Secret Sharing for NP

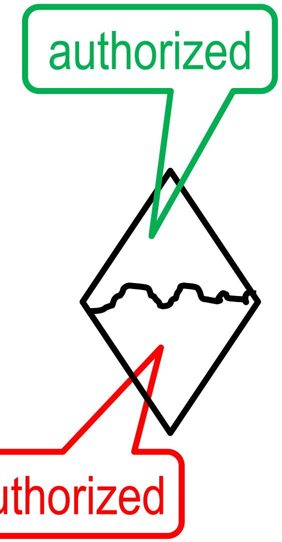
Ilan Komargodski Moni Naor Eylon Yogev

Weizmann Institute of Science

Asiacrypt, Dec 11th 2014

Secret Sharing

- **Dealer** has secret S.
- Gives to users $P_1, P_2, \ldots, P_n$ **shares** $\Pi_1, \Pi_2, \ldots, \Pi_n$.
  - The shares are a **probabilistic function of** S.

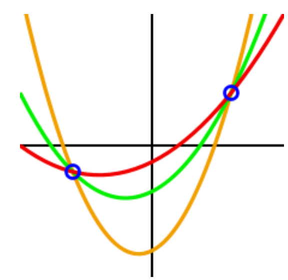


- A subset of users X is either authorized or unauthorized.

$\Pi(X,S)$

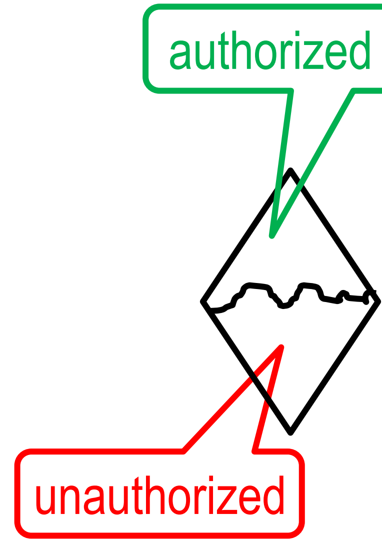
Goal:
- An authorized X can reconstruct S based on their shares.
- An unauthorized X **cannot** gain *any* knowledge about S.

- Introduced by Blakley and Shamir in the late 1970s.
  - Threshold secret sharing



Source: Wikipedia

Access Structures



Access Structure M:

- An indicator function of the authorized subsets.

- To make sense: M should be monotone:
  if $X' \subset X$ and $M(X')=1$ then $M(X)=1$

Perfect secret sharing scheme:

- For any two secrets S_0, S_1, subset X s.t. $M(X)=0$:

$$Dist(\Pi(X,S_0)) = Dist(\Pi(X,S_1)).$$

Or equivalently: for any distinguisher A:

$$|Pr[A(\Pi(X,S_0)) = 1] - Pr[A(\Pi(X,S_1)) = 1]|=0$$

The **complexity** of the scheme: the **size** of the largest share.

Known Results

Theorem [Ito, Saito and Nishizeki 1987] :

For every $\mathcal{M}$ there exists a perfect secret sharing scheme

- might have exponential size shares in the number of parties.

Theorem [Benaloh-Leichter 1988] :

If $\mathcal{M}$ is a **monotone formula** Φ: there is a perfect secret sharing scheme where the size of a share is proportional to $|\Phi|$.

Karchmer-Wigderson generalized this results to **monotone span programs** [1993]

Major question: can we prove **a lower bound on the size** of the shares for ***some*** access structure?

- Even a non constructive result is interesting

Computational Secret Sharing

- **Perfect** secret sharing scheme:

  Any unauthorized subset X gains absolutely ***no*** information:

  – For any A, secrets S_0, S_1, subset X s.t. $M(X)=0$:

  $$|\Pr[A(\Pi(X,S_0)) = 1] - \Pr[A(\Pi(X,S_1)) = 1]| = 0.$$

- **Computational** secret sharing scheme:

  Any unauthorized subset X gains no ***useful*** information:

  $$\Pi(X,S_0) \approx \Pi(X,S_1)$$

  In the **indistinguishability** of encryption style:

  For any PPT A, two secrets S_0, S_1, subset X s.t. $M(X)=0$:

  $$|\Pr[A(\Pi(X,S_0)) = 1] - \Pr[A(\Pi(X,S_1)) = 1]| < neg$$

This is a non-uniform definition

Computational Secret Sharing

Theorem [Yao~89]:
If M can be computed by a **monotone** poly-size circuit C then:

There is a **computational** secret sharing scheme for M.

- Size of a share is proportional to $|C|$.
- Assuming one-way functions.

Construction similar to Yao's **garbled circuit**

- What about monotone access structure that have small **non**-monotone circuits?
  - Matching:
    - Parties correspond to edges in the complete graph.
    - Authorized sets: the subgraphs containing a **perfect matching.**

Open problem: do all monotone functions in P have computational secret sharing schemes?

Secret Sharing for NP

Rudich circa 1990

What about going beyond *P*?

- Efficient **verification** when the authorized set proves that it is authorized
  - Provide a witness

Example:

- Parties correspond to edges in the **complete graph**.
- Authorized sets: subgraphs containing a **Hamiltonian Cycle.**
- The **reconstruction** algorithm should be provided with the **witness**: a cycle.

Secret Sharing and Oblivious Transfer

Theorem:

If one-way functions exist and a computationally secret sharing scheme for the Hamiltonian problem exists then:

Oblivious Transfer Protocols exist.

- In particular Minicrypt = Cryptomania
- Construction is non-blackbox

- No hope ***under standard assumptions*** for perfect or statistical scheme for Hamiltonicity

Includes x

Witness Encryption [Garg, Gentry, Sahai, Waters 2013]

- A witness encryption (Enc_L, Dec_L) for a language $L \in NP$:
  - Encrypt **message** m relative to **string** x: $ct = \mathsf{Enc}_L(x,m)$
  - For any $x \in L$: let $ct = \mathsf{Enc}_L(x,m)$ and let w be **any** witness for x. Then $\mathsf{Dec}_L(ct,w) = m$.
  - For any $x \notin L$: $ct = \mathsf{Enc}_L(x,m)$ computationally hides the message m.

- Gave a candidate construction for witness encryption.
- Byproduct: a candidate construction for secret sharing for a specific language in NP (Exact Cover)

Multilinear Maps, Indistinguishability Obfuscation (iO)…

Our Results

If one-way functions exist then:

- Secret Sharing for $\mathcal{NP}$ and **Witness Encryption** for $\mathcal{NP}$ are (existentially) **equivalent**.
- If there is a **secret sharing** scheme for **one** $\mathcal{NP}$-complete language, then there is one for **all** languages in $\mathcal{NP}$.

Definition of secret sharing for $\mathcal{NP}$

Let M be a monotone access structure in $\mathcal{NP}$.

- **Completeness**:
  For any X s.t. $M(X)=1$, any witness w (for X), and any secret S:

  $$recon(\Pi(X,S),w) = S.$$

  - All operations polytime

Definition of secret sharing for NP: Security

- Let M be a monotone access structure in NP.

Security:

For any adversary $A=(A_{samp},A_{dist})$ such that A_{samp} chooses two secrets S_0,S_1 and a subset X it holds that:

$$|\Pr[M(X)=0 \wedge A_{dist}(\Pi(S_0,X)) = 1] - \Pr[M(X)=0 \wedge A_{dist}(\Pi(S_1,X)) = 1]| < neg.$$

This is a static and uniform definition

- A weaker possible definition is to require that X is **always** unauthorized.

The Construction

For access structure $M \in NP$.

- Define a new language $M' \in NP$:
  - Let $c_1, \ldots, c_n$ be n strings.
  - Then $M'(c_1,\ldots,c_n) = 1$ iff $M(X) = 1$ where:

$$X_i = \begin{cases} 1 \text{ if exist } r_i \text{ s.t. } c_i = com(i, r_i) \\ 0 \text{ otherwise} \end{cases}$$

Computationally hiding: $com(x_1) \approx com(x_2)$
Perfect Binding: $com(x_1)$ and $com(x_2)$ have disjoint support.

Can be constructed from one-way functions in the CRS model with high probability.

The Construction…

The message

Dealer(S):

- Choose $r_1, \ldots, r_n$ uniformly at random.
- For $i \in [n]$, compute $c_i = com(i, r_i)$.
- Compute ct = $WE.Enc_{M'}((c_1, \ldots, c_n), S)$.
- Set $\Pi_i = (r_i, ct)$.

Shared by all

Reconstruction: authorized subset X of parties: $M(X)=1$ and witness w witness for X.

- Witness for M' consists of openings r_i such that $X_i=1$.
- Set $w'=(r'_1, \ldots, r'_n, w)$.

Security

Suppose an adversary $A=(A_{samp}, A_{dist})$ breaks the system.

- Construct an algorithm D that breaks the commitment scheme:
  - For a list of commitments $c_1, \ldots, c_n$ distinguish between two cases:
    - They are commitments of $1, \ldots, n$.
    - They are commitments of $n+1, \ldots, 2n$.

Open Problems

Brakerski: diO

- **Adaptive** choice of the set X.
- Perfect Secret-Sharing Scheme for directed connectivity.
  - How to cope with the fan-out
- Computational Secret Sharing Scheme for Matching.
  - How to cope with negation?
- A secret sharing scheme for *P* based on less heavy cryptographic machinery.

谢谢

ITCS 2015 at the Weizmann Institute of Science

January 11-13, 2015

The **6th Innovations in Theoretical Computer Science (ITCS)** conference, will be held at the Weizmann Institute of Science, Israel

http://www.wisdom.weizmann.ac.il/~naor/itcs2015_main.html

- Sponsored by ACM SIGACT