Secret Sharing Schemes with a large number of players from Toric Varieties

Johan P. Hansen

Institute of Mathematics, University of Aarhus, Denmark

12. march 2015
1 Secret Sharing Schemes
   - Introduction
   - LSSS, thresholds and strong multiplication

2 The methods of toric varieties
   - Our construction
   - Thresholds and strong multiplication

3 Toric surfaces, fans, Cartier divisors and cohomology
   - Example
   - Theorem
Objective of secret sharing

Secret sharing schemes were introduced by Blakley (1979) and Shamir (1979).
Split a secret into shares such that

- any large enough subset of the shares determines the secret
- any small subset of shares provides no information on the secret
Linear Secret Sharing Schemes (LSSS)

- **Linear secret sharing schemes**: The secrets $s$ and their associated shares $(a_1, \ldots, a_n)$ are elements in a vector space over $\mathbb{F}_q$ (called *ideal*, if $s, a_i \in \mathbb{F}_q$).
- **The reconstruction threshold**: The smallest integer $r$ such that any set of at least $r$ of the shares $a_1, \ldots, a_n$ determines the secret $s$.
- The privacy threshold is the largest integer $t$ such that no set of $t$ (or fewer) elements of the shares $a_1, \ldots, a_n$ determines the secret $s$. The scheme is said to have $t$-privacy.
- An ideal linear secret sharing scheme is said to have *multiplication* if the product of the shares determines the product of the secrets. (Application: multiparty computation).
- LSSS has $t$-strong multiplication if it has $t$-privacy and multiplication for any subset of $n - t$ shares.
Our construction

Definition (LSSS)

Let $U \subseteq H = \{0, 1, \ldots, q - 2\} \times \cdots \times \{0, 1, \ldots, q - 2\} \subset \mathbb{Z}^r$ (monomials). Let $T(\mathbb{F}_q)$ be the $\mathbb{F}_q$-rational points on the torus and $P_0 \in T(\mathbb{F}_q)$.

The LSSS is constructed by evaluating elements in $\mathbb{F}_q < U >$ at all the points on $T(\mathbb{F}_q)$:

$$\pi_{T(\mathbb{F}_q)} : \mathbb{F}_q < U > \rightarrow \mathbb{F}_{|T(\mathbb{F}_q)|}$$

$$f \mapsto \pi_{T(\mathbb{F}_q)}(f) = (f(P))_{P \in T(\mathbb{F}_q)}.$$

Choose $f \in \mathbb{F}_q < U >$ at random, such that secret $s = f(P_0) \in \mathbb{F}_q$. It has $n = (q - 1)^r - 1$ shares

$$\pi_{T(\mathbb{F}_q) \setminus \{P_0\}}(f) \in \mathbb{F}_{q^{\mid T(\mathbb{F}_q)\mid - 1}}.$$
Reconstruction and privacy thresholds

Theorem

Let $r$ and $t$ be the reconstruction and privacy thresholds. Then

\[ r = 1 + \text{(the maximal number of zeros of } \pi_T(\mathbb{F}_q)(f)) \]

\[ t = (q - 1)^r - \text{(the maximal number of zeros of } \pi_T(\mathbb{F}_q)(g)) - 2 \]

for some $f \in \mathbb{F}_q < U >$ and for some $g \in \mathbb{F}_q < -H \setminus -U >$, where

\[
\pi_T(\mathbb{F}_q) : \mathbb{F}_q < -H \setminus -U > \rightarrow \mathbb{F}_q^{|T(\mathbb{F}_q)|}
\]

\[ g \mapsto \pi_T(\mathbb{F}_q)(g) = (g(P))_{P \in T(\mathbb{F}_q)} \]
Remark on proof

Proof.

As for the reconstruction threshold $r$, let $A \subseteq T(\mathbb{F}_q)$ with

$$|A| \geq 1 + \left( \text{the maximal number of zeros of } \pi_T(\mathbb{F}_q)(f) \right)$$

for all $f \in \mathbb{F}_q < U >$. The linear morphism

$$\pi_T : \mathbb{F}_q < U > \rightarrow \mathbb{F}_q^{|A|}$$

$$f \mapsto (f(P))_{P \in A}$$

has trivial kernel and therefore injective.

As for privacy threshold $t$ use a similar argument and the following orthogonality lemma.
Lemma

The orthogonal complement to $\pi_T(\mathbb{F}_q)(\mathbb{F}_q < U >)$ in $\mathbb{F}_q^{\mid T(\mathbb{F}_q)\mid}$ is

$$\pi_T(\mathbb{F}_q)(\mathbb{F}_q < -H \setminus -U >) .$$

with respect to the inner product

$$(a_0, \ldots, a_n) \star (b_0, \ldots, b_n) = \sum_{l=0}^{n} a_l b_l \in \mathbb{F}_q .$$
Theorem

Let $U \subseteq H$ and let $U + U = \{u_1 + u_2 | u_1, u_2 \in U\}$ be the Minkowski sum.

The linear secret sharing schemes with $n = (q - 1)^r - 1$ players, has strong multiplication if

$$t \leq n - 1 - \text{(the maximal number of zeros of } \pi_T(\mathbb{F}_q)(h))$$

for all $h \in \mathbb{F}_q < U + U >$. 
Proof.

For \( A \) with \( t \) elements, let \( B := T(\mathbb{F}_q) \setminus (\{P_0\} \cup A) \) with \( n - t \) elements. For \( f, g \in \mathbb{F}_q < U > \), we have that \( f \cdot g \in \mathbb{F}_q < U + U > \). Consider the linear morphism

\[
\pi_B : \mathbb{F}_q < U + U > \rightarrow \mathbb{F}_q^{|B|}
\]

\[
h \mapsto (h(P))_{P \in B}.
\]

evaluating at the points in \( B \).

By assumption \( h \in \mathbb{F}_q < U + U > \) can have at most \( n - t - 1 < n - t = |B| \) zeros, therefore \( h \) can’t vanish identically on \( B \), and we conclude that \( \pi_B \) is injective. Consequently the products \( f(P) \cdot g(P) \) of the shares \( P \in B \) determine the product of the secrets \( f(P_0) \cdot g(P_0) \), and the scheme has strong multiplication by definition.
$M \simeq \mathbb{Z}^2$ and assume that $U = M \cap \Box$ consists of the integral points of a 2-dimensional integral convex polytope $\Box$ in $\mathbb{R}^2$. The convex polytope $\Box$ gives rise to an algebraic surface and we use intersection theory on that surface to bound the number of zeros of the evaluations

$$
\pi_S : \mathbb{F}_q < U > \rightarrow \mathbb{F}_q^{|S|}
$$

$$
f \mapsto (f(P))_{P \in S}
$$

of elements in $\mathbb{F}_q < U >$ at all the points of $T(\mathbb{F}_q)$. 

Johan P. Hansen

Secret Sharing Schemes with a large number of players from Toric Varieties
Let $M$ be an integer lattice $M \cong \mathbb{Z}^2$. Let $N = \text{Hom}_\mathbb{Z}(M, \mathbb{Z})$ be the dual lattice with canonical $\mathbb{Z}$-bilinear pairing $\langle \ , \ \rangle : M \times N \to \mathbb{Z}$.

Given a 2-dimensional integral convex polytope $\Box$ in $\mathbb{R}^2$. The support function $h_\Box : N_\mathbb{R} \to \mathbb{R}$ is defined as $h_\Box(n) := \inf \{ \langle m, n \rangle \mid m \in \Box \}$ and the polytope $\Box$ can be reconstructed from the support function

$$\Box_h = \{ m \in M \mid \langle m, n \rangle \geq h(n) \ \forall n \in N \}. $$

The support function $h_\Box$ is piecewise linear in the sense that $N_\mathbb{R}$ is the union of a non-empty finite collection of strongly convex polyhedral cones in $N_\mathbb{R}$ such that $h_\Box$ is linear on each cone.
A fan is a collection $\Delta$ of strongly convex polyhedral cones in $N_{\mathbb{R}}$ such that every face of $\sigma \in \Delta$ is contained in $\Delta$ and $\sigma \cap \sigma' \in \Delta$ for all $\sigma, \sigma' \in \Delta$.

The normal fan $\Delta$ is the coarsest fan such that $h_{\square}$ is linear on each $\sigma \in \Delta$, i.e. for all $\sigma \in \Delta$ there exists $l_{\sigma} \in M$ such that

$$h_{\square}(n) =< l_{\sigma}, n > \quad \forall n \in \sigma.$$ (1)

The 1-dimensional cones $\rho \in \Delta$ are generated by unique primitive elements $n(\rho) \in N \cap \rho$ such that $\rho = \mathbb{R}_{\geq 0} n(\rho)$. 
Fans and toric surfaces

The toric surface $X_{\square}$ associated to the fan $\Delta$ of $\square$ is

$$X_{\square} = \bigcup_{\sigma \in \Delta} U_\sigma,$$

where $U_\sigma$ is the $k$-valued points of the affine scheme $\text{Spec}(k[S_\sigma])$, i.e. morphisms $u : S_\sigma \to k$ with $u(0) = 1$ and $u(m + m') = u(m)u(m')$ for all $m, m' \in S_\sigma$, where $S_\sigma$ is the additive subsemigroup of $M$

$$S_\sigma = \{ m \in M \mid <m, y> \geq 0 \ \forall y \in \sigma \}.$$
A $\Delta$-linear support function $h$ corresponds to a polytope $\Box$ and gives an associated Cartier divisor

$$D_h = D_\Box := - \sum_{\rho \in \Delta(1)} h(n(\rho)) V(\rho) ,$$

(2)

where $\Delta(1)$ consists of the 1-dimensional cones in $\Delta$. The 1-dimensional cones $\rho \in \Delta$ are generated by unique primitive elements $n(\rho) \in N \cap \rho$ such that $\rho = \mathbb{R}_{\geq 0} n(\rho)$.
Global sections

Lemma

Let $h$ be a $\Delta$-linear support function with associated convex polytope $\Delta$ and Cartier divisor $D_h = D_\Delta$. The vector space $H^0(X, O_X(D_h))$ of global sections of $O_X(D_\Delta)$, i.e. rational functions $f$ on $X_\Delta$ such that $\text{div}(f) + D_\Delta \geq 0$ has dimension $|(M \cap \Delta)|$, that is the number of lattice points in $\Delta$. 
Example

\begin{align*}
(q - 2, q - 2) + (H - a - b) &= (q - 2) - b - a + (H - a - b) \\
(q - 2) + (H - a - b) &= (q - 2) - b - a + (H - a - b)
\end{align*}
Figure: The normal fan and its 1-dimensional cones $\rho_i$, with primitive generators $n(\rho_i)$. 

\[ n(\rho_3) = \left( \frac{-(q-2)}{\gcd(a-b,q-2)}, \frac{-(a-b)}{\gcd(a-b,q-2)} \right) \]
Let $\square$ be the polytope above and let $U = M \cap \square$ be the lattice points.

i) The reconstruction threshold of the LSSS

$$r(U) \leq 1 + (q - 1)^2 - (q - 1 - a).$$

ii) The privacy threshold of the LSSS

$$t(U) \geq b - 1.$$

iii) Assume $2a \leq q - 2$. The LSSS has $t$-strong multiplication for

$$t \leq \min\{b - 1, (q - 2 - 2a) - 1\}.$$