Asymptotically Good Ideal Linear Secret Sharing with Strong Multiplication over *Any* Fixed Finite Field

Ignacio Cascudo[1], Hao Chen[2], Ronald Cramer[3], and Chaoping Xing[4]

[1] Department of Mathematics, University of Oviedo, Spain. Email: icascudo@orion.ciencias.uniovi.es
[2] Software Engineering Institute, East China Normal University, Shanghai 20062, China. Email: haochen@sei.ecnu.edu
[3] CWI, Amsterdam & Mathematical Institute, Leiden University, The Netherlands. URL: http://www.cwi.nl/~cramer
[4] Division of Mathematical Sciences, Nanyang Technological University, Singapore. URL: http://www3.ntu.edu.sg/home/xingcp/

Abstract. This work deals with "MPC-friendly" linear secret sharing schemes (LSSS), a mathematical primitive upon which secure multi-party computation (MPC) can be based and which was introduced by Cramer, Damgaard and Maurer (EUROCRYPT 2000). Chen and Cramer proposed a special class of such schemes that is constructed from algebraic geometry and that enables efficient secure multi-party computation over fixed finite fields (CRYPTO 2006). We extend this in four ways. First, we propose an abstract coding-theoretic framework in which this class of schemes and its (asymptotic) properties can be cast and analyzed. Second, we show that for *every finite field* $\mathbb{F}_q$, there exists an infinite family of LSSS over $\mathbb{F}_q$ that is asymptotically good in the following sense: the schemes are "*ideal*," i.e., each share consists of a single $\mathbb{F}_q$-element, and the schemes have *t-strong multiplication* on n players, where the corruption tolerance $\frac{3t}{n-1}$ tends to a constant $\nu(q)$ with $0 < \nu(q) < 1$ when n tends to infinity. Moreover, when $|\mathbb{F}_q|$ tends to infinity, $\nu(q)$ tends to 1, which is optimal. This leads to explicit lower bounds on $\widehat{\tau}(q)$, our measure of *asymptotic optimal corruption tolerance*. We achieve this by combining the results of Chen and Cramer with a dedicated field-descent method. In particular, in the $\mathbb{F}_2$-case there exists a family of binary t-strongly multiplicative ideal LSSS with $\frac{3t}{n-1} \approx 2.86\%$ when n tends to infinity, a one-bit secret and just a one-bit share for every player. Previously, such results were shown for $\mathbb{F}_q$ with $q \geq 49$ a square. Third, we present an infinite family of ideal schemes with t-strong multiplication that does not rely on algebraic geometry and that works over every finite field $\mathbb{F}_q$. Its corruption tolerance vanishes, yet still $\frac{3t}{n-1} = \Omega(1/(\log\log n)\log n)$. Fourth and finally, we give an improved non-asymptotic upper bound on corruption tolerance.

1 Introduction

This work deals with "MPC-friendly" linear secret sharing schemes (LSSS), an abstract mathematical primitive upon which secure multi-party computation (MPC) can be based and which was introduced by Cramer, Damgaard and Maurer [13]. Chen and Cramer [8] proposed a special class of such schemes that is constructed from algebraic geometry and that enables efficient secure multi-party computation over fixed finite fields. For every finite field $\mathbb{F}_q$ where q is a square with $q \geq 49$, they presented an infinite family of LSSS over $\mathbb{F}_q$ that is asymptotically good in the following sense. First, the schemes are "*ideal*": each share consists of a single $\mathbb{F}_q$-element. Second, the schemes have *t-strong multiplication* [13, 12, 9, 8] on n players, where the corruption tolerance $\frac{3t}{n-1}$ tends by a constant $\nu(q)$ with $0 < \nu(q) < 1$ when n tends to infinity. Moreover, when $|\mathbb{F}_q|$ tends to infinity, $\nu(q)$ tends to 1, which is optimal (since it is well-known that $3t + 1 \leq n$ always). In short, strong multiplication is a property that enables to "perfectly securely" verify multiplicative relations among secret-shared values, with *error probability equal to zero*. This is a crucial subroutine at the heart of MPC. Please refer to [13] for the details.

These schemes of [8] enjoy algebraic properties similar to those of Shamir's scheme (linearity, (strong)-multiplication), and MPC protocols in the strongest information-theoretic model [2, 3] (i.e., perfect security against a computationally unbounded threshold adversary that corrupts some fraction of the players) are quite similar (see [13, 8]). The significance of these schemes, however, derives from the fact that the number of players is not bounded by the size of the finite field as is the case for Shamir's scheme [26]. In fact, in these schemes the number of players is unbounded even if the finite field is fixed. In the corresponding MPC-protocols, the total number of field elements communicated will typically be the same, with the notable difference, however, that the field elements are now taken in a field of constant rather than linearly increasing size. This makes sense, for instance, if the function that is securely computed is defined over a small, constant size field, say $\mathbb{F}_2$. The price to be paid is only a *constant* fractional decrease compared to the corruption tolerance of (non-asymptotic) Shamir-based MPC-protocols, in which up to 1/3 of the players may be corrupted. The construction of these "MPC-friendly" schemes from [8] is based on the existence of families of algebraic curves of finite fields with a good ratio between the number of rational points and their genus and the use of their algebraic function fields. See [13, 8, 6] for a full discussion. Chen, Cramer, Goldwasser, de Haan and Vaikuntanatan [7] have shown similar results for schemes with multiplication rather than strong multiplication by a construction from arbitrary classical codes rather than algebraic geometric ones.

The results from [8, 7] have found remarkable applications in the breakthrough work of Ishai, Kushilevitz, Ostrovsky and Sahai [20] on two-party zero-knowledge for circuit-satisfiability with low communication, in that of Ishai, Prabhakaran and Sahai [19] on oblivious transfer, as well as in the work of Damgaard, Nielsen and Wichs [14] on isolated zero-knowledge. In all these cases this helped improving the communication efficiency. It is important to note that

all these applications use secret sharing and MPC as abstract primitives, where players are *not actual, real-world players* but are part of *virtual* processes. Moreover, the number of these virtual players is typically large in order to make certain error-probabilities small enough or in order to approximate a certain asymptotical advantage. This has amplified the relevance of secure computation and secret sharing even further, and in particular it adds further relevance to asymptotical study of these primitives.

In this paper we extend these results in four ways. First, we propose an abstract coding-theoretic framework in which this class of schemes and its (asymptotic) properties can be cast and analyzed. Concretely, we introduce a special class of codes $\mathcal{C}^\dagger(\mathbb{F}_q)$ and a measure $\widehat{t}(C)$ on a code $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$, the corruption tolerance of C, so that when C is viewed to represent an "ideal" LSSS, $\widehat{t}(C)$ measures the maximum t for which it has t-strong multiplication. We also define the *asymptotic optimal corruption tolerance* $\widehat{\tau}(q)$ of such a class over $\mathbb{F}_q$, the main parameter for our asymptotic analysis.

Second, we show that for *every finite field* $\mathbb{F}_q$, there exists an infinite family of LSSS over $\mathbb{F}_q$ that is asymptotically good in the following sense: the schemes are "*ideal*," i.e., each share consists of a single $\mathbb{F}_q$-element, and the schemes have *t-strong multiplication* on n players, where the corruption tolerance $\frac{3t}{n-1}$ tends to a constant $\nu(q)$ with $0 < \nu(q) < 1$ when n tends to infinity. Moreover, when $|\mathbb{F}_q|$ tends to infinity, $\nu(q)$ tends to 1, which is optimal. This leads to explicit lower bounds on $\widehat{\tau}(q)$. Our method combines the algebraic geometric schemes of Chen and Cramer with our dedicated but elementary field-descent method based on "multiplication-friendly functions," which maps $C \in \mathcal{C}^\dagger(\mathbb{F}_{q^m})$ to $C' \in \mathcal{C}^\dagger(\mathbb{F}_q)$ in such a way that corruption tolerance does not degrade too much. In particular, in the $\mathbb{F}_2$-case there exists a family of binary t-strongly multiplicative ideal LSSS with $\frac{3t}{n-1} \approx 2.86\%$ when n tends to infinity, a one-bit secret and just a one-bit share for every player. Previously, such results were only shown to hold over $\mathbb{F}_q$ with $q \geq 49$ a square.

Third, we present an infinite family of ideal schemes with t-strong multiplication that does not rely on algebraic geometry and that works over every finite field $\mathbb{F}_q$. Its corruption tolerance vanishes, yet still $\frac{3t}{n-1} = \Omega(1/(\log\log n)\log n)$. Fourth and finally, we give an improved non-asymptotic upper bound on corruption tolerance.

The outline of this paper is as follows. After the preliminaries in Section 2, we revisit in Section 3 the results in [7] about the construction of LSSS from linear codes, where we focus mainly on privacy and reconstruction. In some cases we define new notions and prove stronger results needed in the sequel. In Section 4 we define $\mathcal{C}^\dagger(\mathbb{F}_q)$, $\widehat{t}(C)$ and $\widehat{\tau}(q)$, and prove some properties. In Section 5 we show that for every finite fields $\mathbb{F}_q$, the asymptotic optimal corruption tolerance can be bounded away from zero, i.e., $\widehat{\tau}(q) > 0$ for all finite field $\mathbb{F}_q$, and we give explicit lower bounds. In Section 6 we state the consequences for LSSS with strong multiplication explicitly and in Section 7 we present the elementary example with ("not-so-fast") vanishing asymptotic corruption tolerance. In Section 8, we

give our non-asymptotic upper bound on corruption tolerance. In Section 9 we conclude by stating some open problems.

Finally, we note that, in upcoming work [5], we further improve our asymptotic lower bounds on optimal corruption tolerance using more advanced methods from algebraic geometry, especially for small values of q.

2 Preliminaries

2.1 Basic Coding Theory

We review some notions from basic coding theory (see e.g. [22] or [17]) that are relevant to this work and we also introduce some conventions specific to this paper. Let n be a non-negative integer and let k be an integer with $0 \leq k \leq n+1$. An $[n+1,k]_q$-code C over the finite field $\mathbb{F}_q$ is a k-dimensional subspace C of the $n+1$-dimensional $\mathbb{F}_q$-vector space $\mathbb{F}_q^{n+1}$. The length $n+1$ of such a code C is denoted $\ell(C)$. We define $n(C) = \ell(C) - 1$. If $\mathbf{c} \in C$, $(c_0, c_1, \ldots, c_n) \in \mathbb{F}_q^{n+1}$ denotes its coordinate vector. In particular, we use the set $\mathcal{I}(C) = \{0, 1, \ldots, n\}$ to index the coordinates, unless otherwise stated. A linear code over $\mathbb{F}_q$ is an $[n+1,k]_q$-code for some k, n. If $B \subset \mathcal{I}(C)$ is a non-empty set and if $\mathbf{x} = (x_0, x_1, \ldots, x_n) \in \mathbb{F}_q^{n+1}$, $\mathbf{x}_B$ denotes the vector $(x_i)_{i \in B} \in \mathbb{F}_q^{|B|}$, i.e., the vector obtained by restricting $\mathbf{x}$ to those coordinates i with $i \in B$. The *support* $\mathrm{supp}(\mathbf{x})$ of $\mathbf{x} \in \mathbb{F}_q^{n+1}$ is the set of indices $i \in \mathcal{I}(C)$ with $x_i \neq 0$. An element $\mathbf{c} \in C$ is minimal if there is no $\mathbf{c}' \in C \setminus \{\mathbf{0}\}$ with $\mathrm{supp}(\mathbf{c}')$ a proper subset of $\mathrm{supp}(\mathbf{c})$.

A generator matrix G for an $[n+1,k]$-code C is a matrix with entries in $\mathbb{F}_q$ and that has k columns and $n+1$ rows such that the columns of G jointly constitute an $\mathbb{F}_q$-basis of C. The Hamming-weight $w_H(\mathbf{x})$ of $\mathbf{x} = (x_0, x_1, \ldots, x_n) \in \mathbb{F}_q^{n+1}$ is the number of indices with $x_i \neq 0$. Let d be a positive integer with $0 \leq d \leq n+1$. An $[n+1,k,d]_q$-code C is an $[n+1,k]_q$-code whose minimum distance $d_{\min}(C)$ in the Hamming-metric is *at least* d.[5] If C is an $[n+1,k]_q$-code, then $d_{\min}(C) \leq (n+1) - k + 1 = n - k + 2$ by the Singleton-bound.

The dual $C^\perp$ of C is the "orthogonal complement" of C in $\mathbb{F}_q^{n+1}$ according to the standard scalar product $\langle \mathbf{x}, \mathbf{y} \rangle = x_0 y_0 + x_1 y_1 + \cdots + x_n y_n$, where $\mathbf{x} = (x_0, x_1, \ldots, x_n) \in \mathbb{F}_q^{n+1}$ and $\mathbf{y} = (y_0, y_1, \ldots, y_n) \in \mathbb{F}_q^{n+1}$. Thus, $C^\perp$ consists of all $\mathbf{c}^* \in \mathbb{F}_q^{n+1}$ such that $\langle \mathbf{c}, \mathbf{c}^* \rangle = 0$ for all $\mathbf{c} \in C$. If C is an $[n+1,k]_q$-code, then $C^\perp$ is an $[n+1, n+1-k]_q$-code. Note that $d_{\min}(C) + d_{\min}(C^\perp) \leq n+3$.

2.2 Secret Sharing

In this section we give precise definitions of (linear) secret sharing (with strong multiplication). A secret sharing scheme (SSS) $\Sigma = (S_0, S_1, \ldots, S_n)$ is a vector of $n+1$ random variables, where n is a positive integer and where the random variables are all defined on the same finite probability distribution. It is required

[5] The minimum distance of the $[n+1,0]_q$-code $C = \{0\}$ is, by definition, equal to $n+1$.

that $H(S_0|S_1 \dots S_n) = 0$ and that $H(S_0) > 0$. Here $H(\cdot)$ denotes the Shannon-entropy function and $H(\cdot|\cdot)$ denotes conditional entropy. A value taken by S_0 is a "secret", and a value taken by S_i, is a "share" or "the i-th share", $i = 1 \dots n$. Write $\mathcal{P} = \mathcal{P}(\Sigma) = \{1, \dots, n\}$ and $n(\Sigma) = n$. An element $i \in \mathcal{P}$ may sometimes be called "player." If $A \subset \mathcal{P}$ is non-empty, S_A denotes the vector of random variables $(S_i)_{i \in A}$. Note that this bare definition only says that there is some non-constant "secret" that is uniquely determined by the n shares.

The *adversary structure* $\mathcal{A}(\Sigma)$ consists of the empty set as well as any non-empty sets $A \subset \mathcal{P}$ such that $H(S_0|S_A) = H(S_0)$ ("no information about the secret"). The access structure $\Gamma(\Sigma)$ consists of all $B \subset \mathcal{P}$ such that $H(S_0|S_B) = 0$ ("full information about the secret"). By definition, $\mathcal{P} \in \Gamma(\Sigma)$. From a basic information theoretic inequality, $H(S_0) \geq H(S_0|S_B)$ for all non-empty sets $B \subset \mathcal{P}$. Therefore, $\Gamma(\Sigma) \cap \mathcal{A}(\Sigma) = \emptyset$. Let t, r be positive integers. We say that Σ *achieves t-privacy* if $\mathcal{A}(\Sigma)$ includes all sets $A \subset \mathcal{P}$ with $|A| = t$ and we say that Σ *achieves r-reconstruction* if $\Gamma(\Sigma)$ includes all sets $B \subset \mathcal{P}$ with $|B| = r$. Furthermore, $r(\Sigma)$ denotes the minimum integer r for which Σ has r-reconstruction and $t(\Sigma)$ is the largest integer t such that $\mathcal{A}(\Sigma)$ includes all sets $A \subset \mathcal{P}$ with $|A| = t$. A *threshold SSS* is one that achieves t-privacy and $t+1$-reconstruction for some positive integer t. An $(n, t+1, t)$-threshold SSS is one that achieves t-privacy and $t+1$-reconstruction for some integer t, with n being the number of players.

An SSS is *perfect* if $\Gamma(\Sigma) \cup \mathcal{A}(\Sigma) = 2^{\mathcal{P}}$. An element $i \in \mathcal{P}$ is "not a dummy" if there exists a set $B \in \Gamma(\Sigma)$ with $i \in B$ that is minimal with respect to the partial ordering $\Gamma(\Sigma)$ defined by the inclusion-relation. In a perfect SSS it holds that $H(S_i) \geq H(S_0)$ for each $i \in \mathcal{P}$ which is not a dummy ("length of a share is at least length of the secret"). A perfect SSS is ideal if for each such $i \in \mathcal{P}$ equality holds. If $\Gamma(\Sigma)$ does not contain any dummies, it is called *connected*.

A *linear secret sharing scheme* (LSSS) is a tuple $\Sigma = (\mathbb{F}_q, n, e, \mathbf{v}_0, V_1, \dots, V_n)$ where $\mathbb{F}_q$ is a finite field, e, n are positive integers, $\mathbf{v}_0 \in \mathbb{F}_q^e \setminus \{\mathbf{0}\}$, and $V_1, \dots, V_n$ are subspaces of the $\mathbb{F}_q$-vector space $\mathbb{F}_q^e$ such that $\mathbf{v}_0 \in \sum_{i \in \mathcal{P}} V_i$, the subspace of $\mathbb{F}_q^e$ spanned by the V_i's. An LSSS is an SSS in the sense of the definition above if the following conventions are made. Write d_i for the $\mathbb{F}_q$-dimension of V_i, $i = 1 \dots n$. First, for each V_i an $\mathbb{F}_q$-basis $B_i = \{\mathbf{b}_{i1}, \dots, \mathbf{b}_{id_i}\}$ is fixed. Second, the random variables $S_0, S_1, \dots, S_n$ are defined as follows. The secret $s \in \mathbb{F}_q$ is chosen uniformly at random (thereby defining S_0) and $\phi \in \mathrm{Hom}_{\mathbb{F}_q}(\mathbb{F}_q^e, \mathbb{F}_q)$, the $\mathbb{F}_q$-linear map from $\mathbb{F}_q^e$ to $\mathbb{F}_q$, is chosen uniformly random conditioned on $\phi(\mathbf{v}_0) = s$. If $d_i > 0$, the i-th share is $(\phi(\mathbf{b}_{i1}), \dots, \phi(\mathbf{b}_{id_i})) \in \mathbb{F}_q^{d_i}$, thereby defining S_i, $i = 1 \dots n$. For a non-empty set $A \subset \mathcal{P}$, we define $V_A = \sum_{i \in A} V_i$ and we call its $\mathbb{F}_q$-dimension d_A. It can be shown that a non-empty set $B \subset \mathcal{P}$ satisfies $B \in \Gamma(\Sigma)$ if and only if $\mathbf{v}_0 \in V_B$. Equivalently, it can be shown $A \in \mathcal{A}(\Sigma)$ if and only if there exists $\phi \in \mathrm{Hom}_{\mathbb{F}_q}(\mathbb{F}_q^e, \mathbb{F}_q)$ such that $\phi(\mathbf{v}_0) = 1$ and ϕ vanishes on V_A, i.e., $\phi(\mathbf{v}) = 0$ for all $\mathbf{v} \in V_A$. In particular, this means that LSSS are perfect. We define $\dim \Sigma = \sum_{i=1}^{n} d_i$, the dimension of the LSSS. Shamir's scheme is a threshold LSSS.

Given an LSSS Σ we define the *dual access structure* to $\Gamma(\Sigma)$ as $\Gamma(\Sigma)^* = \{A \subset \mathcal{P}, \text{ s.t. } \mathcal{P} \setminus A \notin \Gamma(\Sigma)\}$. For every LSSS Σ over $\mathbb{F}_q$ there exists an LSSS Σ^* over $\mathbb{F}_q$ such that $\dim \Sigma = \dim \Sigma^*$ and $\Gamma(\Sigma^*) = \Gamma(\Sigma)^*$ (see [21, 13]). Note that $r(\Sigma^*) = n - t(\Sigma)$, $t(\Sigma^*) = n - r(\Sigma)$.

Let $\mathbf{v} = (v_1, \ldots, v_e) \in \mathbb{F}_q^e$ and $\mathbf{w} = (w_1, \ldots, w_e) \in \mathbb{F}_q^e$. Then $\mathbf{v} \otimes \mathbf{w} = (v_1 \cdot \mathbf{w}, \ldots, v_e \cdot \mathbf{w}) \in \mathbb{F}_q^{e^2}$ denotes the *Kronecker-product (or tensor-product)* of $\mathbf{v}$ and $\mathbf{w}$. For $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n, \mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$, their *Schur-product* $\mathbf{x} * \mathbf{y} \in \mathbb{F}_q^n$ is defined as $(x_1 y_1, \ldots, x_n y_n)$.

If V and W are subspaces of the $\mathbb{F}_q$-vector space $\mathbb{F}_q^e$, then $V \otimes W$ denotes the subspace of the $\mathbb{F}_q$-vector space $\mathbb{F}_q^{e^2}$ generated by the elements $\mathbf{v} \otimes \mathbf{w}$ with $\mathbf{v} \in V$ and $\mathbf{w} \in W$. If $A \subset \{1, \ldots, n\}$ is non-empty, $\widehat{V}_A$ denotes $\sum_{i \in A} V_i \otimes V_i$, the subspace of the $\mathbb{F}_q$-vector space $\mathbb{F}_q^{e^2}$ spanned by the subspaces $V_i \otimes V_i$. Σ has *t-strong multiplication* ([13, 12, 8]) if the following holds: $0 \leq t \leq n$, Σ achieves t-privacy, $\mathbf{v}_0 \otimes \mathbf{v}_0 \in \widehat{V}_{\mathcal{P}}$, and for each set $B \subset \mathcal{P}$ with $|B| = n - t$, $\mathbf{v}_0 \otimes \mathbf{v}_0 \in \widehat{V}_B$. Σ has *multiplication* if it achieves t-privacy for some $t \geq 1$ and if $\mathbf{v}_0 \otimes \mathbf{v}_0 \in \widehat{V}_{\mathcal{P}}$.

2.3 Algebraic Function Fields and Codes

In this paper we make at some point use of some basic as well as some more advanced results for algebraic function fields. We use the terminology of [27]. For a quick introduction to some of the notions that are needed (function fields, poles, zeroes, divisors, degrees, etc.), please refer to [8]. Let $\mathbb{F}_q$ be a finite field. When we say that $\mathbb{F}$ is an algebraic function field over $\mathbb{F}_q$ we mean that $\mathbb{F}$ is an algebraic function field over $\mathbb{F}_q$ *in one variable* and that $\mathbb{F}_q$ is the *full constant field* of $\mathbb{F}$. $\mathbb{P}_q(\mathbb{F})$ denotes the set of places of degree 1 and $g(\mathbb{F})$ denotes the genus of $\mathbb{F}$. If G is a divisor on $\mathbb{F}$, then $\deg(G)$ denotes its degree and $\mathcal{L}(G) \subset \mathbb{F}$ denotes the Riemann-Roch space of functions $f \in \mathbb{F}$ such that $\mathrm{div}(f) + G$ is an effective divisor or $f = 0$. This is an $\mathbb{F}_q$-vector space.

By the Riemann-Roch Theorem, $\dim_{\mathbb{F}_q} \mathcal{L}(G) = \deg(G) + 1 - g(\mathbb{F}) + \dim_{\mathbb{F}_q} \mathcal{L}(W - G)$, where $\deg(G)$ denotes the degree of the divisor G and where W is any canonical divisor. This implies Riemann's Theorem that $\dim_{\mathbb{F}_q} \mathcal{L}(G) = \deg(G) + 1 - g(\mathbb{F})$ if $\deg(G) > 2g(\mathbb{F}) - 2$. Suppose $\mathbb{P}_q(\mathbb{F}) \geq n + 1$ for some positive integer n. Let $P_0, P_1, \ldots, P_n$ be distinct elements of $\mathbb{P}_q(\mathbb{F})$ and define the divisor $D = P_0 + P_1 + \ldots + P_n$. Suppose G is a divisor on $\mathbb{F}$ such that $\deg(G) > 2 \cdot g(\mathbb{F}) - 2$ and such that the $\mathrm{supp}(G)$, the support of G is disjoint of that of D. Then the $[n + 1, k, d]_q$-code $C(G, D)$ (algebraic-geometric Goppa-code or AG-code) is defined [16] as $C(G, D) = \{(f(P_0), f(P_1), \ldots, f(P_n)) \mid f \in \mathcal{L}(G)\}$. By Riemann's Theorem, $k = \deg(G) + 1 - g(\mathbb{F})$, since for any divisor G' it holds that $\mathcal{L}(G') = \{0\}$ if $\deg(G') < 0$, it follows that $d \geq n + 1 - \deg(G)$. The distance of its dual code can be estimated using the Residue Theorem.

Define $N_q(g)$ as the maximum of $|\mathbb{P}_q(\mathbb{F})|$ where $\mathbb{F}$ ranges over all the function fields whose full field of constants is $\mathbb{F}_q$ and whose genus is g. The *Drinfeld-Vladuts upper bound* (see e.g. [27] or [29]) states that for all finite fields $\mathbb{F}_q$, *Ihara's constant* $A(q) \equiv \limsup_{g \to \infty} \frac{N_q(g)}{g(\mathbb{F})}$, satisfies $A(q) \leq \sqrt{q} - 1$. Note that the *Hasse-Weil bound* (see e.g. [27]) states that $||\mathbb{P}_q(\mathbb{F})| - (q + 1)| \leq 2 \cdot g(\mathbb{F}) \sqrt{q}$.

3 Connecting Secret Sharing and Codes

We describe one connection between secret sharing and codes that is particularly relevant to this work. Let C be a linear code over $\mathbb{F}_q$ with $n(C) \geq 1$. Let $i \in \mathcal{I}(C)$. Under further conditions on C to be formulated precisely later on, consider the following perfect secret sharing scheme, denoted $\Sigma(C, i)$, on the player set $\mathcal{P} = \mathcal{I}(C) \setminus \{i\}$. Let $s \in \mathbb{F}_q$ be the secret, and choose $\mathbf{c} = (c_0, c_1, \ldots, c_n) \in C$ uniformly at random such that $c_i = s$. For all $j \in \mathcal{I}(C) \setminus \{i\}$ the share for the j-th player is c_j. In [7] this approach to secret sharing [23, 24] is exploited to achieve LSSS with multiplication (*no* strong multiplication), t-privacy and r-reconstruction and with very good asymptotic properties over fixed finite fields. While in [7] privacy and reconstruction parameters of these LSSS are bounded exclusively in terms of the minimum distance of the codes involved, in the present paper we need a more accurate understanding of these parameters. This is what we will develop first.

DEFINITION 1 *Let n be an integer with $n \geq 1$ and let $\mathbb{F}_q$ be a finite field. For a non-empty set $B \subset \{0, 1, \ldots, n\}$, the $\mathbb{F}_q$-linear projection map π_B is defined as $\pi_B^{q,n+1} : C \longrightarrow \mathbb{F}_q^{|B|}$, $(c_0, c_1, \ldots, c_n) \mapsto (c_i)_{i \in B}$. When q and n are clear from the context, we write π_B instead. Also, if $B = \{i\}$ for some index i, we write π_i instead of $\pi_{\{i\}}$.*

LEMMA 1 *Let C be a linear code over $\mathbb{F}_q$ with $n(C) \geq 1$. Let $i \in \mathcal{I}(C)$ and let $B \subset \mathcal{I}(C) \setminus \{i\}$ be a non-empty set. Then there exists a function $\rho_{B,i} : \pi_B(C) \longrightarrow \mathbb{F}_q$ such that $\rho_{B,i}(\pi_B(\mathbf{c})) = \pi_i(\mathbf{c})$ for all $\mathbf{c} \in C$ if and only if $\pi_B(\mathbf{c}) \neq \mathbf{0}$ for all $\mathbf{c} \in C$ with $\pi_i(\mathbf{c}) \neq 0$. If such function $\rho_{B,i}$ exists, it is an $\mathbb{F}_q$-linear map.*

PROOF. In the forward direction, suppose $\rho_{B,i}$ exists. Then it is an $\mathbb{F}_q$-linear map, since $\rho_{B,i}(\lambda\mathbf{c} + \mu\mathbf{c}') = \lambda \cdot \rho_{B,i}(\mathbf{c}) + \mu \cdot \rho_{B,i}(\mathbf{c}')$ for all $\lambda, \mu \in \mathbb{F}_q$, $\mathbf{c}, \mathbf{c}' \in C$, by linearity of C. Suppose there is $\mathbf{c} \in C$ with $\pi_i(\mathbf{c}) \neq 0$ and $\pi_B(\mathbf{c}) = \mathbf{0}$. Then, by $\mathbb{F}_q$-linearity of the map, $\rho_{B,i}(\pi_B(\mathbf{c})) = \rho_{B,i}(\mathbf{0}) = 0 \neq \pi_i(\mathbf{c})$, a contradiction. In the other direction, suppose $\rho_{B,i}$ does not exist. Then there exist $\mathbf{c}, \mathbf{c}' \in C$ such that $\pi_i(\mathbf{c}) \neq \pi_i(\mathbf{c}')$ yet $\pi_B(\mathbf{c}) = \pi_B(\mathbf{c}')$. Then $\pi_i(\mathbf{c} - \mathbf{c}') \neq 0$ and $\pi_B(\mathbf{c} - \mathbf{c}') = \mathbf{0}$ by linearity of C. △

Note that by linearity of C, the lemma above also holds when $\pi_i(\mathbf{c}) \neq 0$ is replaced by $\pi_i(\mathbf{c}) = 1$.

DEFINITION 2 *Notation being as in Lemma 1, we say that (i, B) is a* reconstruction-pair *if $\rho_{B,i}$ exists.*

COROLLARY 1 *Let C be a linear code over $\mathbb{F}_q$ with $n(C) \geq 1$ and let $i \in \mathcal{I}(C)$. Let $\mathbf{u}_i \in \mathbb{F}_q^{n(C)+1}$ denote the i-th unit vector, i.e., $(\mathbf{u}_i)_j = 1$ if $i = j$ and $(\mathbf{u}_i)_j = 0$ if $i \neq j$. Then:*

- *$(i, \mathcal{I}(C) \setminus \{i\})$ is a reconstruction-pair if and only if $\mathbf{u}_i \notin C$.*
- *$\pi_i(C) \neq \{0\}$ if and only if $\mathbf{u}_i \notin C^\perp$.*

– *For all* $j \in \mathcal{I}(C)$, $(j, \mathcal{I}(C) \setminus \{j\})$ *is a reconstruction-pair and* $\pi_j(C) \neq \{0\}$ *if and only if* $d_{min}(C) > 1$ *and* $d_{min}(C^\perp) > 1$.

DEFINITION 3 *Let* C *be a code over* $\mathbb{F}_q$ *with* $n(C) \geq 1$. *Let* $i \in \mathcal{I}(C)$ *and suppose* $\mathbf{u}_i \notin C$. *If* $\mathbf{u}_i \in C^\perp$, *then define* $r_i(C) = 0$. *Else, define* $r_i(C)$ *as the smallest positive integer* ρ_i *such that for all* $B \subset \mathcal{I}(C) \setminus \{i\}$ *with* $|B| = \rho_i$ *it holds that* (i, B) *is a reconstruction-pair.*

Note that by Corollary 1, the value $r_i(C)$ is well-defined, and satisfies $0 \leq r_i(C) \leq n(C)$.

DEFINITION 4 *Let* C *be a code over* $\mathbb{F}_q$ *with* $n(C) \geq 1$. *Let* $i \in \mathcal{I}(C)$ *and suppose* $\mathbf{u}_i \notin C^\perp$. *Define* $t_i(C)$ *as the largest positive integer* τ_i *such that for each set* $A \subset \mathcal{I}(C) \setminus \{i\}$ *with* $|A| = \tau_i$ *it holds that* (i, A) *is not a reconstruction-pair. Equivalently, this is satisfied if and only if there exists* $\mathbf{c} \in C$ *with* $\pi_i(\mathbf{c}) = 1$ *and* $\pi_A(\mathbf{c}) = \mathbf{0}$. *If no such integer exists,* $t_i(C) = 0$ *by definition.*

Note that by Corollary 1, the value $t_i(C)$ is well-defined, and satisfies $0 \leq t_i(C) < n(C)$.

LEMMA 2 *Let* C *be a linear code over* $\mathbb{F}_q$ *such that* $\{\mathbf{0}\} \subsetneq C, C^\perp \subsetneq \mathbb{F}_q^{n(C)+1}$. *Then* $d_{min}(C^\perp) = m + 1$, *where* m *is the largest positive integer such that for all non-empty sets* $B \subset \{0, 1, \ldots, n\}$ *with* $|B| = m$, *it holds that* $\pi_B(C) = \mathbb{F}_q^{|B|}$.

PROOF. The conditions imply that $n(C) \geq 1$. Write $d^\perp = d_{\min}(C^\perp)$. For a non-empty set $B \subset \mathcal{I}(C)$, write $W_B = \pi_B(C) \subset \mathbb{F}_q^{|B|}$. Clearly, $W_B \neq \mathbb{F}_q^{|B|}$ if and only if $W_B^\perp \neq \{\mathbf{0}\}$. This latter condition equivalent to the existence of some $\mathbf{c}^* \in C^\perp \setminus \{\mathbf{0}\}$ with $\mathrm{supp}(\mathbf{c}^*) \subset B$, for which we have that $w_H(\mathbf{c}^*) \leq |B|$. Thus, for all $B \subset \mathcal{I}(C)$ with $|B| \leq d^\perp - 1$, it must hold that $W_B = \mathbb{F}_q^{n+1}$. On the other hand, since $C^\perp \neq \{\mathbf{0}\}$, an element $\mathbf{c}^* \in C^\perp \setminus \{\mathbf{0}\}$ can be selected with minimal weight $d^\perp$. Define $B = \mathrm{supp}(\mathbf{c}^*)$. Then $|B| = d^\perp$, and by the characterization above, $W_B \neq \mathbb{F}_q^{n+1}$. △

LEMMA 3 *Let* C *be a code over* $\mathbb{F}_q$ *with* $n(C) \geq 1$ *and let* $i \in \mathcal{I}(C)$. *Then:*

1. *If* $\mathbf{u}_i \notin C$, *then* $r_i(C) \leq n(C) - d_{min}(C) + 2$.
2. *If* $d_{min}(C) > 1$, *then* $\max_{j \in \mathcal{I}(C)} r_j(C) = n(C) - d_{min}(C) + 2$.
3. *If* $\mathbf{u}_i \notin C^\perp$, *then* $d_{min}(C^\perp) - 2 \leq t_i(C)$.
4. *If* $d_{min}(C^\perp) > 1$ *then* $d_{min}(C^\perp) - 2 = \min_{i \in \mathcal{I}(C)} t_i(C)$.

PROOF. As to Claim 1,if $d_{\min}(C) \leq 2$, there is nothing to prove. Else, if we "prune" the code C at $d_{\min}(C) - 2$ coordinates (not including i), then we get a code C' with $d_{\min}(C') > 1$. The claim now follows from Corollary 1. As to Claim 2, $d_{\min}(C) > 1$, then r_i is well-defined for all $i \in \mathcal{I}(C)$. Select an element $\mathbf{c}$ in C of minimal weight $d_{\min}(C)$. Take any $i \in \mathrm{supp}(\mathbf{c})$ and define $B = \mathcal{I}(C) \setminus \mathrm{supp}(\mathbf{c})$. Clearly $|B| = n(C) - d_{\min}(C) + 1$ and (i, B) is not a reconstruction-pair because $\pi_i(\mathbf{c}) \neq 0$ and $\pi_B(\mathbf{c}) = 0$. Therefore $r_i(C) \geq n(C) - d_{\min}(C) + 2$,

which was what remained to be proved. As to Claim 3, this follows directly from Lemma 2. As to Claim 4, if $d_{\min}(C^{\perp}) > 1$, then t_i is well-defined for all $i \in \mathcal{I}(C)$. So if $B \subset \mathcal{I}(C)$ is any set with $|B| = 1 + \min_{i \in \mathcal{I}(C)} t_i(C)$, then for each $j \in B$ there exists $\mathbf{c} \in C$ such that $\pi_j(\mathbf{c}) = 1$ and $\pi_{B'}(\mathbf{c}) = \mathbf{0}$, where $B' = B \backslash \{j\}$. Thus, $\pi_B(C) = \mathbb{F}_q^{|B|}$, and by Lemma 2, $|B| = 1 + \min_{i \in \mathcal{I}(C)} t_i(C) \leq d_{\min}(C^{\perp}) - 1$. Hence, $d_{\min}(C^{\perp}) - 2 \geq \min_{i \in \mathcal{I}(C)} t_i(C)$, which was what remained to be proved. $\triangle$

DEFINITION 5 *Let C be a linear code over $\mathbb{F}_q$ with $n(C) \geq 1$. We define $I(C)$ as the set consisting of all indices $i \in \mathcal{I}(C)$ such that $\mathbf{u}_i \notin C$ and $\mathbf{u}_i \notin C^{\perp}$. $\mathcal{C}(\mathbb{F}_q)$ is the collection of all linear codes C over $\mathbb{F}_q$ such that $I(C) \neq \emptyset$.*

Note that $I(C) \neq \emptyset$ implies $n(C) \geq 1$ and that $I(C) = \mathcal{I}(C)$ if and only if $d_{\min}(C) > 1$ and $d_{\min}(C^{\perp}) > 1$. For completeness we state the following straightforward characterization of $\mathcal{C}(\mathbb{F}_q)$. If C is a linear code over $\mathbb{F}_q$ with $n(C) \geq 1$ and if $I(C) = \emptyset$, then it holds for all $i \in \mathcal{I}(C)$ that the i-th coordinate of elements of C is always equal to zero or that the i-th unit vector $\mathbf{u}_i \in C$. After permutating indices, if necessary, the set C is then equal to a Cartesian product $\mathbb{F}_q \times \cdots \times \mathbb{F}_q \times \{\mathbf{0}\} \times \cdots \times \{\mathbf{0}\}$. On the other hand, if C decomposes as above, then clearly $I(C) = \emptyset$.

THEOREM 1 *Let $C \in \mathcal{C}(\mathbb{F}_q)$ and let $i \in I(C)$. Suppose $\mathbf{c} \in C$ is chosen uniformly at random. Then the following holds.*

1. *$\pi_i(C) \in \mathbb{F}_q$ has the uniform distribution.*
2. *("r-reconstruction") If $B \subset \mathcal{I}(C) \setminus \{i\}$ with $|B| \geq r_i(C)$, then $\pi_B(\mathbf{c})$ determines $\pi_i(\mathbf{c})$ uniquely with probability 1. Thus, $\Sigma(C, i)$ has $r_i(C)$-reconstruction.*
3. *If $d_{min}(C) > t + 1$ for some positive integer t, then $\Sigma(C, i)$ has $(n - t)$-reconstruction.*
4. *("t-privacy") Suppose $t_i(C) \geq 1$. If $A \subset \mathcal{I}(C) \setminus \{i\}$ is non-empty and $|A| \leq t_i(C)$, then $\pi_i(\mathbf{c})$ has the uniform distribution on $\mathbb{F}_q$ and $\pi_A(\mathbf{c})$ is distributed independently from $\pi_i(\mathbf{c})$. Thus, $\Sigma(C, i)$ has $t_i(C)$-privacy.*
5. *If $d_{min}(C^{\perp}) > t + 1$ for some positive integer t, then $\Sigma(C, i)$ has t-privacy.*
6. *Suppose $d_{min}(C^{\perp}) > 1$. The largest positive integer m such that for all $A \subset \mathcal{I}(C)$ with $|A| = m$ it holds that $\pi_A(\mathbf{c}) \in \mathbb{F}_q^{|A|}$ has the uniform distribution, satisfies $m = d_{min}(C^{\perp}) - 1$.*

PROOF. As to Claim 1, $i \in I(C)$ implies in particular that for each $x \in \mathbb{F}_q$ there exists $\mathbf{c} \in C$ such that $\pi_i(\mathbf{c}) = x$. Moreover, their number is equal to the cardinality of the kernel of the map π_i. Hence this number does not depend on x and the claim follows. Claim 2 follows from the definition of $r_i(C)$. As to Claim 3, this follows from Lemma 3 plus pruning. As to Claim 4, if $|A| \leq t_i(C)$, then there exists $\mathbf{c}'' \in C$ with $\pi_i(\mathbf{c}'') = 1$ and $\pi_A(\mathbf{c}'') = \mathbf{0}$. This implies that for each $(x, \mathbf{y})$ with $x \in \mathbb{F}_q$ and $\mathbf{y} \in \pi_B(C)$, there exists $\mathbf{c}'' \in C$ with $\pi_i(\mathbf{c}'') = x$ and $\pi_A(\mathbf{c}'') = \mathbf{y}$. More precisely, their number is equal to the cardinality of the kernel of the map $\pi_{A \cup \{i\}}$, and the claim follows. As to Claim 5, this follows from

Lemma 3. As to Claim 6, by Lemma 2 it holds that for each $\mathbf{y} \in \mathbb{F}_q^{|A|}$, there exists $\mathbf{c} \in C$ with $\pi_A(\mathbf{c}) = \mathbf{y}$. Their number is equal to the cardinality of the kernel of the map π_A, and, as maximality also follows from Lemma 2, the claim follows. $\triangle$

REMARK 1 *Let $C \in \mathcal{C}(\mathbb{F}_q)$ and let $i \in I(C)$. Then $\Sigma(C, i)$ can be viewed as an LSSS.*

PROOF. Assume for simplicity in notation that $i = 0$. Choose a generator matrix G for the code C, i.e., a matrix with k columns and $n+1$ rows such that the columns jointly constitute an $\mathbb{F}_q$- basis of C. Write $\mathbf{v}_0$ for the top row, write $\mathbf{v}_i$ for the i-th row below, and write V_i for the $\mathbb{F}_q$-vector space spanned by it, which is one-dimensional as $\mathbf{v}_i \neq \mathbf{0}$ $(i = 1 \ldots n)$. Since $d_{\min}(C) > 1$, it follows by Lemma 1 that there exists a vector $\mathbf{x} = (x_0, x_1, \ldots, x_n)^T \in \mathbb{F}_q^{n+1}$ such that $G^T\mathbf{x} = \mathbf{0}$ and $x_0 = 1$, where G^T denotes the transpose of G. Thus, $\mathbf{v}_0$ is in the $\mathbb{F}_q$-linear span of the $\mathbf{v}_i$, $i = 1, \ldots, n$. The parameter e from the LSSS definition is equal to k, the dimension of C. Thus, $(\mathbb{F}_q, n, e, \mathbf{v}_0, V_1, \ldots, V_n)$ thus defined is an LSSS by definition. The secret sharing scheme it generates (see Section 2) is identical to choosing $\mathbf{b} \in \mathbb{F}_q^{n+1}$ at random and setting $(s_0, s_1, \ldots, s_n)^T = G\mathbf{b}$. Since G is a generator matrix of C, this secret sharing scheme is identical to $\Sigma(C, i)$. $\triangle$

4 Strongly Multiplicative LSSS from Codes

In this section we define a special class of codes that imply strongly multiplicative LSSS.

DEFINITION 6 *For $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n, \mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$, their* Schur-product $\mathbf{x} * \mathbf{y} \in \mathbb{F}_q^n$ *is defined as $(x_1y_1, \ldots, x_ny_n)$. Let C be a linear code over $\mathbb{F}_q$. The linear code $\widehat{C}$ over $\mathbb{F}_q$ is the linear code $\mathbb{F}_q < \{\mathbf{x} * \mathbf{y}\}_{\mathbf{x},\mathbf{y} \in C} >$, i.e., the $\mathbb{F}_q$-linear span of the vectors of the form $\mathbf{x} * \mathbf{y}$ with $\mathbf{x}, \mathbf{y} \in C$.*

LEMMA 4 *Let C be a linear code over $\mathbb{F}_q$ with $n(C) \geq 1$ and let $i \in \mathcal{I}(C)$. Then: 1) $n(\widehat{C}) = n(C)$. 2) $\mathbf{u}_i \notin \widehat{C}$ implies $\mathbf{u}_i \notin C$. 3) $\mathbf{u}_i \notin C^\perp$ if and only if $\mathbf{u}_i \notin (\widehat{C})^\perp$. 4) $I(\widehat{C}) \subset I(C)$. 5) $1 \leq d_{min}(\widehat{C}) \leq d_{min}(C)$.*

Generally, $\mathbf{u}_i \notin C$ does not necessarily imply $\mathbf{u}_i \notin \widehat{C}$.

DEFINITION 7 *$\mathcal{C}^\dagger(\mathbb{F}_q)$ denotes the set of all $\mathbb{F}_q$-linear codes C with $I(\widehat{C}) \neq \emptyset$.*

Note that $\mathcal{C}^\dagger(\mathbb{F}_q) \neq \emptyset$ for all finite fields $\mathbb{F}_q$.

DEFINITION 8 *For $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$, $\widehat{t}(C) = \max_{i \in I(\widehat{C})} \min\{t_i(C), n(\widehat{C}) - r_i(\widehat{C})\}$. The LSSS $\Sigma(C)$ is by definition $\Sigma(C, i)$ where i is the smallest index where this maximum is attained. Write i_s for this index.*

Note that $r_i(\widehat{C})$ is well-defined in the definition of $\widehat{t}(C)$ since $\widehat{C} \in \mathcal{C}(\mathbb{F}_q)$ and $i \in I(\widehat{C})$.

Generally, $C \in \mathcal{C}(\mathbb{F}_q)$ does not even need to imply $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$. In fact, only for special classes of codes one seems to be able to bound $\widehat{t}(C)$ non-trivially, sometimes in combination with this Corollary to Theorem 1.

COROLLARY 2 *Let $C \in C^\dagger(\mathbb{F}_q)$. Suppose that $d_{min}(C^\perp) > t+1$ and $d_{min}(\widehat{C}) > t+1$ for some integer $t \geq 1$. Then $\widehat{t}(C) \geq t$.*

LEMMA 5 *Let e be a positive integer. Then:*

- $\langle \mathbf{v} \otimes \mathbf{w}, \mathbf{a} \otimes \mathbf{b} \rangle = \langle \mathbf{v}, \mathbf{a} \rangle \cdot \langle \mathbf{w}, \mathbf{b} \rangle$, *for all* $\mathbf{v}, \mathbf{w}, \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^e$.
- *Let* $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^{e^2}$. *Then* $\mathbf{x} = \mathbf{y}$ *if and only if* $\langle \mathbf{x}, \mathbf{a} \otimes \mathbf{b} \rangle = \langle \mathbf{y}, \mathbf{a} \otimes \mathbf{b} \rangle$ *for all* $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^e$.

PROOF. The definitions of tensor product and scalar product imply the first claim. The second follows by combination of the bilinearity of the scalar product and the facts that the $\mathbb{F}_q$-linear span of the vectors $\mathbf{a} \otimes \mathbf{b}$ with $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^e$ is equal to $\mathbb{F}_q^{e^2}$ and that the scalar-product with a given vector is always zero if and only if that vector equals the zero-vector. $\triangle$

THEOREM 2 *Let $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$. Suppose $\widehat{t}(C) \geq 1$ and let t be an integer with $1 \leq t \leq \widehat{t}(C)$. Then: $t \leq \frac{1}{3} \cdot (n(C) - 1)$, $\Sigma(C)$ has $(n(C) - 2t)$-reconstruction, and $\Sigma(C)$ has t-strong multiplication.*

PROOF. We first argue t-strong multiplication. Assume w.l.o.g. that $i_s = 0$ (Definition 8). By Theorem 1, $\Sigma(C)$ satisfies t-privacy. Write $n = n(\widehat{C})$ $(= n(C))$. Since $\widehat{t}(C) \geq 1$, $r_0(\widehat{C}) < n$. Now choose a generator matrix G for C. Write $\mathbf{v}_0$ for its top row, write $\mathbf{v}_i$ for the i-th row below and write V_i for the one-dimensional space V_i spanned by it, $i = 1 \ldots n$. Let $B \subset \{1, \ldots, n\}$ be a nonempty set. First, note that there exists a vector $\lambda \in \mathbb{F}_q^n$ such that $\sum_{i \in B} \pi_i(\lambda)(\mathbf{v}_i \otimes \mathbf{v}_i) = \mathbf{v}_0 \otimes \mathbf{v}_0$ if and only if $\langle \sum_{i \in B} \pi_i(\lambda)(\mathbf{v}_i \otimes \mathbf{v}_i), \mathbf{b} \otimes \mathbf{b}' \rangle = \langle \mathbf{v}_0 \otimes \mathbf{v}_0, \mathbf{b} \otimes \mathbf{b}' \rangle$ for all $\mathbf{b}, \mathbf{b}' \in \mathbb{F}_q^e$. Indeed, the forward direction follows by rewriting and the reverse direction follows from Lemma 5 (2nd item). By re-writing and by using Lemma 5 (1st item), this is equivalent to $\sum_{i \in B} \pi_i(\lambda) \langle \mathbf{v}_i, \mathbf{b} \rangle \langle \mathbf{v}_i, \mathbf{b}' \rangle = \langle \mathbf{v}_0, \mathbf{b} \rangle \langle \mathbf{v}_0, \mathbf{b}' \rangle$ for all $\mathbf{b}, \mathbf{b}' \in \mathbb{F}_q^e$. This may be rewritten as $\langle (G\mathbf{b}) * (G\mathbf{b}'), \mathbf{y} \rangle = 0$ for all $\mathbf{b}, \mathbf{b}' \in \mathbb{F}_q^e$, where $\pi_0(\mathbf{y}) = -1$, $\pi_i(\mathbf{y}) = \pi_i(\lambda)$ if $i \in B$, and $\pi_i(\mathbf{y}) = 0$ for all other indices. Equivalently, $\sum_{i \in B} \lambda_i \pi_i(\mathbf{c}) \pi_i(\mathbf{c}') = \pi_0(\mathbf{c}) \pi_0(\mathbf{c}')$ for all $\mathbf{c}, \mathbf{c}' \in C$, since G is a generator matrix of C. By definition of t, there exists, for each choice of B with $|B| = n - t$, a vector $\lambda \in \mathbb{F}_q^n$ such that the latter condition is satisfied for the set B. We conclude that t-strong multiplication holds, as desired. As to the remaining claims, let $B \subset \{1, \ldots, n\}$ be such that $|B| = n - 2t$. Write $A = \{1, \ldots, n\} \setminus B$. Choose a disjoint partition $A_0 \cup A_1 = A$ with $|A_0| = |A_1| = t$. By Lemma 2 there exists $\mathbf{c}' \in C$ such that $\pi_0(\mathbf{c}') = 1$ and $\pi_{A_0}(\mathbf{c}') = \mathbf{0}$. Let $\mathbf{c} \in C$ be arbitrary and consider the vector $\mathbf{c} * \mathbf{c}' \in \widehat{C}$. Note that this vector has coordinates equal to zero at those indices i with $i \in A_0$. Since $\widehat{C}$ has $(n - t)$-reconstruction,

there exists a vector $\mathbf{x} \in \mathbb{F}_q^n$ such that it has coordinates equal to zero at those indices i with $i \in A_1$ and $\pi_0(\mathbf{c} * \mathbf{c}') = \sum_{i=1}^{n} \pi_i(\mathbf{x})\pi_i(\mathbf{c} * \mathbf{c}')$. It now follows that $\pi_0(\mathbf{c}) = \sum_{i \in B}(\pi_i(\mathbf{x}) \cdot \pi_i(\mathbf{c}'))\pi_i(\mathbf{c})$, for all $\mathbf{c} \in C$. Thus, there is $(n-2t)$-reconstruction. Since there is also t-privacy, it follows that $t \leq \frac{1}{3}(n(C)-1)$. Finally, the remark about fulfilment of the conditions follows from Theorem 1. $\triangle$

We introduce the notion of asymptotic optimal corruption tolerance for the class of codes $\mathcal{C}^\dagger(\mathbb{F}_q)$.

DEFINITION 9 *Let $\mathbb{F}_q$ be a finite field. For $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$, we define $\widehat{\tau}(C) = \frac{3 \cdot \widehat{t}(C)}{n(C)-1}$. We call value $\widehat{\tau}(C)$ the* corruption tolerance *of the code C.*

Note that $0 \leq \widehat{\tau}(C) \leq 1$ always, where the upper bound follows from Theorem 2. Let t, n be positive integers with $3t < n$ and let $\mathbb{F}_q$ be a finite field with $q > n$. If C is a polynomial evaluation code ("Reed-Solomon code") over $\mathbb{F}_q$ of length $n+1$, defined from evaluation of the polynomials of degree at most t, then $\widehat{\tau}(C) = 1$, and, of course, $\Sigma(C)$ is Shamir's $(n, t+1, t)$-threshold LSSS.

DEFINITION 10 *(*Asymptotic optimal corruption tolerance*). Let $\mathbb{F}_q$ be a finite field. Then we define $\widehat{\tau}(q) = \limsup_{C \in \mathcal{C}^\dagger(\mathbb{F}_q)} \widehat{\tau}(C)$.*

Note that $\widehat{\tau}(C) = 1$ implies that $\Sigma(C)$ is an $(n, t+1, t)$-threshold LSSS over $\mathbb{F}_q$, with $n = 3t+1$. For fixed q there are only finitely many $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$ such that $\widehat{\tau}(C) = 1$ (the proof for this statement is easily extracted from [8]; in fact, in Section 8 we prove a stronger statement). Since for each length there are only a finite number of codes of that length when $\mathbb{F}_q$ is constant, this means that for each $\epsilon > 0$ there exists an infinite family of codes $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$ with $\ell(C)$ tending to infinity and $|\widehat{\tau}(q) - \widehat{\tau}(C)| < \epsilon$.

5 Bounding $\widehat{\tau}(q)$ Away from Zero for Arbitrary $\mathbb{F}_q$

The main result of this section is the fact that $\widehat{\tau}(q) > 0$ for every finite field $\mathbb{F}_q$. First, we need to restate and reprove part of the results (Theorems 3 and 6) of [8] on algebraic geometric strongly multiplicative secret sharing in the technical framework of the present paper. Throughout this section $\mathbb{F}_q$ denotes the finite field with q elements.

THEOREM 3 *(Chen and Cramer [8]) Let $\mathbb{F}$ be an algebraic function field over $\mathbb{F}_q$. Suppose $|\mathbb{P}_q(\mathbb{F})| > 4(g(\mathbb{F})+1)$. Let t, n be any integers such that $1 \leq t < n$, $|\mathbb{P}_q(\mathbb{F})| \geq n+1$, and $3t < n - 4 \cdot g(\mathbb{F})$. Then there exists a code $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$ such that $\ell(C) = n+1$ and $\widehat{t}(C) \geq t$. In particular, $\Sigma(C)$ has t-strong multiplication.*

PROOF. By the condition on $|\mathbb{P}_q(\mathbb{F})|$, there exist integers t, n satisfying the constraints from the theorem. Now fix such t, n. By Corollary 2, it is sufficient to show the existence of $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$ with $\ell(C) = n+1$, $d_{\min}(C^\perp) > t+1$

and $d_{\min}(\widehat{C}) > t+1$. Write $g = g(\mathbb{F})$. Let $P_0, P_1, \ldots, P_n \in \mathbb{P}_q(\mathbb{F})$ be distinct places of degree 1, and define the divisor $D = \sum_{i=0}^{n} P_i$. Choose a divisor G with $\mathrm{supp}(G) \cap \mathrm{supp}(D) \neq \emptyset$ and $\deg(G) = 2g + t$. This is possible by the Weak Approximation Theorem (see e.g. [27]). Alternatively, in case $|\mathbb{P}_q(\mathbb{F})| > n+1$, select a place $Q \in \mathbb{P}_q(\mathbb{F}) \setminus \{P_0, P_1, \ldots, P_n\}$ and define $G = (2g+t) \cdot Q$. In any case, it holds that $\dim_{\mathbb{F}_q}(\mathcal{L}(G)) = g+t+1$. Next, define C as the evaluation code $C(D;G)$. Arbitrarily choose $i \in \{0,1,\ldots n\}$, $A \subset \{0,1,\ldots n\} \setminus \{i\}$ with $|A| = t$. Since $2g-2 < \deg(G - P_i - \sum_{j\in A} P_j) < \deg(G - \sum_{j\in A} P_j)$, it holds that $\dim_{\mathbb{F}_q}(\mathcal{L}(G - P_i - \sum_{j\in A} P_j)) < \dim_{\mathbb{F}_q}(\mathcal{L}(G - \sum_{j\in A} P_j))$. Hence, there exists $f \in \mathcal{L}(G)$ such that $f(P_i) = 1$ and $f(P_j) = 0$ for all $j \in A$. In particular, for C as well as for $\widehat{C}$ it holds that the i-th coordinate is not always zero. Second, since $f \cdot g \in \mathcal{L}(2G)$ if $f, g \in \mathcal{L}(G)$, it follows that $\widehat{C} \subset C(D;2G)$. From $\deg(2G) = 4g+2t$ and $4g < n-3t$, it follows that $d_{\min}(\widehat{C}) \geq n+1-\deg(2G) = n+1-(4g+2t) > t+1$. In particular, it follows that $\mathbf{u}_i \notin \widehat{C}$. We conclude that $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$ and $I(C) = \mathcal{I}(C)$, and using Theorem 1, that $t \leq \min_{0\leq j\leq n} t_j(C) = d_{\min}(C^{\perp}) - 2$. Hence $d_{\min}(C^{\perp}) > t+1$. By Corollary 2, $\widehat{t}(C) \geq t$. The claim about t-strong multiplicativity of $\Sigma(C)$ follows from Theorem 2. $\triangle$

It follows from this theorem that $\widehat{\tau}(q) > 0$ if $A(q) > 4$, where $A(q)$ is Ihara's constant (see Section 2). Recall that the Drinfeld-Vladuts bounds states that $A(q) \leq \sqrt{q} - 1$. For our purposes, however, we need a lower bound. Ihara [18] has shown that if q is a square, then $A(q) \geq \sqrt{q} - 1$, so that the Drinfeld-Vladuts bound is sharp. Later, Garcia and Stichtenoth [15] showed this result by more explicit methods (see also [1] for recent results over cubic fields).

THEOREM 4 *(Ihara [18], Garcia and Stichtenoth [15]) Let $\mathbb{F}_q$ be a finite field and let q be a square. Then $A(q) = \sqrt{q} - 1$. More precisely, there exists an infinite family of algebraic function fields (in one variable) $\{\mathbb{F}^{(m)}\}_{m\geq 1}$ over $\mathbb{F}_q$ such that for all $m \geq 1$, $\mathbb{F}_q$ is the full constant field of $\mathbb{F}^{(m)}$, $|\mathbb{P}_q(\mathbb{F}^{(m)})| \geq (q - \sqrt{q})\sqrt{q}^{m-1}$ and $g(\mathbb{F}^{(m)}) \leq \sqrt{q}^m$.*

THEOREM 5 *(Serre [25]) There exists a positive constant $c_* \in \mathbb{R}$ such that for all finite fields $\mathbb{F}_q$ we have $A(q) \geq c_* \cdot \log q$.*

Combining Theorems 3, 4 and 5, we can bound $\widehat{\tau}(q)$ away from zero if either q is a square or q is extremely large [6]. Also, we see that $\widehat{\tau}(q)$ tends to 1 if $|\mathbb{F}_q|$ tends to infinity.

THEOREM 6 *(Chen and Cramer [8])*

- *$\widehat{\tau}(q) \geq 1 - \frac{4}{A(q)}$ if $\mathbb{F}_q$ is a finite field with $A(q) > 4$. In particular, $A(q) > 4$ if q is large enough, more precisely, if $q > 2^{\frac{4}{c}}$. Here, $c \in \mathbb{R}$ is any positive constant so that Theorem 5 holds with $c_* = c$.*[7].

[6] The results in [8] only considered the case $q \geq 49$ with q a square. But the combination of Theorem 3 with Theorem 5 is straightforward, so we attribute that in essence to [8].

[7] Currently, $c_* \geq \frac{1}{91}$ is the best known approximation, see [29]

– $\widehat{\tau}(q) \geq 1 - \frac{4}{\sqrt{q}-1}$ *for all finite fields* $\mathbb{F}_q$ *such that* $q \geq 49$ *and* q *is a square.*
– $\lim_{|\mathbb{F}_q| \to \infty} \widehat{\tau}(q) = 1$, *where* $\mathbb{F}_q$ *ranges over all finite fields.*

Thus, it remains to bound $\widehat{\tau}(q)$ away from zero in the cases where q is small ($2 \leq q < 49$) or $q > 49$ is not a square and q is at most moderately large. We resolve this by means of a dedicated field-descent that allows us to lower bound $\widehat{\tau}(q)$ as a function of $\widehat{\tau}(q^m)$. At its heart it uses the following notion.

DEFINITION 11 *A* multiplication-friendly embedding of the extension field $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ *is a triple* (r, σ, ψ) *where* r *is a positive integer and where* $\sigma : \mathbb{F}_{q^m} \to \mathbb{F}_q^r$ *and* $\psi : \mathbb{F}_q^r \to \mathbb{F}_{q^m}$ *are* $\mathbb{F}_q$*-linear maps such that* $xy = \psi(\sigma(x) * \sigma(y))$ *for all* x, y *in* $\mathbb{F}_{q^m}$. *The integer* r *is called the* expansion.

Note that σ is an *injective* $\mathbb{F}_q$-linear map between $\mathbb{F}_q$-vectorspaces: $\sigma(x) = \sigma(y)$ implies $x = x \cdot 1 = \psi(\sigma(x) * \sigma(1)) = \psi(\sigma(y) * \sigma(1)) = y \cdot 1 = y$. Note that this notion has been studied in the context of asymptotic arithmetic complexity (see [4] and [28]). We can now state and prove our field-descent theorem. Elementary constructions of multiplication-friendly embeddings are given afterwards.

THEOREM 7 *Let* t, r *be integers with* $t, r \geq 1$. *Suppose* $C \in \mathcal{C}^\dagger(\mathbb{F}_{q^m})$ *with* $\widehat{t}(C) \geq t$ *and suppose there exists a multiplication-friendly embedding of* $\mathbb{F}_{q^m}$ *over* $\mathbb{F}_q$ *with expansion* r. *Then there exists* $C_1 \in \mathcal{C}^\dagger(\mathbb{F}_q)$ *such that* $n(C_1) = r \cdot n(C)$ *and* $\widehat{t}(C_1) \geq t$.

PROOF. Write $n = n(C)$. W.l.o.g., $i_s = 0$ (Definition 8), i.e., $\widehat{t}(C)$ is attained for $i = 0$. In particular, $0 \in I(\widehat{C})$. Let π_B denote the projection $\pi_B^{(q^m, n+1)}$ and let π'_B denote the projection $\pi_B^{(q, rn+1)}$ (Definition 1). For an index-set $\mathcal{I}()$, $\mathcal{I}^*()$ denotes $\mathcal{I}() \setminus \{0\}$. Consider the set $G = C \cap (\mathbb{F}_q \bigoplus (\mathbb{F}_{q^m})^n)$, i.e., all $\mathbf{c} \in C$ with $\pi_0(\mathbf{c}) \in \mathbb{F}_q$. Note that $G \neq \emptyset$, G is not an $\mathbb{F}_{q^m}$-linear code, but G is an $\mathbb{F}_q$-linear subspace of the $\mathbb{F}_{q^m}$-linear code C. Let (r, σ, ψ) be a multiplication-friendly embedding of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Define the $\mathbb{F}_q$-linear map $\chi : \mathbb{F}_q \bigoplus (\mathbb{F}_{q^m})^n \to (\mathbb{F}_q)^{1+rn}$ by $(c_0, c_1, \ldots, c_n) \mapsto (c_0, \sigma(c_1), \ldots, \sigma(c_n))$. Now define the $\mathbb{F}_q$-linear code C_1 as $C_1 = \chi(G) \subset \mathbb{F}_q^{rn+1}$. We first show $C_1 \in C^\dagger(\mathbb{F}_q)$. Write $\mathbf{u}_0 = (1, 0, \ldots, 0) \in \mathbb{F}_q^{n+1}$ and $\mathbf{u}'_0 = (1, 0, \ldots, 0) \in \mathbb{F}_q^{rn+1}$. Since $0 \in I(\widehat{C})$, $\mathbf{u}_0 \notin C^\perp$ by Lemma 4, or equivalently, there is $\mathbf{c} \in G$ with $\pi_0(\mathbf{c}) = 1$. Since $\pi'_0(\chi(\mathbf{c})) = 1$, $\mathbf{u}'_0 \notin (C_1)^\perp$, and by Lemma 4, $\mathbf{u}'_0 \notin (\widehat{C_1})^\perp$. Note that if $\sum_k \sigma(x^{(k)}) * \sigma(y^{(k)}) = \mathbf{0} \in \mathbb{F}_q^r$ for some $x^{(k)}$'s and $y^{(k)}$'s in $\mathbb{F}_{q^m}$, then $\sum_k x^{(k)} \cdot y^{(k)} = \sum_k \psi(\sigma(x^{(k)}) * \sigma(y^{(k)})) = \psi(\sum_k \sigma(x^{(k)}) * \sigma(y^{(k)})) = \psi(\mathbf{0}) = 0 \in \mathbb{F}_{q^m}$. Using this, it is verified easily that $\mathbf{u}'_0 \in \widehat{C_1}$ would imply $\mathbf{u}_0 \in \widehat{C}$, a contradiction. In conclusion, $0 \in I(\widehat{C_1})$ and hence, $I(\widehat{C_1}) \neq \emptyset$. We now show $\widehat{t}(C_1) \geq t$. If we call each $j \in \mathcal{I}^*(C)$ a "parent" index, then, using the definition of χ, each of those $\mathbb{F}_{q^m}$-parent indexes can be said to have r $\mathbb{F}_q$-sibling indexes. If $A \subset \mathcal{I}^*(C_1)$ is a non-empty set, then $\beta(A) \subset \mathcal{I}^*(C)$ denotes the set of parent indexes of these siblings. Note that $|\beta(A)| \leq |A|$. Finally, $\alpha(A) \subset \mathcal{I}^*(C_1)$ denotes the set of all siblings of the elements in $\beta(A)$. Note that $A \subset \alpha(A)$. Now let $A \subseteq \mathcal{I}^*(C_1)$ with $|A| = t$. Since

$|\beta(A)| \leq t \leq t_0(C)$, there exists $\mathbf{c} \in G$ such that $\pi_0(\mathbf{c}) = 1$ and $\pi_{\beta(A)}(\mathbf{c}) = \mathbf{0}$. Since $\pi'_0(\chi(\mathbf{c})) = 1$, $\pi'_{\alpha(A)}(\chi(\mathbf{c})) = \mathbf{0}$, and $A \subset \alpha(A)$, it follows that $t_0(C_1) \geq t$. It remains to prove that $r_0(\widehat{C}_1) \leq rn - t$. Let $A_1 \subset \mathcal{I}^*(\widehat{C}_1)$ with $|A_1| = t$ be an arbitrary set. Since $A_1 \subset \alpha(A_1)$, it will be sufficient to show that $(0, B_1)$ is a reconstruction-pair for $\widehat{C}_1$, where $B_1 = \mathcal{I}^*(\widehat{C_1}) \setminus \alpha(A_1)$. Write $B = \mathcal{I}^*(\widehat{C}) \setminus \beta(A_1)$. Note that $|B| \geq n - t$. Since $r_0(\widehat{C}) \leq n - t$, there exists an $\mathbb{F}_{q^m}$-linear reconstruction function $\rho_{B,0}$ for $\widehat{C}$. We extend the definition of the map ψ as follows: if $\mathbf{x} = (x_0, \mathbf{x}_1, \ldots, \mathbf{x}_n) \in \mathbb{F}_q^{1+rn}$, where $x_0 \in \mathbb{F}_q$ and $\mathbf{x}_1, \ldots, \mathbf{x}_n \in \mathbb{F}_q^r$, then $\overline{\psi}(\mathbf{x}) = (x_0, \psi(\mathbf{x}_1), \ldots, \psi(\mathbf{x}_n)) \in \mathbb{F}_{q^m}^{n+1}$. Observe that this map is also $\mathbb{F}_q$-linear and that $\overline{\psi}(\chi(\mathbf{c}) * \chi(\mathbf{c}')) = \mathbf{c} * \mathbf{c}'$ for all $\mathbf{c}, \mathbf{c}' \in G$. Moreover if $\pi'_{B_1}(\mathbf{x}) = \pi'_{B_1}(\mathbf{y})$, then observe that $\pi_B(\overline{\psi}(\mathbf{x})) = \pi_B(\overline{\psi}(\mathbf{y}))$. For arbitrary $\mathbf{c}, \mathbf{c}' \in G$, $\rho_{B,0} \circ \pi_B(\mathbf{c} * \mathbf{c}') = \pi_0(\mathbf{c} * \mathbf{c}') = c_0 c'_0 \in \mathbb{F}_q$. Hence, $\rho_{B,0} \circ \pi_B \circ \overline{\psi}(\chi(\mathbf{c}) * \chi(\mathbf{c}')) = c_0 c'_0$. We conclude by this composition and observation above that there exists an $\mathbb{F}_q$-linear map $\rho'_{B_1,0}$ such that $\rho'_{B_1,0} \circ \pi'_{B_1,0}(\chi(\mathbf{c}) * \chi(\mathbf{c}')) = c_0 c'_0$ for all $\mathbf{c}, \mathbf{c}' \in G$. Therefore, since all elements of $\widehat{C}_1$ are of the form $\sum_i \lambda_i \cdot (\chi(\mathbf{c}_i) * \chi(\mathbf{c}'_i))$ with $\lambda_i \in \mathbb{F}_q$ and $\mathbf{c}_i, \mathbf{c}'_i \in G$, and since $\rho'_{B_1,0} \circ \pi'_{B_1,0}$ is an $\mathbb{F}_q$-linear map, it holds that $r_0(\widehat{C}_1) \leq rn - t$ as claimed. △

We now present some elementary constructions of multiplication-friendly embeddings.

THEOREM 8 *Let $m \geq 2$ be an integer with $q \geq 2m - 2$, then there exists a multiplication-friendly embedding of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ with expansion $2m - 1$.*

PROOF. Let $\alpha \in \mathbb{F}_{q^m}$ such that $1, \alpha, \ldots, \alpha^{m-1}$ is a basis of $\mathbb{F}_{q^m}$ as an $\mathbb{F}_q$-vector space. Consider the $\mathbb{F}_q$-vector space $\mathbb{F}_q[X]_{<m}$ of polynomials in $\mathbb{F}_q[X]$ with degree at most $m - 1$. There is an isomorphism of $\mathbb{F}_q$-vector spaces $\phi : \mathbb{F}_q[X]_{<m} \to \mathbb{F}_{q^m}$ given by $f(X) \mapsto f(\alpha)$. Now take $2m - 2$ distinct elements in $\mathbb{F}_q$, $\beta_1, \beta_2, \ldots, \beta_{2m-2}$, and define the map $\xi : \mathbb{F}_q[X]_{<m} \to (\mathbb{F}_q)^{2m-1}$ given by $f(X) \mapsto (f(\beta_1), \ldots, f(\beta_{2m-2}), \mu(f))$ where $\mu(f)$ denotes the coefficient a_{m-1} of X^{m-1} in $f(X)$. Define $\sigma = \xi \circ \phi^{-1}$. For all $x, y \in \mathbb{F}_{q^m}$, we then have that $\sigma(x) = (f(\beta_1), \ldots, f(\beta_{2m-2}), \mu(f))$ and $\sigma(y) = (g(\beta_1), \ldots, g(\beta_{2m-2}), \mu(g))$ where $f(X)$,$g(X) \in \mathbb{F}_q[X]$ are the unique polynomials of degree at most $m - 1$ with $f(\alpha) = x$, $g(\alpha) = y$. We have $\sigma(x) * \sigma(y) = (fg(\beta_1), \ldots, fg(\beta_{2m-2}), \mu(fg))$. Since $f(X) \cdot g(X) \in \mathbb{F}_q[X]$ is of degree at most $2m - 2$, evaluations in $2m - 2$ points of $\mathbb{F}_q$ determine it up to to multiplicative factor (from $\mathbb{F}_q$). This factor is clearly uniquely determined when, in addition, $\mu(fg)$ is taken into account. It follows that $xy = fg(\alpha)$ is determined uniquely by $\sigma(x) * \sigma(y)$, i.e. there exists a function ψ such that $xy = \psi(\sigma(x) * \sigma(y))$ for all $x, y \in \mathbb{F}_{q^m}$. It is not difficult to see that ψ is $\mathbb{F}_q$-linear. △

A construction without any constraint on q and m is presented next. The expansion in this case is quadratic in the degree of the extension. However, for quadratic extensions it is exactly the same as above.

THEOREM 9 *There exists a multiplication-friendly embedding of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ with expansion $\binom{m+1}{2}$.*

PROOF. Let $\alpha \in \mathbb{F}_{q^m}$ such that $1, \alpha, \ldots, \alpha^{m-1}$ is a basis of $\mathbb{F}_{q^m}$ as an $\mathbb{F}_q$-vector space. Consider the map $\sigma : \mathbb{F}_{q^m} \to (\mathbb{F}_q)^r$ given by $x \mapsto (x_0, \ldots, x_{m-1}, x_0 + x_1, \ldots, x_0 + x_{m-1}, \ldots, x_{m-2} + x_{m-1})$, where $x = \sum_{i=0}^{m-1} x_i \alpha^i$. Given two elements $x, y \in \mathbb{F}_{q^m}$, the coordinates of $\sigma(x) * \sigma(y)$ precisely exhaust all possible expressions $x_i y_i$, as well as all possible expressions $x_i y_i + x_j y_j + x_i y_j + x_j y_i$ for $i \neq j$. Hence, for each pair of indexes (i, j) with $i \neq j$, there exists an $\mathbb{F}_q$-linear map $\phi_{i,j}$ such that $\phi_{i,j}(\sigma(x) * \sigma(y)) = x_i y_j + x_j y_i$. Since $xy = \sum_{k=0}^{2m-2} (\sum_{i+j=k} x_i y_j) \alpha^k = \sum_{i=0}^{m-1} x_i y_i \alpha^{2i} + \sum_{k=0}^{2m-2} (\sum_{i+j=k, i<j} x_i y_j + x_j y_i) \alpha^k$, it follows that there exists an $\mathbb{F}_q$-linear map ψ such that $xy = \psi(\sigma(x) * \sigma(y))$. △

COROLLARY 3 *Let $\mathbb{F}_q$ be a finite field. There exists a multiplication-friendly embedding of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ with expansion equal to 3. Moreover, there exists a multiplication-friendly embedding of $\mathbb{F}_{64}$ over $\mathbb{F}_4$ with expansion equal to 5.*

PROOF. In the case of quadratic extensions, both multiplication-friendly embeddings give the result. For the second case, we apply Theorem 8. △

We are now ready to bound $\widehat{\tau}(q)$ away from zero for all finite fields $\mathbb{F}_q$.

DEFINITION 12 *We define $\nu(q)$ as follows: $\nu(2) = 1/35 \approx 2.86\%$; $\nu(3) = 1/18 \approx 5.56\%$; $\nu(4) = 3/35 \approx 8.57\%$; $\nu(5) = 5/54 \approx 9.26\%$; for q square, $q \geq 49$, $\nu(q) = 1 - \frac{4}{\sqrt{q}-1}$; for the remaining values of q, $\nu(q) = \frac{1}{3}(1 - \frac{4}{q-1})$*

THEOREM 10 *Let $\mathbb{F}_q$ be a finite field. Then $\widehat{\tau}(q) \geq \nu(q)$.*

PROOF. If $q \geq 49$ and q is a square, then $\widehat{\tau}(q) \geq (1 - \frac{4}{\sqrt{q}-1})$ by Theorem 6. Using a degree 2 descent from the combination of Theorem 7 and Corollary 3, this immediately yields $\widehat{\tau}(q) \geq \frac{1}{3} \cdot (1 - \frac{4}{q-1})$ if $7 \leq q < 49$, or if $q > 49$ and q is not a square. For $q = 4$, $\mathbb{F}_{64}$ is a degree 3 extension of $\mathbb{F}_4$. Combining Theorem 7, instantiated with the multiplication-friendly mapping from $\mathbb{F}_{64}$ to $(\mathbb{F}_4)^5$ from Corollary 3, with the fact that $\widehat{\tau}(64) \geq \frac{3}{7}$, it follows that $\widehat{\tau}(4) \geq \frac{1}{5} \cdot \frac{3}{7} = \frac{3}{35}$. For $q = 2, 3, 5$ a further degree 2 descent in combination with the results above leads to $\widehat{\tau}(2) \geq \frac{1}{3} \cdot \frac{3}{35} = \frac{1}{35}$, $\widehat{\tau}(3) \geq \frac{1}{3} \cdot \frac{1}{6} = \frac{1}{18}$, and $\widehat{\tau}(5) \geq \frac{1}{3} \cdot \frac{5}{17} = \frac{5}{54}$. △

We note that it is possible to further improve these lower bounds especially for small values of q using more advanced techniques from algebraic geometry, as we show in upcoming work [5].

6 Consequences for LSSS with Strong Multiplication

We now state the consequences for LSSS with strong multiplication explicitly.

DEFINITION 13 *Let $\Sigma = (S_0, S_1, \ldots, S_n)$ be an SSS. The (average) information rate $\lambda(\Sigma)$ is defined as $\lambda(\Sigma) = \frac{\sum_{i=1}^{n} H(S_i)}{n \cdot H(S_0)}$. $\mathcal{F} = \{\Sigma_n\}_{n \in N}$ is a family of secret sharing schemes if $N \subset \mathbb{N}$ is an infinite set and for all $n \in N$, Σ_n is a secret sharing scheme with $|\mathcal{P}(\Sigma_n)| = n$. The (average) information rate $\lambda(\mathcal{F})$ of the family $\mathcal{F}$ is the function $\lambda_{\mathcal{F}} : N \longrightarrow \mathbb{R}_{\geq 0}$ with $n \mapsto \lambda(\Sigma_n)$.*

DEFINITION 14 *$\mathcal{F} = \{\Sigma_n\}_{n\in N}$ is a* family of ideal LSSS (over $\mathbb{F}_q$) with strong multiplication *if the following properties hold. $\mathcal{F}$ is a family of secret sharing schemes such that for all $n \in N$, $\Sigma_n = (\mathbb{F}_q, n, e^{(n)}, \mathbf{v}_0^{(n)}, V_1^{(n)}, \ldots, V_n^{(n)})$ is an LSSS. Moreover, for each $n \in N$, Σ_n is "ideal", i.e., $\dim V_i^{(n)} = 1$ for $i = 1, \ldots n,$. Finally, for all $n \in N$, Σ_n has t_n-strong multiplication, where t_n is the maximum integer with that property. The* corruption tolerance *$\widehat{t}_{\mathcal{F}}$ of $\mathcal{F}$ is defined as the function $\widehat{t}_{\mathcal{F}} : N \to \mathbb{R}_{\geq 0}$ with $n \mapsto \frac{3t_n}{n-1}$. Such a family is* asymptotically good *if $\limsup_{n\in N} \widehat{t}_{\mathcal{F}}(n) > 0$, and* asymptotically bad *otherwise.*

Combining Theorem 10 with Theorem 2, there are the following consequences for strongly multiplicative LSSS.

THEOREM 11 *Let $\mathbb{F}_q$ be an arbitrary finite field. There exists an asymptotically good family $\mathcal{F} = \{\Sigma_n\}_{n\in N}$ of ideal LSSS over $\mathbb{F}_q$ with strong multiplication such that $\lim_{n\to\infty} \widehat{t}_{\mathcal{F}}(n) = \nu(q)$.*

Note that over $\mathbb{F}_2$, for example, t is at least a 1/105-fraction of n, i.e. 0.95% of the players. Also note that by making q large enough, $\nu(q)$ gets arbitrarily close to 1 and, hence, t gets arbitrarily close to $\frac{1}{3}n$.

7 Asymptotically Bad Yet Elementary Schemes

We have shown that a combination of strong methods from algebraic geometry with a dedicated field-descent method leads to asymptotically good schemes over any finite field. We now show an elementary construction that also works over any finite field $\mathbb{F}_q$. However, it is asymptotically bad. Yet it gives t-strong multiplication for $t = \Omega(n/((\log\log n)\log n))$. A combination of results from [7] with replication gives an elementary family with $t = \Omega(\sqrt{n})$, which is much worse. Our construction here consists of applying a combination of Theorems 7 and 9 to Shamir's LSSS over a tower of extension fields of the base field $\mathbb{F}_q$, where the degree of the extension tends to infinity. For every $m > 0$, define $r_m = (q^m)^{\lfloor q^m/2 \rfloor}$. Consider the $[n+1, t]_{r_m}$-Reed-Solomon code C_m with $n+1 = r_m$ and $t = \lfloor \frac{1}{3}(r_m - 2) \rfloor$, i.e. $\Sigma(C_m)$ is a Shamir's LSSS over $\mathbb{F}_{r_m}$ with $r_m - 1$ players and t-strong multiplication. Now apply the construction in Theorem 7 to the codes C_m, using the multiplication-friendly embedding from Theorem 8, and we descend from LSSS over $\mathbb{F}_{r_m}$ to LSSS over $\mathbb{F}_{q^m}$. Using Theorem 9, we descent again from LSSS over $\mathbb{F}_{q^m}$ to LSSS over $\mathbb{F}_q$. Note that the final number of players is now $(r_m - 1)(2\lfloor q^m/2 \rfloor - 1)\binom{m+1}{2}$

THEOREM 12 *Let $\mathbb{F}_q$ be an arbitrary finite field. The above (elementary) construction yields a family $\mathcal{F} = \{\Sigma_n\}_{n\in N}$ of ideal LSSS over $\mathbb{F}_q$ with $t(n)$-strong multiplication, where $t(n) = \Omega(n/((\log\log n)\log n))$.*

PROOF. Write $n_m = (r_m - 1)(2\lfloor q^m/2 \rfloor - 1)\binom{m+1}{2}$. The code $\widetilde{C}_m$ constructed as above gives an LSSS Σ_{n_m} for n_m players and t_{n_m}-strong multiplication for $t_{n_m} = \lfloor \frac{1}{3}(r_m - 2) \rfloor$. On the other hand, it is easy to see that $m = O(\log\log n_m)$ and $m \cdot q^m = O(\log n_m)$. The desired result follows. △

8 Upper Bounds on Optimal Corruption Tolerance

So far we have presented asymptotic lower bounds on optimal corruption tolerance. We now turn to (non-asymptotic) upper bounds on corruption tolerance of a code. Using arguments given in [8], it follows easily that $\widehat{\tau}(C) < 1$ for all $C \in C^{\dagger}(\mathbb{F}_q)$ with $\ell(C)$ large enough as a function of q (note that $\widehat{\tau}(C) = 1$ is achievable if $n \leq q$). In Theorem 15 below we improve this bound. The improvement is based on a combination of Theorem 2 with Theorem 13, a more general result for LSSS we prove below. Namely, we lower bound the information rate as a function of the *threshold gap*. Here, the *threshold-gap* of an SSS is defined as the difference between its reconstruction- and privacy-thresholds. A further implication is that in all interesting cases, the threshold gap necessarily grows at least as $\Omega(\log n)$, where n is the number of players, in any family of LSSS over $\mathbb{F}_q$ with positive information rate. Let $\Sigma = (\mathbb{F}_q, n, e, \mathbf{v}_0, V_1, \ldots, V_n)$ be an LSSS over $\mathbb{F}_q$.

THEOREM 13 *Set* $\overline{g}(\Sigma) = r(\Sigma) - t(\Sigma)$, *the* threshold gap *of* Σ. *If* $t(\Sigma) \geq 1$ *and* $r(\Sigma) < n$, *then* $\dim \Sigma \geq \frac{n}{\overline{g}(\Sigma)} \cdot \log_q(\frac{n+\overline{g}(\Sigma)+2}{2\overline{g}(\Sigma)})$.

This generalizes a result from [11] where a lower bound in the dimension of any *threshold* LSSS over $\mathbb{F}_2$ is proven. In our result, the threshold gap can be greater than 1 (and q is arbitrary). The proof of Theorem 13 will rely in part on Theorem 14 and Corollary 4 below.

THEOREM 14 *Let* $\mathcal{G}$ *be a non-empty collection of subsets of* $\mathcal{P}(\Sigma)$ *such that* $\mathcal{G} \subset \mathcal{A}(\Sigma)$ *and, for any* $A, B \in \mathcal{G}$ *with* $A \neq B$, $A \cup B \in \Gamma(\Sigma)$. *Then,* $\sum_{A \in \mathcal{G}} d_A \geq |\mathcal{G}| \cdot \log_q(|\mathcal{G}|)$, *where* d_A *is the dimension of* V_A *for all* $A \in \mathcal{G}$.

PROOF. Our proof uses a lower bound technique from Karchmer and Wigderson [21] (and our claim is essentially a slight generalization of their result). Define $H_1 = \{\phi \in \mathrm{Hom}(\mathbb{F}_q^e, \mathbb{F}_q) : \phi(\mathbf{v}_0) = 1\}$. For all non-empty $A \subset \mathcal{P}$, define $H_{1,A} = H_1 \cap V_A^{\perp}$. Note that, by the characterization from Section 2.2, $A \in \Gamma(\Sigma)$ if and only if $H_{1,A} = \emptyset$. By linear algebra, $|H_1| = q^{e-1}$ and $|H_{1,A}| = q^{e-d_A-1}$ if $A \notin \Gamma(\Sigma)$. Moreover, if $A, B \in \mathcal{G}$, then $A \cup B \in \Gamma(\Sigma)$. Hence, $H_{1,A\cup B} = H_{1,A} \cap H_{1,B} = \emptyset$. Therefore, $|\bigcup_{A\in\mathcal{G}} H_{1,A}| = \sum_{A\in\mathcal{G}} |H_{1,A}|$ So $q^{e-1} = |H_1| \geq |\bigcup_{A\in\mathcal{G}} H_{1,A}| = \sum_{A\in\mathcal{G}} |H_{1,A}| = \sum_{A\in\mathcal{G}} q^{e-d_A-1}$. This gives $\sum_{A\in\mathcal{G}} q^{-d_A} \leq 1$. By the log-sum inequality,[8] $\sum_{A\in\mathcal{G}} d_A \geq |\mathcal{G}| \cdot \log_q(\frac{|\mathcal{G}|}{\sum_{A\in\mathcal{G}} q^{-d_A}}) \geq |\mathcal{G}| \cdot \log_q(|\mathcal{G}|)$. $\triangle$

DEFINITION 15 $\mathcal{G} = \{A_1, \ldots, A_m\}$ *is a* greedy partition *of* $\mathcal{P}(\Sigma)$ *if* m *is a positive integer,* $A_1, \ldots, A_m \subset \mathcal{A}(\Sigma)$, $\bigcup_{i=1}^{m} A_i = \mathcal{P}(\Sigma)$, $A_i \cap A_j = \emptyset$ $(1 \leq i < j \leq m)$, *and, for* $k = 1, \ldots, m$, A_k *is maximal in* $\mathcal{A}(\Sigma)$ *subject to* $A_k \subset \mathcal{P} \setminus \bigcup_{j=1}^{k-1} A_j$ $(A_0 = \emptyset)$.

[8] The log-sum inequality asserts that for non-negative real numbers $a_1, \ldots, a_r$ and $b_1, \ldots, b_r$ $\sum_{i=1}^{r} a_i \log_q(\frac{a_i}{b_i}) \geq (\sum_{i=1}^{r} a_i) \log_q \frac{\sum_{i=1}^{r} a_i}{\sum_{i=1}^{r} b_i}$.

Note that if $A, B \in \mathcal{G}$, then $A \cup B \in \Gamma(\Sigma)$. If $t(\Sigma) \geq 1$, there exists a greedy partition by induction. Moreover, the size m of a greedy partition can be bounded in terms of $r(\Sigma)$, since any set in the partition has at most $r(\Sigma) - 1$ elements.

COROLLARY 4 *Suppose $t(\Sigma) \geq 1$ and let $\mathcal{G}$ be a greedy partition of $\mathcal{P}(\Sigma)$. Then* $\dim \Sigma \geq |\mathcal{G}| \cdot \log_q |\mathcal{G}|$. *In particular,* $\dim \Sigma \geq \lceil \frac{n}{r(\Sigma)-1} \rceil \cdot \log_q(\lceil \frac{n}{r(\Sigma)-1} \rceil)$.

PROOF (of Theorem 13). We use a dualization technique from [11]. Set $r = r(\Sigma)$, $t = t(\Sigma)$ and $\overline{g} = \overline{g}(\Sigma)$. Note that if Σ^* is an LSSS over $\mathbb{F}_q$ whose access structure is the dual of Σ's, then $\overline{g}(\Sigma^*) = \overline{g}(\Sigma)$. Sort the players $1, \ldots, n$ so that $d_i \leq d_j$ if $i \leq j$. Let Σ_1 be the LSSS restricted to the first $r+1$ players (this is possible since $r < n$). Clearly $t(\Sigma_1) \geq t(\Sigma)$ and $r(\Sigma_1) \leq r(\Sigma)$, so $\overline{g}(\Sigma_1) \leq \overline{g}(\Sigma)$. There exists an LSSS Σ_1^* over $\mathbb{F}_q$ and defined over the first $r+1$ players such that $\dim \Sigma_1 = \dim \Sigma_1^*$ and $\Gamma(\Sigma_1^*)$ is the dual access structure to $\Gamma(\Sigma_1)$ (see the remark in Section 2.2). Note that $t(\Sigma_1^*) \geq 1$ and that $r(\Sigma_1^*) = r+1-t(\Sigma_1) \leq r+1-t = \overline{g}+1$. By Corollary 4, $\dim \Sigma_1 = \dim \Sigma_1^* \geq \lceil \frac{r+1}{r(\Sigma_1^*)-1} \rceil \cdot \log_q(\lceil \frac{r+1}{r(\Sigma_1^*)-1} \rceil) \geq \lceil \frac{r+1}{\bar{g}} \rceil \cdot \log_q(\lceil \frac{r+1}{\bar{g}} \rceil)$. Because of the sorting of the players, $\dim \Sigma \geq \frac{n}{r+1} \cdot \dim \Sigma_1 \geq \lceil \frac{n}{\bar{g}} \rceil \cdot \log_q(\lceil \frac{r+1}{\bar{g}} \rceil)$. Finally, let Σ^* now be an LSSS over $\mathbb{F}_q$ such that $\dim \Sigma = \dim \Sigma^*$ and $\Gamma(\Sigma^*)$ is the dual access structure to $\Gamma(\Sigma)$ (note that $t(\Sigma^*) \geq 1$ since $r < n$ and $r(\Sigma^*) < n$ since $t \geq 1$). Applying the bound we have just derived, we get $\dim \Sigma^* \geq \lceil \frac{n}{\bar{g}(\Sigma^*)} \rceil \cdot \log_q(\lceil \frac{r(\Sigma^*)+1}{\bar{g}(\Sigma^*)} \rceil)$. But $\bar{g}(\Sigma^*) = \bar{g}$ and $r(\Sigma^*) = n - t$, so $\dim \Sigma = \dim \Sigma^* \geq \lceil \frac{n}{\bar{g}} \rceil \cdot \log_q(\lceil \frac{n-t+1}{\bar{g}} \rceil)$. It is easy to see then that $\dim \Sigma \geq \frac{n}{\bar{g}} \log_q(\frac{n+\bar{g}+2}{2\bar{g}})$.

△

COROLLARY 5 *Let $\mathcal{F} = \{\Sigma_n\}_{n \in N}$ be a family of LSSS over $\mathbb{F}_q$. If the growth rate of the threshold gap is smaller than logarithmic in the number of players, i.e.,* $\limsup_{n \in N} \frac{\bar{g}(\Sigma_n)}{\log_q n} = 0$, *then the information rate satisfies* $\limsup_{n \in N} \lambda_{\mathcal{F}}(n) = 0$.

THEOREM 15 *Let $C \in C^{\dagger}(\mathbb{F}_q)$. We have $\widehat{t}(C) \leq \frac{1}{3} \cdot (n(C) - \frac{1}{2} \cdot \log_q(n(C)+2))$ and therefore $\widehat{\tau}(C) \leq 1 - \frac{\log_q(n(C)+2)-2}{2n(C)-2}$*

PROOF. Assume wlog that $\widehat{t}(C)$ is attained for $i = 0$ (i.e., $i_s = 0$, see Definition 8) and write $t = \widehat{t}(C)$. Then $t_0(C) \geq t$ and $r_0(C) \leq n(C) - 2t$, by Theorem 2. Now set $\bar{g} = \bar{g}(\Sigma(C))$ and $n = n(C)$. So, on the one hand, $\widehat{t}(C) \leq \frac{1}{3}(n - \bar{g})$. On the other hand, $\Sigma(C)$ is an "ideal" LSSS. Theorem 13 then implies $n \geq \frac{n}{\bar{g}} \log_q(\frac{n+\bar{g}+2}{2\bar{g}})$. Thus, $\bar{g} \geq \log_q(\frac{n+2}{2\bar{g}}) \geq \log_q(n+2) - \log_q(2\bar{g})$. Then $\bar{g} + \log_q(2\bar{g}) \geq \log_q(n+2)$, and since $\bar{g} \geq \log_q(2\bar{g})$ for any $\bar{g} \geq 1$, $\bar{g} \geq \frac{1}{2} \log_q(n+2)$. Combining these facts, the result follows. △

Note that this non-asymptotic upper bound on corruption tolerance does not imply $\widehat{\tau}(q) < 1$.

9 Open Problems

First, our main Theorem 10 implies that the asymptotic optimal corruption tolerance $\widehat{\tau}(q)$ satisfies $\widehat{\tau}(q) > 0$ for all finite fields $\mathbb{F}_q$. The proof of that theorem makes crucial use of strong results from algebraic geometry (namely, good towers of algebraic function fields). Is that essential? Though it is not unlikely that "strong algebraic geometry" is inherent to *strong* lower bounds on $\widehat{\tau}(q)$, is there perhaps a more elementary proof just that $\widehat{\tau}(q) > 0$? Second, it seems likely that the bound from Theorem 15 can be sharpened considerably. Third, it is interesting to improve our lower bounds for $\widehat{\tau}(q)$. We have already noted that in forthcoming work we do so for small values of q, using more advanced methods from algebraic geometry.

10 Acknowledgements

Ignacio Cascudo was supported by FICYT (project IB-08-147) and Spanish MICINN (project MTM2007-67884-C04-01 and FPU grant AP2005-0836, co-financed by the European Social Fund). Hao Chen was supported by NNSF China Grant 10871068. Ronald Cramer was supported by his NWO VICI project "Mathematical Foundations of Secure Computation." Chaoping Xing was supported by Singapore's NRF Competitive Research Programme (CRP), NRF-CRP 2200703 and the Singapore MoE Tier 2 grant T208B2206.

References

1. A. Bassa, A. Garcia, and H. Stichtenoth. A new tower over cubic finite fields. Moscow Mathematical Journal, Vol. 8, No. 3, September 2008, pp. 401–418.
2. M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. *Proceedings of STOC 1988*, pp. 1–10. ACM Press, 1988.
3. D. Chaum, C. Crépeau, and I. Damgaard. Multi-party unconditionally secure protocols. *Proceedings of STOC 1988*, pp. 11–19. ACM Press, 1988.
4. D.V. Chudnovsky, G.V. Chudnovsky. Algebraic complexities and algebraic curves over finite fields. *Proceedings of the National Academy of Sciences of the United States of America*, vol. 84, no. 7, pp. 1739–1743, April 1987.
5. I. Cascudo, R .Cramer, C. Xing. Ongoing work, 2009.
6. H. Chen, R. Cramer, R. de Haan, I. Cascudo Pueyo. Strongly multiplicative ramp schemes from high degree rational points on curves. *Proceedings of 27th Annual IACR EUROCRYPT*, Istanbul, Turkey, Springer Verlag LNCS, vol. 4965, pp. 451–470, April 2008.
7. H. Chen, R. Cramer, S. Goldwasser, R. de Haan, V. Vaikuntanathan. Secure Computation from Random Error Correcting Codes. *Proceedings of 26th Annual IACR EUROCRYPT*, Barcelona, Spain, Springer Verlag LNCS, vol. 4515, pp. 329–346, May 2007.
8. H. Chen and R. Cramer. Algebraic Geometric Secret Sharing Schemes and Secure Multi-Party Computation over Small Fields. *Proceedings of 26th Annual IACR CRYPTO*, Springer Verlag LNCS, vol. 4117, pp. 516–531, Santa Barbara, Ca., USA, August 2006.

9. R. Cramer, V. Daza, I. Gracia, J. Jimenez Urroz, G. Leander, J. Martí-Farré, and C. Padró. On codes, matroids and secure multi-party computation from linear secret sharing schemes. *Proceedings of 25th Anual CRYPTO*, Springer-Verlag, vol. 3621, pp. 327–343, August 2005.
10. R. Cramer, S. Fehr, M. Stam. Primitive Sets over Number Fields and Black-Box Secret Sharing. *Proceedings of 25th Annual IACR CRYPTO*, Santa Barbara, Ca., USA, Springer Verlag LNCS, vol. 3621, pp. 344–360, August 2005.
11. R. Cramer and S. Fehr. Optimal Black-Box Secret Sharing over Arbitrary Abelian Groups. *Proceedings of 22nd Annual IACR CRYPTO*, Santa Barbara, Ca., USA, Springer Verlag LNCS, vol. 2442, pp. 272–287, August 2002.
12. R. Cramer, I. Damgaard, and S. Dziembowski. On the complexity of verifiable secret sharing and multi-party computation. *Proceedings of STOC 2000*, pp. 325–334. ACM Press, 2000.
13. 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.
14. I. Damgaard, J. Buus Nielsen, D. Wichs. Isolated Proofs of Knowledge and Isolated Zero Knowledge. *Proceedings of 27th Annual IACR EUROCRYPT*, Istanbul, Turkey, Springer Verlag LNCS, vol. 4965, pp. 509–526, May 2008.
15. A. García, H. Stichtenoth. On the asymptotic behavior of some towers of function fields over finite fields. *J. Number Theory*, 61:248–273, 1996.
16. V. D. Goppa. Codes on algebraic curves. *Soviet Math. Dokl*, 24:170–172, 1981.
17. W. G. Huffman, V. Pless. Fundamentals of Error Correcting Codes. Cambridge University Press, 2003.
18. Y. Ihara. Some remarks on the number of rational points of algebraic curves over finite fields. J. Fac. Sci. Tokyo 28 (1981), 3:721724.
19. Y. Ishai, M. Prabhakaran, A. Sahai. Founding Cryptography on Oblivious Transfer–Efficiently. *Proceedings of 28th Annual IACR CRYPTO*, Santa Barbara, Ca., USA, Springer Verlag LNCS, vol. 5157, pp. 572–591, August 2008.
20. Y. Ishai, E. Kushilevitz, R. Ostrovsky, A. Sahai. Zero-knowledge from secure multiparty computation. *Proceedings of 39th STOC*, San Diego, Ca., USA, pp. 21–30, 2007.
21. M. Karchmer and A. Wigderson. On span programs. *Proceedings of the Eigth Annual Structure in Complexity Theory Conference*, pp. 102–111, IEEE, 1993.
22. J. H. van Lint. *Introduction to Coding Theory.* Graduate Texts in Mathematics. Springer Verlag, 1999.
23. J. L. Massey. Minimal codewords and secret sharing. In *Proceedings of the 6-th Joint Swedish-Russian Workshop on Information Theory*, pp. 269–279, Molle, Sweden, August 1993.
24. J. L. Massey. Some applications of coding theory in cryptography. *Codes and Ciphers: Cryptography and Coding IV*, pp. 33–47, 1995.
25. J. -P. Serre. Rational points on curves over finite fields. 1985, notes of lectures at Harvard University.
26. A. Shamir. How to share a secret. *Comm. of the ACM*, 22(11):612–613, 1979.
27. H. Stichtenoth. Algebraic function fields and codes. Springer Verlag, 1993.
28. I. Shparlinski, M. Tsfasman, S. Vladuts. Curves with many points and multiplication in finite fields. *Coding Theory and Algebraic Geometry*, 145–169, Springer Verlag, 1992.
29. M. Tsfasman, S. Vladuts, D. Nogin. Algebraic-geometric codes: Basic Notions. AMS, Mathematical Surveys and Monographs, Vol. 139, 2007.