Secret Sharing for Slice Functions

A secret sharing scheme over \( n \) parties is a randomized algorithm that distributes a one-bit secret among \( n \) shares.

\[
\text{Sharing Algo : } s \in \{0, 1\} \mapsto (\text{share}_1, \ldots, \text{share}_n).
\]

The secret sharing scheme is associated to a monotone boolean function \( F : \{0, 1\}^n \to \{0, 1\} \), such that for any subset of parties \( T \subseteq [n] \),

- \( F(T) = 1 \implies s \) can be recovered from \( \{\text{share}_i\}_{i \in T} \),
- \( F(T) = 0 \implies s \) is independent from \( \{\text{share}_i\}_{i \in T} \).

One of the major long-standing questions in information-theoretic cryptography is to minimize the (total) size of the shares in a secret sharing scheme for arbitrary monotone functions \( F \). [Ito-Saito-Nishizeki'89]

---

**General Secret Sharing**

A secret sharing scheme over \( n \) parties is a randomized algorithm that distributes a one-bit secret among \( n \) shares.

\[
\text{Sharing Algo : } s \in \{0, 1\} \mapsto (\text{share}_1, \ldots, \text{share}_n).
\]

The secret sharing scheme is associated to a monotone boolean function \( F : \{0, 1\}^n \to \{0, 1\} \), such that for any subset of parties \( T \subseteq [n] \),

- \( F(T) = 1 \implies s \) can be recovered from \( \{\text{share}_i\}_{i \in T} \),
- \( F(T) = 0 \implies s \) is independent from \( \{\text{share}_i\}_{i \in T} \).

One of the major long-standing questions in information-theoretic cryptography is to minimize the (total) size of the shares in a secret sharing scheme for arbitrary monotone functions \( F \). [Ito-Saito-Nishizeki'89]

**Previous Works**

<table>
<thead>
<tr>
<th>General Secret Sharing</th>
<th>Linear Secret Sharing*</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 2^n ) (naive solution)</td>
<td>( n^2 ) ( \log n ) [Csirmaz'97]</td>
</tr>
<tr>
<td>( O(\text{monotone formula size}) \leq \frac{2^n}{\text{poly}(n)} ) [Benaloh-Leichter'88]</td>
<td>( 2^n/\text{poly}(n) )</td>
</tr>
<tr>
<td>( \forall F ), the share size is no more than ( O(\text{monotone span program size}) \leq \frac{n^2}{\text{poly}(n)} ) [Karchmer-Wigderson'93]</td>
<td>( \frac{n^2}{\text{poly}(n)} )</td>
</tr>
<tr>
<td>Lower Bounds: ( n^2 ) ( \log n ) [Csirmaz'97]</td>
<td>( \frac{2n}{\text{poly}(n)} )</td>
</tr>
</tbody>
</table>

**Our Results**

**New Upper Bounds:**

<table>
<thead>
<tr>
<th>General Secret Sharing</th>
<th>Linear Secret Sharing*</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 2.0994n )</td>
<td>( 2.0999n )</td>
</tr>
</tbody>
</table>

\( \forall F \), the share size is no more than \( \frac{n^2}{\log n} \) \[Csirmaz'97\] and \( \frac{2n}{\text{poly}(n)} \)

**Formula-Based Secret Sharing and its Bottleneck**

- Monotone function \( F \) is computed by a monotone formula
- Generate a tag for each wire
- Output wire: the secret \( s \)
- AND gate: additively share its output wire tag
- OR gate: copy its output wire tag
- The \( i \)-th party’s share: all tags of input wire \( x_i \)
- Total share size \( \approx \) formula size of \( F \leq 2^n/\text{poly}(n) \)

**Proof Outline**

Every monotone function has secret sharing scheme with share size \( 2^{(o(n))} \), which is the corollary of the following two theorems.

**[Liu-Vaikuntanathan-Wee'18]**

- Every \textit{slice functions} function \( F \) s.t.
  \[ |x| > n/2 \implies F(x) = 1 \text{ and} \]
  \[ |x| < n/2 \implies F(x) = 0, \]
  has a secret sharing scheme \( /w \) share size \( 2^{O(\sqrt{n})} \).

**[This work]**

- Every monotone function can be computed by a monotone formula s.t.
  - Formula size: \( 2^{o(n)} \)
  - Constant depth
  - Base gates: AND, OR, slice functions

**Open Problems**

- Every monotone function is computed by a monotone formula of size \( 2^{(n)} \) using slice functions as gates? (It implies every monotone function has a secret sharing scheme with \( 2^{(n)} \) share size.)
- Does amortization help improve information ratio?

---

**Secret Sharing for all Functions** \[This work\]

\( \iff \)

**Secret Sharing for Slice Functions** \[LV'18\]

\( \iff \)

**Multi-party Conditional Disclosure of Secret** \[LV'17\]

\( \iff \)

**2-party Conditional Disclosure of Secret** \[LV'17\]

\( \iff \)

**2-server PIR** \[Yek'08,Efr'09,DG'15\]