SECRET SHARING SCHEMES WITH A LARGE NUMBER OF PLAYERS FROM TORIC VARIETIES

JOHAN P. HANSEN

Abstract. A general theory for constructing linear secret sharing schemes over a finite field $\mathbb{F}_q$ from toric varieties is introduced. The number of players can be as large as $(q-1)^r - 1$ for $r \geq 1$. We present general methods to obtain the reconstruction and privacy thresholds as well as conditions for multiplication on the associated secret sharing schemes.

In particular we apply the method on certain toric surfaces. The main results are ideal linear secret sharing schemes where the number of players can be as large as $(q-1)^2-1$, we determine bounds for the reconstruction and privacy thresholds and conditions for strong multiplication using the cohomology and the intersection theory on toric surfaces.

Contents

Notation.

- $\mathbb{F}_q$ – the finite field with q elements of characteristic p.
- $\mathbb{F}_q^*$ – the invertible elements in $\mathbb{F}_q$.
- $k = \overline{\mathbb{F}_q}$ – an algebraic closure of $\mathbb{F}_q$.
- $M \simeq \mathbb{Z}^r$ a free $\mathbb{Z}$-module of rank r.
- $\square \subseteq M_{\mathbb{R}} = M \otimes_{\mathbb{Z}} \mathbb{R}$ – an integral convex polytope.
- $X = X_{\square}$ – the toric variety associated to the polytope $\square$.
- $T = T_N = U_0 \subseteq X$ – the torus.
- $H = \{0, 1, \ldots, q-2\} \times \cdots \times \{0, 1, \ldots, q-2\} \subset M$.

1. Introduction

1.1. **Secret sharing.** Secret sharing schemes were introduced in [3] and [17] and provide a method to split a *secret* into several pieces of information (*shares*) such that any large enough subset of the shares determine the secret, while any small subset of shares provides no information on the secret.

Secret sharing schemes have found applications in cryptography, when the schemes has certain algebraic properties. *Linear secret sharing schemes* (LSSS) are schemes where the secrets s and their associated shares $(a_1, \ldots, a_n)$ are elements in a vector space over some finite ground field $\mathbb{F}_q$. The schemes are called *ideal* if the

Date: 22. march 2014.
2010 *Mathematics Subject Classification.* 94A62, 94A60, 14M25.
Key words and phrases. Secret Sharing, Toric Varieties.
Part of this work was done while visiting Institut de Mathématiques de Luminy, MARSEILLE, France. I thank for the hospitality shown to me.

secret s and the shares a_i are elements in that ground field $\mathbb{F}_q$. Specifically, if $s, \tilde{s} \in \mathbb{F}_q$ are two secrets with share vectors $(a_1, \dots a_n), (\tilde{a}_1, \dots \tilde{a}_n) \in \mathbb{F}_q^n$, then the share vector of the secret $s+\lambda\tilde{s} \in \mathbb{F}_q$ is $(a_1+\lambda\tilde{a}_1, \dots, a_n+\lambda\tilde{a}_n) \in \mathbb{F}_q^n$ for any $\lambda \in \mathbb{F}_q$.

The reconstruction threshold of the linear secret sharing scheme is the smallest integer r such that any set of at least r of the shares $a_1, \dots, a_n$ determines the secret s. The *privacy threshold* is the largest integer t such that no set of t (or fewer) elements of the shares $a_1, \dots, a_n$ 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 af the shares determines the product of the secrets. It has *t-strong multiplication* if it has *t-privacy* and has multiplication for any subset of $n-t$ shares obtained by removing any t shares.

The properties of multiplication was introduced in [8]. Such schemes with multiplication can be utilized in the domain of multiparty computation (MPC), see [5], [2], [9] and [4].

1.2. **Toric varieties and secret sharing.** In [11], [12] and [13] we developed methods to construct linear error correcting codes from toric varieties and derived the code parameters using the cohomology and the intersection theory on toric varieties. In [14] we utilized the method and the results to construct quantum codes.

This method of toric varieties also applies to construct algebraic geometric ideal secret sharing schemes (LSSS) defined over a finite ground field $\mathbb{F}_q$ with q elements. In a certain sense our construction resembles that of [6], where LSSS schemes were constructed from algebraic curves, however the methods to obtain the parameters are completely different.

The linear secret sharing schemes we obtain are *ideal* and the number of players can be of the magnitude q^r for any positive integer r. They are obtained by evaluating certain rational functions in $\mathbb{F}_q$-rational points on toric varieties.

The thresholds and conditions for strong multiplication are derived from estimates on the maximal number of zeroes of rational functions dobtained via the cohomology and intersection theory on the underlying toric variety. In particular, we focus on toric surfaces.

We present examples of linear secret sharing schemes which are *quasi-threshold* and have *strong multiplication* [8] with respect to certain adversary structures.

Specifically, for any pair of integers a, b, with $0 \leq b \leq a \leq q-2$, we produce linear secret sharing schemes with $(q-1)^2-1$ players which are *quasi-threshold*, i.e., the reconstruction threshold is at most $1+(q-1)^2-(q-1-a)$ and the privacy threshold is at least $b-1$. The schemes have *t-strong multiplication* with respect to the threshold adversary structure if $t \leq \min\{b-1, (q-2-2a)-1\}$.

noget

For the general theory of toric varieties we refer to [16], [10] and [7].

2. Preliminaries

2.1. **Linear Secret Sharing Schemes.** This section presents basic definitions and concepts pertaining to linear secret sharing schemes as introduced in [8] and [6].

Let be $\mathbb{F}_q$ be a finite field with q elements.

A *ideal linear secret sharing scheme* $\mathcal{M}$ over a finite field $\mathbb{F}_q$ on a set $\mathcal{P}$ of n players is given by a positive integer e, a sequence $V_1, \dots V_n$ of 1-dimensional linear subspaces $V_i \subset \mathbb{F}_q^e$ and a non-zero vector $u \in \mathbb{F}_q^e$.

An *adversary structure* $\mathcal{A}$, for a secret sharing scheme $\mathcal{M}$ on the set of players $\mathcal{P}$, is a collection of subsets of $\mathcal{P}$, with the property that subsets of sets in $\mathcal{A}$ are also sets in $\mathcal{A}$. In particular, the *adversary structure* $\mathcal{A}_{t,n}$ consists of all the subsets of size at most t of the set $\mathcal{P}$ of n players, and the *access structure* $\Gamma_{r,n}$ consists of all the subsets of size at least r of the set $\mathcal{P}$ of n players.

For any subset A of players, let $V_A = \sum_{i \in A} V_i$ be the $\mathbb{F}_q$-subspace spanned by all the V_i for $i \in A$.

The *access structure* $\Gamma(\mathcal{M})$ of $\mathcal{M}$ consists of all the subsets B of players with $u \in V_B$, and $\mathcal{A}(\mathcal{M})$ consists of all the other subsets A of players, that is $A \notin \Gamma(\mathcal{M})$.

A linear secret sharing scheme $\mathcal{M}$ is said to *reject* a given adversary structure $\mathcal{A}$, if $\mathcal{A} \subseteq \mathcal{A}(\mathcal{M})$. Therefore $A \in \mathcal{A}(\mathcal{M})$ if and only there is a linear map from $\mathbb{F}_q^e$ to $\mathbb{F}_q$ vanishing on V_A, while non-zero on u.

The scheme $\mathcal{M}$ works as follows. For $i = 1, \dots n$, let $v_i \in V_i$ be bases for the 1-dimensional vector spaces. Let $s \in \mathbb{F}_q$ be a *secret*. Choose at random a linear morphism $\phi : \mathbb{F}_q^e \to \mathbb{F}_q$, subject to the condition $\phi(u) = s$, and let $a_i = \phi(v_i)$ for $i = 1, \dots, n$ be the *shares*

$$\begin{array}{rcll} \phi : \mathbb{F}_q^e & \to & \mathbb{F}_q & \\ u & \mapsto & s & \\ v_i & \mapsto & a_i & \text{for } i = 1, \dots, n \end{array}$$

Then

- the shares $\{a_i = \phi(v_i)\}_{i \in A}$ determine the secret $s = \phi(u)$ uniquely if and only if $A \in \Gamma(\mathcal{M})$,
- the shares $\{a_i = \phi(v_i)\}_{i \in A}$ reveal no information on the secret $s = \phi(u)$, i.e., when $A \in \mathcal{A}(\mathcal{M})$.

Definition 1. Let $\mathcal{M}$ be a linear secret sharing scheme.

The *reconstruction threshold* of $\mathcal{M}$ is the smallest integer r such that any set of at least r of the shares $a_1, \ldots, a_n$ determine the secret s, i.e., $\Gamma_{r,n} \subseteq \Gamma(\mathcal{M})$.

The *privacy threshold* is the largest integer t such that no set of t (or less) elements of the shares $a_1, \ldots, a_n$ determine the secret s, i.e., $\mathcal{A}_{t,n} \subseteq \mathcal{A}(\mathcal{M})$. The scheme $\mathcal{M}$ is said to have *t-privacy*.

Definition 2. An ideal linear secret sharing scheme $\mathcal{M}$ has the *strong multiplication property* with respect to an adversary structure $\mathcal{A}$ if the following holds.

1. $\mathcal{M}$ rejects the adversary structure $\mathcal{A}$.
2. Given two secrets s and $\tilde{s}$. For each $A \in \mathcal{A}$, the products $a_i \cdot \tilde{a}_i$ of all the shares of the players $i \notin A$ determine the product $s \cdot \tilde{s}$ of the two secrets.

3. Linear secret sharing schemes on tori

Let $M \simeq \mathbb{Z}^r$ be a free $\mathbb{Z}$-module of rank r over the integers $\mathbb{Z}$.

For any subset $U \subseteq M$, let $\mathbb{F}_q < U >$ be the linear span in $\mathbb{F}_q[X_1^{\pm 1}, \ldots, X_r^{\pm 1}]$ of the monomials

$$\{X^u = X_1^{u_1} \cdot \cdots \cdot X_r^{u_r} |\ u = (u_1, \ldots, u_r) \in U\} \ .$$

This is a $\mathbb{F}_q$-vectorspace of dimension equal to the number of elements in U.

Let $T(\mathbb{F}_q) = (\mathbb{F}_q^*)^r$ be the $\mathbb{F}_q$-rational points on the torus and let $S \subseteq T(\mathbb{F}_q)$ be a any subset. The linear map that evaluates elements in $\mathbb{F}_q < U >$ at all the points in S is denoted by π_S:

$$\begin{array}{rcl} \pi_S : \mathbb{F}_q < U > & \to & \mathbb{F}_q^{|S|} \\ f & \mapsto & (f(P))_{P \in S} \ . \end{array}$$

In this notation $\pi_{\{P\}}(f) = f(P)$.

Definition 3. Let $S \subseteq T(\mathbb{F}_q)$ be a any subset such that $P_0 \in S$. The linear secret sharing schemes (LSSS) $\mathcal{M}(U)$ with *support* S and $n = |S| - 1$ players is obtained as follows:

- Let $s_0 \in \mathbb{F}_q$ be a *secret* value. Select $f \in \mathbb{F}_q < U >$ at random, such that $\pi_{\{P_0\}}(f) = f(P_0) = s_0$.
- Define the n *shares* as

$$\pi_{S \setminus \{P_0\}}(f) = (f(P))_{P \in S \setminus \{P_0\}} \in \mathbb{F}_q^{|S|-1} = \mathbb{F}_q^n \ .$$

The main objectives are to study *privacy*, *reconstruction* of the secret from the shares and the property *strong multiplication* of the scheme as introduced in Definition 1 and Definition 2.

In order to present the general theory for the linear secret sharing schemes $\mathcal{M}(U)$ above, we make some preliminary definitions and observations.

3.0.1. *Translation.* Let $U \subseteq M$ be a subset, let $v \in M$ and consider the translate $v + U := \{v + u |\ u \in U\} \subseteq M$.

Lemma 4. *Translation induces an isomorphim of vectorspaces*

$$\begin{array}{rcl} \mathbb{F}_q < U > & \to & \mathbb{F}_q < v + U > \\ f & \mapsto & f^v := X^v \cdot f \ . \end{array}$$

We have that

i) The evalutations of $\pi_{T(\mathbb{F}_q)}(f)$ and $\pi_{T(\mathbb{F}_q)}(f^v)$ have the same number of zeroes on $T(\mathbb{F}_q)$.

ii) The minimal number of zeros on $T(\mathbb{F}_q)$ of evaluations of elements in $\mathbb{F}_q < U >$ and $\mathbb{F}_q < v + U >$ are the same.

iii) For $v = (v_1, \ldots, v_r)$ with v_i divisible by $q - 1$, the evaluations $\pi_S(f)$ and $\pi_S(f^v)$ are the same for any subset S of $T(\mathbb{F}_q)$.

Proof. The first claim is obvious, the inverse morphism is obtained by multiplication with X^{-v}.

Evaluating at a point $P = (\xi^{i_1}, \ldots, \xi^{i_r}) \in T(\mathbb{F}_q)$, where $\xi \in \mathbb{F}_q^*$ is a primitive element, we obtain for $v = (v_1, \ldots, v_r)$ that

$$f^v(P) = \xi^{i_1 v_1 + \cdots + i_r v_r} f(P) \ .$$

Therefore $f(P) = 0$ if and only if $f^v(P) = 0$. In particular we have that f and f^v have the same number of zeroes in $T(\mathbb{F}_q)$.

Under the assumption of *iii)*, X^v evaluates to 1, and the conclusion follows. □

An immediate consequence of *iii)* above is the following.

Corollary 5. *Let $U \subseteq M$ be a subset and let*

$$\bar{U} := \{(\bar{u}_1, \ldots, \bar{u}_r) |\ \bar{u}_i \in \{0, \ldots, q-2\} \text{ and } \bar{u}_i \equiv u_i \mod q - 1\}$$

be its reduction modulo $q - 1$. Then $\pi_S(\mathbb{F}_q < U >) = \pi_S(\mathbb{F}_q < \bar{U} >)$ for any subset $S \subseteq T(\mathbb{F}_q)$.

3.0.2. *Orthogonality.* Let $U \subseteq M$ be a subset, define its opposite as $-U := \{-u|\ u \in U\} \subseteq M$. The opposite maps the monomial X^u to X^{-u} and induces by linearity an isomorphim of vectorspaces

$$\begin{aligned} \mathbb{F}_q < U > &\to \mathbb{F}_q < -U > \\ X^u &\mapsto X^{-u} \\ f &\mapsto \hat{f}\ . \end{aligned}$$

On $\mathbb{F}_q^{|T(\mathbb{F}_q)|}$, we have the inner product

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

with $n = |T(\mathbb{F}_q)| - 1$.

Lemma 6. *Let $f, g \in \mathbb{F}_q < M >$ and assume $f \neq \hat{g}$, then*

$$\pi_{T(\mathbb{F}_q)}(f) \star \pi_{T(\mathbb{F}_q)}(g) = 0$$

Proof. □

Let

$$H = \{0, 1, \ldots, q-2\} \times \cdots \times \{0, 1, \ldots, q-2\} \subset M\ .$$

Corollary 7. *Let $U \subseteq H$ be a subset. Then we have*

i) For $f \in \mathbb{F}_q < U >$ and $g \notin \mathbb{F}_q < -H \setminus -U >$, we have that $\pi_{T(\mathbb{F}_q)}(f) \star \pi_{T(\mathbb{F}_q)}(g) = 0$.

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

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

Proof. Let $u = (u_1, \ldots, u_r) \in U$ and $v = (v_1, \ldots, v_r) \in -H \setminus -U$, then $u_{i_0} \neq -v_{i_0}$ for at least one index $i_0 = 1, \ldots, r$. We can assume $i_0 = 1$.

Let $\xi \in \mathbb{F}_q^*$ be a primitive element, then $T(\mathbb{F}_q) = \{P_{i_1,\ldots,i_r} = (\xi^{i_1}, \ldots, \xi^{i_r})|\ i_j = 0, \ldots, q-2\}$ and

$$X^{u+v}(P_{i_1,\ldots,i_r}) = \xi^{i_1(u_1+v_1)} \cdots \xi^{i_r(u_r+v_r)}\ .$$

For any fixed $i_2, \ldots, i_r$, we have

$$\sum_{i_1=0}^{q-2} X^{u+v}(P_{i_1,\ldots,i_r}) = \Big(\sum_{i_1=0}^{q-2} \xi^{i_1(u_1+v_1)}\Big) \cdot \Big(\xi^{i_2(u_2+v_2)} \cdots \xi^{i_r(u_r+v_r)}\Big) = 0\ ,$$

the first factor on the right hand side being zero, because $u_1 + v_1 \neq 0$. Therefore

$$\pi_{T(\mathbb{F}_q)}(X^u) \star \pi_{T(\mathbb{F}_q)}(X^v) = \sum_{i_1,\ldots,i_r} X^{u+v}(P_{i_1,\ldots,i_r}) = 0\ .$$

As all elements in the basis of $\pi_{T(\mathbb{F}_q)}(\mathbb{F}_q < U >)$ is orthogonal to all elements in the basis of $\pi_{T(\mathbb{F}_q)}(\mathbb{F}_q < -H \setminus -U >)$, the claim in *i)* follows by linearity.

The claim in *ii)* also follows by linearity because the dimensions of $\pi_{T(\mathbb{F}_q)}(\mathbb{F}_q < U >)$ and $\pi_{T(\mathbb{F}_q)}(\mathbb{F}_q < -H \setminus -U >)$ add up to the dimension of the ambient space $\mathbb{F}_q^{|T(\mathbb{F}_q)|}$.

□

Theorem 8. *Let $U \subseteq H = \{0, 1, \ldots, q-2\} \times \cdots \times \{0, 1, \ldots, q-2\} \subset M$ as above. Let $T(\mathbb{F}_q) = (\mathbb{F}_q^*)^r$ be the $\mathbb{F}_q$-rational points on the torus and let $P_0 \in T(\mathbb{F}_q)$ be a fixed point.*

The linear secret sharing schemes $\mathcal{M}(U)$ of Definition 3 is constructed evaluating elements in $\mathbb{F}_q < U >$ at all the points on $T(\mathbb{F}_q)$

$$\begin{aligned} \pi_{T(\mathbb{F}_q)} : \mathbb{F}_q < U > &\to \mathbb{F}_q^{|T(\mathbb{F}_q)|} \\ f &\mapsto \pi_{T(\mathbb{F}_q)}(f) = (f(P))_{P \in T(\mathbb{F}_q)}\ . \end{aligned}$$

Specifically, the secret $s \in \mathbb{F}_q$ has the $n = (q-1)^r - 1$ shares

$$\pi_{T(\mathbb{F}_q)\setminus\{P_0\}}(f) \in \mathbb{F}_q^{|T(\mathbb{F}_q)|-1}\ ,$$

where $f \in \mathbb{F}_q < U >$ is chosen at random such that $s = \pi_{P_0}(f) = f(P_0)$.

Let $r(U)$ and $t(U)$ be the reconstruction and privacy thresholds of $\mathcal{M}(U)$ as defined in Definition 1.

Then

$$\begin{aligned} r(U) = &\quad 1 + (\text{the maximal number of zeros of } \pi_{T(\mathbb{F}_q)}(f)) \\ t(U) = &\quad (q-1)^r - (\text{the maximal number of zeros of } \pi_{T(\mathbb{F}_q)}(g)) - 2 \end{aligned}$$

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

$$\begin{aligned} \pi_{T(\mathbb{F}_q)} : \mathbb{F}_q < -H \setminus -U > &\to \mathbb{F}_q^{|T(\mathbb{F}_q)|} \\ g &\mapsto \pi_{T(\mathbb{F}_q)}(g) = (g(P))_{P \in T(\mathbb{F}_q)} \ . \end{aligned}$$

Proof. Let $A \subseteq T(\mathbb{F}_q)$ with

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

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

$$\begin{aligned} \pi_T : \mathbb{F}_q < U > &\to \mathbb{F}_q^{|A|} \\ f &\mapsto (f(P))_{P \in A} \end{aligned}$$

has trivial kernel and therefore injective; consequently A belongs to the access structure $\Gamma(\mathcal{M}(U))$ of the scheme $\mathcal{M}(U)$ by definition.

Let $A \subseteq T \setminus \{P_0\}$ with

$$|A| \leq (q-1)^r - (\text{the maximal number of zeros of } \pi_{T(\mathbb{F}_q)}(g)) - 2$$

for all $g \in \mathbb{F}_q < -H \setminus -U >$. This implies that $|T(\mathbb{F}_q) \setminus A| \geq$ (the maximal number of zeros of $\pi_{T(\mathbb{F}_q)}(g)) + 2$ for all $g \in \mathbb{F}_q < -H \setminus -U >$.

Consider the morphism

$$\begin{aligned} \pi_{T(\mathbb{F}_q)\setminus A} : \mathbb{F}_q < -H \setminus -U > &\to \mathbb{F}_q^{|T(\mathbb{F}_q)\setminus A|} \\ g &\mapsto (g(P))_{P \in T(\mathbb{F}_q)\setminus A} \end{aligned}$$

evaluating in all points outside A.

The vector $y \in \mathbb{F}_q^{|T(\mathbb{F}_q)\setminus A|}$ with $\pi_{P_0}(y) = 1$ and $\pi_{T(\mathbb{F}_q)\setminus(A\cup\{P_0\})}(y) = 0$ has $|T(\mathbb{F}_q) \setminus A| - 1$ zeros. This number is strictly larger than the maximal number of zeros of $\pi_{T(\mathbb{F}_q)}(g)$ for any $g \in \mathbb{F}_q < -H \setminus -U >$, therefore $y \notin \pi_{T(\mathbb{F}_q)\setminus A}(\mathbb{F}_q < -H \setminus -U >)$.

Choose a non-zero vector $x \in \mathbb{F}_q^{|T(\mathbb{F}_q)\setminus A|}$ orthogonal to

$$\pi_{T(\mathbb{F}_q)\setminus A}(\mathbb{F}_q < -H \setminus -U >) \subset \mathbb{F}_q^{|T(\mathbb{F}_q)\setminus A|}$$

such that $x \star y \neq 0$. This implies that $\pi_{\{P_0\}}(x) \neq 0$, and we can assume that $\pi_{\{P_0\}}(x) = 1$. Define by extension $c \in \mathbb{F}_q^{|T(\mathbb{F}_q)|}$, such that $\pi_A(c) = 0$ and $\pi_{T(\mathbb{F}_q)\setminus A}(c) = x$.

Then by construction $c \star \pi_{T(\mathbb{F}_q)}(\mathbb{F}_q < -H \setminus -U >) = 0$.

By dimension reasons $\pi_{T(F_q)} : \mathbb{F}_q < H > \to \mathbb{F}_q^{|T(\mathbb{F}_q)|}$ is an isomorphism, and $c = \pi_{T(\mathbb{F}_q)}(g)$ for some $g \in \mathbb{F}_q < H >$. Therefore $g \in \mathbb{F}_q < U >$ by orthogonality as shown Corollary 7.

By construction $\pi_{P_0}(g) = 1$ and $\pi_A(g) = 0$, and therefore A belongs to the access structure $\mathcal{A}(\mathcal{M}(U))$ of the scheme $\mathcal{M}(U)$ by definition. □

Theorem 9. *Let* $U \subseteq H \subset M$ *and let* $U + U = \{u_1 + u_2 |\ u_1, u_2 \in U\}$ *be the Minkowski sum.*

The linear secret sharing schemes $\mathcal{M}(U)$ *of Definition 3 and Theorem 8, with* $n = (q-1)^r - 1$ *players, has strong multiplication with respect to* $\mathcal{A}_{t,n}$ *for* $t \leq t(U)$, *where* $t(U)$ *is the adversary threshold of* $\mathcal{M}(U)$, *if*

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

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

Proof. For $A \in \mathcal{A}_{t,n}$, let $B := T(\mathbb{F}_q) \setminus (\{P_0\} \cup A)$ with $|B| = n - t$ 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

$$\begin{aligned} \pi_B : \mathbb{F}_q < U + U > &\to \mathbb{F}_q^{|B|} \\ h &\mapsto (h(P))_{P \in B} \ . \end{aligned}$$

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 indentically on B, and we conclude that π_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. □

4. The method of toric varieties

We will from now on focus on the 2-dimensional lattice $M \simeq \mathbb{Z}^2$ and assume that $U = M \cap \Box$ consists of the integral points of a 2-dimensional integral convex polytope $\Box$ in $M_{\mathbb{R}} = M \otimes_{\mathbb{Z}} \mathbb{R}$. We will study the associated linear secret sharing scheme $\mathcal{M}(U)$ of Definition 3. The same theory applies for higher dimension.

In this case 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

$$\begin{aligned} \pi_S : \mathbb{F}_q < U > &\to \mathbb{F}_q^{|S|} \\ f &\mapsto (f(P))_{P \in S} \end{aligned}$$

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

For the general theory of toric varieties we refer to [10] and [16]. Here we will recollect some of the theory for toric surfaces.

4.1. **Toric surfaces and their cohomology.** Let M be an integer lattice $M \simeq \mathbb{Z}^2$. Let $N = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$ be the dual lattice with canonical $\mathbb{Z}$-bilinear pairing $< \ , \ >: M \times N \to \mathbb{Z}$.

Let $M_{\mathbb{R}} = M \otimes_{\mathbb{Z}} \mathbb{R}$ and $N_{\mathbb{R}} = N \otimes_{\mathbb{Z}} \mathbb{R}$ with canonical $\mathbb{R}$-bilinear pairing $< \ , \ >: M_{\mathbb{R}} \times N_{\mathbb{R}} \to \mathbb{R}$.

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

$$\Box_h = \{m \in M | \ < m, n > \geq \ h(n) \quad \forall n \in N\}. \tag{2}$$

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 Δ of strongly convex polyhedral cones in $N_{\mathbb{R}}$ such that every face of $\sigma \in \Delta$ is contained in Δ and $\sigma \cap \sigma' \in \Delta$ for all $\sigma, \sigma' \in \Delta$.

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

$$h_{\Box}(n) =< l_\sigma, n > \quad \forall n \in \sigma. \tag{3}$$

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

Upon refinement of the normal fan, we can assume that two successive pairs of $n(\rho)$'s generate the lattice and we obtain *the refined normal fan.*

Let $k = \overline{\mathbb{F}_q}$ be an algebraic closure of $\mathbb{F}_q$.

The 2-dimensional *algebraic torus* $T_N \simeq k^* \times k^*$ is defined by $T_N := \mathrm{Hom}_{\mathbb{Z}}(M, k^*)$. The multiplicative character $\mathbf{e}(m)$ for $m \in M$ is the homomorphism

$$\begin{aligned} e(m) : T_N &\to k^* \\ t &\mapsto t(m) \end{aligned}$$

Specifically, if $\{n_1, n_2\}$ and $\{m_1, m_2\}$ are dual $\mathbb{Z}$-bases of N and M and we denote $u_j := \mathbf{e}(m_j)$, $j = 1, 2$, then we have an isomorphism $T_N \simeq k^* \times k^*$ sending t to $(u_1(t), u_2(t))$. For $m = \lambda_1 m_1 + \lambda_2 m_2$ we have

$$\mathbf{e}(m)(t) = u_1(t)^{\lambda_1} u_2(t)^{\lambda_2}. \tag{4}$$

The *toric surface* $X_{\Box}$ associated to the fan Δ of $\Box$ is

$$X_{\Box} = \cup_{\sigma \in \Delta} U_\sigma \ ,$$

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

$$\mathcal{S}_\sigma = \{m \in M | < m, y > \geq 0 \ \forall y \in \sigma\}.$$

The *toric surface* $X_{\Box}$ is irreducible, non-singular and complete under the assumption that we are working with the refined normal fan. If $\sigma, \tau \in \Delta$ and τ is a face of σ, then U_τ is an open subset of U_σ. Obviously $\mathcal{S}_0 = M$ and $U_0 = T_N$ such that the algebraic torus T_N is an open subset of $X_{\Box}$.

T_N *acts algebraically* on $X_{\Box}$. On $u \in U_\sigma$ the action of $t \in T_N$ is obtained as

$$(tu)(m) := t(m)u(m) \quad \text{for } m \in \mathcal{S}_\sigma \ ,$$

such that $tu \in U_\sigma$ and U_σ is T_N-stable.

The orbits of this action are in one-to-one correspondance with Δ. For each $\sigma \in \Delta$ let

$$\mathrm{orb}(\sigma) := \{u : M \cap \sigma \to k^* | u \text{ is a group homomorphism}\} \ .$$

Then $\mathrm{orb}(\sigma)$ is a T_N-orbit in $X_{\Box}$. Define $V(\sigma)$ to be the closure of $\mathrm{orb}(\sigma)$ in $X_{\Box}$.

A Δ-linear support function h gives rise to a polytope $\square$ as in (9) and an associated Cartier divisor

$$D_h = D_\square := -\sum_{\rho\in\Delta(1)} h(n(\rho))\, V(\rho)\ , \tag{5}$$

where $\Delta(1)$ consists of the 1-dimensional cones in Δ. In particular

$$D_m = \operatorname{div}(\mathbf{e}(-m)), \quad m \in M.$$

Lemma 10. *Let h be a Δ-linear support function with associated convex polytope $\square$ as in (9) and Cartier divisor $D_h = D_\square$ as in (5).*

The vector space $\mathrm{H}^0(X, O_X(D_h))$ of global sections of $O_X(D_\square)$, i.e., rational functions f on $X_\square$ such that $\operatorname{div}(f) + D_\square \geq 0$ has dimension $|(M \cap \square)|$, that is the number af lattice points in $\square$, and has

$$\{\mathbf{e}(m) | m \in M \cap \square = U\}$$

as a basis.

4.2. **Intersection theory on a toric surface.** For a Δ-linear support function h and a 1-dimensional cone $\rho \in \Delta(1)$ we will determine the intersection number $(D_h; V(\rho))$ between the Cartier divisor D_h of (5) and $V(\rho)) = \mathbb{P}^1$.

This number is obtained in [16, Lemma 2.11]. The 1-dimensional cone $\rho \in \Delta(1)$ is the common face of two 2-dimensional cones $\sigma', \sigma'' \in \Delta(2)$. Choose primitive elements $n', n'' \in N$ such that

$$\begin{aligned} n' + n'' &\in \mathbb{R}\rho \\ \sigma' + \mathbb{R}\rho &= \mathbb{R}_{\geq 0} n' + \mathbb{R}\rho \\ \sigma'' + \mathbb{R}\rho &= \mathbb{R}_{\geq 0} n'' + \mathbb{R}\rho \end{aligned}$$

Lemma 11. *For any $l_\rho \in M$, such that h coincides with l_ρ on ρ, let $\overline{h} = h - l_\rho$. Then*

$$(D_h; V(\rho)) = -(\overline{h}(n') + \overline{h}(n'').$$

In the 2-dimensional non-singular case let $n(\rho)$ be a primitive generator for the 1-dimensional cone ρ. There exists an integer a such that

$$n' + n'' + an(\rho) = 0,$$

$V(\rho)$ is itself a Cartier divisor and the above gives the self-intersection number

$$(V(\rho); V(\rho)) = a\ .$$

More generally the self-intersection number of a Cartier divisor D_h is obtained in [16, Prop. 2.10].

Lemma 12. *Let D_h be a Cartier divisor and let $\square_h$ be the polytope associated to h as in (9). Then*

$$(D_h; D_h) = 2\operatorname{vol}_2(\square_h)\ ,$$

where vol_2 is the normalized Lesbesgue-measure.

4.3. **The support of the secret sharing schemes.** The secret sharing scheme $\mathcal{M}(U)$ of Definition 3 is obtained by evaluating certain rational functions in a suitable subset S of $\mathbb{F}_q$-rational points, which in certain cases is contained in the intersection of two ample divisor on the toric varieties X.

Remark 13. For $i = 1, 2$, let $I_i, J_i \subseteq \mathbb{F}_q^*$ with $I_1 \cap J_2 = I_2 \cap J_1 = \emptyset$, and introduce the two rational functions

$$F_i = \prod_{\psi\in I_1} (e(m_1) - \psi)^{n_{1,\psi}} \prod_{\psi\in J_1} (e(m_2) - \psi)^{n_{2,\psi}}\ , \quad i = 1, 2\ ,$$

where the integer exponents satisfy $n_{1,\psi} \geq 1$ and $n_{2,\psi} \geq 1$.

For $i = 1, 2$, let $D_i = (F_i)_0$ be their divisor of zeroes and let $|D_i|$ be their support. It is important to note that the supports are independent of the choice of the exponents $n_{1,\psi} \geq 1$ and $n_{2,\psi} \geq 1$.

The support set S of the linear secret sharing scheme $\mathcal{M}(U)$ can in certain cases be realized as a subset of $|D_i| \cap |D_2| \subseteq \mathbb{F}_q^* \times \mathbb{F}_q^*$.

As a set $S \subseteq (I_1 \times J_2) \cup (I_2 \times J_1) \subseteq \mathbb{F}_q^* \times \mathbb{F}_q^*$ with $|S| = (|I_1| \cdot |J_2|) + (|I_2| \cdot |J_1|)$ elements, but it is important to have in mind, that $S \subseteq \mathbb{F}_q^* \times \mathbb{F}_q^*$ is realized as the support of the intersection of two divisors in many different ways, namely one for each choice of the exponents $n_{1,\psi} \geq 1$ and $n_{2,\psi} \geq 1$.

4.4. **Linear secret sharing schemes from convex polytopes and evaluations on toric varieties.** In Definition 3 we assume that $U \subseteq M$ is the lattice points of an integral convex polytope $\square$, i.e., $U = \square \cap M$.

We exhibit the linear secret sharing schemes $\mathcal{M}(U)$ of Definition 3 as evaluations of rational functions in $\mathbb{F}_q$-rational points on the toric variety $X_\square$ associated to the normal fan of $\square$.

Remark 14. For each $t \in T \simeq k^* \times k^*$, we evaluate the rational functions in $\mathrm{H}^0(X, O_X(D_\square))$

$$\begin{aligned} \mathrm{H}^0(X, O_X(D_\square)) &\to k \\ f &\mapsto f(t) \ . \end{aligned}$$

Let $\mathrm{H}^0(X, O_X(D_\square))^{\mathrm{Frob}}$ be the rational functions in $\mathrm{H}^0(X, O_X(D_\square))$, that are invariant under the action of the Frobenius, that is functions that are $\mathbb{F}_q$-linear combinations of the functions $\mathbf{e}(m)$ in (4). From Lemma 10 $\mathbb{F}_q < U >= \mathrm{H}^0(X, O_X(D_\square))^{\mathrm{Frob}}$.

Evaluating in all points of $T(\mathbb{F}_q)$, we obtain the evaluations

$$\begin{aligned} \mathbb{F}_q < U >= \mathrm{H}^0(X, O_X(D_h))^{\mathrm{Frob}} &\to \mathbb{F}_q^{|T(\mathbb{F}_q|} \\ f &\mapsto (f(t))_{t \in T(\mathbb{F}_q)} \\ \mathbf{e}(m) &\mapsto (\mathbf{e}(m)(t))_{t \in T(\mathbb{F}_q)} \end{aligned}$$

as in (4).

Let

$$S = \{P_0, \ldots, P_n\} \subseteq T(\mathbb{F}_q) = \mathbb{F}_q^* \times \mathbb{F}_q^*, \quad n < (q-1)^2$$

be a set of distinct $\mathbb{F}_q$-rational points.

The linear secret sharing scheme $\mathcal{M}(U)$ was constructed as follows. Let $s_0 \in \mathbb{F}_q$ be a secret value. Select at random $f \in \mathrm{H}^0(X, O_X(D_h))^{\mathrm{Frob}}$ such that $f(P_0) = s_0$ and define the shares

$$s_1 := f(P_1), \ldots, s_n := f(P_n) \ .$$

To estimate the privary and adversary thresholds and assure strong multiplication we have according to Theorem 8 and Theorem 9 to bound the number of points, where the rational functions in $\mathbb{F}_q < V >$ evaluates to zero for various sets V.

Assume the support set S of $\mathcal{M}(U)$ of Definition 3 is stratified by the intersections with the zeros of $\mathbf{e}(m_1) - \psi$, where $\psi \in I_1 \cup I_2 \subseteq \mathbb{F}_q^*$ as in Remark 13. A rational function f can either vanish identically on a stratum or have a finite number of zeroes along the stratum.

4.4.1. *Identically vanishing.* Assume that f is identically zero along precisely a of these strata. As $\mathbf{e}(m_1) - \psi$ and $\mathbf{e}(m_1)$ have the same divisors of poles, they have equivalent divisors of zeroes, so

$$(\mathbf{e}(m_1) - \psi)_0 \sim (\mathbf{e}(m_1))_0.$$

Therefore

$$\mathrm{div}(f) + D_\square - a(\mathbf{e}(m_1))_0 \geq 0$$

or equivalently

$$f \in \mathrm{H}^0(X, O_X(D_\square - a(\mathbf{e}(m_1))_0).$$

Depending on the polytope $\square$ this gives an upper bound for the number a, using Lemma 10.

4.4.2. *Vanishing in a finite number of points.* On any of the $\#I_1 \cup \#I_2 - a$ other strata the number of zeroes of f is according to [15] at most the intersection number

$$(D_\square - a(\mathbf{e}(m_1))_0; (\mathbf{e}(m_1))_0). \tag{6}$$

This number can be calculated using Lemma 11 and Lemma 12.

The above gives a method to construct toric codes from surfaces and obtain their precise parameters, this was done by the author in various cases in [11], [12] and [13].

5. Secret Sharing Schemes with $(q-1)^2 - 1$ players over $\mathbb{F}_q$

Let $X_\square$ be the toric variety associated to the normal fan of the integral convex polytope $\square$ with corresponding support function h and Cartier Divisor D_h.

Let $U = M \cap \square$ be the lattice points in $\square$ and let $\mathcal{M}(U)$ be the linear secret sharing scheme with support $S = T(\mathbb{F}_q)$ as defined in Definition 3.

5.1. **Hirzebruch surfaces.** Let d, e, r be positive integers and let $\square$ be the polytope in $M_{\mathbb{R}}$ with vertices $(0,0),(d,0),(d,e+rd),(0,e)$ rendered in Figure 1 and with refined normal fan depicted in Figure 2. The related toric surface is called a *Hirzebruch surface*. Let $U = M \cap \square$ be the lattice points in $\square$.

We have the following primitive generators for the 1-dimensional cones

$$n(\rho_1) = \begin{pmatrix} 1 \\ 0 \end{pmatrix},\ n(\rho_2) = \begin{pmatrix} 0 \\ 1 \end{pmatrix},\ n(\rho_3) = \begin{pmatrix} -1 \\ 0 \end{pmatrix},\ n(\rho_4) = \begin{pmatrix} r \\ -1 \end{pmatrix}\ .$$

Let σ_1 be the cone generated by $n(\rho_1)$ and $n(\rho_2)$, σ_2 be the cone generated by $n(\rho_2)$ and $n(\rho_3)$, σ_3 the cone generated by $n(\rho_3)$ and $n(\rho_4)$ and σ_4 the cone generated by $n(\rho_4)$ and $n(\rho_1)$.

The support function is:

$$h_{\square}\begin{pmatrix} n_1 \\ n_2 \end{pmatrix} = \begin{cases} \begin{pmatrix} 0 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_1, \\ \begin{pmatrix} d \\ 0 \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_2, \\ \begin{pmatrix} d \\ e+rd \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_3, \\ \begin{pmatrix} 0 \\ e \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_4. \end{cases}$$

For all pairs of 1-dimensional cones $\rho_i, \rho_j \in \Delta(1), i = 1, \ldots, 4$, the intersection numbers $(V(\rho_i); V(\rho_j))$ are determined by the methods of 4.2 and the results are presented in Table 1.

From the Hirzebruch surfaces with $I_1 = J_2 = \mathbb{F}_q^* \times \mathbb{F}_q^*$ and $I_2 = J_1 = \emptyset$ in the notation of Remark 13, we obtain using the above method the following result.

Proposition 15. *Assume that $d \leq q-2$, $e \leq q-2$ and that $e + rd \leq q-2$.*

Then the number of lattice points in $\square$) is

$$|U| = |(M \cap \square)| = (d+1)(e+1) + r\frac{d(d+1)}{2}\ .$$

The maximal number of zeros of a function $f \in \mathbb{F}_q < U >$ on $T(\mathbb{F}_q)$ is precisely

$$\max\{d(q-1) + (q-1-d)e, (q-1)(e+dr)\}$$

and the reconstruction threshold $r(U)$ of the secret sharing scheme $\mathcal{M}(U)$ is

$$r(U) = 1 + \max\{d(q-1) + (q-1-d)e, (q-1)(e+dr)\}\ . \tag{7}$$

Proof. The first claim is trivial.

As for the second let $m_1 = (1,0)$. The $\mathbb{F}_q$-rational points of $T \simeq \overline{\mathbb{F}}_q^{\,*} \times \overline{\mathbb{F}}_q^{\,*}$ belong to the $q-1$ lines on $X_{\square}$ given by

$$\prod_{\eta \in \mathbb{F}_q^*} (\mathbf{e}(m_1) - \eta) = 0\ .$$

Let $0 \neq f \in \mathrm{H}^0(X, O_X(D_h))$. Assume that f is zero along precisely a of these lines.

As $\mathbf{e}(m_1) - \eta$ and $\mathbf{e}(m_1)$ have the same divisors of poles, they have equivalent divisors of zeroes, so

$$(\mathrm{div}(\mathbf{e}(m_1) - \eta))_0 \sim (\mathrm{div}(\mathbf{e}(m_1)))_0.$$

Therefore

$$\mathrm{div}(f) + D_h - a(\mathrm{div}(\mathbf{e}(m_1)))_0 \geq 0$$

or equivalently

$$f \in \mathrm{H}^0(X, O_X(D_h - a(\mathrm{div}(\mathbf{e}(m_1)))_0).$$

This implies that $a \leq d$ according to Lemma 10.

On any of the other $q-1-a$ lines the number of zeroes of f is according to the discussion above at most the intersection number

$$(D_h - a(\mathrm{div}(\mathbf{e}(m_1)))_0; (\mathrm{div}(\mathbf{e}(m_1)))_0).$$

This number can be calculated using Lemma 11 and Lemma 12. and is easily determined using the intersection table above and the fact that $(\mathrm{div}(\mathbf{e}(m_1)))_0 = V(\rho_1) + rV(\rho_4)$.

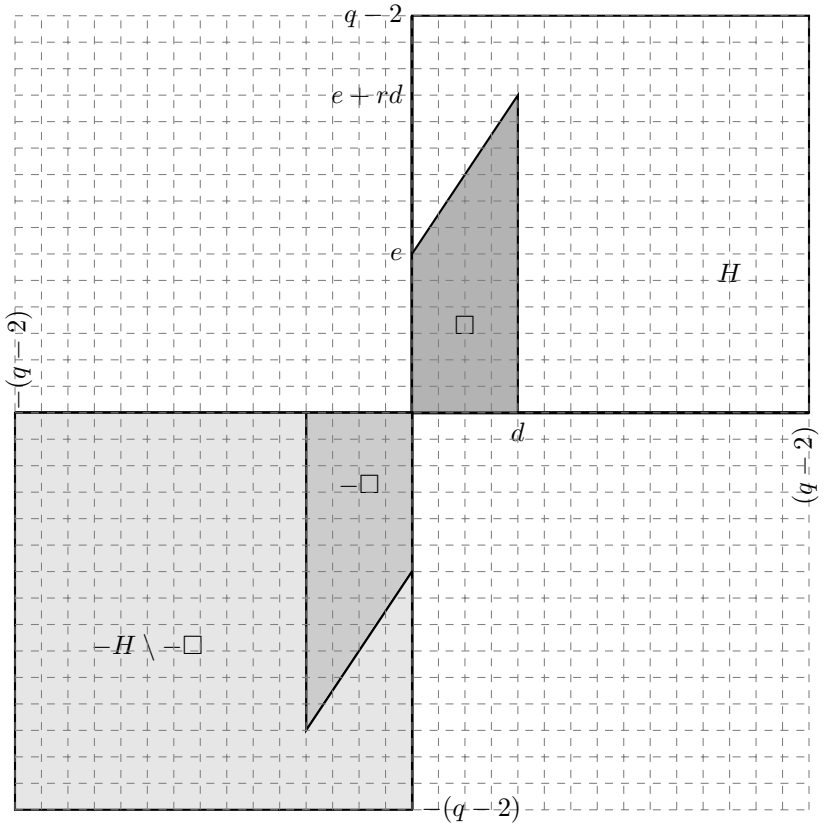
We get

$$(D_h - a(\mathrm{div}(\mathbf{e}(m_1)))_0; (\mathrm{div}(\mathbf{e}(m_1)))_0) = e + (d-a)r.$$

As $0 \leq a \leq d$, we conclude the total number of zeroes for f is at most

$$a(q-1) + (q-1-a)(e + (d-a)r) \leq \max\{d(q-1) + (q-1-d)e, (q-1)(e+dr)\}\ ,$$

FIGURE 1. Hirzebruch surfaces. The convex polytope H with vertices $(0,0),(q-2,0),(q-2,q-2),(0,q-2)$, the convex polytope $\square$ with vertices $(0,0),(d,0),(d,e+rd),(0,e)$ and their opposite convex polytopes $-H$ and $-\square$. Also the (non-convex) polytope $-H \setminus -\square$ is depicted.



	$V(\rho_1)$	$V(\rho_2)$	$V(\rho_3)$	$V(\rho_4)$
$V(\rho_1)$	$-r$	1	0	1
$V(\rho_2)$	1	0	1	0
$V(\rho_3)$	0	1	r	1
$V(\rho_4)$	1	0	1	0

TABLE 1. The intersection numbers for the four 1-dimensional cones of the fan of the Hirzebruch surface

consequently we have, according to Theorem 8, the inequality

$$r(U) \leq 1 + \max\{d(q-1) + (q-1-d)e, (q-1)(e+dr)\} \ . \tag{8}$$

To obtain equality in (8) we exhibit functions with the maximal number of zeros on $T(\mathbb{F}_q)$.

Let $b_1, \ldots, b_{e+rd} \in \mathbb{F}_q^*$ be pairwise different elements. The function

$$x^d(y-b_1)\cdot\cdots\cdot(y-b_{e+rd}) \in \mathrm{H}^0(X, O_X(D_h))^{\mathrm{Frob}}$$

evaluates to zero in the $(q-1)(e+rd)$ points

$$(x, b_j), x \in \mathbb{F}_q^*, \quad j = 1, \ldots, e+rd \ .$$

Let $a_1, \ldots, a_d \in \mathbb{F}_q^*$ be pairwise different elements and let $b_1, \ldots, b_e \in \mathbb{F}_q^*$ be pairwise different elements. The function

$$(x-a_1)\cdot\cdots\cdot(x-a_d)(y-b_1)\cdot\cdots\cdot(y-b_e) \in \mathrm{H}^0(X, O_X(D_h))^{\mathrm{Frob}}$$

evaluates to zero in the $d(q-1)+(q-1)e-de$ points

$$(a_i, y), (x, b_j), \quad x, y \in \mathbb{F}_q^* \ .$$

□

Remark 16. The polytope $-H \setminus -U$ is not convex, so our method do not determine the privacy threshold $t(U)$. It would be interesting to examine the methods of [1] on order bounds for toric codes in this context.

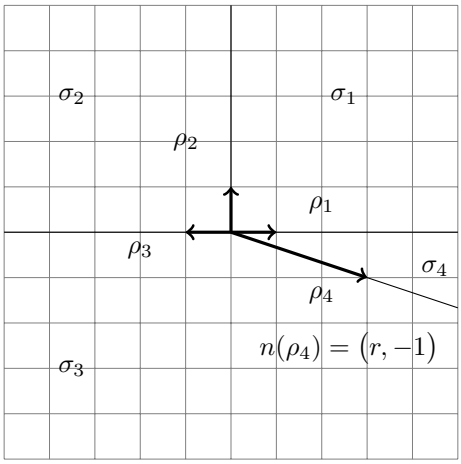


FIGURE 2. The normal fan and its 1-dimensional cones ρ_i, with primitive generators $n(\rho_i)$, and 2-dimensional cones σ_i for $i = 1, \ldots, 4$ of the polytope $\square$ in Figure1.

5.2. **Toric surfaces with associated linear secret sharing schemes with strong multiplication.** Let a, b be positive integers $0 \leq b \leq a \leq q-2$, and let $\square$ be the polytope in $M_{\mathbb{R}}$ with vertices $(0,0), (a,0), (b, q-2), (0, q-2)$ rendered in Figure 3 and with normal fan depicted in Figure 4.

The primitive generators of the 1-dimensional cones are

$$n(\rho_1) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \; n(\rho_2) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \; n(\rho_3) = \begin{pmatrix} \frac{-(q-2)}{\gcd(a-b, q-2)} \\ \frac{-(a-b)}{\gcd(a-b, q-2)} \end{pmatrix}, n(\rho_4) = \begin{pmatrix} 0 \\ -1 \end{pmatrix} .$$

For $i = 1, \ldots, 4$, the 2-dimensional cones σ_i are shown in Figure 4. The faces of σ_1 are $\{\rho_1, \rho_2\}$, the faces of σ_2 are $\{\rho_2, \rho_3\}$, the faces of σ_3 are $\{\rho_3, \rho_4\}$ and the faces of σ_4 are $\{\rho_4, \rho_1\}$.

The support function of $\square$ is:

$$h_{\square} \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} = \begin{cases} \begin{pmatrix} 0 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_1, \\ \begin{pmatrix} a \\ 0 \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_2, \\ \begin{pmatrix} b \\ q-2 \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_3, \\ \begin{pmatrix} 0 \\ q-2 \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_4. \end{cases} \tag{9}$$

The related toric surface is in general singular as $\{n(\rho_2), n(\rho_3)\}$ and $\{n(\rho_3), n(\rho_4)\}$ are not bases for the lattice M. We can desingularize by subdividing the cones σ_2 and σ_3, however our calculations will only involve the cones σ_1 and σ_2, so we refrain from that.

For all pairs of 1-dimensional cones $\rho_i, \rho_j \in \Delta(1), i = 1, \ldots, 4$, the intersection numbers $(V(\rho_i); V(\rho_j))$ are determined by the methods of 4.2. We only need the self-intersection number $(V(\rho_1); V(\rho_1))$, and as

$$n(\rho_2) + n(\rho_4) + 0 \cdot n(\rho_1) = 0 \; ,$$

we have that

$$(V(\rho_1); V(\rho_1)) = 0 \tag{10}$$

by the remark following Lemma 11.

Let $U = M \cap \square$ be the lattice points in $\square$.

From the toric surfaces constructed from $\square$ with $I_1 = J_2 = \mathbb{F}_q^* \times \mathbb{F}_q^*$ and $I_2 = J_1 = \emptyset$ in the notation of Remark 13, we obtain the following result.

Theorem 17. *Assume a, b are integers with $0 \leq b \leq a \leq q-2$.*

Let $\square$ be the polytope in $M_{\mathbb{R}}$ with vertices $(0,0), (a,0), (b, q-2), (0, q-2)$ rendered in Figure 3, and let $U = M \cap \square$ be the lattice points in $\square$.

i) The maximal number of zeros of $\pi_{T(\mathbb{F}_q)}(f)$ for $f \in \mathbb{F}_q < U >$ is less than or equal to

$$(q-1)^2 - (q-1-a) \; .$$

ii) The reconstruction threshold $r(U)$ of the secret sharing scheme $\mathcal{M}(U)$ of Definition 3 satisfy

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

iii) The privacy threshold $t(U)$ of the secret sharing scheme $\mathcal{M}(U)$ satisfy

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

iv) Assume $2a \leq q-2$. The secret sharing scheme $\mathcal{M}(U)$ has t-strong multiplication for

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

Proof. Let $m_1 = (1,0)$. The $\mathbb{F}_q$-rational points of $T \simeq {\overline{\mathbb{F}}_q}^* \times {\overline{\mathbb{F}}_q}^*$ belong to the $q-1$ lines on $X_\square$ given by

$$\prod_{\eta \in \mathbb{F}_q^*} (\mathbf{e}(m_1) - \eta) = 0 \ .$$

Let $0 \neq f \in \mathrm{H}^0(X, O_X(D_h))$. Assume that f is zero along precisely c of these lines.

As $\mathbf{e}(m_1) - \eta$ and $\mathbf{e}(m_1)$ have the same divisors of poles, they have equivalent divisors of zeroes, so

$$(\mathbf{e}(m_1) - \eta)_0 \sim (\mathbf{e}(m_1))_0 \ .$$

Therefore

$$\mathrm{div}(f) + D_h - c(\mathbf{e}(m_1))_0 \geq 0$$

or equivalently

$$f \in \mathrm{H}^0(X, O_X(D_h - c(\mathbf{e}(m_1))_0) \ .$$

This implies that $c \leq a$ according to Lemma 10.

On any of the other $q-1-c$ lines the number of zeroes of f is according to the discussion in 4.4.2 at most the intersection number

$$(D_h - c(\mathbf{e}(m_1))_0; (\mathbf{e}(m_1))_0) \ .$$

This number can be calculated using Lemma 11 using the observation that $(\mathbf{e}(m_1))_0 = V(\rho_1)$.

We get from (9) and (10) that

$$\begin{gathered}(D_h - c(\mathbf{e}(m_1))_0; (\mathbf{e}(m_1))_0) = \\ (D_h; (\mathbf{e}(m_1))_0) - c(\mathbf{e}(m_1))_0; (\mathbf{e}(m_1))_0) = \\ -h_\square \begin{pmatrix} 0 \\ 1 \end{pmatrix} - h_\square \begin{pmatrix} 0 \\ -1 \end{pmatrix} = q-2 \ ,\end{gathered}$$

as $l_{\rho_1} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \in M$.

As $0 \leq c \leq a$, we conclude the total number of zeroes for f is at most

$$c(q-1) + (q-1-c)(q-2) \leq a(q-1) + (q-1-a)(q-2) = (q-1)^2 - (q-1-a)$$

proving *i).*

According to Theorem 8, we have the inequality of *ii)*

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

We obtain *iii)* by using the result in *i)* on the polytope $(q-2, q-2) + \big(-H \setminus -\square\big)$ with vertices $(0,0), (q-2-b, 0), (q-2-a, q-2)$ and $(q-2, q-2)$. The maksimal number of zeros of $\pi_{T(\mathbb{F}_q)}(g)$ for $g \in \mathbb{F}_q < -H \setminus -U >$ is by Lemma 4 and the result in *i)* less than or equal to $(q-1)^2 - (q-1-(q-2-b)) = (q-1)^2 - 1 - b$ and *iii)* follows from Theorem 8.

To prove *iv)* assume $t \leq (q-2-2a)-1$ and $t \leq b-2$. We will use Theorem 9.

Consider the Minkowski sum $U+U$ and let $V = \overline{U+U}$ be its reduction modulo $q-1$ as in Corollary 5. Under the assumption $2a \leq q-2$, we have that $V = \overline{U+U}$ is the lattice points of the integral convex polytope with vertices $(0,0), (2a, 0), (2b, q-2)$ and $(0, q-2)$.

By the result in *i)* the maksimal number of zeros of $\pi_{T(\mathbb{F}_q)}(h)$ for $h \in \mathbb{F}_q < V >$ is less than or equal to $(q-1)^2 - (q-1-2a)$. As the number of players is $n = (q-1)^2 - 1$, the right hand side of the condition (1) of Theorem 9 is least $(q-2-2a)-1$, which by assumption is at least t.

By assumption $t \leq b-1$ and from *iii)* we have that $b-1 \leq t(U)$. We conclude that $t \leq t(U)$.

□

FIGURE 3. The convex polytope H with vertices $(0,0),(q-2,0),(q-2,q-2),(0,q-2)$ and the convex polytope $\square$ with vertices $(0,0),(a,0),(b,q-2),(0,q-2))$ are shown. Also their opposite convex polytopes $-H$ and $-\square$, the complement $-H \setminus -\square$ and its translate $(q-2,q-2)+\big(-H \setminus -\square\big)$ are depicted. Finally the convex hull of the reduction modulo $q-1$ of the Minkowski sum $U+U$ of the lattice points $U = \square \cap M$ in $\square$, is rendered. It has vertices $(0,0),(2a,0),(2b,q-2)$ and $(0,q-2)$.

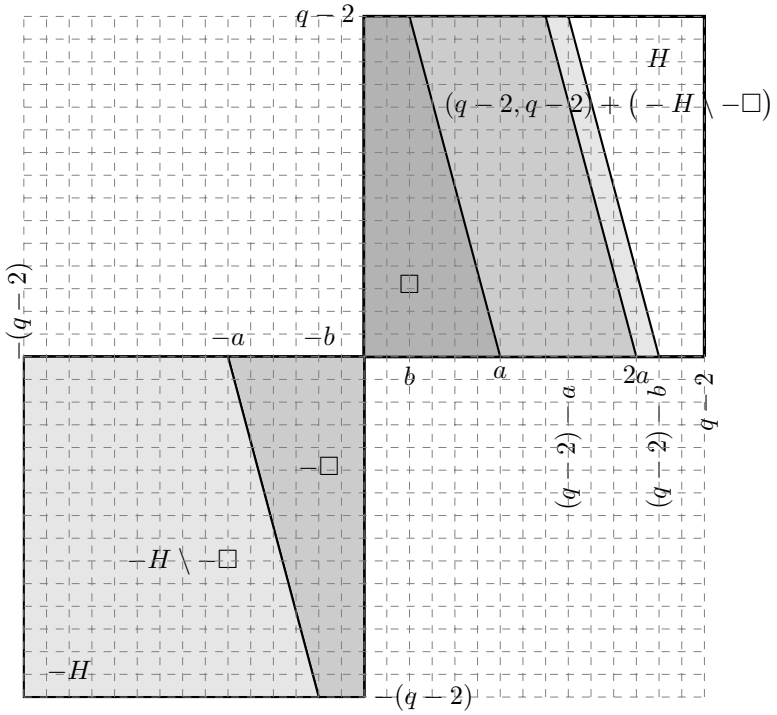
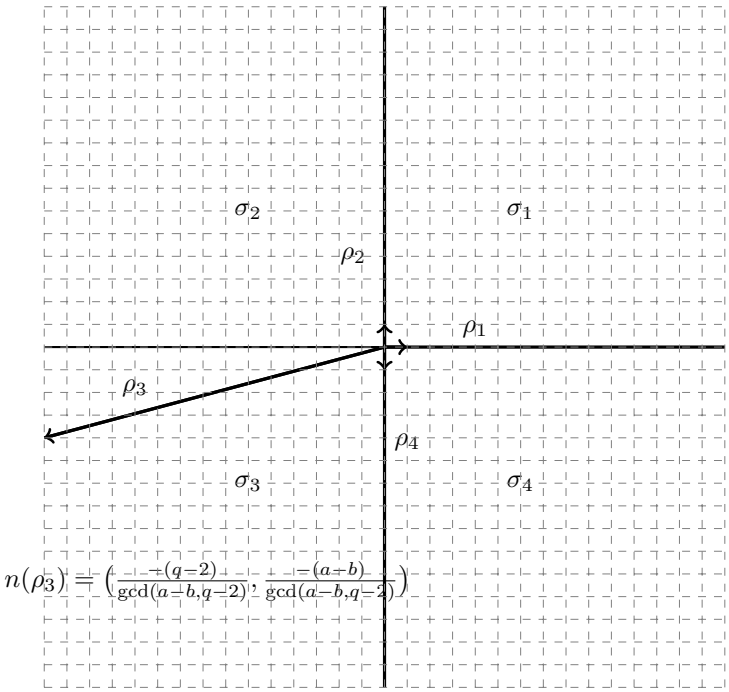


FIGURE 4. The normal fan and its 1-dimensional cones ρ_i, with primitive generators $n(\rho_i)$, and 2-dimensional cones σ_i for $i = 1,\ldots,4$ of the polytope $\square$ in Figure 3.



References

[1] Peter Beelen and Diego Ruano. The order bound for toric codes. In Maria Bras-Amorós and Tom Høholdt, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 5527 of *Lecture Notes in Computer Science*, pages 1–10. Springer Berlin Heidelberg, 2009.

[2] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In Simon [18], pages 1–10.

[3] G.R. Blakley. Safeguarding cryptographic keys. In *Proceedings of the 1979 AFIPS National Computer Conference*, pages 313–317, Monval, NJ, USA, 1979. AFIPS Press.

[4] I. Cascudo. *On Asymptotically Good Strongly Multiplicative Linear Secret Sharing*. PhD thesis, University of Oviedo, 2010.

[5] David Chaum, Claude Crépeau, and Ivan Damgård. Multiparty unconditionally secure protocols (extended abstract). In Simon [18], pages 11–19.

[6] Hao Chen and Ronald Cramer. Algebraic geometric secret sharing schemes and secure multi-party computations over small fields. In Cynthia Dwork, editor, *Advances in Cryptology - CRYPTO 2006*, volume 4117 of *Lecture Notes in Computer Science*, pages 521–536. Springer Berlin Heidelberg, 2006.

[7] David A. Cox, John B. Little, and Henry K. Schenck. *Toric varieties*. Graduate Studies in Mathematics 124. Providence, RI: American Mathematical Society (AMS). xxiv, 841 p. , 2011.

[8] Ronald Cramer, Ivan Damgård, and Ueli Maurer. General secure multi-party computation from any linear secret-sharing scheme. In Bart Preneel, editor, *Advances in Cryptology — EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 316–334. Springer Berlin Heidelberg, 2000.

[9] Ronald Cramer, Ivan Damgård, and Jesper Buus Nielsen. *Secure Multiparty Computation and Secret Sharing - An Information Theoretic Appoach*. book draft, 2012.

[10] William Fulton. *Introduction to toric varieties*. Annals of mathematics studies. Princeton Univ. Press, Princeton, NJ, 1993.

[11] Johan P. Hansen. *Toric Surfaces and Codes*, pages 42–43. IEEE, 1998.

[12] Johan P. Hansen. *Toric surfaces and error-correcting codes*, pages 132–142. Springer, 2000.

[13] Johan P. Hansen. Toric varieties hirzebruch surfaces and error-correcting codes. *Applicable Algebra in Engineering, Communication and Computing*, 13(4):289–300, 2002.

[14] Johan P. Hansen. Quantum codes from toric surfaces. *I E E E Transactions on Information Theory*, 59(2):1188–1192, 2013.

[15] Søren Have Hansen. Error-correcting codes from higher-dimensional varieties. *Finite Fields and Their Applications*, 7(4):530 – 552, 2001.

[16] Tadao Oda. *Convex bodies and algebraic geometry*. Springer, 1988.

[17] Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.

[18] Janos Simon, editor. *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA*. ACM, 1988.

Department of Mathematics, Aarhus University, Ny Munkegade 118, DK-8000 Aarhus C, Denmark
E-mail address: matjph@imf.au.dk