# The Arithmetic Codex[*]

Ignacio Cascudo[†] Ronald Cramer[‡] Chaoping Xing[§]

Version 4: November 13, 2012 [¶]

**Abstract**

We introduce the notion of an *arithmetic codex*, or *codex* for short. Codices encompass several well-established notions from cryptography (various types of *arithmetic* secret sharing schemes, which all enjoy additive as well as multiplicative properties) and from algebraic complexity (bilinear complexity of multiplication in algebras) in a single 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 existence of certain *asymptotically good* schemes. It is intriguing that their construction requires asymptotically good towers of algebraic function fields over a finite field: 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 Preliminaries

Let $K$ be a field. In this paper, a $K$-algebra $S$ is a commutative ring $S$ with multiplicative unity $1_S$ such that $K \subset S$ is a subring (so, $1_K = 1_S$ by definition). In particular, $S$ is a $K$-vector space. Products of $K$-algebras (e.g., the $n$-fold product $K^n$) will be viewed as $K$-algebras with component-wise multiplication as ring-multiplication and with $K$ "diagonally embedded", i.e., $\lambda \in K$ is given by $(\lambda, \ldots, \lambda)$ in the product.

Products of extension fields of $K$ are among the most elementary examples of $K$-algebras. There is the following classical characterization theorem for this case.

Theorem 1 *Suppose $S$ is a $K$-algebra having finite dimension as a $K$-vector space. Then the following holds.*

- *$S$ has $0$ as its only nilpotent if and only if $S$ is a finite product of finite-degree extension fields of $K$.*

[*] 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`.

[¶] *Change log: Not taking the property claimed in Lemma 1 (Version 3) as a condition in the codex definition as introduced in this eprint paper, was meant to further simplify our prior definitions. However, this Lemma 1 is incorrect [6]. A similar mistake appears in the talk notes from the electronic proceedings as handed out at Proc. IEEE Symp. Inf. Theory, Sept. 2012 (see Remark 3 there). In this Version 4 we have corrected it by, once again, taking it as a condition in the definition. Note that the mistake does not appear in prior codex definitions (such as the one presented at Eurocrypt 2011).*

- *$S$ has non-zero discriminant if and only if $S$ is a finite product of finite-degree* separable *extension fields of $K$.*

Note that if $K$ is a *perfect* field (such as $K = \mathbb{F}_q$, the finite field of order $q$), these two classes coincide. There is a rich literature on $K$-algebras that includes many other, sometimes much more involved classes. However, there is no complete classification as yet. In this paper, we are mostly interested in the case where $K$ is a finite field and the $K$-algebras are finite products of finite-degree extension fields of that finite field. That said, the definitions to follow are general and not restricted to this choice.

## 2 The Codex Definition

Let $S$ be a $K$-algebra and let $n \geq 1$ be an integer. Suppose that $C \subset K^n$ is a $K$-linear subspace and that $\psi : C \longrightarrow S$ is a surjective $K$-vector space morphism (so $\dim_K(S) \leq n$).

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

Definition 2 (Projection Maps) *Let $\mathbf{x} \in K^n$. Then $\mathbf{x} = (x_i)_{i=1}^n$ is the* standard coordinate-vector *of $\mathbf{x}$. Let $A \subset \{1, \ldots, n\}$ be a non-empty set. The projection map*

$$\pi_A : K^n \longrightarrow K^{|A|},$$

$$\mathbf{x} \mapsto (x_i)_{i \in A}$$

*selects the $A$-indexed coordinates. Sometimes $\mathbf{x}_A$ is used as a shorthand for $\pi_A(\mathbf{x})$.*

Let $d, t, r$ be integers with $d \geq 1$ and $0 \leq t < r \leq n$. The three crucial properties of codices are as follows, informally speaking. First, each element of $\mathbf{s} \in S$ is "presented" in the sense that $\psi(\mathbf{x}) = \mathbf{s}$ for some $\mathbf{x} \in C$. Second, the coordinate-wise product (in $K^n$) of any $d$ $C$-elements uniquely determines the product of the $d$ $S$-elements presented by them. In fact, any $r$ coordinates of this coordinate-wise product suffice. Moreover, in each of these cases, there exists a $K$-linear map by which it can be determined. Third, any $t$ coordinates of a generic ("random") $C$-element are jointly independent ("give no information") about the $S$-element that this $C$-element presents. The formal definition is as follows.

Definition 3 (Codex) *The pair $\mathcal{C} = (C, \psi)$ is an $(n, t, d, r)$-*codex *for $S$ over $K$ if the following holds.*

1. *The map $\psi$ is* surjective.
2. *There is $(d, r)$-*product reconstruction*. This means that, for each set $B \subset \{1, \ldots, n\}$ with $|B| = r$, there exists a $K$-linear map*

$$\rho^B : K^n \longrightarrow S$$

*such that*

*(a)* $\rho^B(\prod_{i=1}^d \mathbf{x}_i) = \prod_{i=1}^d \psi(\mathbf{x}_i)$ *for all* $(\mathbf{x}_1, \ldots, \mathbf{x}_d) \in C^d$.

*(b)* $\rho^B(\mathbf{y}) = 0$ *for all* $\mathbf{y} \in K^n$ *with* $\pi_B(\mathbf{y}) = \mathbf{0}$.

3. *There is* $t$-disconnection. *By definition,* $\mathcal{C}$ *is* 0*-disconnected. If* $t > 0$*, then* $\mathcal{C}$ *is* $t$*-disconnected if for each* $A \subset \{1, \ldots, n\}$ *with* $|A| = t$*, the map*

$$\phi_A : C \longrightarrow S \times \pi_A(C)$$

$$\mathbf{x} \mapsto (\psi(\mathbf{x}), \pi_A(\mathbf{x}))$$

*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*.*

Note that the case $d = 1$ is oblivious of the multiplicative structure of $S$. Though we will be mostly interested in the case $d > 1$, the case $d = 1$ is interesting in its own right. See below. Also note that if $t = 0$, there is no privacy guarantee. On the other hand, $r \leq n$. So product-reconstruction is guaranteed by definition.

Suppose $K$ is a finite field and $|A| = t$. Then $C$ is finite and $\phi_A$ is a regular map. Therefore, if $\mathbf{x}$ is uniformly random on $C$, then $\phi_A(\mathbf{x})$ is uniformly random on $S \times \pi_A(C)$. Thus, $\psi(\mathbf{x})$ has the uniform distribution on $S$ and, furthermore, $\psi(\mathbf{x})$ and $\pi_A(\mathbf{x})$ are independently distributed. This has the following consequence. Consider the linear secret sharing scheme where $\mathbf{x} \in C$ is selected uniformly at random such that $\psi(\mathbf{x})$ equals the intended secret $\mathbf{s} \in S$ and where the $n$ individual coordinates of $\mathbf{x}$ are the shares. Then there is $t$-privacy. If $d = 1$, there is $r$-reconstruction. It can be shown that if $d > 1$, then there there is $(r - dt)$-reconstruction in this scheme.

Definition 4 (Arithmetic Secret Sharing) *If* $K$ *is a finite field,* $d \geq 2$ *and* $t \geq 1$*, then* $\mathcal{C}$ *is an* $(n, t, d, r)$-arithmetic secret sharing scheme *(with secret-space* $S$ *and share-space* $K$*).*

Remark 1 (On Applications of Arithmetic Secret Sharing) *As a opposed to the notion of "plain secret sharing", which is very suggestive as to how it may actually be used in cryptographic protocols, the notion of arithmetic secret sharing is less intuitive. For instance, the way the properties of these schemes are exploited in secure computation can hardly be guessed straight from their definition. Please refer to [8] for a high-level explanation of two of the main applications of arithmetic secret sharing to secure computation. See also the references in Section 5.*

Definition 5 (Arithmetic Embeddings) *If* $\dim_K S = \dim_K C$ *(as vector spaces) and if* $d \geq 2$ *then* $\mathcal{C}$ *is an* $(n, d)$-arithmetic embedding *(of* $S$ *over* $K$*).*

Remark 2 *If* $d = 2$*, then the smallest* $n$ *such that an* $(n, 2)$*-arithmetic embedding of* $S$ *over* $K$ *exists is the* bilinear multiplication complexity *of* $S$ *over* $K$*, a classical notion from algebraic complexity theory [5]. 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 of a codex 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. Third, codices often support "efficient decoding" of the $S$-element even if a presentation $x \in C$ comes with some errors, by a linearization argument that makes generic use of the properties of the codex[1]. See [19] for efficient decoding in the presence of $t$ such errors in an $(n, t, 2, n-t)$-codex and see [8] for a more general result. Finally, it is also possible to define natural notions of duality. It is also sometimes useful to introduce additional parameters pertaining to $C$, its powers or some of their duals.

Definition 6 *Suppose $C \subset K^n$ is a $K$-linear subspace. Let $d \geq 1$ be an integer. Then $m_d(C)$ denotes the set of all $\mathbf{z} \in K^n$ such that $\mathbf{z} = \prod_{i=1}^{d} \mathbf{x}_i$ for some $(\mathbf{x}_1, \ldots, \mathbf{x}_d) \in C^d$.*

Definition 7 (Powers of a Space) *Suppose $C \subset K^n$ is a $K$-linear subspace. Let $d \geq 1$ be an integer. Then $C^{*d} \subset K^n$ is the $K$-linear subspace of $K^n$ generated by $m_d(C)$.*

## 3 Some Examples of Codices

We give some first examples. These are all based on (a generalization of) *Lagrange's Interpolation Theorem*:

Theorem 2 *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 $\deg f \leq M-1$.*

Proof. Since the $K$-dimensions on both sides are identical, it is sufficient to argue injectivity. Suppose $f \in K[X]_{\leq M-1}$, $f \neq 0$, has each of the $x_i$'s as a root. Since the $h_i$'s are pairwise co-prime, their product divides $f$. But then $\deg f \geq M$, a contradiction. △

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

Theorem 3 *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 $\mathbf{p}_0 \in \overline{\mathbb{F}_q} \setminus \mathbb{F}_q$ such that $\mathbb{F}_{q^k} = \mathbb{F}_q(\mathbf{p}_0)$. The map $\psi' : C \to \mathbb{F}_{q^k}$ is defined similarly to $\psi$, except

[1] In fact these properties allow us to apply a generalization of the arguments in Berlekamp-Welch decoding algorithm and the decoding algorithm based on error correcting pairs of [36]– see also [24]

that evaluation is at $\mathbf{p}_0$ instead of $q_1, \ldots, q_k$. The proofs for both cases are similar. We only argue the second.

First, the map $\psi'$ 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 $\mathbf{p}_0$. 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 $(\mathbf{u}, \mathbf{v}) \in \mathbb{F}_{q^k} \times \mathbb{F}_q^t$, there is a (unique) $f \in \mathbb{F}_q[X]_{\leq t+k-1}$ such that $f(\mathbf{p}_0) = \mathbf{u}$ and $(f(p_i))_{i \in A} = \mathbf{v}$. Since $C$ is identified with $\mathbb{F}_q[X]_{\leq t+k-1}$, there is a (unique) $\mathbf{c} \in C$ such that $\psi'(\mathbf{c}) = \mathbf{u}$ and $\pi_A(\mathbf{c}) = \mathbf{v}$.

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 $\psi'$, i.e., identify $\overline{\mathbf{c}} \in \overline{C}$ with its corresponding $\overline{f} \in \mathbb{F}_q[X]_{\leq r-1}$, followed by evaluation at $\mathbf{p}_0$. It follows that, for all $\mathbf{c}_1, \ldots, \mathbf{c}_d \in C$, $\overline{\psi}' \circ \pi_B(\mathbf{c}_1 \cdots \mathbf{c}_d) = \psi'(\mathbf{c}_1) \cdots \psi'(\mathbf{c}_d)$. $\triangle$

We now have the following examples.

1. For any $k > 1$, there is an $(2k-1, 0, 2, 2k-1)$-codex for $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ such that the dimension of the underlying $\mathbb{F}_q$-linear code equals $k$. This corresponds to a *bilinear multiplication algorithm* for $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$. This is a classical notion in algebraic complexity theory, see [5]. *Condition*: $q \geq 2k-1$.

2. *Shamir's secret sharing scheme* [39] is an $(n, t, 1, t+1)$-codex for $\mathbb{F}_q$ over $\mathbb{F}_q$. *Conditions*: $q > n$, $1 \leq t < n$.

3. If, additionally, $t < \frac{1}{2}n$, it has *multiplication*. If, in fact, $t < \frac{1}{3}n$, then it has *strong multiplication* (see [17]). This corresponds to an $(n, t, 2, n)$-codex for $\mathbb{F}_q$ over $\mathbb{F}_q$, respectively, an $(n, t, 2, n-t)$-codex for $\mathbb{F}_q$ over $\mathbb{F}_q$. These properties were first used in [4, 12] in the context of secure multi-party computation. *Conditions*: $q > n$, $1 \leq t < \frac{1}{2}n$ (resp. $1 \leq t < \frac{1}{3}n$).

4. *Franklin-Yung*'s variation [25] on Shamir's scheme, also known as a "packed secret sharing scheme" (with strong multiplication) corresponds to an $(n, t, 2, n-t)$-codex for $\mathbb{F}_q^k$ over $\mathbb{F}_q$. *Conditions*: $k \geq 1$, $q > n+k-1$, $1 \leq t < \frac{1}{3}(n-2k+2)$.

5. *A variation on Franklin-Yung*'s scheme [14], where $\mathbb{F}_q^k$ is replaced by $\mathbb{F}_{q^k}$. This corresponds to $(n, t, 2, n-t)$-codex for $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$. *Conditions*: $k > 1$, $q \geq n$, $1 \leq t < \frac{1}{3}(n-2k+2)$.

6. *Construction from Self-Dual Codes* [15]. Another type of elementary examples is as follows. Any $\mathbb{F}_q$-linear self-dual code of length $n+1$ and minimum distance $d \geq 2$, gives rise to an $(n, d-2, 2, n)$-codex for $\mathbb{F}_q$ over $\mathbb{F}_q$. Various other constructions based on general linear codes (e.g., high information rate ramp schemes with/without multiplicative properties) can also be found in [15]. A special case already appeared in [17], though in different language.

By using "the point at infinity" there is an "extra evaluation point" in several of the above constructions. For instance, in the 4th example this corresponds to the "degree $t+k-1$ coefficient" of the polynomials. This way, the condition in the 1st example becomes $q \geq 2k-2$

instead of $q \geq 2k-1$, in the 2nd and 3rd it becomes $q \geq n$ instead of $q > n$ and in the 4th it becomes $q \geq n+k-1$ instead of $q > n+k-1$.

# 4 Remarks on the Powering Operation

The powering operation is in general *not benign* as $C^{*d}$ may quickly fill all of $K^n$. So if $C$ has some "nice property" (typically requiring "redundancy"), then generally one should *not expect* $C^{*d}$ to have it as well (not even for small $d > 1$).

Here we give some easy indications why.

Lemma 1 *Suppose $C \subset K^n$ $(n > 1)$ is a $K$-linear subspace generated by $\mathbf{1}, \mathbf{x} \in C$, where $\mathbf{x}$ has pairwise distinct, non-zero coordinates and where $\mathbf{1}$ denotes the the vector* $(1, \ldots, 1) \in K^n$. *Then $C^{*(n-1)} = K^n$.*

Proof. This is a direct consequence of the properties of Vandermonde-determinants. The conditions imply that there are $n$ vectors in $C^{*(n-1)}$ that correspond one-to-one with the columns of some regular Vandermonde-matrix. Hence, $C^{*(n-1)}$ equals $K^n$. $\triangle$

Definition 8 (Distance and Dual Distance) *For a $K$-linear subspace $C \subset K^n$ with $C \neq \{\mathbf{0}\}, K^n$, define its* distance *$d_H(C)$ as the smallest Hamming-weight $w_H(x)$ taken over all non-zero vectors $\mathbf{x} \in C$. Moreover, define its* dual distance *$d_H^{\perp}(C)$ as $d_H(C^{\perp})$, where $C^{\perp} \subset K^n$ is the "orthogonal complement" of $C$, i.e., the $K$-linear space consisting of all vectors in $K^n$ orthogonal to $C$ (with respect to the standard inner product).*

Lemma 2 *Suppose $C \subset K^n$ $(n > 2)$ is a $K$-linear subspace with $C \neq \{\mathbf{0}\}, K^n$. Suppose $t$ is an integer such that $d_H^{\perp}(C) > t > 1$. Then $C^{*\lceil \frac{n-1}{t-1} \rceil} = K^n$.*

Proof. The conditions imply that $\pi_A(C) = K^t$ for all $A \subset \{1, \ldots, n\}$ with $|A| = t$. Now construct the $n$ standard basis-vectors $\mathbf{u}_i$ of $K^n$ one-by-one, as follows. Without loss of generality, consider just $\mathbf{u}_1 = (1, 0, \ldots, 0) \in K^n$. Select a vector in $C$ such that its "left-most" coordinate equals 1, followed by a window of $t - 1 > 0$ consecutive 0's. Next, do as before, except that the window of 0's starts right after where the previous ended. Repeat this until the "end of the vector has been reached" (where, in the very last step, the window may possibly be of smaller size than $t-1$, of course). This way, $\lceil \frac{n-1}{t-1} \rceil$ vectors in $C$ are obtained whose coordinate-wise product equals $\mathbf{u}_1$. $\triangle$

# 5 Asympotical Results

Asymptotic study of bilinear complexity of multiplication in finite extensions of a finite field was initiated by Chudnovsky and Chudnovsky [16] 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 and Zink [42] from their 1982 breakthrough improvement of the Gilbert-Vashamov error correcting bound (which relies on deep results from algebraic geometry [30] in combination with Goppa's idea [28] 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 and Vladuts [40]. See [5] for an overview, as well as for generalizations. Some more recent papers on the topic include [1, 11, 37].

Motivated by showing a suitable asymptotic version of the "Fundamental Theorem on Information-Theoretically Secure Multi-Party Computation" [4, 12] by Ben-Or, Goldwasser and Wigderson and Chaum, Crépeau and Damgaard from 1988, Chen and Cramer [13] 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 and Zink.

In 2007, the results of [13] played a central role in the surprising work of Ishai, Kushilevitz, Ostrovsky and Sahai [33] 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 [13] concern *two-party secure computation* [34, 21, 22], *OT-combiners* [29], *correlation extractors* [32], *amortized zero knowledge* [20] and *OT from noisy channels* [31]. For a full discussion and for some detailed examples of codices are used in applications, see [8].

The results of [13] were strengthened in [7]. A more powerful paradigm for the construction of arithmetic secret sharing schemes based on novel algebraic geometric ideas was presented in [8]. We first review the results from [13]. For terminology and theory on algebraic function fields, we refer to Stichtenoth [41] and for more details on the constructions, we refer to [13], [8].

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 4 (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 5 *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 6 ([13, 8]) *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 5 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 5, 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 [13] and [8] (or [9]) $\triangle$

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 7 *("Existence from solving by degree") [13] 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 3, 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 8 *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.*

For "good" constructions, $|\mathbb{P}^{(1)}(F)|$ should be as large as possible compared to $g(F)$. The classical Hasse-Weil bound gives an upper bound on 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 [30] first showed by using modular curves that $A(q) \geq \sqrt{q} - 1$ for any square $q$, i.e., $q = p^m$ where $p > 0$ is a prime integer and $m > 0$ is an even integer. Therefore, the Drinfeld-Vlăduţ upper bound is sharp for all square $q$. An explicit construction in this case was given by Garcia and Stichtenoth [26].

No single exact value of $A(q)$ is known if $q$ is a non-square. However, some important lower bounds are known. We mention here just two results. Recently, Garcia,Stichtenoth, Bassa and Beelen [27] showed an explicit tower of function fields over finite fields of the form $\mathbb{F}_{p^{2m+1}}$ ($p \geq 2$ an integer prime and $m > 0$ an integer) that implies $A(p^{2m+1}) \geq \frac{2(p^{m+1}-1)}{p+1+\epsilon}$ with $\epsilon = \frac{p-1}{p^m-1}$. Serre, using class field theory, showed 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 have the following asymptotical result by Chen and Cramer.

Theorem 9 *[13] Fix a finite field $\mathbb{F}_q$ and fix an integer $d \geq 2$. Suppose $A(q) > 2d$. There there exists an infinite family of codices $(n, t, d, n-t)$-codices for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ with uniformity such that $n \longrightarrow \infty$, $k = \Omega(n)$ and $t = \Omega(n)$.*

See [8] for the full statement, which also addresses efficient "recovery from $t$ malicious errors" (even in higher powers of the underlying codes). These schemes can be efficiently constructed and operated. Note that the condition in the theorem is satisfied, for instance, if $q$ is a square and $q > (2d+1)^2$, or if $q$ is sufficiently large.

Also, the condition $A(q) > 2d$ can be relaxed. First, in [7], a version of Theorem 9 is shown which is valid for any finite field $\mathbb{F}_q$, with $d = 2$. The idea is to combine Theorem 9 over an extension field $\mathbb{F}_{q^\ell}$ for which $A(q^\ell) > 4$ with a dedicated field descent involving an arithmetic embedding of $\mathbb{F}_{q^\ell}$ over $\mathbb{F}_q$. This descent annihilates uniformity, however. Moreover, it does not generalize to all fields $\mathbb{F}_q$ when $d > 2$.

In [8, 9], a more sophisticated and novel algebraic geometric approach for solving the Riemann-Roch systems is introduced. In Theorem 7 we have insisted in solving all equations $\ell(D_i) = 0$ of Theorem 6 by setting the parameters in such a way that $\deg D_i < 0$. However this does not necessarily lead to the best results. Instead, it not only uses information about the asymptotic ratio between the number of rational points and the genus, but also information on the ratio between (the logarithm of the) order of the $d$-torsion subgroup of the (degree-0 divisor) class group and the genus. Our notion of *torsion limit* of a tower of function fields introduced in [8] captures the combination. For instance, for an optimal tower (attaining the Drinfeld-Vladuts bound), we ask the latter ratio to be as small as possible. Considerations about the $d$-torsion arise because the "$d$-parameter" in codices causes some of the $m_i$'s to be equal to $d$. Our current most general approach to solving the associated Riemann-Roch systems then involves combinatorial arguments exploiting torsion limit information. Upper bounds for this torsion limit lead then to a significant weakening of the condition $A(q) > 2d$ from Theorem 9 while *maintaining uniformity* (which is important in some applications).

General bounds on the torsion limit can be obtained from a classical result on Abelian varieties by Weil and via the Weil-pairing, as shown in [8, 9]. However, as shown there as well, in some cases much better bounds can be established. The basic idea is to apply a combination of the Deuring-Shafarevich $p$-rank formula with the Riemann-Hurwitz genus formula to certain eligible Artin-Schreier towers so as to obtain a recursion involving $p$-ranks and genuses only, from which information about the torsion limit is finally extracted by solving the recursion. At present, one of the requirements for this idea to work is that, in consecutive steps of the extension, the "error terms" in both formulas (arising from ramification in the tower) differ by a non-zero constant so that, at the end of the day, the desired recursion is simply obtained from the two formulas by Gaussian Elimination. Further requirements in particular concern sufficiently precise knowledge of the genus in each step of the tower. Currently, the best results are attained by applying this idea to the tower defined (over any field $\mathbb{F}_q$ where $q = p^{2e}$ for some $e > 0$) by Garcia and Stichtenoth in [26]. There are some other optimal towers known where this idea applies as well, but there the result is not nearly as good [3].

Finally, it is very interesting to note that there is no elementary (probabilistic) construction known for the asymptotically good arithmetic secret sharing schemes from Theorem 9: the only known construction is algebraic geometric and requires asymptotically good towers of functions fields.[2] This is, so far, in contrast with the theory of error correcting codes, where asymptotically good families are implied by elementary (probabilistic) methods.[3]

# 6 Limitations

We now state some limitations on codices. We shall be primarily concerned with arithmetic secret sharing schemes.

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

Lemma 3 *[10] An $(n, t, d, r)$-codex for $S$ over $\mathbb{F}_q$ is in particular an $(n, t, 1, r-(d-1)t)$-codex for $S$ over $\mathbb{F}_q$.*

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

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 10 *[10] For any $(n, t, 1, r)$-codex for $S$ over $\mathbb{F}_q$ with $t \geq 1$ it holds that $r - t \geq \frac{n-t+1}{q}$.*

Note that there is a stronger version of this theorem that is stated in terms of the share-entropy, see [10] as well. As an application of Theorem 10, consider $(n, t, 2, n-t)$-codices for $\mathbb{F}_q$ over $\mathbb{F}_q$. These play a distinguished role in secure multi-party computation, see [17]. From Lemma 3, $\frac{3t}{n-1} \leq 1$. Note that equality can be achieved in the non-asymptotic case. Asymptotically, however, we have the following. Let $\mathbb{F}_q$ be a finite field. For each $n \geq 1$, let $T(n, q)$ denote the largest integer $t$ such that there exists a $(n, t, 2, n-t)$-codex for $\mathbb{F}_q$ over $\mathbb{F}_q$. Now define $\widehat{\tau}(q) = \limsup_{n\to\infty} \frac{3\cdot T(n,q)}{n-1}$.

Theorem 11 *[10] For each finite field $\mathbb{F}_q$, $\widehat{\tau}(q) < 1$.*

Note that, by [13, 7], $\widehat{\tau}(q) > 0$ for each finite field $\mathbb{F}_q$.

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

[2] This is also the case for asymptotically good arithmetic embeddings of finite field. Yet another, very recent example is that of binary linear codes with asymptotically good square [38].

[3] By [15], $(n, t, 2, n)$-codices for $\mathbb{F}_q$ over $\mathbb{F}_q$ with large $t$ are implied by self-dual $\mathbb{F}_q$-linear codes of length $n+1$ with large minimum distance $d$. While self-dual codes admit elementary asymptotically good constructions, these codices are not useful in any of the recent results we have mentioned, starting with [33]. At the cost of halving the information-rate, it is also possible to use random linear codes, see [15]. There are some relevant applications, though, for instance to *passive-case* i. t. secure MPC with single field elements as secrets. See [15, 14] also for generic constructions of high-information rate ramp schemes from arbitrary linear codes (as well as from algebraic geometric codes), where reconstruction (privacy) is argued from distance (dual distance) of the codes.

Theorem 12 *[10] 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 of length $n-t$, dimension $k$ (where $k$ is the dimension of $S$) and minimum distance at least $n-r+1$.*

Note that application of the Singleton bound implies $r \geq k+t$. A more interesting result, however, is obtained by applying, for example, the Griesmer bound. In combination with a dualization technique enabling stronger bounds for large $t$ and with Lemma 3, this implies the following.

Theorem 13 *[10] For any $(n, t, d, r)$-codex for $S$ over $\mathbb{F}_q$, where $t, d \geq 1$ 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 $S$, except for its $K$-dimension. We show a different limitation when $S = \mathbb{F}_{q^k}$ (see [5] for lower bounds on bilinear complexity).

Theorem 14 *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 is an $(n, t, d, r)$-codex $(C, \psi)$ for $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ and $d \geq q+1$ holds. Since $k \geq 2$, there are elements $x, y \in \mathbb{F}_{q^k} \setminus \{0\}$ with $x^{q-1} \neq y^{q-1}$. Let $\mathbf{c}, \mathbf{w} \in C$ be such that $\psi(\mathbf{c}) = x$ and $\psi(\mathbf{w}) = y$. Since $\mathbf{x}^q = \mathbf{x}$ for all $\mathbf{x} \in \mathbb{F}_q^n$, we have $\mathbf{c}^q \mathbf{w}^{d-q} = \mathbf{c}\mathbf{w}^{d-1}$. Let $\mathbf{a} \in C^d$ be such that its first $q$ coordinates equal $\mathbf{c}$ and the remaining $d-q$ equal $\mathbf{w}$ and let $\mathbf{b} \in C^d$ be such that its 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 $g : m_d(C^d) \rightarrow \mathbb{F}_{q^k}$, we have

$$g \circ m_d(\mathbf{a}) = g \circ m_d(\mathbf{b}).$$

On the other hand

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

This contradicts $(d, r)$-reconstruction of $(C, \psi)$. △

# References

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

[2] O. Barkol, Y. Ishai and E. Weinreb. On d-Multiplicative Secret Sharing. Journal of Cryptology, Volume 23, Number 4, pp. 580–593, 2012.

[3] A. Bassa, P. Beelen. The Hasse-Witt invariant in some towers of function fields over finite fields. Bulletin of the Brazilian Mathematical Society 41 (2010), no. 4, 567-582.

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

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

[6] I. Cascudo, R. Cramer, D. Mirandola, C. Padró, C. Xing, 2012.

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

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

[9] 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

[10] 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

[11] 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.

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

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

[14] H. Chen, R. Cramer, R. de Haan, I. Cascudo Pueyo. Strongly multiplicative ramp schemes from high degree rational points on curves. *Proc. of 27th Annual IACR EUROCRYPT*, Istanbul, Turkey, Springer Verlag LNCS, vol. 4965, pp. 451-470, April 2008.

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

[16] 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.

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

[18] R. Cramer, I. Damgaard, and U. Maurer. Span Programs and General Secure Multi-Party Computation. BRICS Technical Report Series RS-97-28, November 1997, Aarhus University. *Note*: early, weaker version of [17] that does include some relevant material that was left out of [17].

[19] R. Cramer, V. Daza, I. Gracia, J. Jiménez Urroz, G. Leander, J. Martí-Farré, C. Padró. On Codes, Matroids and Secure Multi-Party Computation from Linear Secret Sharing Schemes. *IEEE Transactions on Information Theory*, 54(6): 2644-2657 (2008), June 2008.

[20] R. Cramer, I. Damgaard, V. Pastro. On the Amortized Complexity of Zero Knowledge Protocols for Multiplicative Relations. *Proc. 6th ICITS*, 2012. Preliminary version at http://eprint.iacr.org/2011/301.

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

[22] I. Damgaard, S. Zakarias. Multiparty Computation for Boolean Circuits with Constant Overhead in the Preprocessing Model. Preprint, 2012. Available from `http://eprint.iacr.org/2012/512`.

[23] I. Duursma and S. Park. Coset bounds for algebraic geometric codes. Finite Fields and Their Applications, Volume 16, Issue 1, pp. 36-55, January 2010.

[24] I. Duursma. Algebraic geometry codes: general theory. In D. Ruano, E. Martínez-Moro, C. Munuera, editor, Advances in algebraic geometry codes, pages 1–48. World Scientific, New Jersey, 2008.

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

[26] 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.

[27] 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

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

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

[30] 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.

[31] 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.

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

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

[34] Y. Ishai, M. Prabhakaran, A. Sahai. Founding Cryptography on Oblivious Transfer-Efficiently. *Proc. of 28th Annual IACR CRYPTO*, Santa Barbara, Ca., USA, Springer Verlag LNCS, vol. 5157, pp. 572-591, August 2008.

[35] C. Padró. Applications of Combinatorics to Information-Theoretic Cryptography. Manuscript, September 2012. Available from `http://www3.ntu.edu.sg/home/carlespl/ceunotes.pdf`.

[36] R. Pellikaan. On decoding by error location and dependent sets of error positions. Discrete Math., vol. 106/107, pp. 369-381, 1992.

[37] H. Randriambololona. Bilinear complexity of algebras and the Chudnovsky-Chudnovsky interpolation method. Journal of Complexity, Volume 28, Issue 4, pp. 489-517, August 2012.

[38] H. Randriambololona. Asymptotically good binary linear codes with asymptotically good self-intersection spans. Preprint, 2012. See `http://arxiv.org/pdf/1204.3057v2.pdf`

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

[40] 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.

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

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

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