ARIEL UNIVERSITY / Department of Computer Science

Introduction:

Secret sharing schemes are ideal for storing information that is highly sensitive and highly important. Secret sharing refers to methods for distributing a secret amongst a group of participants, each of whom is allocated a share of the secret. The secret can be reconstructed only when a sufficient set T of shares are combined together when certain set show up, while other sets learn nothing about the secret. A secret sharing scheme realizes an access structure $f : 2^{[n]} \to \{0, m-1\}$ by guaranteeing that for each sufficient set of shares the secret is uniformly distributed over a set of 1 secret, and for each insufficient set of shares the secret distributed over set of $m-1$ potential secrets.

[IKS13] : **Fractional secret sharing** generalizes traditional secret sharing by allowing a fine-grained control over the amount of uncertainty about the secret. Fractional secret sharing scheme realizes a fractional access structure $f : 2^{[n]} \to \{0, \dots, m-1\}$ by guaranteeing that for each set $T \subseteq [n]$ of parties, the secret is uniformly distributed over a set of $f(T)+1$ potential secrets.

Related work:

[I+13] : In the **STACS 13' paper** that introduced the concept, **Ishai et al** put forward a construction for symmetric access structures f, where $f(T)$ depends only on the size of T, with the quite efficient share size of $n\lceil\log(\max\{n,m\})\rceil$. However, for other f, their secret complexity is $\Omega(s)$,such that s is the number of A sets, such that $f(A) < m-1$. For many families of access structure s is $2^{\Omega(n)}$.

Motivation:

In the proposed research we want a better understanding about the share complexity of fractional secret sharing for non-symmetric functions. For standard secret sharing scheme, more efficient constructions than $\Omega(s)$ are often known. We improve [I+13] construction, to get better share complexity for certain f's.

Main ideas:

- Following [I+13], reduce fractional secret sharing to standard secret sharing scheme for $f^{-1}(k)$ for each k.
- [I+13] use a concrete secret sharing scheme for each $f^{-1}(k)$, which is very inefficient.
- Replace the scheme used for each k with the best known one. Better schemes than currently used are known for many cases. [I+13] already do it for symmetric access structures.
- We need efficient schemes for all k simultaneously.

Main result:

- We put forward a natural fractional access structure f, related to
- s-t-connectivity, which has an efficient fractional secret sharing.
- We construct a efficient scheme for $\bigcup_{j\le k} f^{-1}(j)$ for each k.

Result details:

- Fractional access structure : fractional s-t-connectivity - $f : 2^{[n]} \to \{0,1,m-1\}$, such that if there are no s-t path the secret distributed over set of $m-1$ potential secrets, if there is one s-t path the secret distributed over set of 2 potential secrets, and if there are two s-t paths the secret distributed over set of 1 secret.
- Construct a formula with $n^{O(\log(n))}$ leaves for each $f^{-1}(j<k)$.
- [BL88] : monotone formulas F for $f : 2^{[n]} \to \{0,1\}$ (such that 0 is matching to $m-1$ and 1 is matching to 0 we mentioned before) → secret sharing scheme of size $\#l\ (F)$, such that $\#l$ is the number of leaves in F.

How to construct a formula F ?

* Formula for two distinct paths k=0 is :

$$F = P^2(s,t)$$

$$P^2(s,t) = \bigvee_{i=1}^{n} P^2(u,v,m) \bigvee_{1\le m_1<m_2\le n} \left(P^1(u,v,m_1) \wedge P^1(u,v,m_2) \right)$$

$$P^1(u,v,m) = \bigvee_{w\in V} \left(P^1\left(u,w,\left\lceil\frac{m}{2}\right\rceil\right) \wedge P^1\left(w,v,\left\lfloor\frac{m}{2}\right\rfloor\right) \right)$$

$$P^2(u,v,m) = \bigvee_{w_1\ne w_2, w_1,w_2\in V} \left(P^1\left(u,w_1,\left\lceil\frac{m}{2}\right\rceil\right) \wedge P^1\left(w_1,v,\left\lfloor\frac{m}{2}\right\rfloor\right) \wedge P^1\left(u,w_2,\left\lceil\frac{m}{2}\right\rceil\right) \wedge P^1\left(w_2,v,\left\lceil\frac{m}{2}\right\rceil\right) \right)$$

$$\bigvee_{w\in V} \left(P^2\left(u,w,\left\lceil\frac{m}{2}\right\rceil\right) \wedge P^1\left(w,v,\left\lfloor\frac{m}{2}\right\rfloor\right) \right) \bigvee_{w\in V} \left(P^1\left(u,w,\left\lceil\frac{m}{2}\right\rceil\right) \wedge P^2\left(w,v,\left\lfloor\frac{m}{2}\right\rfloor\right) \right)$$

* Formula for one path k=1 is already known : follows from the proof of Savitch's theorem.

By :
Tom Suad.
Advisor :
Anat Paskin-Cherniavsky.