcal{G}(\mathcal{A}, \theta)$.*

Fourier Analysis

- Space of functions $\mathbb{Z}_q^n \to \mathbb{C}$.
- Character for $a \in \mathbb{Z}_q^n$: $\chi_a : \mathbb{Z}_q^n \to \mathbb{C}$, $\chi_a = \omega^{\langle a, x\rangle}$, where $\omega = e^{2\pi i/q}$.
- Characters are an orthonormal basis with respect to the inner product $\langle f, g\rangle = \mathbb{E}_x[f(x)\overline{g(x)}]$.
- $\chi_a \chi_b = \chi_{a+b}$, $\chi_a^{-1} = \overline{\chi_a} = \chi_{-a}$.
- $f = \sum_{a \in \mathbb{Z}_q^n} \hat{f}(a)\chi_a$, $\hat{f}(a) = \langle f, \chi a\rangle = \mathbb{E}_x[f(x)\overline{\chi_a(x)}]$.