Contemporary Mathematics

Secret Sharing Schemes with Strong Multiplication and a Large Number of Players from Toric Varieties

Johan P. Hansen

Abstract. This article consider Massey's construction for constructing linear secret sharing schemes from toric varieties over a finite field $\mathbb{F}_q$ with q elements. The number of players can be as large as $(q-1)^r - 1$ for $r \geq 1$. The schemes have strong multiplication, such schemes can be utilized in the domain of multiparty computation.

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.

2010 *Mathematics Subject Classification.* 94A62, 94A60, 14M25 .

Part of this work was done while visiting Institut de Mathématiques de Luminy, MARSEILLE, France. I thank for the hospitality shown to me.

This work was supported by the Danish Council for Independent Research, grant no. DFF-4002-00367.

- $\square \subseteq M_{\mathbb{R}} = M \otimes_{\mathbb{Z}} \mathbb{R}$ – an integral convex polytope.
- $X = X_{\square}$ – the toric variety associated to the polytope $\square$.
- $T = T_N = U_0 \subseteq X$ – the torus.
- $H = \{0, 1, \dots, q-2\} \times \cdots \times \{0, 1, \dots, q-2\} \subset M$.

1. Introduction

1.1. Secret sharing.

Secret sharing schemes were introduced in [**3**] and [**26**] and provide a method to split a *secret* into several pieces of information (*shares*) so that any large enough subset of the shares determines 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 $(a_1, \dots, a_n)$ are elements in a vector space over some finite ground field $\mathbb{F}_q$. The schemes are called *ideal* if the 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 so 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 of 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 [**10**]. Such schemes with multiplication can be utilized in the domain of multiparty computation (MPC), see [**6**], [**2**], [**5**] and [**11**].

1.2. Toric varieties and secret sharing.

In [**14**], [**15**] and [**16**] 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 [**17**] we utilized the method and the results to construct quantum codes.

Massey's construction of linear secret sharing schemes from error-correcting codes [**22**] also applies to our codes on toric varieties. In a certain sense our construction resembles that of [**7**], where LSSS schemes were constructed from Goppa codes on 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 are $q^r - 1$ for any positive integer r. The classical Shamir scheme only allows $q - 1$ players, however, there are methods to allow schemes with more players using linear codes [**8**], this article presents such a method.

The schemes 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 maximum number of zeroes of rational functions obtained 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* [**10**] 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 $t \leq \min\{b-1, (q-2-2a)-1\}$.

For the general theory of toric varieties, we refer to [**23**], [**13**] and [**9**].

2. Preliminaries

2.1. Linear Secret Sharing Schemes. This section presents basic definitions and concepts pertaining to linear secret sharing schemes as introduced in [**22**],[**10**], [**7**] and [**8**].

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

An *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 if 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 2.1. Let $\mathcal{M}$ be a linear secret sharing scheme.

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

The *privacy threshold* is the largest integer t so that no set of t (or less) elements of the shares $a_1, \dots, a_n$ 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 2.2. 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 with multiplication on tori

In [**14**], [**15**] and [**16**] we introduced linear codes from toric varieties and estimated the minimum distance of such codes using intersection theory. Our method to estimate the minimum distance of toric codes has subsequently been supplemented, e.g., [**18**], [**29**], [**19**], [**24**], [**1**],[**20**] [**28**], and [**21**].

Linear secret sharing schemes obtained from linear codes were introduced by James L. Massey in [**22**] and were generalized in [**8**, Section 4.1]. A scheme with n players is obtained from a linear C code of length $n+1$ and dimension k with privacy threshold $t = d' - 2$ and reconstruction threshold $r = n - d + 2$, where d is the minimum distance of the code and d' the minimum distance of the dual code.

We utilize the Massey construction to obtain linear secret sharing schemes from toric codes.

Under certain conditions the linear secret sharing schemes from toric codes have the strong multiplication property.

3.1. The construction.

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 $\mathbb{F}_q[X_1^{\pm 1}, \dots, X_r^{\pm 1}]$ of the monomials

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

This is a $\mathbb{F}_q$-vector space 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 any subset. The linear map that evaluates elements in $\mathbb{F}_q < U >$ at all the points in S is denoted by π_S:

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

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

The toric code is the image $C = \pi_S(\mathbb{F}_q < U >)$ and we obtain a the linear secret sharing scheme from C by the Massey construction.

Definition 3.1. Let $S \subseteq T(\mathbb{F}_q)$ be any subset so 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 2.1 and Definition 2.2.

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

3.1.1. *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 3.2. *Translation induces an isomorphism of vector spaces*

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

We have that

- *i) The evaluations 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 $v = (v_1, \dots, v_r)$ 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 $T(\mathbb{F}_q)$.*

The lemma and generalizations has been used in several articles classifying toric codes, e.g., [**18**].

An immediate consequence of *iii)* above is the following corollary, which also can be found in [**24**, Theorem 3.3].

Corollary 3.3. *Let $U \subseteq M$ be a subset and let*

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

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

3.1.2. *Orthogonality - dual code.* In Proposition 3.5 we present the dual code of $C = \pi_S(\mathbb{F}_q < U >)$.

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 isomorphism of vector spaces

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

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

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

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

Lemma 3.4. *Let $f, g \in \mathbb{F}_q < M >$ and assume $f \neq \hat{g}$, then*

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

Let

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

With this inner product we obtain the following proposition, e.g. [**4**, Proposition 3.5] and [**25**, Theorem 6].

Proposition 3.5. *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

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

i.e., the dual code of $C = \pi_{T(\mathbb{F}_q)}(\mathbb{F}_q < U >)$ is $\pi_{T(\mathbb{F}_q)}(\mathbb{F}_q < -H \setminus -U >)$.

Theorem 3.6. *Let $r(U)$ and $t(U)$ be the reconstruction and privacy thresholds of $\mathcal{M}(U)$ as defined in Definition 2.1.*

Then

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

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

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

Proof. The minimal distance of an evaluation code and the maximum number of zeros of a function add to the length of the code.

The bound for $r(U)$ is based on the minimum distance d of the code $C = \pi_{T(\mathbb{F}_q)}(\mathbb{F}_q < U >) \subseteq \mathbb{F}_q^{|T(\mathbb{F}_q)|}$, the bound for $t(U)$ is based on the on the minimum distance d' of the dual code $C' = \pi_{T(\mathbb{F}_q)}(\mathbb{F}_q < -H \setminus -U > \subseteq \mathbb{F}_q^{|T(\mathbb{F}_q)|}$, using Proposition 3.5 to represent the dual code as an evaluation code.

The codes have length $|T(\mathbb{F}_q)|$, hence,

$$\begin{aligned} r(U) \geq |T(\mathbb{F}_q)| - d + 2 &= (\text{the maximum number of zeros of zeros of } \ + 2\pi_{T(\mathbb{F}_q)}(f)) \\ t(U) \leq d' - 2 &= |T(\mathbb{F}_q)| - (\text{the maximum number of zeros of } \pi_{T(\mathbb{F}_q)}(g)) - 2 \ . \end{aligned}$$

The results follow from the construction of Massey [**22**, Section 4.1]. □

Of interest is to consider the *coset distance* that is greater than or equal to the minimum distance, which has been used in [**12**] to estimate the parameters of secret sharing schemes coming from Algebraic-Geometry codes.

Theorem 3.7. *Let $U \subseteq H \subset M$ and let $U + U = \{u_1 + u_2 | \ u_1, u_2 \in U\}$ be the Minkowski sum. Let*

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

The linear secret sharing schemes $\mathcal{M}(U)$ of Definition 3.1 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

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

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

$$\begin{aligned} \pi_B : \mathbb{F}_q < U + U > &\rightarrow \mathbb{F}_q^{|B|} &(3.1)\\ h &\mapsto (h(P))_{P \in B} &(3.2) \end{aligned}$$

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 cannot vanish identically 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. □

To determine the product of the secrets from the product of the shares amounts to decoding the linear code obtained as the image in (3.1).

4. Toric surfaces and linear secret sharing schemes with strong multiplication

Let $M \simeq \mathbb{Z}^2$ be a 2-dimensional lattice and assume that $U = M_{\mathbb{R}} \cap \square$ consists of the integral points of a 2-dimensional integral convex polytope $\square$ in $M_{\mathbb{R}} = M \otimes_{\mathbb{Z}} \mathbb{R}$. Let $N = \operatorname{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$ be the dual lattice with canonical $\mathbb{Z}$-bilinear pairing $< \ , \ >: M \times N \rightarrow \mathbb{Z}$.

The support function $h_\square : N_{\mathbb{R}} \rightarrow \mathbb{R}$ is defined as $h_\square(n) := \inf\{< m, n > | m \in \square\}$ and the polytope $\square$ can be reconstructed from the support function

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

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

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

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

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 $T_N := \operatorname{Hom}_{\mathbb{Z}}(M, k^*)$. The multiplicative character $\mathbf{e}(m)$ for $m \in M$ is the homomorphism

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

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

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

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

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

Define $V(\sigma)$ to be the closure of $\operatorname{orb}(\sigma)$ in $X_\Box$.

A Δ-linear support function h gives rise to a polytope $\Box$ and an associated Cartier divisor

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

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 4.1. *Let h be a Δ-linear support function with associated convex polytope $\Box$ and Cartier divisor $D_h = D_\Box$.*

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

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

as a basis.

For a Δ-linear support function h and a 1-dimensional cone $\rho \in \Delta(1)$ the intersection number $(D_h; V(\rho))$ between the Cartier divisor D_h of (4) and $V(\rho)) = \mathbb{P}^1$ is obtained in [**23**, 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 $n', n'' \in N$ so 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 4.2. *For any $l_\rho \in M$, such that h coincides with l_ρ on ρ, let $\overline{h} = h - l_\rho$. Then*

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

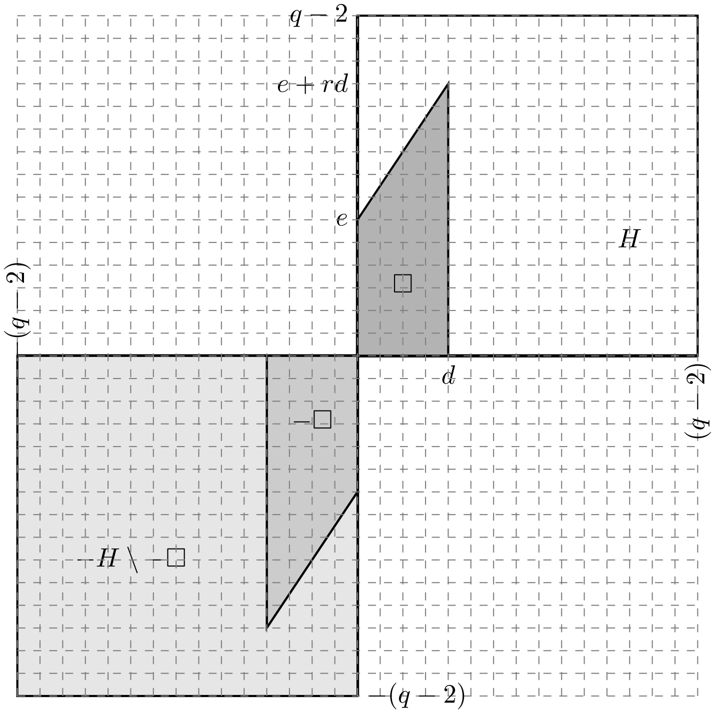
In the 2-dimensional non-singular case let $n(\rho)$ be a primitive generator for the 1-dimensional cone ρ. There exists an integer a such that

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

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

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

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 $\Box$ with vertices $(0,0),(d,0),(d,e+rd),(0,e)$ and their opposite convex polytopes $-H$ and $-\Box$. Also the (non-convex) polytope $-H \setminus -\Box$ is depicted.



4.1. Hirzebruch surfaces. Let d, e, r be positive integers and let $\Box$ 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.*

We obtain the following result as a consequence of Theorem 3.6 and the bounds obtained in [**16**] on the number of zeros of functions on such surfaces.

THEOREM 4.3. *Let $\Box$ be the polytope in $M_{\mathbb{R}}$ with vertices $(0,0),(d,0),(d,e+rd),(0,e)$. Assume that $d \leq q-2$, $e \leq q-2$ and that $e+rd \leq q-2$. Let $U = M \cap \Box$ be the lattice points in $\Box$.*

Let $\mathcal{M}(U)$ be the linear secret sharing schemes of Definition 3.1 with support *$T(\mathbb{F}_q)$ and $(q-1)^2-1$ players.*

Then the number of lattice points in $\Box$ is

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

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

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

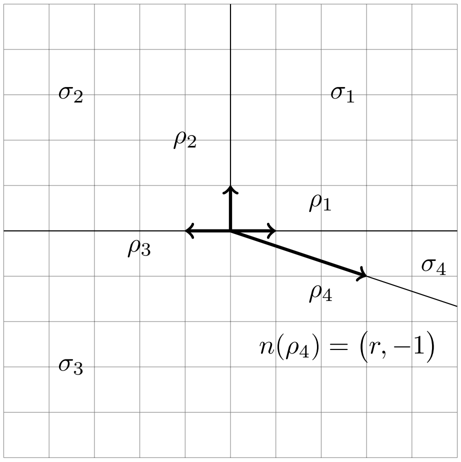


FIGURE 2. The normal fan and its 1-dimensional cones ρ_i, with primitive generators $n(\rho_i)$, and 2-dimensional cones σ_i for $i = 1, \dots, 4$ of the polytope $\square$ in Figure 1.

and the reconstruction threshold as defined in Definition 2.1 of $\mathcal{M}(U)$ *is*

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

REMARK 4.4. The polytope $-H \setminus -U$ is not convex, so our method using intersection theory does not determine the privacy threshold $t(U)$. It would be interesting to examine the methods and results of [**18**], [**29**], [**19**], [**24**], [**1**],[**20**] [**28**], and [**21**] for toric codes in this context.

4.2. 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.

Under these assumptions the polytopes $\square$, $-H \setminus -\square$ and $\square + \square$ are convex and we can use intersection theory on the associated toric surface to bound the number of zeros of functions and thresholds.

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 $i = 1, \dots, 4$, 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 $\Box$ is:

$$h_{\Box}\begin{pmatrix}n_1\\n_2\end{pmatrix}=\begin{cases}\begin{pmatrix}0\\0\end{pmatrix}\cdot\begin{pmatrix}n_1\\n_2\end{pmatrix} & \text{if } \begin{pmatrix}n_1\\n_2\end{pmatrix}\in\sigma_1,\\ \begin{pmatrix}a\\0\end{pmatrix}\cdot\begin{pmatrix}n_1\\n_2\end{pmatrix} & \text{if } \begin{pmatrix}n_1\\n_2\end{pmatrix}\in\sigma_2,\\ \begin{pmatrix}b\\q-2\end{pmatrix}\cdot\begin{pmatrix}n_1\\n_2\end{pmatrix} & \text{if } \begin{pmatrix}n_1\\n_2\end{pmatrix}\in\sigma_3,\\ \begin{pmatrix}0\\q-2\end{pmatrix}\cdot\begin{pmatrix}n_1\\n_2\end{pmatrix} & \text{if } \begin{pmatrix}n_1\\n_2\end{pmatrix}\in\sigma_4.\end{cases}\tag{4.1}$$

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 $\rho_i, \rho_j \in \Delta(1), i = 1, \dots, 4$, the intersection numbers $(V(\rho_i); V(\rho_j))$ are determined by the methods above, however, 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

$$(V(\rho_1); V(\rho_1)) = 0 \tag{4.2}$$

by the remark following Lemma 4.2.

Theorem 4.5. *Assume a, b are integers with $0 \leq b \leq a \leq q-2$.*

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

Let $\mathcal{M}(U)$ be the linear secret sharing schemes Definition 3.1 with support *$T(\mathbb{F}_q)$ and $n = (q-1)^2 - 1$ players.*

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 as defined in Definition 2.1 satisfies

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

iii) The privacy threshold as defined in Definition 2.1 satisfies

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

iv) Assume $2a \leq q-2$. The secret sharing scheme 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 $X_{\Box}$ 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 4.1.

On any of the other $q-1-c$ lines the number of zeroes of f is 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 4.2 using the observation that $(\mathbf{e}(m_1))_0 = V(\rho_1)$.

We get from (4.1) and (4.2) 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 3.6, 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 maximum number of zeros of $\pi_{T(\mathbb{F}_q)}(g)$ for $g \in \mathbb{F}_q < -H \setminus -U >$ is by Lemma 3.2 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 3.6.

To prove *iv)* assume $t \leq (q-2-2a)-1$ and $t \leq b-2$. We will use Theorem 3.7.

Consider the Minkowski sum $U + U$ and let $V = \overline{U+U}$ be its reduction modulo $q-1$ as in Corollary 3.3. 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 maksimum 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 (3.7) of Theorem 3.7 is at 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 $(0,q-2)$.

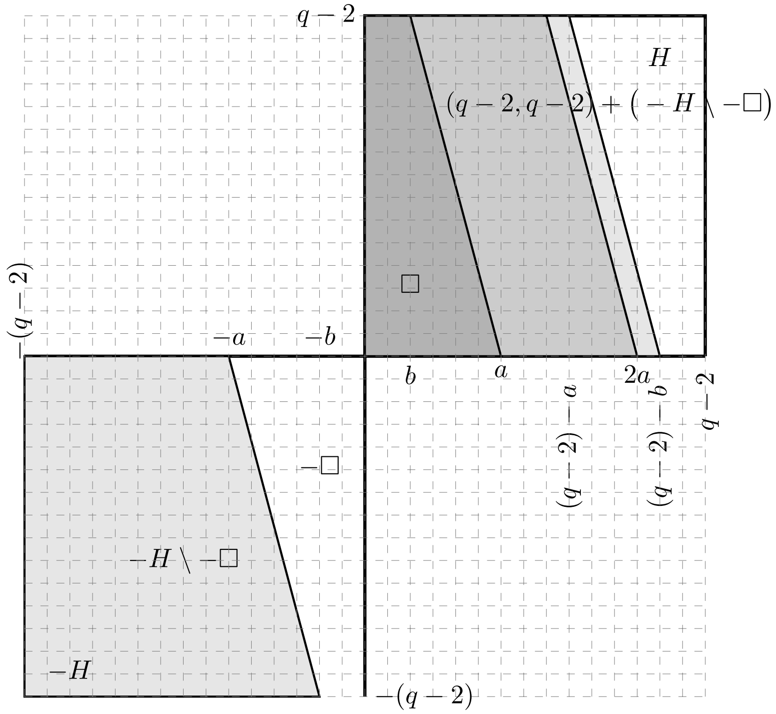
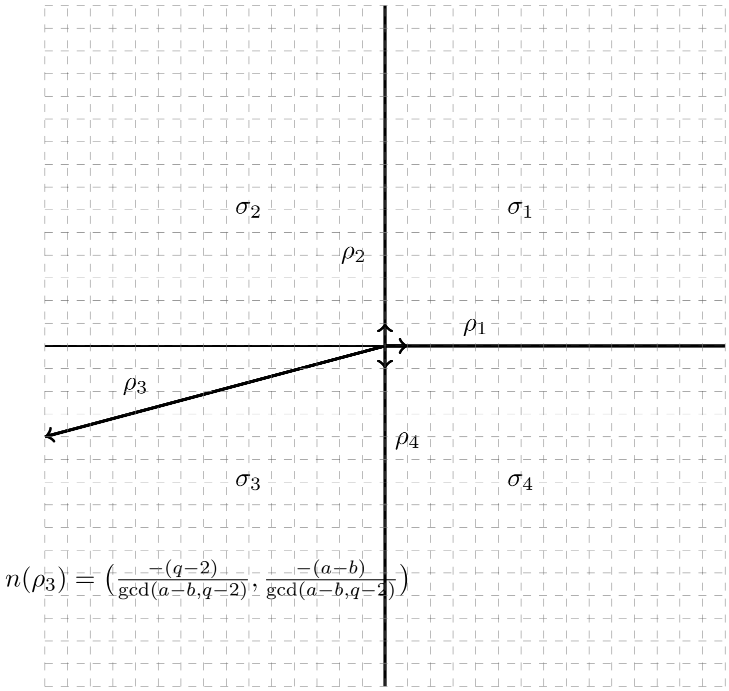


FIGURE 4. The normal fan and its 1-dimensional cones ρ_i, with primitive generators $n(\rho_i)$, and 2-dimensional cones σ_i for $i = 1, \dots, 4$ of the polytope $\square$ in Figure 3.


σ_2
σ_1
ρ_2
ρ_1
ρ_3
ρ_4
σ_3
σ_4
$n(\rho_3) = \left(\frac{-(q-2)}{\gcd(a-b,q-2)}, \frac{-(a-b)}{\gcd(a-b,q-2)}\right)$

References

1. Peter Beelen and Diego Ruano, *The order bound for toric codes*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (Maria Bras-Amors and Tom Høholdt, eds.), Lecture Notes in Computer Science, vol. 5527, Springer Berlin Heidelberg, 2009, pp. 1–10.
2. Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson, *Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract)*, in Simon [**27**], pp. 1–10.
3. G.R. Blakley, *Safeguarding cryptographic keys*, Proceedings of the 1979 AFIPS National Computer Conference (Monval, NJ, USA), AFIPS Press, 1979, pp. 313–317.
4. Maria Bras-Amorós and Michael E. O'Sullivan, *Duality for some families of correction capability optimized evaluation codes*, Adv. Math. Commun. **2** (2008), no. 1, 15–33. MR 2377234
5. I. Cascudo, *On Asymptotically Good Strongly Multiplicative Linear Secret Sharing*, Ph.D. thesis, University of Oviedo, 2010.
6. David Chaum, Claude Crépeau, and Ivan Damgård, *Multiparty unconditionally secure protocols (extended abstract)*, in Simon [**27**], pp. 11–19.
7. Hao Chen and Ronald Cramer, *Algebraic geometric secret sharing schemes and secure multiparty computations over small fields*, Advances in Cryptology - CRYPTO 2006 (Cynthia Dwork, ed.), Lecture Notes in Computer Science, vol. 4117, Springer Berlin Heidelberg, 2006, pp. 521–536.
8. Hao Chen, Ronald Cramer, Shafi Goldwasser, Robbert de Haan, and Vinod Vaikuntanathan, *Secure computation from random error correcting codes*, Advances in cryptology—EUROCRYPT 2007, Lecture Notes in Comput. Sci., vol. 4515, Springer, Berlin, 2007, pp. 291–310. MR 2449216
9. David A. Cox, John B. Little, and Henry K. Schenck, *Toric varieties*, Graduate Studies in Mathematics, vol. 124, American Mathematical Society, Providence, RI, 2011. MR 2810322

10. Ronald Cramer, Ivan Damgård, and Ueli Maurer, *General secure multi-party computation from any linear secret-sharing scheme*, Advances in Cryptology EUROCRYPT 2000 (Bart Preneel, ed.), Lecture Notes in Computer Science, vol. 1807, Springer Berlin Heidelberg, 2000, pp. 316–334 (English).
11. Ronald Cramer, Ivan Damgård, and Jesper Buus Nielsen, *Secure multiparty computation and secret sharing*, Cambridge University Press, 2015.
12. Iwan M. Duursma and Seungkook Park, *Coset bounds for algebraic geometric codes*, Finite Fields Appl. **16** (2010), no. 1, 36–55. MR 2588125
13. William Fulton, *Introduction to toric varieties*, Annals of mathematics studies, Princeton Univ. Press, Princeton, NJ, 1993.
14. Johan P. Hansen, *Toric surfaces and codes*, Information Theory Workshop, IEEE, 1998, pp. 42–43.
15. ———, *Toric surfaces and error-correcting codes*, Coding theory, cryptography and related areas (J. Buchmann, T. Hoeholdt, H. Stichtenoth, and H. Tapia-Recillas, eds.), Springer, 2000, pp. 132–142.
16. ———, *Toric varieties Hirzebruch surfaces and error-correcting codes*, Applicable Algebra in Engineering, Communication and Computing **13** (2002), no. 4, 289–300.
17. ———, *Quantum codes from toric surfaces*, I E E E Transactions on Information Theory **59** (2013), no. 2, 1188–1192.
18. John Little and Hal Schenck, *Toric surface codes and Minkowski sums*, SIAM J. Discrete Math. **20** (2006), no. 4, 999–1014 (electronic). MR 2272243
19. John Little and Ryan Schwarz, *On toric codes and multivariate Vandermonde matrices*, Appl. Algebra Engrg. Comm. Comput. **18** (2007), no. 4, 349–367.
20. John B. Little, *Remarks on generalized toric codes*, Finite Fields Appl. **24** (2013), 1–14. MR 3093852
21. John B. Little, *Toric codes and finite geometries*, arxiv **abs/1504.07494** (2015).
22. James L. Massey, *Some applications of code duality in cryptography*, Mat. Contemp. **21** (2001), 187–209, 16th School of Algebra, Part II (Portuguese) (Brasília, 2000). MR 2017562
23. Tadao Oda, *Convex bodies and algebraic geometry*, Springer, 1988 (eng).
24. Diego Ruano, *On the parameters of r-dimensional toric codes*, Finite Fields Appl. **13** (2007), no. 4, 962–976. MR 2360532
25. ———, *On the structure of generalized toric codes*, J. Symbolic Comput. **44** (2009), no. 5, 499–506. MR 2499927
26. Adi Shamir, *How to share a secret.*, Commun. ACM **22** (1979), no. 11, 612–613.
27. Janos Simon (ed.), *Proceedings of the 20th annual acm symposium on theory of computing, may 2-4, 1988, chicago, illinois, usa*, ACM, 1988.
28. Ivan Soprunov, *Lattice polytopes in coding theory*, J. Algebra Comb. Discrete Struct. Appl. **2** (2015), no. 2, 85–94. MR 3345095
29. Ivan Soprunov and Jenya Soprunova, *Toric surface codes and Minkowski length of polygons*, SIAM J. Discrete Math. **23** (2008/09), no. 1, 384–400. MR 2476837

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