The Arithmetic Codex*

Ignacio Cascudo† Ronald Cramer‡ Chaoping Xing§

July 13, 2012

Abstract

We introduce the notion of *arithmetic codex*, or *codex* for short. It encompasses several well-established notions from cryptography (arithmetic secret sharing schemes, i.e., enjoying additive as well as multiplicative properties) and algebraic complexity theory (bilinear complexity of multiplication) in a natural mathematical framework.

Arithmetic secret sharing schemes have important applications to secure multiparty computation and even to *two*-party cryptography. Interestingly, several recent applications to two-party cryptography rely crucially on the existing results on "*asymptotically good* families" of suitable such schemes. Moreover, the construction of these schemes requires asymptotically good towers of function fields over finite fields: no elementary (probabilistic) constructions are known in these cases. Besides introducing the notion, we discuss some of the constructions, as well as some limitations.

1 Definitions

Let K be a field. For our purposes, a K-algebra R is a commutative ring R with multiplicative unity 1_R such that $K \subset R$ is a subring.[1] Note that R is in particular a K-vector space. A product of K-algebras (such as the n-fold product K^n) will be viewed as a K-algebra with component-wise multiplication as ring-multiplication and with K thought of as "diagonally embedded", i.e., $x \in K$ is given by $(x, \ldots, x)$ in the product.

Let S be a K-algebra and let $R = K^n$ for some positive integer n. Suppose $C \subset R$ is a K-linear subspace and suppose that $\psi : C \longrightarrow S$ is a surjective K-vector space morphism (so, in particular, $\dim_K(S) \leq n$).

Definition 1 *If $s \in S$ and $x \in C$ are such that $\psi(x) = s$, then x is said to* present *s.*

Definition 2 *The multiplication map m_d is defined by*

$$m_d : C^d \longrightarrow R \ , \ (x_1, \ldots, x_d) \mapsto x_1 \cdots x_d.$$

The multiplication map M_d is defined by

$$M_d : S^d \longrightarrow S \ , \ (s_1, \ldots, s_d) \mapsto s_1 \cdots s_d.$$

*Presented at the IEEE Information Theory Workshop 2012 (ITW), Lausanne, Switzerland, September 2012 (invited talk by Cramer). An earlier version was presented as part of Cramer's invited talk at the 30th Annual IACR EUROCRYPT, May 2011, Tallinn, Estonia.

†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.

§Division of Mathematical Sciences, Nanyang Technological University, Singapore. Email: xingcp@ntu.edu.sg.

[1] By definition, this means of course that $1_K = 1_R$.

DEFINITION 3 *The map* $\psi^{(d)}$ *is defined as*

$$\psi^{(d)} : C^d \longrightarrow S^d \ , \ (x_1, \ldots, x_d) \mapsto (\psi(x_1), \ldots, \psi(x_d)).$$

DEFINITION 4 *Let* $x, x' \in R$. *Then* $x = (x_i)_{i=1}^n$ *is the* standard coordinate-vector *of* x. *Let* $A \subset \{1, \ldots, n\}$ *be a non-empty set. The projection* $\pi_A : K^n \longrightarrow K^{|A|}$, $x \mapsto (x_i)_{i \in A}$ *selects the* A*-indexed coordinates. Sometimes* x_A *is used as a shorthand for* $\pi_A(x)$.

Let t, r be integers with $0 \leq t < r \leq n$. The two crucial features of codices are as follows, informally speaking. First, the product of any d C-elements uniquely determines the product of the S-elements presented by them. In fact, any r coordinates already determine this uniquely. And second, any t coordinates of a C-element are jointly independent of the S-element presented by this C-element.

DEFINITION 5 (CODEX) *The pair* (C, ψ) *is an* (n, t, d, r)-codex *for* S *over* K *if the following holds.*

1. *(*(d, r)-product reconstruction*) For each* $B \subset \{1, \ldots, n\}$ *with* $|B| = r$, *there is a function* $g : m_d(C^d) \longrightarrow S$ *(depending on* B*), where* $m_d(C^d)$ *is the set of* d*-products over* C, *such that the following holds:*
   (a) $g(x) = g(y)$ *for all* $x, y \in m_d(C^d)$ *with* $\pi_B(x) = \pi_B(y)$, *i.e.,* g *only depends on the* B*-indexed coordinates.*
   (b) $M_d \circ \psi^{(d)} = g \circ m_d$, *i.e., multiplying the* S*-elements represented by a* d*-vector of* C*-elements is the same as first multiplying the* C*-elements and then applying* g.
2. *(*t-disconnection*) By definition, any pair* (C, ψ) *is* 0*-disconnected. If* $t > 0$, *then* (C, ψ) *is* t*-disconnected if for each* $A \subset \{1, \ldots, n\}$ *with* $|A| = t$, *the map*

$$\phi_A : C \longrightarrow S \times \pi_A(C) \ , \ x \mapsto (\psi(x), \pi_A(x))$$

   is surjective. If, additionally, $\pi_A(C) = \mathbb{F}_q^t$ *for all sets* $A \subset \{1, \ldots, n\}$ *with* $|A| = t$, *there is* uniformity.

DEFINITION 6 *Suppose* (C, ψ) *is an* (n, t, d, r)-codex *for* S *over* K. *If* $\dim_K S = \dim_K C$ *(as vector spaces) and if* $d \geq 2$ *then it is an* (n, d)-arithmetic embedding *(of* S *over* K*). If* K *is a finite field,* $d \geq 2$ *and* $t \geq 1$, *then it is an* (n, t, d, r)-arithmetic secret sharing scheme *(with secret-space* S *and share-space* K*).*

REMARK 1 *If* K *is a finite field, then* C *is finite and* ϕ_A *is a regular map. Therefore, if* $x \in C$ *is chosen uniformly at random, then* $\phi_A(x)$ *has the uniform distribution on* $S \times \pi_A(C)$. *It follows at once that* $\psi(x)$ *and* $\pi_A(x)$ *are independently distributed.*

REMARK 2 *The case* $d = 1$ *is degenerate in some sense, as it is oblivious of the multiplicative structure of* S. *If, in addition,* K *is a finite field, it's just a linear secret sharing scheme.*

REMARK 3 *If* $C^{*d} \subset R$ *is the* K*-linear subspace of* R *generated by the set* $m_d(C^d)$, *then, by multi-linear algebra, each of the reconstruction maps* g *extends uniquely to a* K*-linear map from* C^{*d} *to* S.

If $d = 2$, then the smallest n for which there is an $(n, 2)$-arithmetic embedding of S over K is actually the *bilinear multiplication complexity* of S over K. This is a classical notion from algebraic complexity theory. See [3] for history and references. Especially the case where K is a finite field $\mathbb{F}_q$ and S is an extension field $\mathbb{F}_{q^k}$ (for some integer $k > 1$) has been extensively studied.

Our notion distinguishes itself in several ways. These include the following. First, through t-disconnection and uniformity (as well as (d, r)-product reconstruction as opposed to the more common $(2, n)$-product reconstruction). Second, arithmetic secret sharing schemes with secret-space $\mathbb{F}_q^k$ and share-space $\mathbb{F}_q$ have particularly important cryptographic applications, whereas bilinear complexity is trivial here. From a cryptographic point of view, our notion encompasses all known variations on arithmetic secret sharing.

2 Some Examples

We give some first examples of codices. These are all based on (a generalization of) *Lagrange's Interpolation Theorem*, as given below.

THEOREM 1 *Let $\overline{K}$ denote an algebraic closure of K. Suppose $x_1, \ldots, x_m \in \overline{K}$ satisfy the property that their respective minimal polynomials $h_i(X) \in K[X]$ are pair-wise distinct, i.e., x_i, x_j are not Galois-conjugate over K if $i \neq j$. For $i = 1, \ldots, m$, write $\delta_i = \deg h_i$ $(= \dim_K[K(x_i) : K])$.*

Then the evaluation map

$$\mathcal{E} : K[X]_{\leq M-1} \longrightarrow \bigoplus_{i=1}^{m} K(x_i) \ , \ f \mapsto (f(x_i))_{i=1}^{m}$$

is an isomorphism of K-vector spaces, where $M = \sum_{i=1}^{m} \delta_i$ and where $K[X]_{\leq M-1}$ denotes the K-vector space of polynomials $f(X) \in K[X]$ such that $\deg f \leq M - 1$.

We now show constructions of codices for the algebras $S = \mathbb{F}_q^k$ and $S = \mathbb{F}_{q^k}$, respectively.

THEOREM 2 *Let $\mathbb{F}_q$ be a finite field. Suppose n, d, k are positive integers and t is a non-negative integer such that $d(t + k - 1) < n$. Then:*

- *There is an $(n, t, d, d(t + k - 1) + 1)$-codex for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ if $n + k \leq q$.*
- *There is an $(n, t, d, d(t + k - 1) + 1)$-codex for $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ if $n \leq q$ and $k \geq 2$.*

In both cases, it holds that there is uniformity if $t \geq 1$.

PROOF. Let $p_1, \ldots, p_n \in \mathbb{F}_q$ be pair-wise distinct. This is possible since $n \leq q$. Define C as the $\mathbb{F}_q$-linear subspace $\{(f(p_1), \ldots, f(p_n)) \mid f(X) \in \mathbb{F}_q[X]_{\leq t+k-1}\} \subset \mathbb{F}_q^n$. Since $t+k-1 < n$, this gives a one-to-one identification between $\mathbb{F}_q[X]_{\leq t+k-1}$ and C.

In the first case, select pairwise distinct $q_1, \ldots, q_k \in \mathbb{F}_q \setminus \{p_1, \ldots, p_n\}$. This is possible since $k \leq q - n$. Define the map $\psi : C \to \mathbb{F}_q^k$ by first identifying $c \in C$ with its corresponding $f \in \mathbb{F}_q[X]_{\leq t+k-1}$, followed by the evaluations $(f(q_1), \ldots, f(q_k))$. In the second case, select $p_0 \in \overline{\mathbb{F}_q} \setminus \mathbb{F}_q$ such that $\mathbb{F}_{q^k} = \mathbb{F}_q(p_0)$. The map $\psi' : C \to \mathbb{F}_{q^k}$ is defined similarly to ψ, except that evaluation is at p_0 instead of $q_1, \ldots, q_k$. The proofs for both cases are similar. We only argue the second.

First, the map ψ' is surjective, as follows. The space $\mathbb{F}_q[X]_{\leq k-1}$ can be identified one-to-one with $\mathbb{F}_{q^k}$ (as vector space), via evaluation at p_0. So the extension of this evaluation to

the large space $\mathbb{F}_q[X]_{\leq t+k-1}$ is surjective. Since C is identified with $\mathbb{F}_q[X]_{\leq t+k-1}$, the claim holds.

Next, suppose $t \geq 1$ and let $A \subset \{1, \ldots, n\}$ with $|A| = t$. The map $\phi_A : C \longrightarrow \mathbb{F}_{q^k} \times \mathbb{F}_q^t$ is surjective, as follows. For each $(u, v) \in \mathbb{F}_{q^k} \times \mathbb{F}_q^t$, there is a (unique) $f \in \mathbb{F}_q[X]_{\leq t+k-1}$ such that $f(p_0) = u$ and $(f(p_i))_{i \in A} = v$. Since C is identified with $\mathbb{F}_q[X]_{\leq t+k-1}$, there is a (unique) $c \in C$ such that $\psi'(c) = u$ and $\pi_A(c) = v$.

Finally, there is $(d, d(t+k-1)+1)$-product reconstruction, as follows. Let $B \subset \{1, \ldots, n\}$ with $|B| = d(t + k - 1) + 1 := r$. This makes sense, since $d(t + k - 1) + 1 \leq n$. Define $\overline{C}$ as the $\mathbb{F}_q$-linear subspace $\{(f(p_i))_{i \in B} \mid f(X) \in \mathbb{F}_q[X]_{\leq r-1}\} \subset \mathbb{F}_q^r$. This gives a one-to-one identification of $\overline{C}$ with $\mathbb{F}_q[X]_{\leq r-1}$. For any $f_1, \ldots, f_d \in \mathbb{F}_q[X]_{\leq k+t-1}$, it holds that $\prod_{i=1}^d f_i \in \mathbb{F}_q[X]_{\leq r-1}$. Therefore, $C^{*d} \subset \overline{C}$. Define $\overline{\psi}' : \overline{C} \to \mathbb{F}_{q^k}$ similarly to ψ', i.e., identify $\overline{c} \in \overline{C}$ with its corresponding $\overline{f} \in \mathbb{F}_q[X]_{\leq r-1}$, followed by evaluation at p_0. It follows that, for all $c_1, \ldots, c_d \in C$, $\overline{\psi}' \circ \pi_B(c_1 \cdots c_d) = \psi'(c_1) \cdots \psi'(c_d)$. $\triangle$

- The first construction with $k = 1$, $d = 1$ and $t \geq 1$ is Shamir's threshold secret sharing scheme [27]. If $t < \frac{n}{2}$, it has multiplication and if $t < \frac{n}{3}$ it has strong multiplication (see [13]). These properties were first used in [2, 9] in the context of secure multi-party computation.

- The second construction with $t = 0$, $k > 1$, $d = 2$, $2k-1 = n$ is a "bilinear multiplication algorithm" for $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$. See [3].

- The first construction with $k > 1$, $d = 2$, $t \geq 1$ is the Franklin-Yung "packed secret sharing scheme" [16]. If $2t + 2k - 2 < n$, it has multiplication and if $3t + 2k - 2 < n$, it has strong multiplication.

- The second construction with $t \geq 1$ and $d = 2$ is the scheme from [11].

By using "the point at infinity" there is an extra evaluation point (whose value corresponds to the coefficient of degree $t + k - 1$ of the polynomials). Thus, the condition from the first construction becomes $n + k \leq q + 1$ instead and similarly for the second.

3 Asympotics

Asymptotic study of bilinear complexity of multiplication in finite extensions of a finite field was initiated by Chudnovsky/Chudnovsky [12] in 1986. Here, $\mathbb{F}_q$ is fixed and an unbounded number of finite extensions of $\mathbb{F}_q$ considered. The purpose is to derive upper bounds on the asymptotic ratio between bilinear complexity of multiplication in an extension and its degree. Using a variation on the techniques of Tsfasman/Vladuts/Zink [30] from their 1982 breakthrough improvement of the Gilbert-Vashamov error correcting bound (which relies on deep results from algebraic geometry [21] in combination with Goppa's idea [19] of algebraic geometry codes), they showed that, surprisingly, this ratio is bounded from above by a constant (depending on q). Subsequent work gives better estimates for these constants. This work was continued by Shparlinski/Tsfasman/Vladuts [28]. See [3] for an overview, as well as for generalizations. Some more recent papers on the topic include [1, 8, 26].

Motivated by showing a suitable asymptotic version of the "Fundamental Theorem on Information-Theoretically Secure Multi-Party Computation" [2, 9] by Ben-Or/Goldwasser/Wigderson and Chaum/Crépeau from 1988, Chen/Cramer [10] initiated in 2006 the study of "asymptotically good arithmetic secret sharing schemes" and showed the first positive results for the strongest notions, using yet another variation on the algebraic geometric techniques of Tsfasman-Vladuts-Zink.

In 2007, the results of [10] played a central role in the surprising work of Ishai/Kushilevitz/Ostrovsky/Sahai [24] on the "secure multi-party computation in the head" paradigm and its application to communication-efficient zero-knowledge for circuit satisfiability. This caused nothing less than a paradigm shift that perhaps appears even as counter-intuitive: secure *multi-party* computation (an in particular, asymptotically good arithmetic secret sharing) is a very powerful abstract primitive for *communication-efficient two-party cryptography.* Subsequent fundamental results that also rely on the asymptotics from [10] concern two-party secure computation [25, 15], OT-combiners [20], correlation extractors [23], and OT from noisy channels [22]. For a full discussion, see [5]. More recently, it was shown in [14] how a combination of the schemes from [10] with ideas from [13] (inspired by [2, 9]) leads to a method for "zero-knowledge verification of secret multiplications" with rather low amortized complexity.

The results of [10] were strengthened in [4]. In [5] the authors presented a more powerful paradigm for the construction of arithmetic secret sharing schemes that is based on novel algebraic geometric ideas.

We first review the results from [10]. For terminology and theory on algebraic function fields, we refer to Stichtenoth [29] and for more details on the constructions, we refer to [10], [5].

Let F be an algebraic function field with full field of constants $\mathbb{F}_q$. Its genus is $g(F)$. The set of places of F is $\mathbb{P}(F)$ and the set of places of degree k is $\mathbb{P}^{(k)}(F)$. The group of divisors on F is denoted by $\mathrm{Div}(F)$. Given $D \in \mathrm{Div}(F)$, its Riemann-Roch space is $\mathcal{L}(D)$ and the dimension of $\mathcal{L}(D)$ as an $\mathbb{F}_q$-vector space is $\ell(D)$. Note that $\ell(D) = 0$ if $\deg D < 0$.

THEOREM 3 (RIEMANN-ROCH) *Let $K \in \mathrm{Div}(F)$ be a canonical divisor. Then, for each $D \in \mathrm{Div}(F)$, it holds that $\ell(D) = \deg D - g(F) + 1 + \ell(K - D)$.*

This theorem implies the following generalization of Lagrange's interpolation theorem.

THEOREM 4 *Let $P_1, \ldots, P_m \in \mathbb{P}(F)$ be pairwise distinct. Write $P = \sum_{i=1}^{m} P_i \in \mathrm{Div}(F)$ and write $\deg P_i = d_i$ for $i = 1, \ldots, m$. Let $D \in \mathrm{Div}(F)$ be such that its support does not include any of the P_i's and such that $\ell(D) > 0$. Let $K \in \mathrm{Div}(F)$ be a canonical divisor of F. The evaluation map*

$$\mathcal{E} : \mathcal{L}(D) \to \bigoplus_{i=1}^{m} \mathbb{F}_{q^{d_i}} \ , \ f \mapsto (f(P_i))_{i=1}^{m}$$

has the following properties.

- *It is injective if $\ell(D - P) = 0$*
- *It is surjective if $\ell(K - D + P) = 0$*

THEOREM 5 ([10, 5]) *Suppose n, d, t, r, k are positive integers such that $|\mathbb{P}^{(1)}(F)| \geq n + k$ and such that $1 \leq t < r \leq n$. Let $P_1, \ldots, P_n, Q_1, \ldots, Q_k \in \mathbb{P}^{(1)}(F)$ be pairwise distinct. Define $Q = \sum_{i=1}^{k} Q_i \in \mathrm{Div}(F)$ and, for each non-empty set $A \subseteq \{1, \ldots, n\}$, define $P_A := \sum_{i \in A} P_i \in \mathrm{Div}(F)$. Let $K \in \mathrm{Div}(F)$ be a canonical divisor.*

If the system of "Riemann-Roch equations"

$$\begin{cases} \ell(K - X + Q + P_A) = 0 & \text{for all } A \subset \{1, \ldots, n\}, |A| = t \\ \ell(dX - P_B) = 0 & \text{for all } B \subset \{1, \ldots, n\}, |B| = r \end{cases}$$

has a solution $X := G$, where $G \in \mathrm{Div}(F)$, then there exists an (n, t, d, r)-codex for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ with uniformity.

PROOF. We give a sketch as follows. Note that if there is a solution, we may without loss of generality assume its support is disjoint from $P_1, \ldots, P_n, Q_1, \ldots, Q_k$. Let G be such a solution. Let $C := \{(f(P_1), \ldots, f(P_n)) : f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n$.

Define the evaluation map $\mathcal{E} : \mathcal{L}(G) \to \mathbb{F}_q^n$ by $f \mapsto (f(P_1), \ldots, f(P_n))$. From the assumptions and Theorem 4 it is not difficult to see this is injective and that, therefore, there is an inverse $\mathcal{E}^{-1} : C \to \mathcal{L}(G)$. Define the map $\mathcal{E}_0 : \mathcal{L}(G) \to \mathbb{F}_q^k$ by $f \mapsto (f(Q_1), \ldots, f(Q_k))$ and define $\psi = \mathcal{E}_0 \circ \mathcal{E}^{-1}$.

The theorem now follows from Theorem 4, together with the fact that for any $f_1, \ldots, f_d \in \mathcal{L}(G)$, it holds that $\prod_{i=1}^d f_i \in \mathcal{L}(dG)$. For a more detailed proof, see [10] and [5] (or [6]) $\triangle$

A sufficient condition for solvability is the existence of a (positive) integer m such that if $G \in \mathrm{Div}(F)$ and $\deg G = m$ then $\deg(K - G + Q + P_A) < 0$ for all sets A of size t and $\deg(dG - P_B) < 0$ for all B of size r. Indeed, if such an m exists, then *any* divisor of degree m is a solution. Note that the degree of $K - G + Q + P_A$ (resp. $dG - P_B$) is the same for all A (resp. B) of size t (resp. r). If $\deg D > 2g(F) - 2$, then $\ell(D) = \deg D - g(F) + 1$. This is a corollary to the Riemann-Roch Theorem. Using this fact, it follows that setting $m = 2g-1+k+t$ and $r = dm+1$ suffices, under the assumption that $d(2g(F)+k+t-1)+1 \leq n$. This leads to the following theorem.

THEOREM 6 *("Existence from solving by degree") [10] Let F be an algebraic function field with $\mathbb{F}_q$ as its full field of constants. Suppose n, d, t, k are positive integers such that $d(2g(F)+k+t-1)+1 \leq n \leq |\mathbb{P}^{(1)}(F)|-k$. Then there exists an $(n, t, d, d(2g(F)+k+t-1)+1)$-codex for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ with uniformity.*

In comparison to Theorem 2, the condition $q + 1 \geq n + k$ has become $|\mathbb{P}^{(1)}(F)| \geq n + k$, which is weaker. However, this does not come entirely for free, as the second condition $d(2g(F) + k + t - 1) + 1 \leq n$ involves the genus of F. Before we study these results asymptotically, let us point out that a similar result holds for codices for $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$.

THEOREM 7 *Let F be an algebraic function field with $\mathbb{F}_q$ as its full field of constants. Suppose n, d, t, k are positive integers such that $k \geq 2$, $|\mathbb{P}^{(k)}(F)| \geq 1$ and $d(2g(F) + k + t - 1) + 1 \leq n \leq |\mathbb{P}^{(1)}(F)|$. Then there exists an $(n, t, d, d(2g(F) + k + t - 1) + 1)$-codex for $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ with uniformity.*

As we can see, the constructions depend on $|\mathbb{P}^{(1)}(F)|$ and $g(F)$: we would like $|\mathbb{P}^{(1)}(F)|$ to be as large as possible compared to $g(F)$. The classical Hasse-Weil bound upper bounds the number of places of degree 1 as a function of the genus g and q. It states that $|\mathbb{P}^{(1)}(F)| \leq q + 1 + 2qg(F)$. Asymptotically, a better upper bound is known. Write $N_q(g) = \max_F |\mathbb{P}^{(1)}(F)|$, where F ranges over all function fields with $\mathbb{F}_q$ as its full field of constants and having genus g. The quantity $A(q) := \limsup_{g\to\infty} \frac{N_q(g)}{g}$ is Ihara's constant. The Drinfeld-Vlăduţ upper bound states that $A(q) \leq \sqrt{q} - 1$. On the positive side, Ihara [21] first showed by using modular curves that $A(q) \geq \sqrt{q} - 1$ for any square q, i.e., $q = p^m$ where p is a prime integer and m is a positive, even integer. Therefore, the Drinfeld-Vlăduţ upper bound is sharp for all square q. Explicit families of function fields over $\mathbb{F}_q$ for q square attaining this value were constructed by Garcia and Stichtenoth [17].

On the other hand, no single exact value of $A(q)$ is known if q is a non-square. However, some lower bounds have been obtained so far. We mention here two known results. One is the recent result by Garcia/Stichtenoth/Bassa/Beelen [18] who showed an explicit tower of function fields over finite fields $\mathbb{F}_{p^{2m+1}}$ for any integer prime p and any integer $m \geq 1$. Their result gives

$$A(p^{2m+1}) \geq \frac{2(p^{m+1} - 1)}{p + 1 + \epsilon} \quad \text{with} \quad \epsilon = \frac{p - 1}{p^m - 1}.$$

On the other hand, Serre made use of class field theory to show that there is an absolute positive real constant c such that $A(q) \geq c \cdot \log(q)$ for all finite fields $\mathbb{F}_q$.

We obtain the following asymptotical result, which appeared, for the case $d = 2$, in [10].

THEOREM 8 *[10] Let $d \geq 2$ and $\mathbb{F}_q$ be a finite field such that $A(q) > 2d$. Then for an infinite number of n, there exist (n, t_n, d, r_n) codices for $\mathbb{F}_q^{k_n}$ over $\mathbb{F}_q$ with uniformity where $t_n = \Omega(n)$, $k_n = \Omega(n)$ and $n - r_n = \Omega(n)$. In particular, this holds for any field $\mathbb{F}_q$ with q square, $q > (2d+1)^2$ and also for any sufficiently large q.*

We note that these schemes can be efficiently constructed and operated. The condition $A(q) > 2d$ can be relaxed. First, in [4], the authors proved a version of Theorem 8 for the case $d = 2$ which is valid for any finite field $\mathbb{F}_q$; however in this version, uniformity is not satisfied (which, however, is important in some applications). The idea is to combine Theorem 8 over an extension field $\mathbb{F}_q^k$ for which $A(q^k) > 4$ with a dedicated field descent based on a $(m, 0, 2, m)-$codex for $\mathbb{F}_q^k$ over $\mathbb{F}_q$. It is the descent step that destroys the uniformity property. Besides, it is not generalizable to every $\mathbb{F}_q$ for $d > 2$ either.

In [5], [6], a quite different approach was used. In Theorem 6 we have insisted in solving all equations $\ell(D_i) = 0$ of Theorem 5 by setting the parameters in such a way that $\deg D_i < 0$. However this does not necessarily lead to the best results. Instead, in [5], [6] a much more sophisticated and novel algebraic geometric approach for solving the Riemann-Roch systems is introduced. It not only uses information about the number of rational points and the genus of function fields, but also information on the order of the d-torsion subgroup of the (degree-0 divisor) class group. This leads to a significant weakening of the condition $A(q) > 2d$ while maintaining uniformity. Some of the best results are attained after establishing particularly favorable upper bounds for the p-rank of the function fields in a well-chosen optimal tower using the Deuring-Shafarevich Theorem. From a computational perspective, this approach is (at present) not efficient in general. It is an open problem to improve this situation.

Finally, it is interesting to point out that there are no elementary (probabilistic) constructions known for the asymptotically good arithmetic secret sharing schemes used in the recent applications in two-party cryptography (starting with [24]) and used in an asymptotic version [10] of the fundamental results of [2, 9] on secure multi-party computation: all known relevant constructions, starting with the schemes from [10], are algebraic geometric and require asymptotically good towers of functions fields. Note that this is, so far at least, in contrast with the theory of error correcting codes, where asymptotically good families *can* be obtained by elementary (probabilistic) methods.[2]

4 Limitations

We now state some limitations on codices. We shall restrict ourselves to arithmetic secret sharing schemes, so $t \geq 1$.

The main strategy for proving bounds on arithmetic secret sharing schemes is via the lemma below.

LEMMA 1 *[7] An (n, t, d, r)-arithmetic codex for S over $\mathbb{F}_q$ is in particular an $(n, t, 1, r - (d-1)t)$-arithmetic codex for S over $\mathbb{F}_q$.*

Therefore, bounds on linear secret sharing schemes imply bounds on arithmetic secret sharing schemes.

[2] As an aside, note that $(n, t, 2, n)$-codices for $\mathbb{F}_q$ over $\mathbb{F}_q$ are implied by self-dual $\mathbb{F}_q$-linear codes, for which elementary asymptotically good constructions are known. However, these codices enjoy rather limited applications (basically, passive-case secure multi-party computation with single field elements as secrets) and are not useful in any of the recent applications we have mentioned, starting with [24].

As we have seen, the algebraic geometric approach gives asymptotically good results. However, compared to the elementary non-asymptotic case, the product-reconstruction parameter is increased by a factor that depends on the ratio between the genus and the number of rational points. A loss is unavoidable, as we now show. First, consider the case $d = 1$.

THEOREM 9 *[7] For any $(n, t, 1, r)$-codex for S over $\mathbb{F}_q$ with $t \geq 1$ it holds that $r - t \geq \frac{n-t+1}{q}$.*

If the dimension of S is large, there is the following connection with the theory of error correcting codes.

THEOREM 10 *[7] If there exists an $(n, t, 1, r)$-codex for S over $\mathbb{F}_q$, then there exists a $\mathbb{F}_q$-linear error-correcting code D of $n - t$, dimension k (where k is the dimension of S) and minimum distance at least $n - r + 1$.*

By applying the Singleton bound, it follows right away that $r \geq k + t$ for an $(n, t, 1, r)$-codex for S over $\mathbb{F}_q$, where k is the dimension of S.

A more interesting result is obtained by applying other bounds, for example the Griesmer bound. In [7] these observations, together with a dualization technique enabling stronger bounds for large t, imply several limitations on $(n, t, 1, r)$-codices. In combination with Lemma 1, this implies the following for the case $d \geq 1$.

THEOREM 11 *[7] For any (n, t, d, r)-codex for S over $\mathbb{F}_q$, where $t \geq 1$ and k denotes the dimension of S, it holds that*

$$r \geq dt + \frac{n - t + 1}{q} + f_+(q, k, n, t),$$

where

$$f_+(q, k, n, t) = \max\{0, k - 1 - \frac{n - t + 1}{q(q + 1)}\}.$$

If in addition $r \leq n - 1$, then

$$r \geq dt + \frac{n + 2}{2q - 1} + h_+(q, k, n)$$

where

$$h_+(q, k, n) := \max\left\{0, \frac{2q}{2q + 1}\left(k - 1 - \frac{1}{q} \cdot \frac{n + 2}{2q - 1}\right)\right\}.$$

The bounds above are independent of the algebra S, except that some involve the dimension k of S as an $\mathbb{F}_q$-vector space. Lower bounds on the bilinear complexity of algebras S have been studied extensively in the literature. We do not address this topic here but we refer the reader to [3]. We show a different type of limitation for the case $S = \mathbb{F}_{q^k}$.

THEOREM 12 *For any (n, t, d, r)-codex for $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ such that the integer k satisfies $k \geq 2$, it holds that $d \leq q$.*

PROOF. Suppose there exists an (n, t, d, r)-codex (C, ψ) for $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ and $d \geq q + 1$ holds. Note first that, since $k \geq 2$, there exist elements $x, y \in \mathbb{F}_q^k \setminus \{0\}$ with $x^{q-1} \neq y^{q-1}$. Let $\mathbf{c}$, $\mathbf{w}$ be elements in C with $\psi(\mathbf{c}) = x$ and $\psi(\mathbf{w}) = y$. Now since the identity $\mathbf{x}^q = \mathbf{x}$ holds for $\mathbf{x} \in \mathbb{F}_q^n$, we have $\mathbf{c}^q \mathbf{w}^{d-q} = \mathbf{c}\mathbf{w}^{d-1}$. Then let $\mathbf{a} \in C^d$ be the element where the first q coordinates equal $\mathbf{c}$ and the remaining $d - q$ equal $\mathbf{w}$ and let $\mathbf{b} \in C^d$ be the element where the first coordinate is $\mathbf{c}$ and the rest equal $\mathbf{w}$. By the observation above, $m_d(\mathbf{a}) = m_d(\mathbf{b})$.

Therefore for any function $g : m_d(C^d) \to \mathbb{F}_{q^k}$ we have $g \circ m_d(\mathbf{a}) = g \circ m_d(\mathbf{b})$. On the other hand

$$M_d \circ \psi^{(d)}(\mathbf{a}) = x^q y^{d-q} \neq xy^{d-1} = M_d \circ \psi^{(d)}(\mathbf{b}).$$

Therefore (d, r)-reconstruction of (C, ψ) cannot hold, which is a contradiction. $\triangle$

Note that the theorem above holds regardless of t, r and therefore holds even for the "weakest" case of $(n, 0, d, n)$-codices for $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$.

References

[1] S. Ballet, R. Rolland. On the bilinear complexity of the multiplication in finite fields. Séminaires et Congrès 11, 2005, 179-188.

[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] P. Bürgisser, M. Clausen, M.A. Shokrollahi. Algebraic Complexity Theory. Series: Grundlehren der mathematischen Wissenschaften, Vol. 315, Springer, 1997.

[4] I. Cascudo, H. Chen, R. Cramer, C. Xing. Asymptotically Good Ideal Linear Secret Sharing with Strong Multiplication over *Any* Finite Field. *Proceeding of 29th Annual IACR CRYPTO*, Santa Barbara, Ca., USA, Springer Verlag LNCS, vol. 5677, pp. 466-486, August 2009.

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

[6] I. Cascudo, R. Cramer, C. Xing. Torsion Limits and Riemann-Roch Systems for Function Fields and Applications. Manuscript, 2012. Available at http://arxiv.org/abs/1207.2936

[7] I. Cascudo, R. Cramer, C. Xing. Bounds on the Threshold Gap in Secret Sharing over Small Fields. Manuscript, 2012. Available at http://eprint.iacr.org/2012/319

[8] I. Cascudo, R. Cramer, C. Xing, A. Yang. Asymptotic Bound for Multiplication Complexity in the Extensions of Small Finite Fields. *IEEE Transactions on Information Theory*, Vol. 58, Issue 7, pp. 4930 - 4935, 2012.

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

[10] 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.

[11] 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.

[12] D.V. Chudnovsky, G.V. Chudnovsky. Algebraic complexities and algebraic curves over finite fields. *Proc. Natl. Acad. Sci. USA*, vol. 84, no. 7, pp. 1739-1743, April 1987.

[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] R. Cramer, I. Damgaard, V. Pastro. On the Amortized Complexity of Zero Knowledge Protocols for Multiplicative Relations. To appear in 6th International Conference on Information Theoretic Security, 2012. Preliminary version in http://eprint.iacr.org/2011/301.

[15] I. Damgaard, Y. Ishai and M. Krøigaard. Perfectly Secure Multiparty Computation and the Computational Overhead of Cryptography. *Proceedings of 29th Annual IACR EUROCRYPT*, Nice, France, Springer Verlag LNCS, vol. 6110, pp. 445-465, May 2010.

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

[17] A. Garcia, H. Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlăduţ bound. Invent. Math. 121, pp. 211-222, 1995.

[18] A. Garcia, H. Stichtenoth, A. Bassa, P. Beelen. Towers of function fields over non-prime finite fields. Preprint, 2012. See http://arxiv.org/abs/1202.5922

[19] V. D. Goppa. Codes on algebraic curves. *Soviet Math. Dokl*, 24:170-172, 1981.

[20] D. Harnik, Y. Ishai, E. Kushilevitz, J. Nielsen. OT-Combiners via Secure Computation. *Proceedings of TCC 2008*, pp. 393-411.

[21] Y. Ihara. Some remarks on the number of rational points of algebraic curves over finite fields. J. Fac. Sci. Tokyo 28 (1981), 3, pp. 721-724.

[22] Y. Ishai, E. Kushilevitz, R. Ostrovsky, M. Prabhakaran, A. Sahai, J. Wullschleger. Constant-rate OT from Noisy Channels. *Proceeding of 31st Annual IACR CRYPTO*, Santa Barbara, Ca., USA, Springer Verlag LNCS, vol. 6842, pp. 667-684, August 2011.

[23] Y. Ishai, E. Kushilevitz, R. Ostrovsky, A. Sahai. Extracting Correlations. *Proc. 50th IEEE FOCS*, pp. 261-270, 2009.

[24] 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.

[25] 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.

[26] H. Randriambololona. Bilinear complexity of algebras and the Chudnovsky-Chudnovsky interpolation method. Preprint, 2011. (see http://arxiv.org/pdf/1107.0336v5.pdf)

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

[28] I. Shparlinski, M. Tsfasman, S. Vlăduţ. Curves with many points and multiplication in finite fields. Lecture Notes in Math., vol. 1518, Springer-Verlag, Berlin, 1992, pp. 145-169.

[29] H. Stichtenoth. Algebraic function fields and codes. Springer Verlag, 1993. (New edition: 2009).

[30] M. Tsfasman, S. Vlăduţ, Th. Zink. Modular curves, Shimura curves, and Goppa codes, better than Varshamov Gilbert bound. Math. Nachr. 109, 21-28, 1982.

[31] S. G. Vlăduţ, V. G. Drinfeld. Number of points of an algebraic curve. Funct. Anal. Appl. vol. 17, pp. 53-54, 1983.