On secret sharing with nonlinear product reconstruction

Ignacio Cascudo* Ronald Cramer† Diego Mirandola‡ Carles Padró §
Chaoping Xing¶

Abstract

Multiplicative linear secret sharing is a fundamental notion in the area of secure multi-party computation (MPC) and, since recently, in the area of two-party cryptography as well. In a nutshell, this notion guarantees that "the product of two secrets is obtained as a linear function of the vector consisting of the coordinate-wise product of two respective share-vectors". This paper focuses on the following foundational question, which is novel to the best of our knowledge. Suppose we *abandon the latter linearity condition* and instead require that this product is obtained by *some*, not-necessarily-linear "product reconstruction function". *Is the resulting notion equivalent to multiplicative linear secret sharing?* We show the (perhaps somewhat counter-intuitive) result that this relaxed notion is strictly *more general*. Concretely, fix a finite field $\mathbb{F}_q$ as the base field $\mathbb{F}_q$ over which linear secret sharing is considered. Then we show there exists an (exotic) linear secret sharing scheme with an unbounded number of players n such that it has t-privacy with $t \approx \sqrt{n}$ and such that it does admit a product reconstruction function, yet this function is *necessarily* nonlinear. Our proof is based on combinatorial arguments involving bilinear forms. It extends to similar separation results for important variations, such as strongly multiplicative secret sharing.
Keywords: (arithmetic) secret sharing.

1 Introduction

Multiplicative linear secret sharing is a fundamental notion in the area of secure multi-party computation (MPC). By extension, this holds in the area of two-party cryptography as well, by virtue of recently discovered deep applications of MPC to two-party cryptography as initiated in [8].

While linear secret sharing is additive in the sense that "the sum of share-vectors corresponds to the sum of the secrets", multiplicative linear secret sharing enjoys the further property that "the product of two secrets is obtained as a linear function of the vector consisting of the coordinate-wise product of two respective share-vectors". There are several important (more demanding) variations on this notion, such as strongly multiplicative secret sharing. First framed and studied in [6] in the late 1990s as an abstract property

*CWI Amsterdam, The Netherlands. Email: i.cascudo@cwi.nl.

†CWI Amsterdam & Mathematical Institute, Leiden University, The Netherlands. Email: cramer@cwi.nl, cramer@math.leidenuniv.nl.

‡CWI Amsterdam, The Netherlands. Email: diego@cwi.nl.

§Division of Mathematical Sciences, Nanyang Technological University, Singapore. Email: cpadro@ma4.upc.edu. This author's work was supported by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03.

¶Division of Mathematical Sciences, Nanyang Technological University, Singapore. Email: xingcp@ntu.edu.sg. This author's work was supported by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03

of a linear secret sharing scheme, [1] it had been implicit in several results since the mid 1980s (notably [1, 3, 7]) in the context of application of Shamir's secret sharing scheme [9] to (information-theoretically) secure multi-party computation. The *asymptotical* (constant-rate) theory of strongly multiplicative schemes has been initiated in [4], using algebraic geometry. [2] It has found several notable applications, starting with [8]. For a full discussion and references, please refer to [2].

This paper focuses on the following foundational question, which is novel to the best of our knowledge. Suppose we *abandon the latter linearity condition* and instead require that the product of the two secrets is obtained by application of *some*, *not-necessarily-linear* "product reconstruction function". *Is the resulting notion equivalent to multiplicative linear secret sharing?*

We show the (perhaps somewhat counter-intuitive) result that this relaxed notion is strictly *more general*. Concretely, fix a finite field $\mathbb{F}_q$ as the base field $\mathbb{F}_q$ over which linear secret sharing is considered. Then we show there exists an (exotic) linear secret sharing scheme with an unbounded number of players n such that it has t-privacy with $t \approx \sqrt{n}$ and such that it does admit a product reconstruction function, yet this function is *necessarily* nonlinear.

Our proof is based on combinatorial arguments involving bilinear forms. Our results extend to similar separation results for important variations, such as strongly multiplicative secret sharing. It is an interesting question whether there are applications of this "exotic", novel class of secret sharing schemes with nonlinear product reconstruction [3] to cryptographic protocols, but we will not offer any speculations here.

To give a flavor of our main result, we adopt the language of quadratic forms for the time being. Fix a finite field $\mathbb{F}_q$ as the base field $\mathbb{F}_q$ over which linear secret sharing is considered. Assume, for the moment, that its characteristic is different from 2. Let k be a positive integer. Choosing the standard basis on $\mathbb{F}_q^k$, there is a natural one-to-one correspondence between quadratic forms on $\mathbb{F}_q^k$ and the symmetric $k \times k$ matrices over $\mathbb{F}_q$. The rank of a quadratic form is equal to the rank of the corresponding symmetric matrix. Let's say that a set of elements $x_1, \ldots, x_m \in \mathbb{F}_q^k$ is *in general position* (i.g.p.) if the only quadratic form Q on $\mathbb{F}_q^k$ that satisfies $Q(x_1) = \ldots = Q(x_m) = 0$ is the nil-form, i.e., $Q \equiv 0$. Note that $m \geq k(k+1)/2$ (which is sharp). Suppose $k, n, \ell, \ell' \in \mathbb{Z}_{>0}$ and $\pi_0, \pi_1, \ldots, \pi_n \in \mathbb{F}_q^k$ are such that

- the Hamming-weight of each of $\pi_1, \ldots, \pi_n$ is at most ℓ, while the Hamming-weight of π_0 is at least ℓ'.
- $\pi_0, \pi_1, \ldots, \pi_n$ are i.g.p., whereas $\pi_1, \ldots, \pi_n$ are *not* i.g.p.
- the (unique) quadratic form Q on $\mathbb{F}_q^k$ such that $Q(\pi_1) = \ldots = Q(\pi_n) = 0$ and $Q(\pi_0) = 1$ has rank at least 5.

Then, as we show, there is an $\mathbb{F}_q$-linear secret sharing scheme Σ with t-privacy such that $t \approx \ell'/\ell$ and such that Σ does have product-reconstruction, yet it is necessarily nonlinear. Furthermore, we show that the conditions above can be satisfied, using combinatorial arguments. It turns out we can take $n = k(k+1)/2 - 1$, for infinitely many values of $k \in \mathbb{N}$. Moreover, ℓ can be taken as a (small) constant and ℓ' can be set to (almost) k. Hence, n

[1] It was shown, in particular, when and how a multiplicative scheme can be obtained from just a linear secret sharing scheme. However, this does not work for strong multiplicativity.

[2] Later, this asymptotical theory has also been developed in the case of *multiplicative* schemes using classical coding theory in [5]. The results there do not seem to carry over easily to strong multiplicative schemes.

[3] All applications of multiplicative linear secret sharing we are aware of, make essential use of linearity of product reconstruction.

is unbounded and $t = \Omega(\sqrt{n})$. We also give a generalized approach that may in principle lead to a better privacy-ratio. In the rest of the paper, we use the language of bilinear forms instead of quadratic forms as this easily facilitates a single, exact characterization of our problem over all finite fields and not just in characteristic different from 2.

This paper is organized as follows. In Section 2, we fix notations for linear algebra and state a few basic lemmas for reference later on. In Section 3, we review the standard definition of multiplicative linear secret sharing (see Definition 3.1). In Section 4, we formally define our relaxation of multiplicative linear secret sharing in Definition 4.1 and state our main separation result, i.e., the existence of the "exotic scheme", in Main Theorem 4.3.

In Section 5, we recall some elementary theory of bilinear forms. This is convenient in some of our proofs in Section 6, where we show that each of the multiplicativity notion and its relaxed notion of product reconstruction can be captured in terms of the existence of vectors and matrices with certain algebraic conditions imposed on them (see Theorems 6.1 and 6.3). In Theorem 6.7 we give sufficient separating conditions, phrased once again in the same language, implying that *only* the relaxed notion is satisfied.

Finally, in Section 7, we show by algebraic combinatorial means that the sufficient conditions from Theorem 6.7 can be satisfied by some linear secret sharing scheme with an unbounded number of players n and with t-privacy such that $t \approx \sqrt{n}$. That completes the proof of the separation result from Main Theorem 4.3. Our results hold for each finite field $\mathbb{F}_q$. The case where $\mathbb{F}_q$ has odd characteristic and $q \neq 3$ is treated in Proposition 7.1, while the characteristic 2 case is treated in Proposition 7.2 and the case $q = 3$ in Proposition 7.3. In Section 8, we argue how our results extend to strongly multiplicative secret sharing and state a generalization of our separation strategy.

2 Preliminaries

Throughout this paper, let p, m, n, k be positive integers with p prime.

We fix notations for linear algebra and state a few basic lemmas for reference later on. Let $\mathbb{F}_q$ denote the finite field of cardinality $q = p^m$. The prime number p is the *characteristic* of $\mathbb{F}_q$. If $S \subset \mathbb{F}_q^k$ is a non-empty set, then $\mathbb{F}_q\langle S\rangle$ denotes the $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^k$ generated by the elements of S. The *dual space* $(\mathbb{F}_q^k)^*$ is the $\mathbb{F}_q$-vector space consisting of all $\mathbb{F}_q$-linear maps $\phi : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q$ (the space of linear forms). It is isomorphic to $\mathbb{F}_q^k$. An isomorphism from $\mathbb{F}_q^k$ onto $(\mathbb{F}_q^k)^*$ is given by the map $a \mapsto a^*$, where a^* denotes the $\mathbb{F}_q$-linear form $a^* : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q\ ,\ x \mapsto \langle a, x\rangle$. Here, $\langle\cdot,\cdot\rangle$ denotes the standard inner-product on $\mathbb{F}_q^k$.

For reference later on, we include the following trivial lemma.

Lemma 2.1. *Let $V \subset \mathbb{F}_q^k$ be an $\mathbb{F}_q$-linear subspace and let $x \in \mathbb{F}_q^k$. Then $x \notin V$ if and only if there is an $\mathbb{F}_q$-linear form $a^* : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q$ such that a^* vanishes on V (i.e., a^* is identically 0 on V) but $a^*(x) = 1$.*

Finally, the set of $k \times k$ matrices over $\mathbb{F}_q$ is denoted by $\mathbb{F}_q^{k\times k}$, which we will view as an $\mathbb{F}_q$-vector space in the natural way (i.e., via matrix-addition). In expressions involving matrices and vectors, $x \in \mathbb{F}_q^k$ is represented as a column-vector and x^t is its transpose. A matrix $B \in \mathbb{F}_q^{k\times k}$ is *symmetric* if $B = B^t$ and it is *anti-symmetric* if $B = -B^t$.

Definition 2.2 (Tensor Product). *Let $v = (v_1, \ldots, v_k) \in \mathbb{F}_q^k$ and let $w = (w_1, \ldots, w_k) \in \mathbb{F}_q^k$. The* tensor product *of v and w is the matrix $v \otimes w \in \mathbb{F}_q^{k\times k}$, i.e., the $k \times k$-matrix with $v_j \cdot w_i$ in the entry (i, j).*

Note that $v \otimes v$ is a symmetric matrix, for each $v \in \mathbb{F}_q^k$.

In some of our proofs in Section 6, we will need the following well-known characterization of the rank of a square matrix in terms of the tensor product.

LEMMA 2.3. *Let $M \in \mathbb{F}_q^{k\times k}$. Then the rank* $\operatorname{rk} M$ *of the matrix M equals the minimum integer $\ell_0 \geq 0$ such that there exist $v^{(1)}, \ldots, v^{(\ell_0)}, w^{(1)}, \ldots, w^{(\ell_0)} \in \mathbb{F}_q^k$ with $M = \sum_{i=1}^{\ell_0} v^{(i)} \otimes w^{(i)}$.*

PROOF. If $M = 0$, the claim holds by the convention that the "empty sum" equals 0. Now suppose $M \neq 0$. Let $S = \{v^{(1)}, \ldots, v^{(\ell)}\}$ be a basis for the column space of M. Then each column of M can be expressed as a linear combination of the elements in S. Collecting, for each $v^{(i)}$, its contributions along these k columns in a vector $w^{(i)} \in \mathbb{F}_q^k$, this gives $M = \sum_{i=1}^{\ell} v^{(i)} \otimes w^{(i)}$. Hence, ℓ_0 is well-defined and it follows that $\ell_0 \leq \operatorname{rk} M$. To show that $\ell_0 \geq \operatorname{rk} M$, note that, if $M = \sum_{i=1}^{\ell} v^{(i)} \otimes w^{(i)}$ with $v^{(1)}, \ldots, v^{(\ell)}, w^{(1)}, \ldots, w^{(\ell)} \in \mathbb{F}_q^k$, then the column space of M is contained in the space generated by $\{v^{(1)}, \ldots, v^{(\ell)}\}$. △

3 Multiplicative Linear Secret Sharing

For the purposes of this paper, a *linear secret sharing scheme* Σ over $\mathbb{F}_q$ is a tuple $(n, k, (\pi_i)_{i=0}^n)$ such that

- $\pi_0 \in \mathbb{F}_q^k \setminus \{0\}$ and $\pi_1, \ldots, \pi_n \in \mathbb{F}_q^k$.
- $\pi_0 \in \mathbb{F}_q\langle\{\pi_i\}_{i=1}^n\rangle$.

The set $\{1, \ldots, n\}$ is the *player set*. Let $A \subset \{1, \ldots, n\}$ be a non-empty set. If $\pi_0 \in \mathbb{F}_q\langle\{\pi_i\}_{i\in A}\rangle$, then A is *accepting*. Otherwise, A is *rejecting*. By default, the empty set is rejecting. From the definitions, it follows that the player set is accepting.

Let $s \in \mathbb{F}_q$, the *secret*. Select $x \in \mathbb{F}_q^k$ uniformly at random such that $\pi_0^*(x) = s$. This is possible since $\pi_0 \neq 0$. The elements $\pi_1^*(x), \ldots, \pi_n^*(x)$ are the *shares*. The *joint shares of A* corresponds to the vector $(\pi_i^*(x))_{i\in A} \in \mathbb{F}_q^{|A|}$.

If A is accepting, then there is an $\mathbb{F}_q$-linear form

$$\rho^A : \mathbb{F}_q^{|A|} \longrightarrow \mathbb{F}_q,$$

the *(linear) reconstruction function for A*, such that

$$\rho^A((\pi_i^*(x))_{i\in A}) = \pi_0^*(x) = s,$$

for all $x \in \mathbb{F}_q^k$. In other words, "if A is accepting, the secret can be reconstructed (linearly) from the joint shares of A."

Suppose A is non-empty and rejecting and consider the random variable $(\pi_i^*(x))_{i\in A}$. Then this random variable does not depend on the choice of secret s. To prove this claim, the key observation is that $\pi_0 \notin \mathbb{F}_q\langle\{\pi_i\}_{i\in A}\rangle$ if and only if there exists $z \in \mathbb{F}_q^k$ (where z may depend on A) such that $\pi_0^*(z) = 1$ and $\pi_i^*(z) = 0$ for all $i \in A$, which follows by direct application of Lemma 2.1. Indeed, let $s' \in \mathbb{F}_q$ be an arbitrary secret and write $\lambda = s' - s$. Then the distribution of $x + \lambda z$ equals that of x, it holds that $\pi_0^*(x + \lambda z) = s + \lambda = s'$, and $(\pi_i^*(x + \lambda z))_{i\in A} = (\pi_i^*(x) + \lambda\pi_i^*(z))_{i\in A} = (\pi_i^*(x))_{i\in A}$.

The *access structure* $\Gamma(\Sigma)$ of the scheme collects the accepting sets, whereas the *adversary structure* $\mathcal{A}(\Sigma)$ collects the rejecting sets. Let t, r be integers with $0 \leq t < r \leq n$. The scheme has *r-reconstruction* if $\Gamma(\Sigma)$ contains all subsets of $\{1, \ldots, n\}$ of cardinality at least r and it has *t-privacy* if $\mathcal{A}(\Sigma)$ contains all subsets of $\{1, \ldots, n\}$ of cardinality at most t. By definition, the scheme is n-reconstructing. Of course, it could be r-reconstructing as well, for some $r < n$. Note that the definition of linear secret sharing does not guarantee any privacy.

Although any interesting schemes do in fact offer privacy, it is convenient not to include this as a requirement in the definition here.

Note that we will not consider any of the more general definitions of linear secret sharing from the literature in this paper, such as those allowing the secrets (and/or the shares) to be vectors rather than single field elements. In the Section 8, we will discuss extensions to strongly multiplicative linear secret sharing [6, 4].

DEFINITION 3.1 (Multiplicative linear secret sharing [6]). *Let* $\Sigma = (n, k, (\pi_i)_{i=0}^n)$ *be an LSSS over* $\mathbb{F}_q$. *It is* multiplicative (M1) *if there is an* $\mathbb{F}_q$*-linear form* $\rho : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$ *such that, for all* $x, y \in \mathbb{F}_q^k$,

$$\rho(z_1, \ldots, z_n) = \pi_0^*(x) \cdot \pi_0^*(y),$$

where

$$(z_1, \ldots, z_n) = (\pi_1^*(x) \cdot \pi_1^*(y), \ \ldots \ , \pi_n^*(x) \cdot \pi_n^*(y)).$$

In other words, "the product of two secrets is obtained as a *linear* function of the vector consisting of the coordinate-wise product of two respective share-vectors". This is a special property that is not generally satisfied by linear secret sharing schemes. Please refer to [6, 5] for more information about constructions and bounds.

4 Our contributions

The focus in this paper is on the following theoretical question, which is novel to the best of our knowledge. Consider multiplicative linear secret sharing, where "the product of two secrets is obtained as a *linear* function of the vector consisting of the coordinate-wise product of two respective share-vectors". Suppose we abandon the linearity condition and instead make the relaxed requirement that this product is obtained by *some*, not-necessarily-linear function. *Is the resulting notion equivalent to multiplicative linear secret sharing?* We show the (perhaps somewhat counter-intuitive) result that this relaxed notion is strictly *more general*.

DEFINITION 4.1 (Relaxation of Multiplicative Secret Sharing). *Let* $\Sigma = (n, k, (\pi_i)_{i=0}^n)$ *be an LSSS over* $\mathbb{F}_q$. *The scheme has* product reconstruction (M2) *if, for all* $x, x', y, y' \in \mathbb{F}_q^k$ *with*

$$\pi_1^*(x)\pi_1^*(y) = \pi_1^*(x')\pi_1^*(y'), \ \ldots, \ \pi_n^*(x)\pi_n^*(y) = \pi_n^*(x')\pi_n^*(y'),$$

it holds that

$$\pi_0^*(x)\pi_0^*(y) = \pi_0^*(x')\pi_0^*(y').$$

Note that the product reconstruction condition is equivalent to the existence of a product reconstruction *function* $\rho' : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$ such that

$$\rho'(\pi_1^*(x) \cdot \pi_1^*(y), \ldots, \pi_n^*(x) \cdot \pi_n^*(y)) = \pi_0^*(x) \cdot \pi_0^*(y),$$

for all $x, y \in \mathbb{F}_q^k$. In particular, a multiplicative linear secret sharing scheme (see Definition 3.1) is one for which an $\mathbb{F}_q$*-linear* product reconstruction function exists. Thus, the M1 condition implies the M2 condition.

REMARK 4.2. *There does not appear to be much that one can say, a priori, about the complexity of such not-necessarily-linear product reconstruction functions. At best, one can say that in order to determine the product of two secrets from the coordinate-wise product of two corresponding share-vectors, it suffices to solve a system of quadratic equations.*

MAIN THEOREM 4.3. *Let $\mathbb{F}_q$ be the finite field of q elements. There exists a function $t_q(n) \in \Omega(\sqrt{n})$ such that for infinitely many values of $n \in \mathbb{N}$, there exists a linear secret sharing scheme $\Sigma = (n, k, (\pi_i)_{i=0}^n)$ over $\mathbb{F}_q$ such that it has $t_q(n)$-privacy and such that it admits a product reconstruction function (M2). However, such function is necessarily not $\mathbb{F}_q$-linear. Therefore, it is not a multiplicative linear secret sharing scheme (i.e., not M1).*

Extension to *strongly* multiplicative linear secret sharing (where the M1 property is required for certain proper subsets of the player set as well), is discussed in Section 8.

5 Some theory of bilinear forms

We recall some elementary theory of bilinear forms. It is only used in the *proofs* of the theorems in Section 6. The statements of those theorems do *not* depend on it.

5.1 Definitions and basic properties

DEFINITION 5.1 (Bilinear Forms). *A* bilinear form *on $\mathbb{F}_q^k$ is a map $B : \mathbb{F}_q^k \times \mathbb{F}_q^k \to \mathbb{F}_q$ such that, for all $x, y, z \in \mathbb{F}_q^k$, $\lambda \in \mathbb{F}_q$, the following holds.*

- $B(x + y, z) = B(x, z) + B(y, z)$.
- $B(x, y + z) = B(x, y) + B(x, z)$.
- $B(\lambda x, y) = B(x, \lambda y) = \lambda B(x, y)$.

The $\mathbb{F}_q$-vector space consisting of all bilinear forms on $\mathbb{F}_q^k$ is denoted by $\mathrm{Bil}(\mathbb{F}_q^k)$.

DEFINITION 5.2. *For a bilinear form $B \in \mathrm{Bil}(\mathbb{F}_q^k)$, the bilinear form $B^t \in \mathrm{Bil}(\mathbb{F}_q^k)$ is given by $B^t(x, y) := B(y, x)$ for all $x, y \in \mathbb{F}_q^k$.*

DEFINITION 5.3. *Let $B \in \mathrm{Bil}(\mathbb{F}_q^k)$. Then:*

a) B is symmetric if $B = B^t$;

b) B is alternating if $B(x, x) = 0$, for all $x \in \mathbb{F}_q^k$.

The $\mathbb{F}_q$-vector space consisting of all symmetric (resp. alternating) bilinear forms on $\mathbb{F}_q^k$ is denoted $\mathrm{Sym}(\mathbb{F}_q^k)$ *(resp.* $\mathrm{Alt}(\mathbb{F}_q^k)$*).*

LEMMA 5.4. *For all $B \in \mathrm{Alt}(\mathbb{F}_q^k)$, it holds that $B = -B^t$. If the characteristic is different from 2, the converse also holds.*

PROOF. For all $x, y \in \mathbb{F}_q^k$, it holds that $B(x + y, x + y) = B(x, x) + B(x, y) + B(y, x) + B(y, y)$. Since $B(x, x) = B(y, y) = B(x + y, x + y) = 0$, it follows that $B(x, y) = -B(y, x)$. On the other hand, if $B = -B^t$, then $B(x, x) = -B(x, x)$ for all $x \in \mathbb{F}_q^k$. This implies $B(x, x) = 0$ for all $x \in \mathbb{F}_q^k$ if the characteristic is different from 2. △

REMARK 5.5 (Matrix Correspondence). *Bilinear forms correspond 1-1 with matrices, as follows. A bilinear form $B \in \mathrm{Bil}(\mathbb{F}_q^k)$ corresponds to the matrix $B \in \mathbb{F}_q^{k \times k}$ such that $B(x, y) = x^t B y$, for all $x, y \in \mathbb{F}_q^k$. The* rank *of a bilinear form is the rank of the matrix corresponding to it. We use this correspondence without explicit reference.*

REMARK 5.6. *The rank of a bilinear form $B \in \mathrm{Bil}(\mathbb{F}_q^k)$ is equal to the rank of the linear map $B_1 : \mathbb{F}_q^k \to (\mathbb{F}_q^k)^*$, where, for every $x \in \mathbb{F}_q^k$, the linear form $B_1(x)$ is defined by $B_1(x)(y) = B(x, y)$.*

REMARK 5.7. *For each $\pi, \sigma \in \mathbb{F}_q^k$, the bilinear form on $\mathbb{F}_q^k$ defined by $(x, y) \mapsto \pi^*(x) \cdot \sigma^*(y)$ corresponds to the matrix $\pi \otimes \sigma$.*

Using this correspondence, the bilinear form B^t is identified with the transposed matrix of B. Therefore, symmetric bilinear forms correspond to symmetric matrices. According to the Lemma 5.4, in characteristic different from 2, the alternating forms B correspond 1-1 to the anti-symmetric matrices. Now consider the case of characteristic 2. Since symmetric and anti-symmetric matrices coincide in that case, the lemma then only gives the necessary condition that the matrix of an alternating form is symmetric. However, it can be verified that, in characteristic 2, a necessary and sufficient condition is that the matrix is symmetric *and* its main diagonal consists entirely of zeros. Now note that, in characteristic different from 2, all anti-symmetric matrices have their main diagonal consisting entirely of zeros. Therefore, regardless of characteristic, the alternating forms correspond 1-1 to the anti-symmetric matrices whose main diagonal consists entirely of zeros.

5.2 Connection with linear forms on the space of symmetric tensors

In some of our proofs in Section 6 we will consider bilinear forms B on $\mathbb{F}_q^k$ as functions on the diagonal of $\mathbb{F}_q^k \times \mathbb{F}_q^k$, i.e., the subspace consisting of the elements $(\pi, \pi) \in \mathbb{F}_q^k \times \mathbb{F}_q^k$. We will need the following observations.

First note that the bilinear forms B, B' agree on the diagonal of $\mathbb{F}_q^k \times \mathbb{F}_q^k$ if and only if $B - B' \in \mathrm{Alt}(\mathbb{F}_q^k)$. Hence, given just its evaluations on the diagonal, the bilinear form is uniquely determined up to an additive alternating factor. Equivalently, the space of bilinear form evaluations on the diagonal is isomorphic to the quotient $\mathrm{Bil}(\mathbb{F}_q^k)/\mathrm{Alt}(\mathbb{F}_q^k)$.

There is, in fact, an even stronger interpretation of the latter quotient. By multi-linear algebra (precisely, universality of tensor product), it holds that the linear forms on *the space of symmetric tensors on* $\mathbb{F}_q^k$ correspond 1-1 to the bilinear forms on $\mathbb{F}_q^k$, taken modulo the alternating forms.

DEFINITION 5.8 (Space of Symmetric Tensors). *The $\mathbb{F}_q$-vector space $S^2(\mathbb{F}_q^k) \subseteq \mathbb{F}_q^{k \times k}$ is the $\mathbb{F}_q$-linear span of the set of matrices $\{v \otimes v : v \in \mathbb{F}_q^k\}$.*

REMARK 5.9. *$S^2(\mathbb{F}_q^k)$ corresponds 1-1 with the symmetric matrices in $\mathbb{F}_q^{k \times k}$. So its dimension is $\frac{k(k+1)}{2}$. Since $S^2(\mathbb{F}_q^k)$ is generated by terms of the form $v \otimes v$, there is a basis consisting exclusively of such terms. This is immediate if $k = 1$. If $k > 1$, consider the following example. If $e_1, \ldots, e_k \in \mathbb{F}_q^k$ is a basis of $\mathbb{F}_q^k$, then the terms $e_i \otimes e_i$, $(e_i + e_j) \otimes (e_i + e_j)$ with $1 \leq i < j \leq k$ constitute a basis of $S^2(\mathbb{F}_q^k)$.*

Concretely, for each linear form $\phi : \mathrm{S}^2(\mathbb{F}_q^k) \longrightarrow \mathbb{F}_q$, there is a bilinear form B on $\mathbb{F}_q^k$, unique up to an additive alternating factor, such that $\phi(x \otimes x) = B(x, x)$ for all $x \in \mathbb{F}_q^k$. In the other direction, a bilinear form B on $\mathbb{F}_q^k$ determines a unique linear form ϕ on $\mathrm{S}^2(\mathbb{F}_q^k)$ with $\phi(x \otimes x) = B(x, x)$ for all $x \in \mathbb{F}_q^k$. We will use this to turn certain bilinear problems into linear ones. Formally, let $(\mathrm{S}^2(\mathbb{F}_q^k))^*$ denote the space of linear forms $\phi : \mathrm{S}^2(\mathbb{F}_q^k) \longrightarrow \mathbb{F}_q$. Then this result can be formally stated as follows.

THEOREM 5.10. *As $\mathbb{F}_q$-vector spaces, $\mathrm{Bil}(\mathbb{F}_q^k)/\mathrm{Alt}(\mathbb{F}_q^k) \backsimeq (\mathrm{S}^2(\mathbb{F}_q^k))^*$. An isomorphism is given by the assignment $B + \mathrm{Alt}(\mathbb{F}_q^k) \mapsto \phi_B$, where ϕ_B is the unique linear form on $\mathrm{S}^2(\mathbb{F}_q^k)$ such that $\phi_B(x \otimes x) = B(x, x)$ for all $x \in \mathbb{F}_q^k$.*

6 Characterizations and separation conditions

Throughout this section, let $\mathbb{F}_q$ be a finite field and let $\Sigma = (n, k, (\pi_i)_{i=0}^n)$ be an LSSS over $\mathbb{F}_q$.

In this section we characterize properties M1 and M2, or rather, their negations, separately. In addition, we present convenient sufficient conditions for an LSSS to be M2 but not M1.

THEOREM 6.1 (Not-M1 Characterization). *Σ is not M1 if and only if there exists a matrix $T \in \mathbb{F}_q^{k\times k}$ such that $\pi_1^t T \pi_1 = \cdots = \pi_n^t T \pi_n = 0$ and $\pi_0^t T \pi_0 = 1$.*

PROOF. By Definition 3.1, Σ is M1 if and only if there exist $\lambda_1, \ldots, \lambda_n \in \mathbb{F}_q$ such that $\pi_0^*(x)\pi_0^*(y) - \sum_{i=1}^n \lambda_i \pi_i^*(x)\pi_i^*(y) = 0$, for all $x, y \in \mathbb{F}_q^k$. Setting

$$M = \pi_0 \otimes \pi_0 - \sum_{i=1}^n \lambda_i \pi_i \otimes \pi_i,$$

it follows by Remark 5.7 that $x^t M y = 0$ for all $x, y \in \mathbb{F}_q^k$, or, equivalently, $M = 0$. Thus, Σ is not M1 if and only if

$$\pi_0 \otimes \pi_0 \notin \mathbb{F}_q\langle \pi_1 \otimes \pi_1, \ldots, \pi_n \otimes \pi_n \rangle.$$

By Lemma 2.1, the latter condition holds if and only if there is a linear form

$$\phi : \mathrm{S}^2(\mathbb{F}_q^k) \to \mathbb{F}_q$$

with

$$\phi(\pi_1 \otimes \pi_1) = \cdots = \phi(\pi_n \otimes \pi_n) = 0 \quad \text{and} \quad \phi(\pi_0 \otimes \pi_0) = 1.$$

By Theorem 5.10, the latter condition is equivalent to the existence of a bilinear form T on $\mathbb{F}_q^k$ (unique up to an additive alternating term; but that does not matter here) such that $\phi = \phi_T$. Phrased in terms of the matrix correspondence, this means that

$$\phi_T(\pi_1 \otimes \pi_1) = \pi_1^t T \pi_1 = 0, \ldots, \phi_T(\pi_n \otimes \pi_n) = \pi_n^t T \pi_n = 0 \quad \text{and} \quad \phi_T(\pi_0 \otimes \pi_0) = \pi_0^t T \pi_0 = 1.$$

This concludes the proof. △

REMARK 6.2. *Equivalently, Σ is not M1 if and only if there is a linear form ϕ on $S^2(\mathbb{F}_q^k)$ such that $\phi(\pi_1 \otimes \pi_1) = \cdots = \phi(\pi_n \otimes \pi_n) = 0$ and $\phi(\pi_0 \otimes \pi_0) = 1$.*

THEOREM 6.3 (Not-M2 Characterization). *Σ is not M2 if and only if there exists a matrix $B \in \mathbb{F}_q^{k\times k}$ such that $\pi_1^t B \pi_1 = \cdots = \pi_n^t B \pi_n = 0$, $\pi_0^t B \pi_0 = 1$, and $\mathrm{rk}(B) \le 2$.*

PROOF. From the definitions, it follows that Σ is not M2 if and only if there exist $x, y, x', y' \in \mathbb{F}_q^k$ with

$$\pi_1^*(x)\pi_1^*(y) - \pi_1^*(x')\pi_1^*(y') = \cdots = \pi_n^*(x)\pi_n^*(y) - \pi_n^*(x')\pi_n^*(y') = 0$$

and

$$\pi_0^*(x)\pi_0^*(y) - \pi_0^*(x')\pi_0^*(y') = 1.$$

Define the matrix

$$B_{x,y,x',y'} = x \otimes y - x' \otimes y' \in \mathbb{F}_q^{k\times k}.$$

Equivalently, Σ is not M2 if and only if there exist $x, y, x', y' \in \mathbb{F}_q^k$ such that

$$\pi_1^t(B_{x,y,x',y'})\pi_1 = 0, \ldots, \pi_n^t(B_{x,y,x',y'})\pi_n = 0 \quad , \quad \pi_0^t(B_{x,y,x',y'})\pi_0 = 1.$$

By Lemma 2.3, the matrices of the form $B_{x,y,x',y'}$ for some $x, y, x', y' \in \mathbb{F}_q^k$ are exactly the matrices of rank at most 2. This concludes the proof. △

REMARK 6.4. *Equivalently, Σ is not M2 if and only if there is a linear form ϕ on $S^2(\mathbb{F}_q^k)$ and a matrix $B \in \mathbb{F}_q^{k\times k}$ such that $\phi(\pi_1 \otimes \pi_1) = \cdots = \phi(\pi_n \otimes \pi_n) = 0$, $\phi(\pi_0 \otimes \pi_0) = 1$, $\phi = \phi_B$, and $\mathrm{rk}(B) \leq 2$.*

The combination of Theorems 6.1 and 6.3 gives rise to a characterization of linear secret sharing schemes that are M2 but not M1. Towards demonstrating the existence of such schemes, we give convenient *sufficient* conditions in Theorems 6.7 and 6.10 below. Before proceeding, we give a definition and a lemma that are useful in the proofs of those theorems.

DEFINITION 6.5. *Let ϕ be a linear form on $S^2(\mathbb{F}_q^k)$. Let $T \in \mathbb{F}_q^{k\times k}$ be an arbitrary matrix such that $\phi = \phi_T$, i.e., the linear form defined by T agrees with ϕ. Then $\sigma(\phi) := \mathrm{rk}(T + T^t)$.*

LEMMA 6.6. *Let ϕ be a linear form on $S^2(\mathbb{F}_q^k)$. Suppose $T, B \in \mathbb{F}_q^{k\times k}$ satisfy $\phi = \phi_T = \phi_B$, i.e., the linear forms defined by T, resp. B, agree with ϕ. Then:*

1. *$B + B^t = T + T^t$. Therefore, $\sigma(\phi)$ is well-defined.*
2. *$\mathrm{rk}(T), \mathrm{rk}(B) \geq \sigma(\phi)/2$.*

PROOF. If $\phi_T = \phi_B$, then $B = T + A$ for some $A \in \mathbb{F}_q^{k\times k}$ corresponding to an alternating form, by Theorem 5.10. Moreover, $B + B^t = (T + T^t) + (A + A^t) = (T + T^t)$, where the equality on the right follows by Lemma 5.4. Finally, $2 \cdot \mathrm{rk}(B) \geq \mathrm{rk}(B + B^t) = \mathrm{rk}(T + T^t)$, where the inequality on the left is a direct consequence of Lemma 2.3. △

THEOREM 6.7 (Sufficient Separation Conditions). *Suppose Σ satisfies the following conditions.*

1. *The $\mathbb{F}_q$-span of the set $\{\pi_0 \otimes \pi_0, \pi_1 \otimes \pi_1, \ldots, \pi_n \otimes \pi_n\}$ is all of $S^2(\mathbb{F}_q^k)$. In particular, $n \geq \frac{k(k+1)}{2} - 1 = \dim S^2(\mathbb{F}_q^k) - 1$.*
2. *The $\mathbb{F}_q$-span H of the set $\{\pi_1 \otimes \pi_1, \ldots, \pi_n \otimes \pi_n\}$ is a hyperplane in $S^2(\mathbb{F}_q^k)$, i.e., H is a subspace of dimension $\frac{k(k+1)}{2} - 1$.*
3. *There is a matrix $T \in \mathbb{F}_q^{k\times k}$ such that*
   (a) *$\pi_1^t T \pi_1 = \cdots = \pi_n^t T \pi_n = 0$*
   (b) *$\pi_0^t T \pi_0 = 1$*
   (c) *$\mathrm{rk}(T + T^t) \geq 5$*

Then Σ has product reconstruction (is M2) but Σ does not have linear product reconstruction (is not M1).

PROOF. The conditions of Theorem 6.1 are satisfied, so Σ is not M1. The combination of conditions 1 and 2 implies the existence of a unique linear form ϕ on $S^2(\mathbb{F}_q^k)$ such that $\phi(\pi_1 \otimes \pi_1) = \cdots = \phi(\pi_n \otimes \pi_n) = 0$ and $\phi(\pi_0 \otimes \pi_0) = 1$.

Assume, towards a contradiction, that Σ is not M2. Let $B \in \mathbb{F}_q^{k\times k}$ be as in Remark 6.4. Note that it holds that $\phi = \phi_B$ and $\mathrm{rk}(B) \leq 2$. By Lemma 6.6, it follows that $\sigma(\phi) \leq 4$. However, by the conditions 3a, 3b, 3c on T, $\phi = \phi_T$ and $\sigma(\phi) \geq 5$. This is a contradiction. Hence, the assumption is false and Σ is M2. △

The following is a cautionary remark when trying to satisfy the conditions of Theorem 6.7; it shows that the situation is "tighter" than it may appear at first sight.

REMARK 6.8. *Fix some $\pi_0, \pi_1, \ldots, \pi_n \in \mathbb{F}_q^k$. Assume these satisfy conditions 1 and 2. There exist* many *T's satisfying conditions 3a and 3b. However, this abundance doesn't give any leverage to satisfy condition 3c, once all π_i's are fixed. Indeed, the rank value in condition 3c corresponds to $\sigma(\phi)$, where ϕ is the unique linear form determined by conditions 1,2,3a,3b.*

We include the following straightforward remark for reference later on.

REMARK 6.9. *Fix some $\pi_0, \pi_1, \ldots, \pi_n \in \mathbb{F}_q^k$. Assume $\{\pi_1 \otimes \pi_1, \ldots, \pi_n \otimes \pi_n\}$ spans a hyperplane H and $T \in \mathbb{F}_q^{k \times k}$ satisfies $\pi_1^t T \pi_1 = \cdots = \pi_n^t T \pi_n = 0$ and $\pi_0^t T \pi_0 = 1$. Then $\{\pi_0 \otimes \pi_0, \pi_1 \otimes \pi_1, \ldots, \pi_n \otimes \pi_n\}$ spans $S^2(\mathbb{F}_q^k)$.*

This is argued as follows. It is sufficient to show that $\pi_0 \otimes \pi_0 \notin H$. To this end, we view T as a linear form ϕ_T on $S^2(\mathbb{F}_q^k)$. Towards a contradiction, suppose $\pi_0 \otimes \pi_0 \in H$. Then $\phi_T(\pi_0 \otimes \pi_0) = 0$, since ϕ_T vanishes on H. But $\phi_T(\pi_0 \otimes \pi_0) = 1$ by assumption, a contradiction.

When the characteristic of $\mathbb{F}_q$ is different from 2, we have the following sufficient conditions as well.

THEOREM 6.10. *Suppose char $\mathbb{F}_q \neq 2$ and suppose Σ satisfies the following conditions.*

1. *The $\mathbb{F}_q$-span of the set $\{\pi_0 \otimes \pi_0, \pi_1 \otimes \pi_1, \ldots, \pi_n \otimes \pi_n\}$ is all of $S^2(\mathbb{F}_q^k)$. In particular, $n \geq \frac{k(k+1)}{2} - 1 = \dim S^2(\mathbb{F}_q^k) - 1$.*
2. *The $\mathbb{F}_q$-span H of the set $\{\pi_1 \otimes \pi_1, \ldots, \pi_n \otimes \pi_n\}$ is a hyperplane in $S^2(\mathbb{F}_q^k)$, i.e., H is a subspace of dimension $\frac{k(k+1)}{2} - 1$.*
3. *There is a* symmetric *matrix $T \in \mathbb{F}_q^{k \times k}$ such that*
   - *(a) $\pi_1^t T \pi_1 = \cdots = \pi_n^t T \pi_n = 0$,*
   - *(b) $\pi_0^t T \pi_0 = 1$,*
   - *(c') $\mathrm{rk}(T) \geq 5$.*

Then Σ has product reconstruction (is M2) and Σ does not have linear product reconstruction (is not M1).

PROOF. The conditions imply those of Theorem 6.7. In order to see this, note that the only thing we need to prove is condition 3c) in Theorem 6.7, i.e., that $\mathrm{rk}(T + T^t) \geq 5$. But since T is symmetric, $T + T^t = 2T$ and since the characteristic is different from 2, $\mathrm{rk}(2T) = \mathrm{rk}(T)$, which by the new assumption 3c′) is at least 5. So we can apply Theorem 6.7. △

7 Proof of Main Theorem 4.3: the "Exotic Schemes"

In this section we give the proof of Main Theorem 4.3, which postulates the existence of t-private linear secret sharing schemes enjoying product reconstruction (M2) yet no linear product reconstruction (not M1), where $t \approx \sqrt{n}$ and n is the number of players. To this end, we show the following three propositions. Together these imply Main Theorem 4.3.

PROPOSITION 7.1. *Let $\mathbb{F}_q$ be a finite field with* $\mathrm{char}\,\mathbb{F}_q \neq 2$ *and $q \neq 3$ and let $k \geq 5$ be an integer. Define $n = k(k+1)/2 - 1$. Then there exist $\pi_0, \pi_1, \ldots, \pi_n \in \mathbb{F}_q^k$ such that the following holds.*

1. *The linear secret sharing scheme* $\Sigma = (n, k, (\pi_i)_{i=0}^n)$ *over* $\mathbb{F}_q$ *has* t*-privacy with* $t = \lceil \frac{k}{2} \rceil - 1$.

2. Σ *satisfies the conditions of Theorem 6.10. Hence,* Σ *is M2 but not M1.*

PROPOSITION 7.2. *Let* $\mathbb{F}_q$ *be a finite field with* $\operatorname{char} \mathbb{F}_q = 2$ *and let* $k \geq 6$ *be an even integer. Define* $n = k(k+1)/2 - 1$. *Then there exist* $\pi_0, \pi_1, \ldots, \pi_n \in \mathbb{F}_q^k$ *such that the following holds.*

1. *The linear secret sharing scheme* $\Sigma = (n, k, (\pi_i)_{i=0}^n)$ *over* $\mathbb{F}_q$ *has* t*-privacy with* $t = \frac{k}{2} - 2$.

2. Σ *satisfies the conditions of Theorem 6.7. Hence,* Σ *is M2 but not M1.*

PROPOSITION 7.3. *Let* $\mathbb{F}_3$ *be the finite field with three elements and let* $k \geq 5$ *be an integer. Define* $n = k(k+1)/2 - 1$. *Then there exist* $\pi_0, \pi_1, \ldots, \pi_n \in \mathbb{F}_q^k$ *such that the following holds.*

1. *The linear secret sharing scheme* $\Sigma = (n, k, (\pi_i)_{i=0}^n)$ *over* $\mathbb{F}_3$ *has* t*-privacy with* $t = \lceil \frac{k-1}{3} \rceil - 1$.

2. Σ *satisfies the conditions of Theorem 6.10. Hence,* Σ *is M2 but not M1.*

REMARK 7.4. *By a straightforward rank argument, the achieved* t*-privacy with* $t \approx \sqrt{n}$ *is (asymptotically)* optimal *for separation approaches based on Theorem 6.7. However, the combination of Theorems 6.1 and 6.3 does not seem to rule out (much) better results. In fact, Theorem 8.2 may in principle provide a viable approach towards achieving this.*

7.1 Proof of Proposition 7.1: the odd characteristic case, $q \neq 3$

Let $\mathbb{F}_q$ be a finite field with $\operatorname{char} \mathbb{F}_q \neq 2$ and $q \neq 3$. We need the following technical lemma.

LEMMA 7.5. *There exists* $a \in \mathbb{F}_q$ *such that*

(i) $4a + 1 \neq 0$,

(ii) $X^2 + 2aX + 1 \in \mathbb{F}_q[X]$ *has two distinct roots in* $\mathbb{F}_q$.

PROOF. The polynomial $X^2 + 2aX + 1 \in \mathbb{F}_q[X]$ has discriminant $\Delta = 4a^2 - 4$, hence it has two distinct roots in $\mathbb{F}_q$ if and only if $a^2 - 1 = b^2$ for some $b \in \mathbb{F}_q$, $b \neq 0$. So we have to prove that there exist $a, b \in \mathbb{F}_q$, $b \neq 0$, such that $(a+b)(a-b) = 1$. Let $c \in \mathbb{F}_q$, $c \neq 0, c \neq c^{-1}$. The existence of such a c is guaranteed as $\operatorname{char} \mathbb{F}_q \neq 2$ and $q \neq 3$. Then the linear system

$$\begin{cases} a + b = c \\ a - b = c^{-1} \end{cases}$$

gives a solution $a = (c + c^{-1})/2, b = (c - c^{-1})/2$ to our problem. In particular, note that $b \neq 0$ as $c \neq c^{-1}$. Finally note that $(-a)^2 - 1 = a^2 - 1 = b^2$, hence both a and $-a$ satisfy *(ii)*, and the conclusion now follows as either a or $-a$ satisfies *(i)*. △

REMARK 7.6. *Note that, in particular, if* -1 *is a square in* $\mathbb{F}_q$ *then* $a = 0$ *satisfies Lemma 7.5.*

Let $k \geq 5$ be an integer and define $n = k(k+1)/2 - 1$. Take an element $a \in \mathbb{F}_q$ satisfying the conditions in Lemma 7.5 and let $\alpha, \beta \in \mathbb{F}_q$ be the two distinct roots of $X^2 + 2aX + 1 \in \mathbb{F}_q[X]$. Let $\gamma \in \mathbb{F}_q$ be such that $\gamma \neq 0$ and $f(\gamma) \neq 0$, where $f = X^2 + 2a(k-1)X + a(k-1)(k-2) + k - 1 \in \mathbb{F}_q[X]$. The parameter $\gamma \in \mathbb{F}_q$ is well-defined as the degree of f equals 2 and $q > 3$. Define the sets

$$S_\alpha := \{e_j + \alpha e_\ell : 1 \leq j < \ell \leq k\} \quad , \quad S'_\beta := \{e_1 + \beta e_\ell : 1 < \ell \leq k\}.$$

Note that $|S_\alpha \cup S'_\beta| = |S_\alpha| + |S'_\beta| = n$, since $\alpha \neq \beta$. Write $\pi_1, \ldots, \pi_n$ for the elements of $S_\alpha \cup S'_\beta$. Define $\pi_0 = (1, \ldots, 1, \gamma)$. We claim that the LSSS $\Sigma = (n, k, (\pi_i)_{i=0}^n)$ satisfies properties 1 and 2 of Proposition 7.1.

As to property 1, since π_0 has weight k (since $\gamma \neq 0$) and since $\pi_1, \ldots, \pi_n$ have weight at most 2, the element π_0 cannot be in the span of any subset of $\{\pi_1, \ldots, \pi_n\}$ of cardinality $\lceil \frac{k}{2} \rceil - 1$.

To show property 2, we must show that Σ satisfies conditions 1,2 and 3 of Theorem 6.10. Define the symmetric matrix $T' \in \mathbb{F}_q^{k \times k}$ such that it has its main diagonal entirely consisting of 1's and the value a in all other entries. For $1 \leq i \leq n$, the following holds. If $\pi_i \in S_\alpha$ then $\pi_i^t T' \pi_i = \alpha^2 + 2a\alpha + 1 = 0$. If $\pi_i \in S'_\beta$ then $\pi_i^t T' \pi_i = \beta^2 + 2a\beta + 1 = 0$. Thus, $\pi_i^t T' \pi_i = 0$ for all $i = 1, \ldots, n$. Furthermore,

$$\delta := \pi_0^t T' \pi_0 = \gamma^2 + 2a(k-1)\gamma + a(k-1)(k-2) + k - 1 \neq 0.$$

Finally, the 5×5 submatrix of T' given by its first 5 rows and 5 columns has determinant $(a-1)^4(4a+1) \neq 0$. Hence, $\operatorname{rk} T' \geq 5$. This means that the symmetric matrix $T := \delta^{-1} T'$ satisfies condition 3.

Condition 2 is verified as follows. We claim that $\pi_1 \otimes \pi_1, \ldots, \pi_n \otimes \pi_n$, *together with* $e_1 \otimes e_1$, span $S^2(\mathbb{F}_q^k)$. As the dimension of this space is $n+1$, it follows that $\pi_1 \otimes \pi_1, \ldots, \pi_n \otimes \pi_n$ span a hyperplane. The claim is proved by showing that each of the elements of the basis of $S^2(\mathbb{F}_q^k)$ given by

$$\{e_j \otimes e_j : 1 \leq j \leq k\} \cup \{e_j \otimes e_\ell + e_\ell \otimes e_j : 1 \leq j < \ell \leq k\},$$

is spanned.

For $2 \leq \ell \leq k$, define the vectors $v_\ell := e_1 + \alpha e_\ell \in S_\alpha$ and $v'_\ell := e_1 + \beta e_\ell \in S'_\beta$. Note that these vectors are among $\pi_1, \ldots, \pi_n$. Then each element of the form $e_1 \otimes e_\ell + e_\ell \otimes e_1$ and $e_\ell \otimes e_\ell$ can be written as a linear combination of $v_\ell \otimes v_\ell, v'_\ell \otimes v'_\ell$ and $e_1 \otimes e_1$. Indeed, noting that $\alpha, \beta, \alpha - \beta$ are nonzero, it holds that

$$e_1 \otimes e_\ell + e_\ell \otimes e_1 = \alpha^{-1}\beta^{-1}(\alpha - \beta)^{-1} \left(\alpha^2 v'_\ell \otimes v'_\ell - \beta^2 v_\ell \otimes v_\ell + (\beta^2 - \alpha^2) e_1 \otimes e_1 \right),$$
$$e_\ell \otimes e_\ell = \alpha^{-2} \left(v_\ell \otimes v_\ell - e_1 \otimes e_1 - \alpha(e_1 \otimes e_\ell + e_\ell \otimes e_1) \right).$$

Also, for $2 \leq j < \ell \leq k$, define $w_{j,\ell} := e_j + \alpha e_\ell \in S_\alpha$. Note that, again, these vectors are among $\pi_1, \ldots, \pi_n$. Then each element of the form $e_j \otimes e_\ell + e_\ell \otimes e_j$ can be written as a linear combination of $w_{j,\ell} \otimes w_{j,\ell}$ with the vectors constructed above, as

$$e_j \otimes e_\ell + e_\ell \otimes e_j = \alpha^{-1} \left(w_{j,\ell} \otimes w_{j,\ell} - e_j \otimes e_j - \alpha^2 e_\ell \otimes e_\ell \right).$$

Condition 1 is now satisfied on account of Remark 6.9. This concludes the proof.

Example 7.7. *We work over* $\mathbb{F}_5$. *Let* $k = 5$, *so* $n = 14$. *In this case the element* -1 *is a square, hence* $a = 0$ *satisfies the required properties. Then we can choose* $\alpha = 2$, $\beta = 3$ *(the two distinct roots of* -1 *in* $\mathbb{F}_5$*) and* $\gamma = 2$. *In particular,* T' *is simply the* 5×5 *identity matrix and* T *is the scalar matrix* $2T'$. *Then the LSSS* $\Sigma = (14, 5, (\pi_i)_{i=0}^{14})$, *where the* π_i*'s are given by the columns of*

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 2 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 1 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 1 & 1 & 0 & 0 & 3 & 0 & 0 \\ 1 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 2 & 0 & 1 & 0 & 0 & 3 & 0 \\ 2 & 0 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 2 & 2 & 0 & 0 & 0 & 3 \end{pmatrix},$$

is M2 but not M1 and has 2*-privacy.*

7.2 Proof of Proposition 7.2: the characteristic 2 case

Let $\mathbb{F}_q$ be a finite field with $\operatorname{char}\mathbb{F}_q = 2$ and let $k \geq 6$ be an even integer. Define $n = k(k+1)/2 - 1$. Define the sets U, U', U'' as follows.

- $U := \{e_j : 1 \leq j \leq k\}$,
- $U' := \{e_j + e_\ell : 1 \leq j < \ell \leq k\} \setminus \{e_{2r-1} + e_{2r} : 1 \leq r \leq \frac{k}{2}\}$,
- $U'' := \{e_1 + e_2 + e_{2r-1} + e_{2r} : 2 \leq r \leq \frac{k}{2}\}$.

Note that $|U \cup U' \cup U''| = |U| + |U'| + |U''| = k + (k(k-1)/2 - k/2) + (k/2 - 1) = k(k+1)/2 - 1 = n$. Denote the elements of $U \cup U' \cup U''$ by $\pi_1, \ldots, \pi_n$. Define

$$\pi_0 = \begin{cases} e_2 + \cdots + e_k & \text{if } 4 \mid k \\ e_1 + \cdots + e_k & \text{if } 4 \nmid k \end{cases}.$$

We claim that the LSSS $\Sigma = (n, k, (\pi_i)_{i=0}^n)$ satisfies the properties 1 and 2 of Proposition 7.2.

Projecting on the last $k-2$ coordinates in $\mathbb{F}_q^k$, there is weight $k-2$ for π_0 and weight at most 2 for each of $\pi_1, \ldots, \pi_n$. Hence π_0 is not in the span of any subset of $\{\pi_1, \ldots, \pi_n\}$ with cardinality $\frac{k-2}{2} - 1 = \frac{k}{2} - 2$. This proves property 1.

To show property 2, we must show that Σ satisfies conditions 1,2 and 3 of Theorem 6.7. To this end, we start by defining a matrix $T \in \mathbb{F}_q^{k \times k}$ satisfying condition 3. Note that T cannot be symmetric, since then $T + T^t = 0$ (as the characteristic equals 2). Define $T \in \mathbb{F}_q^{k \times k}$ as the matrix with 1's in positions $(2r-1, 2r)$, for $r = 1, \ldots, \frac{k}{2}$, and 0's everywhere else. In other words, T is the matrix having $k/2$ main diagonal blocks $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ and 0's everywhere else.

If $\pi = (x_1, \ldots, x_k) \in \mathbb{F}_q^k$ then $\pi^t T \pi = x_1 x_2 + \cdots + x_{k-1} x_k$. It is verified at once that $\pi_i^t T \pi_i = 0$ for all $i = 1, \ldots, n$ and $\pi_0^t T \pi_0 = 1$. Moreover, $T + T^t$ has full rank $k \geq 6$. Hence T satisfies condition 3.

Finally, we claim that $\pi_1 \otimes \pi_1, \ldots, \pi_n \otimes \pi_n$ are linearly independent. As the dimension of the whole space equals $n+1$, the claim implies that these span a hyperplane. This settles condition 2. On account of Remark 6.9, condition 1 is then also satisfied. This concludes the proof.

It remains to justify the claim. It is sufficient to show that $\pi_1 \otimes \pi_1, \ldots, \pi_n \otimes \pi_n$, *together with* $(e_1 + e_2) \otimes (e_1 + e_2)$, generate all elements of the set

$$\{e_j \otimes e_j : 1 \leq j \leq k\} \cup \{(e_j + e_\ell) \otimes (e_j + e_\ell) : 1 \leq j < \ell \leq k\},$$

which is the $\mathbb{F}_q$-basis of $S^2(\mathbb{F}_q^k)$ given in Remark 5.9.

The symmetric tensors of elements of U (i.e., the elements $\pi_i \otimes \pi_i$, where $\pi_i \in U$) are exactly the elements of the set $\{e_j \otimes e_j : 1 \leq j \leq k\}$ and the symmetric tensors of elements of U' give all elements $(e_j + e_\ell) \otimes (e_j + e_\ell)$ with $1 \leq j < \ell \leq k$, except those of the form $(e_{2r-1} + e_{2r}) \otimes (e_{2r-1} + e_{2r})$ with $r = 1, \ldots, \frac{k}{2}$.

For $r = 1$, $(e_{2r-1} + e_{2r}) \otimes (e_{2r-1} + e_{2r})$ is exactly the vector added to the set of the $\pi_i \otimes \pi_i$'s. For $2 \leq r \leq \frac{k}{2}$, the element $(e_{2r-1} + e_{2r}) \otimes (e_{2r-1} + e_{2r})$ is generated as

$$\begin{aligned}(e_{2r-1} + e_{2r}) \otimes (e_{2r-1} + e_{2r}) = {} & (e_1 + e_2 + e_{2r-1} + e_{2r}) \otimes (e_1 + e_2 + e_{2r-1} + e_{2r}) + \\ & + (e_1 + e_2) \otimes (e_1 + e_2) + (e_1 + e_{2r-1}) \otimes (e_1 + e_{2r-1}) + \\ & + (e_1 + e_{2r}) \otimes (e_1 + e_{2r}) + (e_2 + e_{2r-1}) \otimes (e_2 + e_{2r-1}) + \\ & + (e_2 + e_{2r}) \otimes (e_2 + e_{2r}).\end{aligned}$$

Note that the first summand is the symmetric tensor of $e_1 + e_2 + e_{2r-1} + e_{2r} \in U''$, which is among $\pi_1 \otimes \pi_1, \ldots, \pi_n \otimes \pi_n$, the second is the vector added to complete the basis and all other summands are symmetric tensors of elements of U'. This concludes the proof of the claim.

EXAMPLE 7.8. *The LSSS over* $\mathbb{F}_2$ $\Sigma = (20, 6, (\pi_i)_{i=0}^{20})$*, where the* π_i*'s are given by the columns of*

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix},$$

is M2 but not M1 and has 1*-privacy (and actually this example also has* 2*-privacy, even though this was not guaranteed by Proposition 7.2).*

7.3 Proof of Proposition 7.3: the case of $\mathbb{F}_3$

We work over the finite field $\mathbb{F}_3$. Let $k \geq 5$ be an integer and $n = k(k+1)/2 - 1$. In this case we do not have a standard way to pick exactly the n vectors $\pi_1, \ldots, \pi_n \in \mathbb{F}_3^k$ satisfying the conditions of the proposition. So we consider a larger set of vectors and prove that, in this set, there are such n vectors. Define the sets

$$U := \{e_j \pm e_\ell : 1 \leq j < \ell \leq k \text{ and } j \neq \ell \bmod 2\},$$
$$U' := \{e_j \pm e_\ell \pm e_r : 1 \leq j < \ell < r \leq k \text{ and } j = \ell = r \bmod 2\}.$$

Let $m = |U \cup U'|$, write $\pi_1, \ldots, \pi_m$ for the elements of $U \cup U'$. Note that $m > n$. Assume, for now, that the $\mathbb{F}_3$-span of $\{\pi_1 \otimes \pi_1, \ldots, \pi_m \otimes \pi_m\}$ is a hyperplane in $\mathrm{S}^2(\mathbb{F}_3^k)$, i.e. a subspace of dimension n. We will prove this fact later. This implies that this set contains a basis of this hyperplane and, maybe renumbering the π_i's, we may assume that the basis is $\{\pi_1 \otimes \pi_1, \ldots, \pi_n \otimes \pi_n\}$. Finally define

$$\pi_0 = \begin{cases} e_1 + \cdots + e_k & \text{if } k \text{ is odd,} \\ e_1 + \cdots + e_{k-1} & \text{if } k \text{ is even.} \end{cases}$$

We claim that the LSSS $\Sigma = (n, k, (\pi_i)_{i=0}^n)$ satisfies properties 1 and 2 of Proposition 7.3.

Having weight at least $k-1$, π_0 cannot be in the span of any $\lceil \frac{k-1}{3} \rceil - 1$ elements of $\{\pi_1, \ldots, \pi_n\}$, whose weight is at most 3. This proves property 1.

In order to show property 2 using Theorem 6.10, define the symmetric, diagonal matrix $T \in \mathbb{F}_3^{k \times k}$ having (j,j)-th entry equal to 1 if j is odd and to -1 otherwise. It is straightforward to check that $\pi_i^t T \pi_i = 0$ for all $i = 1, \ldots, n$ and $\pi_0^t T \pi_0 = 1$. Also, $\operatorname{rk} T = k \geq 5$. So T satisfies condition 3.

Condition 2 follows immediately by the claim that $\mathbb{F}_3\langle \pi_1 \otimes \pi_1, \ldots, \pi_m \otimes \pi_m \rangle$ is a hyperplane in $\mathrm{S}^2(\mathbb{F}_3^k)$. Condition 1 then follows by Remark 6.9, concluding the proof.

It only remains to prove that $\mathbb{F}_3\langle \pi_1 \otimes \pi_1, \ldots, \pi_m \otimes \pi_m \rangle$ is a hyperplane in $\mathrm{S}^2(\mathbb{F}_3^k)$. We prove that $\pi_1 \otimes \pi_1, \ldots, \pi_m \otimes \pi_m$, *together with* $e_1 \otimes e_1$, span $\mathrm{S}^2(\mathbb{F}_3^k)$. Recall that

$$\{e_j \otimes e_j : 1 \leq j \leq k\} \cup \{e_j \otimes e_\ell + e_\ell \otimes e_j : 1 \leq j < \ell \leq k\}$$

is a basis of $\mathrm{S}^2(\mathbb{F}_3^k)$. For all even j, $e_j \otimes e_j$ is spanned as

$$e_j \otimes e_j = 2(e_1 \otimes e_1 + (e_1 + e_j) \otimes (e_1 + e_j) + (e_1 - e_j) \otimes (e_1 - e_j)).$$

In particular, $e_2 \otimes e_2$ is spanned. Then for all odd $j \geq 3$, $e_j \otimes e_j$ is spanned as

$$e_j \otimes e_j = 2(e_2 \otimes e_2 + (e_2 + e_j) \otimes (e_2 + e_j) + (e_2 - e_j) \otimes (e_2 - e_j)).$$

We have thus spanned all vectors of the form $e_j \otimes e_j$. We span $e_j \otimes e_\ell + e_\ell \otimes e_j$ for $j < \ell$, $j \neq \ell \bmod 2$ as

$$e_j \otimes e_\ell + e_\ell \otimes e_j = 2(e_j + e_\ell) \otimes (e_j + e_\ell) - 2(e_j - e_\ell) \otimes (e_j - e_\ell).$$

It remains to span all vectors of the form $e_j \otimes e_\ell + e_\ell \otimes e_j$ with $j < \ell$ and $j = \ell \bmod 2$. Note that we have not yet used vectors from U'. Let r be such that $r = j = \ell \bmod 2$ but $j \neq r \neq \ell$. Assume $j < \ell < r$, one can deal analogously with all other cases. For simplicity, put $v^+_{j,\ell,r} := e_j + e_\ell + e_r \in U'$ and $v^-_{j,\ell,r} := e_j + e_\ell - e_r \in U'$. Note that these vectors are among $\pi_1, \ldots, \pi_m$. Then

$$e_j \otimes e_\ell + e_\ell \otimes e_j = 2(v^+_{j,\ell,r} \otimes v^+_{j,\ell,r} + v^-_{j,\ell,r} \otimes v^-_{j,\ell,r} + e_j \otimes e_j + e_\ell \otimes e_\ell + e_r \otimes e_r)$$

and we conclude.

8 Extensions

We discuss some extensions of our result.

8.1 Strong multiplication

We first argue that we can obtain a similar separation result for the notion of strong multiplication. For a set A consisting of $n-t$ players, consider the LSSS $\Sigma_A = (n-t, k, (\pi_i)_{i\in\{0\}\cup A})$, which contains only the share functions corresponding to A (and the same secret function).

An LSSS $\Sigma = (n, k, (\pi_i)_{i=0}^n)$ is t-strong multiplicative if Σ has t-privacy and, for *every* set A consisting of $n - t$ players, Σ_A is multiplicative (M1).

We can show the following separation result:

THEOREM 8.1. *Let $\mathbb{F}_q$ be the finite field of q elements, with $q \neq 3$. There exists a function $\hat{t}_q(n) \in \Omega(\sqrt[3]{n})$ such that for an unbounded number $n \in \mathbb{N}$, there exists a linear secret sharing scheme $\Sigma = (n, k, (\pi_i)_{i=0}^n)$ over $\mathbb{F}_q$ such that Σ has $\hat{t}_q(n)$-privacy and for each set A consisting of $n - \hat{t}_q(n)$ players, Σ_A admits a product reconstruction function (M2). However (for every such A) such function is necessarily not $\mathbb{F}_q$-linear. Therefore, Σ is not a $\hat{t}_q(n)$-strongly multiplicative linear secret sharing scheme.*

PROOF. The proof consists in modifying properly the schemes obtained in Main Theorem 4.3. Namely, given $\Sigma' = (n', k, (\pi_i)_{i=0}^{n'})$ satisfying the properties guaranteed by Main Theorem 4.3 (which has t-privacy for $t := t_q(n')$), we consider the LSSS Σ where we *replicate* $t+1$ times each share from Σ'. Therefore we now have $n := (t+1)n'$ players. Since "there are no new shares", it is clear that the new scheme still has t-privacy and that Σ (and hence any subscheme Σ_A) does not have linear multiplication. On the other hand, for any set A consisting of $n - t$ players, Σ_A clearly contains all shares $\pi_1, \ldots, \pi_n$ in Σ' and hence it has product reconstruction because Σ' does. Since $t = \Omega(\sqrt{n'})$, we have $t = \Omega(\sqrt[3]{n})$. △

8.2 A generalization of Theorem 6.7

As we pointed out in Remark 7.4, Theorem 6.7 can only yield schemes where $t \in O(\sqrt{n})$ and in that sense, our Main Theorem 4.3 and explicit constructions from Section 7 are optimal. However, we can generalize Theorem 6.7 by requiring that, first, the set $\{\pi_i \otimes \pi_i : i = 1, \ldots, n\}$ generates a space of dimension $\frac{k(k+1)}{2} - h$, for some integer $h \geq 1$ and, second, there is an h-dimensional vector space $\mathcal{M} \subseteq \mathbb{F}_q^{k\times k}$ such that any nonzero matrix in $\mathcal{M}$ verifies the conditions in Theorem 6.7. Theorem 6.7 is then the case $h = 1$. Potential examples where

$h > 1$ would therefore have a smaller (when considered as a function of k) number of shares, namely $n = \frac{k(k+1)}{2} - h$. More precisely, we have the following result.

THEOREM 8.2. *Let $\mathbb{F}_q$ be a finite field, and let h be an integer with $1 \leq h < \frac{k(k+1)}{2}$. Suppose $\Sigma = (n, k, (\pi_i)_{i=0}^n)$ is an LSSS over $\mathbb{F}_q$ satisfying the following conditions.*

1. *The $\mathbb{F}_q$-span of the set $\{\pi_0 \otimes \pi_0, \pi_1 \otimes \pi_1, \ldots, \pi_n \otimes \pi_n\}$ is a subspace of $S^2(\mathbb{F}_q^k)$ of dimension $\frac{k(k+1)}{2} - h + 1$. In particular, $n \geq \frac{k(k+1)}{2} - h$.*
2. *The $\mathbb{F}_q$-span H of the set $\{\pi_1 \otimes \pi_1, \ldots, \pi_n \otimes \pi_n\}$ is a subspace of $S^2(\mathbb{F}_q^k)$ of dimension $\frac{k(k+1)}{2} - h$.*
3. *There is an* $\mathbb{F}_q$-vector space $\mathcal{M} \subseteq \mathbb{F}_q^{k \times k}$ of dimension h, *consisting of matrices such that*
   (a) $\pi_1^t M \pi_1 = \cdots = \pi_n^t M \pi_n = 0$ *for* all $M \in \mathcal{M}$.
   (b) $\pi_0^t T \pi_0 = 1$ *for* some $T \in \mathcal{M}$.
   (c) $\mathrm{rk}(M + M^t) \geq 5$ *for* all $M \in \mathcal{M} \setminus \{0\}$.

Then Σ has product reconstruction (is M2) but Σ does not have linear product reconstruction (is not M1).

REMARK 8.3. *We point out that conditions* 2, 3*a*) *and* 3*b*) *imply condition* 1, *by arguments similar to the ones in Remark 6.9.*

Note also that in condition 3*b*) *we only need* one *matrix $T \in \mathcal{M}$ such that $\pi_0^t T \pi_0 = 1$.*

PROOF. We proceed similarly to the proof of Theorem 6.7. The property that Σ is not M1 is again immediate from the existence of T and Theorem 6.1.

We now prove that Σ is M2. Let B be any matrix of rank at most 2 such that $\pi_i^t B \pi_i = 0$ for $i = 1, \ldots, n$. Note that, by 3*c* the only alternating matrix contained in $\mathcal{M}$ is the zero matrix, since all alternating matrices are antisymmetric. Therefore, by Theorem 5.10, the linear forms ϕ_M on $\mathrm{S}^2(\mathbb{F}_q^k)$ with $M \in \mathcal{M}$ are all *distinct*. Hence the set $V = \{\phi_M : M \in \mathcal{M}\}$ is a vector space of dimension h. Note that every $\phi \in V$ satisfies $\phi(H) = 0$. Then, by linear algebra and since, by condition 2, H has dimension $\frac{k(k+1)}{2} - h$, any linear form ϕ on $\mathrm{S}^2(\mathbb{F}_q^k)$ with $\phi(H) = 0$ must be in V. In particular, we have $\phi_B(H) = 0$, so $\phi_B = \phi_M$ for some $M \in \mathcal{M}$. But, if $\phi_M \neq 0$, 3*c* would imply $5 \leq \sigma(\phi_M) = \sigma(\phi_B) \leq 4$, which is a contradiction. Therefore $\phi_B = 0$ and $\pi_0^t B \pi_0 = 0$. △

References

[1] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. *Proc. of STOC 1988*, pp. 1–10. ACM Press, 1988.

[2] I. Cascudo, R. Cramer, C. Xing. The Torsion-Limit for Algebraic Function Fields and Its Application to Arithmetic Secret Sharing. *Proc. of 31st Annual IACR CRYPTO*, Santa Barbara, Ca., USA, Springer Verlag LNCS, vol. 6842, pp. 685-705, August 2011.

[3] D. Chaum, C. Crépeau, and I. Damgaard. Multi-party unconditionally secure protocols. *Proc. of STOC 1988*, pp. 11–19. ACM Press, 1988.

[4] H. Chen and R. Cramer. Algebraic Geometric Secret Sharing Schemes and Secure Multi-Party Computation over Small Fields. *Proc. of 26th Annual IACR CRYPTO*, Springer Verlag LNCS, vol. 4117, pp. 516-531, Santa Barbara, Ca., USA, August 2006.

[5] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, V. Vaikuntanathan. Secure Computation from Random Error Correcting Codes. *Proc. of 27th Annual IACR EUROCRYPT*, Barcelona, Spain, Springer Verlag LNCS, vol. 4515, pp. 291-310, 2007.

[6] R. Cramer, I. Damgaard, and U. Maurer. General secure multi-party computation from any linear secret sharing scheme. *Proceedings of 19th Annual IACR EUROCRYPT*, Brugge, Belgium, Springer Verlag LNCS, vol. 1807, pp. 316-334, May 2000.

[7] M. K. Franklin, M. Yung. Communication Complexity of Secure Computation (Extended Abstract). *Proc. of STOC 1992*, pp. 699-710

[8] Y. Ishai, E. Kushilevitz, R. Ostrovsky, A. Sahai. Zero-knowledge from secure multiparty computation. *Proc. of 39th STOC*, San Diego, Ca., USA, pp. 21-30, 2007.

[9] A. Shamir. How to share a secret. *Comm. of the ACM*, 22(11):612-613, 1979.