# The Torsion-Limit for Algebraic Function Fields and Its Application to Arithmetic Secret Sharing

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

[1] CWI Amsterdam, The Netherlands
i.cascudo@cwi.nl
[2] CWI Amsterdam & Mathematical Institute, Leiden University, The Netherlands
cramer@cwi.nl, cramer@math.leidenuniv.nl
[3] Division of Mathematical Sciences, Nanyang Technological University, Singapore
xingcp@ntu.edu.sg.

**Abstract.** An $(n, t, d, n-t)$-arithmetic secret sharing scheme (with uniformity) for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ is an $\mathbb{F}_q$-linear secret sharing scheme where the secret is selected from $\mathbb{F}_q^k$ and each of the $n$ shares is an element of $\mathbb{F}_q$. Moreover, there is $t$-privacy (in addition, any $t$ shares are uniformly random in $\mathbb{F}_q^t$) and, if one considers the $d$-fold "component-wise" product of any $d$ sharings, then the $d$-fold component-wise product of the $d$ respective secrets is $(n-t)$-wise uniquely determined by it. Such schemes are a fundamental primitive in information-theoretically secure multi-party computation. Perhaps counter-intuitively, secure *multi-party* computation is a very powerful primitive for *communication-efficient two-party* cryptography, as shown recently in a series of surprising results from 2007 on. Moreover, the existence of *asymptotically good* arithmetic secret sharing schemes plays a crucial role in their communication-efficiency: for each $d \geq 2$, if $A(q) > 2d$, where $A(q)$ is Ihara's constant, then there exists an infinite family of such schemes over $\mathbb{F}_q$ such that $n$ is unbounded, $k = \Omega(n)$ and $t = \Omega(n)$, as follows from a result at CRYPTO'06. Our main contribution is a novel paradigm for constructing asymptotically good arithmetic secret sharing schemes from towers of algebraic function fields. It is based on a new limit that, for a tower with a given Ihara limit and given positive integer $\ell$, gives information on the cardinality of the $\ell$-torsion sub-groups of the associated degree-zero divisor class groups and that we believe is of independent interest. As an application of the bounds we obtain, we relax the condition $A(q) > 2d$ from the CRYPTO'06 result substantially in terms of our torsion-limit. As a consequence, this result now holds over *nearly all finite fields* $\mathbb{F}_q$. For example, if $d = 2$, it is sufficient that $q = 8, 9$ or $q \geq 16$.

## 1 Introduction

An $(n, t, d, n-t)$-arithmetic secret sharing scheme (with uniformity) for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ is an $\mathbb{F}_q$-linear secret sharing scheme where $k, n, t \geq 1, d \geq 2$, the secret is selected from $\mathbb{F}_q^k$ and each of the $n$ shares is an element of $\mathbb{F}_q$. Moreover, there is $t$-privacy (in addition, any $t$ shares are uniformly random in $\mathbb{F}_q^t$) and, if one

P. Rogaway (Ed.): CRYPTO 2011, LNCS 6841, pp. 685–705, 2011.

considers the $d$-fold "component-wise" product of any $d$ sharings, then the $d$-fold component-wise product of the $d$ respective secrets is $(n-t)$-wise uniquely determined by it.

Such schemes, first based on Shamir's scheme and later abstracted and generalized, are fundamental to (information-theoretically) secure multi-party computation [2,6,15,10]. Please refer to Section 5 for details about two main, well-known applications. Note that both concern protocols for "secure multiplication" and that the properties of arithmetic secret sharing are used somewhat differently from what their definition perhaps seems to suggest on first encounter. Secure multiplication is a fundamental primitive in its own right, as secure multi-party computation is often based on combinations of secure addition and secure multiplication, the latter typically being demanding and involved while the former is typically much more straightforward. Arithmetic secret sharing allows efficient recovery of the secret in the presence of faulty shares, by a generalization of a result from [12] (see Section 5) and also gives rise to verifiable secret sharing [10].

A series of surprising results, concerning zero-knowledge for circuit satisfiability ("MPC in the Head"), two-party secure computation, OT-combiners, correlation extractors, and OT from noisy channels [23,24,18,22,13,21], has caused nothing less than a paradigm shift that perhaps appears even as counter-intuitive: secure *multi-party* computation is a very powerful abstract primitive for *communication-efficient two-party cryptography.* All these results use arithmetic secret sharing schemes, typically with $d = 2$ (see also [11] for an application with $d > 2$). Note that both [22,21] are information-theoretic in nature, require the uniformity property, and also use the error correction procedure.

Also surprisingly, the existence of *asymptotically good* arithmetic secret sharing schemes plays a crucial role in the communication-efficiency of these recent, fundamental results on two-party cryptography: as follows from [7], for each $d \geq 2$, if $A(q) > 2d$ (where $A(q)$ is Ihara's constant from algebraic geometry, see Section 2) then there exists an infinite family of such schemes over $\mathbb{F}_q$ such that $n$ is unbounded, $k = \Omega(n)$ and $t = \Omega(n)$. Using these schemes (for $d = 2$), "constant-rate communication" has been achieved in those results, due to the removal of logarithmic terms caused by approaches using (appropriate modes of) Shamir's scheme [32]. Note that the original motivation of [7] was to give a communication-efficient asymptotic version of the "fundamental theorem of perfect information-theoretically secure multi-party computation" of [2,6], by combining the asymptotically good scheme from [7] with the results from [10]. In particular, the field $\mathbb{F}_q$ of computation can be fixed, the number $n$ of players is unbounded, and a malicious $t$-adversary is tolerated with $t = \Omega(n)$.

In [9], an extension of [7] is given where $\mathbb{F}_q^k$ is replaced by $\mathbb{F}_{q^k}$. It follows by the results of [4] that asymptotically good $(n, t, d, n-t)$-arithmetic secret sharing schemes for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ exist over *any finite field*, with the caveat that the uniformity property does *not* hold after application of the dedicated descent technique to the result from [7]. Therefore, $A(q) > 2d$ is the weakest known condition under which asymptotically good $(n, t, d, n-t)$-arithmetic secret sharing schemes *with uniformity* (for $\mathbb{F}_q^k$ over $\mathbb{F}_q$) are known to exist. All these asymptotic results

rely crucially on good towers of algebraic function fields, and currently *do not seem to admit more elementary proofs avoiding this.*[1]

The Drinfeld-Vlăduţ bound states that $A(q) \leq \sqrt{q} - 1$. By Ihara [20], $A(q) = \sqrt{q} - 1$ if $q$ is a square. By Serre's Theorem [31], $A(q) \geq c \cdot \log q$ for some absolute real constant $c > 0$ (for which the current best lower bound is about $\frac{1}{96}$). If we take $d = 2$, for example, then the condition $A(q) > 4$ is satisfied if $q \geq 49$ is a square (alternatively, $q$ is a large enough cubic [3,1]) or if $q$ is *very* large. Thus, existence is unresolved for *many* values of $q$.

Our main contribution is a novel paradigm for constructing asymptotically good arithmetic secret sharing schemes from towers of algebraic function fields. It is based on a new limit that, for a tower with a given Ihara limit and given positive integer $\ell$, gives information on the cardinality of the $\ell$-torsion sub-groups of the associated degree-zero divisor class groups. Our "torsion limit," which we believe is of independent interest, can in general be upper bounded using Weil's classical theorem on torsion in Abelian varieties (and in many cases using the Weil-pairing). However, the resulting bound is far too pessimistic, as we present a tower for which our torsion limit is *considerably smaller*, yet it attains the Drinfeld-Vlăduţ bound.

By means of this paradigm, we *weaken* the condition $A(q) > 2d$ to $A(q) > 1 + J_d(q, A(q))$, where $J_d(q, A(q))$ upper-bounds a "$d$-torsion" rate (based on the logarithm of the cardinality of the $d$-torsion, divided by the genus) taken over all infinite families of curves defined over $\mathbb{F}_q$ such that the genus tends to infinity and such that the Drinfeld–Vlăduţ bound is attained.

More precisely, the bounds we obtain on this torsion limit allow us to show the existence of the claimed arithmetic secret sharing schemes by solving an appropriate system of "Riemann-Roch type of equations" over an algebraic function field (in fact, one such system for each algebraic function field in a given infinite family). Each such equation is of the form $\ell(\lambda_i X + Y_i) = 0$, where $X$ is the divisor to be solved for, $\lambda_i \in \{-1, d\}$, $Y_i$ is a given divisor, and $\ell(\cdot)$ denotes Riemann-Roch dimension. The solution $X$ of such a system defines a certain AG-code with properties as claimed. The necessity of studying $d$-torsion arises from the fact that $\lambda_i = d$ does occur.

Concretely, for $d = 2$ we prove that for *all* finite fields $\mathbb{F}_q$ with $q \geq 16$ (as well as for $q = 8, 9$), asymptotically good $(n, t, d, n - t)$-arithmetic secret sharing schemes with uniformity (for $\mathbb{F}_q^k$ over $\mathbb{F}_q$) exist. This settles existence in the affirmative for *nearly all finite fields*. As an application, the results from [22,21] can in principle be based on smaller finite fields.

Finally, using our paradigm we also improve the explicit lower bounds on the asymptotic optimal normalized corruption tolerance $\widehat{\tau}(q)$ from [4] for all $q$ with $q \leq 81$ and $q$ square, as well as for all $q$ with $q \leq 9$. For instance, $\widehat{\tau}(64) \geq 0.52$,

[1] The existence of asymptotically good $(n, t, 2, n)$-arithmetic secret sharing schemes for $\mathbb{F}_q$ over $\mathbb{F}_q$ (so $k = 1$!) can be shown by elementary means [8], with asymptotically good self-dual error correcting codes as a special case. But this is a *much weaker* class that neither supports the mentioned applications in two-party cryptography, nor the asymptotic version of the "fundamental MPC theorem" given in [7].

whereas previously the best known lower bound was 0.42. As an application, the asymptotic version of the Fundamental Theorem in principle tolerates a stronger adversary (by a constant factor). Our results also have a bearing on the study of the asymptotic complexity of multiplication in finite extension fields of $\mathbb{F}_q$, but we do not elaborate on this here.

This paper is organized as follows. Our main contributions are captured in Definition 2 (the torsion-limit), Theorem 1 (bounds for this limit), Theorem 6 (sufficient conditions for Riemann-Roch system solvability) and Main Theorems 1 and 2 (claimed arithmetic secret sharing schemes). After giving some preliminaries in Section 2, we introduce our torsion limit in Section 3 and show our bounds. In Section 4 we introduce Riemann-Roch systems of equations and show how these may be solved using the bounds from Section 3. In Section 5 we introduce an elementary framework in which our quantitative results can be conveniently stated and apply our bounds to obtain the claimed arithmetic secret sharing schemes. Efficiency issues are also discussed there.

## 2 Preliminaries

For a prime power $q$, let $\mathbb{F}_q$ be a finite field of $q$ elements. An *algebraic function field* over $\mathbb{F}_q$ in one variable is a field extension $F \supset \mathbb{F}_q$ such that $F$ is a finite algebraic extension of $\mathbb{F}_q(x)$ for some $x \in F$ that is transcendental over $\mathbb{F}_q$. $F/\mathbb{F}_q$ denotes a function field with full constant field $\mathbb{F}_q$; $g(F)$ and $N(F)$ are the genus and the number of rational places of $F$ respectively. $\mathbb{P}(F)$ denotes the set of places of $F$, which is an infinite set, and $\mathbb{P}^{(k)}(F)$ is the (finite) subset consisting of the places of degree $k$ of $F$. $N_i(F)$ is the number of rational places of the constant field extension $\mathbb{F}_{q^i}F$, i.e., $N_i(F) = N(\mathbb{F}_{q^i}F)$ (note that $N(F) = N_1(F)$); $\mathrm{Div}(F)$ is the divisor group of $F$ and $\mathrm{Div}^0(F)$ its subset consisting of the divisors of degree 0; $\mathrm{Prin}(F)$ is the principal divisor group of $F$; $\mathrm{Cl}(F)$ is the divisor class group $\mathrm{Div}(F)/\mathrm{Prin}(F)$ of $F$ and $\mathrm{Cl}_0(F) = \mathcal{J}_F$ is the zero divisor class group $\mathrm{Div}^0(F)/\mathrm{Prin}(F)$ of $F$, which is a finite group of cardinality $h(F) = |\mathrm{Cl}_0(F)|$ (the class number); $\mathcal{A}_r(F)$ is the set of effective divisors of degree $r \geq 0$, which is a finite set, and $A_r(F)$ denotes its cardinality; $\mathrm{Cl}_r(F)$ is the set of $\{[D] : \deg(D) = r\}$, where $[D]$ stands for the divisor class containing $D$ and $\mathrm{Cl}_r^+(F)$ is the subset of $\mathrm{Cl}_r(F)$ of classes which contain an effective divisor, i.e., $\{[D] : \deg(D) = r, D \geq 0\}$. In case there is no confusion, we omit $F$ in some of the above notations. For instance, $A_r(F)$ is denoted by $A_r$ if it is clear in the context. For a divisor $G$ of $F$, $\mathcal{L}(G) := \{f \in F^* : \mathrm{div}(f) + G \geq 0\} \cup \{0\}$ is its Riemann-Roch space. It is a finite dimensional space over $\mathbb{F}_q$. Its dimension $\ell(G)$ satisfies $\ell(G) = \deg(G) + 1 - g(F) + \ell(K - G)$ where $K$ is a canonical divisor of degree $2g(F)-2$ (Riemann-Roch theorem). Therefore, $\ell(G) \geq \deg(G)+1-g(F)$, with equality if $\deg(G) \geq 2g(G) - 1$. The zeta function of $F$ is defined by the following power series

$$Z_F(T) := \mathrm{Exp}\left(\sum_{i=1}^{\infty} \frac{N_i(F)}{i} T^i\right) = \sum_{i=0}^{\infty} A_i(F) T^i.$$

In fact (Weil), $Z_F(T) = \frac{L_F(T)}{(1-T)(1-qT)}$ where $L_F(T)$ is a polynomial of degree $2g(F)$ in $\mathbb{Z}[T]$, called *L-polynomial* of $F$. Furthermore, $L_F(0) = 1$. If we factorize $L_F(T)$ into a linear product $\prod_{i=1}^{2g(F)}(w_iT - 1)$ in $\mathbb{C}[T]$, then Weil showed that $|w_i| = \sqrt{q}$ for all $1 \leq i \leq 2g(F)$. The Functional Equation of the $L$-polynomial states $L_F(T) = q^{g(F)}T^{2g(F)}L_F(1/qT)$. Finally we know $L_F(1) = h(F)$. All these facts about the $L$-polynomial can be found in [34]. Again, when $F$ is clear from the context we write $Z(T)$ and $L(T)$ for its zeta function and $L$-polynomial, respectively. From the definition of zeta function, one obtains $N_m(F) = q^m + 1 - \sum_{i=1}^{2g(F)} w_i^m$ for all $m \geq 1$. This gives the Hasse-Weil bound $N(F) = N_1(F) \leq q + 1 + 2g(F)\sqrt{q}$. Define $N_q(g) = \max_F N(F)$, where $F$ ranges over all function fields of genus $g$ over $\mathbb{F}_q$, and define $A(q) := \limsup_{g\to\infty} N_q(g)/g$, Ihara's constant. Vlăduţ and Drinfeld showed $A(q) \leq \sqrt{q}-1$. Ihara [20] showed that $A(q) \geq \sqrt{q}-1$ for any square power $q$. Hence, $A(q) = \sqrt{q} - 1$ for all square powers. Zink [42], and Bezerra et al. [3] (see also Bassa et al. [1]) showed that $A(q^3) \geq \frac{2(q^2-1)}{q+2}$ Serre showed that there is a absolute constant $c > 0$ such that $A(q) \geq c \cdot \log(q)$ for all prime powers $q$. In [41], Xing and Yeo showed that $A(2) \geq 0.258$. Very recently, Duursma and Mak have reported in [14] the stronger bound $A(2) \geq 0.316$. For a family $\mathcal{F} = \{F/\mathbb{F}_q\}$ of function fields with $g(F) \to \infty$ such that $\lim_{g(F)\to\infty} N(F)/g(F)$ exists, one can define this limit to be the *Ihara* limit, denoted by $A(\mathcal{F})$. It is clear that there exists a family $\mathcal{E} = \{E/\mathbb{F}_q\}$ of function fields such that $g(E) \to \infty$ and the Ihara limit $A(\mathcal{E})$ is equal to $A(q)$.

Remark 1. *In general, we can define the Ihara limit for any family $\mathcal{F} = \{F/\mathbb{F}_q\}$ of function fields with $g(F) \to \infty$ by $\limsup_{g(F)\to\infty} N(F)/g(F)$. However, for convenience of this paper, we define the Ihara limit only for those families $\{E/\mathbb{F}_q\}$ whose limit $\lim_{g(E)\to\infty} N(E)/g(E)$ exists.*

## 3 Torsion Point Limits

For the applications in this paper, we are interested in considering, in addition to the Ihara limit of a family of function fields, a limit for the number of torsion points of the zero divisor class groups of these function fields.

Let $F/\mathbb{F}_q$ be a function field. For a positive integer $r > 1$, we denote by $\mathcal{J}_F[r]$ the $r$-torsion point group in $\mathcal{J}_F$, i.e., $\mathcal{J}_F[r] := \{[D] \in \mathcal{J}_F : r[D] = 0\}$.

Definition 1. *For each family $\mathcal{F} = \{F/\mathbb{F}_q\}$ of function fields with $g(F) \to \infty$, we define*

$$J_r(\mathcal{F}) := \liminf_{F\in\mathcal{F}} \frac{\log_q |\mathcal{J}_F[r]|}{g(F)}.$$

We define an asymptotic notion involving both $J_r(\mathcal{F})$ and the Ihara limit $A(\mathcal{F})$.

Definition 2 (The torsion-limit). *For a prime power $q$, $r \in \mathbb{Z}_{>1}$ and $a \in \mathbb{R}$, let $\mathfrak{F}$ be the set of families $\{\mathcal{F}\}$ of function fields over $\mathbb{F}_q$ such that genus in each family tends to $\infty$ and the Ihara limit $A(\mathcal{F}) \geq a$ for every $\mathcal{F} \in \mathfrak{F}$. Then the asymptotic quantity $J_r(q, a)$ is defined by $J_r(q, a) = \liminf_{\mathcal{F}\in\mathfrak{F}} J_r(\mathcal{F})$.*

Thus, for a given family, the limit $J_r(\mathcal{F})$ measures the $r$-torsion against the genus. The corresponding constant $J_r(q,a)$ measures, for a given Ihara limit $a$ and for given $r$, the "least possible $r$-torsion." Note that $A(q)$, Ihara's constant, is the supremum of $A(\mathcal{F})$ taken over all asymptotically good $\mathcal{F}$ over $\mathbb{F}_q$. Now we are ready to state the main results of this section.

THEOREM 1. *Let $\mathbb{F}_q$ be a finite field and let $r > 1$ be a prime.*

(i) *If $r \mid (q-1)$, then $J_r(q, A(q)) \leq \frac{2}{\log_r q}$.*
(ii) *If $r \nmid (q-1)$, then $J_r(q, A(q)) \leq \frac{1}{\log_r q}$*
(iii) *If $q$ is square and $r \mid q$, then $J_r(q, \sqrt{q}-1) \leq \frac{1}{(\sqrt{q}+1)\log_r q}$.*

The *first* part of Theorem 1, as well as the second part when, additionally, $r|q$, is proved directly using a theorem of Weil [38,27] on torsion in Abelian varieties. [2] The second part, in the case $r \nmid q$ and $r \nmid (q-1)$, can be proved by using Weil pairing for abelian varieties and we will show it in Section 3.1 below. The most interesting is perhaps the bound in the *third part*, which is substantially smaller (we prove that bound in Section 3.2).

THEOREM 2. *Let $\mathbb{F}_q$ be a finite field of characteristic $p$.*

(i) *If $r \geq 2$ is an integer, then $J_r(q, A(q)) \leq \log_q(dr)$, where $d = \gcd(r, q-1)$.*
(ii) *Write $r$ as $p^\ell m$ for some $\ell \geq 0$ and a positive integer $m$ co-prime to $p$. If $q$ is a square, then $J_r(q, \sqrt{q}-1) \leq \frac{\ell}{\sqrt{q}+1}\log_q(p) + \log_q(cm)$, where $c = \gcd(m, q-1)$.*

PROOF. The result follows quite directly from the case of prime $r$ considered in Theorem 1 together with some observations about group torsion. We prove this formally in Section 3.3 below. △

Finally, we show existence of certain function field families that is essential for our applications in Section 5.

THEOREM 3. *For every $q \geq 8$ except for $q = 11$ or $13$, there exists a family $\mathcal{F}$ of function fields over $\mathbb{F}_q$ such that the Ihara limit $A(\mathcal{F})$ exists and it satisfies $A(\mathcal{F}) > 1 + J_2(\mathcal{F})$.*

PROOF. We prove it in two steps. The first one is to prove that the result is true for all $q \geq 17$ by using class field theory. The second step is to show that the result holds for $q = 8, 9, 16$ by looking at each individual $q$. For $q \geq 17$, we prove the result only for odd $q$. For even $q$, we can similarly get it by considering the Artin-Schreier extensions. Choose 7 nonzero square elements $t_1, \ldots, t_7$ in $\mathbb{F}_q$ (this is possible since $(q-1)/2 \geq 7$). For each $i$, consider the extension $K_i = \mathbb{F}_q(x, y_i)$, where $y_i^2 = x + t_i$. Then the place $x$ is completely splitting in

[2] If $K$ is algebraically closed, then, for any $m \neq 0$, $A[m]$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^{2g}$ if $m$ is co-prime to the characteristic $p$ of $K$; and $A[p]$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^a$ for some $0 \leq a \leq g$, where $g$ is the dimension of $A$. See also [30]. This implies upper bounds if $K$ is not algebraically closed.

$K_i$. Let $K$ be the field $\mathbb{F}_q(x,y)$, where $y^2 = \prod_{i=1}^{7}(x+t_i)$. Then $K$ is a subfield of $K_1 \cdots K_7/\mathbb{F}_q(x)$ such that $[K : \mathbb{F}_q(x)] = 2$ and $K_1 \cdots K_7/K$ is an unramified abelian extension. The three places, $\infty$ and those lying above $x$, are completely splitting in $K_1 \cdots K_7/K$. Since the 2-rank of the Galois group of $K_1 \cdots K_7/K$ is 6 which is equal to $2 + 2\sqrt{3+1}$, $K$ has an infinite $(2,S)$-Hilbert class field tower $\mathcal{F}$, where $S$ consists of the three places $\infty$ and those lying above $x$. This yields $A(\mathcal{F}) \geq 3/(g(K)-1) = 3/2$ (see [31] or [29, Corollary 2.7.8]). Now we have $A(\mathcal{F}) \geq 3/2 > 1 + 2/\log_2(17) \geq 1 + 2/\log_2 q \geq 1 + J_2(\mathcal{F})$. For $q = 8$, by the lower bound for cubics from Section 2 we know that there exists a family $\mathcal{F}$ over $\mathbb{F}_8$ such that $A(\mathcal{F}) \geq 3/2$. Thus, $A(\mathcal{F}) \geq \frac{3}{2} > 1 + \frac{1}{3} \geq 1 + J_2(\mathcal{F})$. For $q = 9$, by the result for squares from Section 2 we know that there exists a family $\mathcal{F}$ over $\mathbb{F}_9$ such that $A(\mathcal{F}) = 2$. Thus, $A(\mathcal{F}) = 2 > 1 + \frac{2}{\log_2 9} \geq 1 + J_2(\mathcal{F})$. For $q = 16$, by the result for squares from Section 2 we know that there exists a family $\mathcal{F}$ over $\mathbb{F}_{16}$ such that $A(\mathcal{F}) = 3$. Thus, $A(\mathcal{F}) = 3 > 1 + \frac{1}{4} \geq 1 + J_2(\mathcal{F})$. △

### 3.1 Proof Theorem 1(ii)

For an abelian variety $A$ defined over a field $k$ and a positive integer $m$, the $m$-torsion point group, denoted by $A[m]$, is defined to be the set of the points over the algebraic closure $\bar{k}$ annihilated by $m$. We know that $A[m]$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^{2g}$ if $m$ is co-prime to the characteristic $p$ of $k$; and $A[p]$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^a$ for a non-negative integer $a \leq g$, where $g$ is the dimension of $A$ (see [38,27]). We also denote by $A(k)$ the set of $k$-rational points. Thus, the set of $m$-torsion $k$-rational points is $A(k)[m] = A(k) \cap A[m]$. If $m$ is co-prime with the characteristic of $k$, then we can define the Weil pairing to be a map $e_m$ from $A[m] \times \hat{A}[m]$ to $G_m$, where $\hat{A}$ denotes the dual abelian variety of $A$ and $G_m \simeq \mathbb{Z}/m\mathbb{Z}$ is the group of $m$-th roots of unity in $\bar{k}$. The Weil paring $e_m$ has some properties such as bilinear, non-degenerate, commuting with the Galois action of $\mathrm{Gal}(\bar{k}/k)$ (see [26]), etc. More precisely:

(i) $e_m(S_1+S_2,T) = e_m(S_1,T)e_m(S_2,T)$; $e_m(S,T_1+T_2) = e_m(S,T_1)e_m(S,T_2)$;
(ii) If $e_m(S,T) = 1$ for all $S \in A[m]$, then $T = 0$;
(iii) $e_m(S^\sigma, T^\sigma) = e_m(S,T)^\sigma$.

If there is a polarization $\lambda$ from $A$ to $\hat{A}$, we get a pairing: $e_m^\lambda$ from $A[m] \times A[m]$ to $G_m$ defined by $e_m^\lambda(P,Q) = e_m(P,\lambda(Q))$. From now on, we assume that $A$ is a Jacobian over $k$. Then there is a principal polarization $\lambda$ from $A$ to $\hat{A}$ which is an isomorphism. In this case, we denote $e_m^\lambda$ by $w_m$, i.e., $w_m$ is a pairing from $A[m] \times A[m]$ to $G_m$. It is clear that $w_m$ satisfies all three properties above as well. From the bilinear property, we have $w_m(tP,Q) = w_m(P,Q)^t$ and $w_m(P,tQ) = w_m(P,Q)^t$ for any $t \geq 0$ and $P, Q \in A[m]$. To derive an upper bound on the size of $r$-torsion points, we need the following result which can be derived easily by using linear algebra.

Lemma 1. *For a prime $r$, consider an $\mathbb{F}_r$-vector space $W$ of dimension $n$ and a non-degenerate bilinear map $e : W \times W \longrightarrow \mathbb{F}_r$, i.e., $e(\mathbf{x}+\mathbf{z},\mathbf{y}) = e(\mathbf{x},\mathbf{y}) + e(\mathbf{z},\mathbf{y})$,*

*$e(\mathbf{x}, \mathbf{y}+\mathbf{z}) = e(\mathbf{x}, \mathbf{y}) + e(\mathbf{x}, \mathbf{z})$, and if $e(\mathbf{x}, \mathbf{u}) = 0$ for all $\mathbf{x} \in W$, then $\mathbf{u} = \mathbf{0}$. If $V$ is an $\mathbb{F}_r$-subspace of $W$ with $e(\mathbf{x}, \mathbf{y}) = 0$ for all $\mathbf{x}, \mathbf{y} \in V$, then $\dim_{\mathbb{F}_r} V \leq n/2$.*

Applying Lemma 1 to the Weil paring $w_r$, we obtain the following:

COROLLARY 1. *If $V$ is an $\mathbb{F}_r$-subspace of $A[r]$ such that $w_r(P, Q) = 1$ for all $P, Q \in V$, then $\dim_{\mathbb{F}_r}(V) \leq g$.*

PROOF. Let $\zeta$ be a $r$th primitive root of unity and consider the bilinear map $(P, Q) \mapsto a \in \mathbb{Z}/r\mathbb{Z}$, where $a$ satisfies $\zeta^a = w_r(P, Q)$. Now apply Lemma 1. △

PROPOSITION 1. *Let $k = \mathbb{F}_q$ and assume that a prime $r$ does not divide $q - 1$. If $A$ is a Jacobian variety over $k$, then $\dim(A(k)[r]) \leq g$.*

PROOF. If $r$ is the characteristic of $k$, then it follows from the Weil bound. Now assume that $r$ is not the characteristic of $k$. It is easy to verify that $A(k)[r]$ is an $\mathbb{F}_r$-subspace of $A[r]$. For any $\sigma$ in the Galois group $\mathrm{Gal}(\bar{k}/k)$, one has $w_r(P, Q) = w_r(P^\sigma, Q^\sigma) = w_r(P, Q)^\sigma$. This implies that $w_r(P, Q)$ is an element of $k$. However, the only $r$-th root of unity in $k$ is 1. We get $w_r(P, Q) = 1$ for all $P, Q \in A(k)[r]$. Our desired result follows from Corollary 1. △

### 3.2 Proof of Theorem 1(iii)

Let $\mathbb{F}_q$ be a finite field. Write $p$ for its characteristic. For a function field $F$ over $\mathbb{F}_q$ denote by $\gamma(F)$ the $p$-rank of $F$. It holds that $\gamma(F) \geq \log_p(J_F[p])$. Assume $q$ is a square. Consider the tower $\mathcal{F} = (F^{(0)} \subset F^{(1)} \subset \cdots)$ over $F_q$ introduced in [16], recursively defined by $F^{(0)} = \mathbb{F}_q(x_0)$ and $F^{(n+1)} = F^{(n)}(x_{n+1})$, where $x_n^{\sqrt{q}-1} x_{n+1}^{\sqrt{q}} + x_{n+1} = x_n^{\sqrt{q}}$. The following facts can be found in [16].

1. The tower $\mathcal{F}$ attains Drinfeld-Vlăduţ bounds, i.e., its limit $A(\mathcal{F})$ is given by $A(\mathcal{F}) := \lim_{n\to\infty} \frac{N(F^{(n)})}{g(F^{(n)})} = \sqrt{q} - 1$.
2. For any place $P \in \mathbb{P}(F^{(n-1)})$ and any place $Q \in \mathbb{P}(F^{(n)})$ such that $Q|P$ we have $d(Q|P) = (\sqrt{q} + 2)(e(Q|P) - 1)$, where $d(Q|P)$ and $e(Q|P)$ denote the different exponent and ramification index.
3. $g(F^{(n)}) = q^{\frac{n+1}{2}} + q^{\frac{n}{2}} - q^{\frac{n+2}{4}} - 2q^{\frac{n}{2}} + 1$ if $n \equiv 0 \pmod 2$ and $g(F^{(n)}) = q^{\frac{n+1}{2}} + q^{\frac{n}{2}} - \frac{1}{2}q^{\frac{n+3}{4}} - \frac{3}{2}q^{\frac{n+1}{4}} - q^{\frac{n-1}{4}} + 1$ if $n \equiv 1 \pmod 2$.

We will now show

THEOREM 4. *It holds that $\gamma(F^{(n)}) = (\sqrt{q}^{n/2} - 1)^2$ if $n \equiv 0 \pmod 2$ and $\gamma(F^{(n)}) = (\sqrt{q}^{(n-1)/2} - 1)(\sqrt{q}^{(n+1)/2} - 1)$ if $n \equiv 1 \pmod 2$.*
*In particular $\lim_{n\to\infty} \frac{g(F^{(n)})}{\gamma(F^{(n)})} = \sqrt{q} + 1$.*

Then Theorem 1(iii) is a direct corollary of the above theorem.

Without loss of generality we can assume that the constant fields of the function fields are $\overline{\mathbb{F}}_q$. We will use the following theorem.

THEOREM 5 (DEURING-SHAFAREVICH (SEE E.G. [19])). *Let $E/F$ be a Galois extension of function fields over $\overline{\mathbb{F}}_q$. Suppose its Galois group is a p-group.*
*Then* $\gamma(E) - 1 = [E : F](\gamma(F) - 1) + \sum_{P\in\mathbb{P}(F)} \sum_{Q\in\mathbb{P}(E),Q|P}(e(Q|P) - 1)$.

PROOF OF THEOREM 4: Consider the extension $F^{(n)}/F^{(n-1)}$. As this is an Artin-Schreier extension, it is Galois and its Galois-group is a $p$-group. By Riemann-Hurwitz (see e.g. [34] and fact 2. above), and by Deuring-Shafarevich, respectively,

$$2\cdot g(F^{(n)})-2 = \sqrt{q}\cdot(2g(F^{(n-1)})-2)+(\sqrt{q}+2)\cdot \sum_{P\in\mathbb{P}(F^{(n-1)})} \sum_{\substack{Q\in\mathbb{P}(F^{(n)})\\ Q|P}} (e(Q|P)-1),$$

$$\gamma(F^{(n)}) - 1 = \sqrt{q}\cdot(\gamma(F^{(n-1)}) - 1) + \sum_{P\in\mathbb{P}(F^{(n-1)})} \sum_{\substack{Q\in\mathbb{P}(F^{(n)})\\ Q|P}} (e(Q|P) - 1).$$

Combining these two equations we find

$$\gamma(F^{(n)}) = \sqrt{q}\cdot\gamma(F^{(n-1)})+2\cdot(g(F^{(n)})-2\sqrt{q}\cdot g(F^{(n-1)})-\sqrt{q}^2+\sqrt{q})(\sqrt{q}+2)^{-1}.$$

Using the fact that $\gamma(F^{(0)}) = 0$ and applying induction, the result follows. △

### 3.3 Proof of Theorem 2

We first show how to lift the previous results from $A(k)[r]$ to $A(k)[r^t]$.

LEMMA 2. *Let $k = \mathbb{F}_q$ and let $r$ be a prime. If $A$ is an Abelian variety over $k$ with $|A(k)[r]| \le a$, then $|A(k)[r^t]| \le a^t$ for every $t \ge 1$.*

PROOF. We prove it by induction. The case $t = 1$ is the given condition. Assume it holds for $t-1$. Consider the map $[r]_k : A(k)[r^t] \to A(k)[r^{t-1}], P \mapsto rP$. Clearly the kernel of $[r]_k$ is $A(k)[r]$. Thus, $|A(k)[r^t]| = |\mathrm{Ker}([r]_k)| \times |\mathrm{Im}([r]_k)| \le a \times a^{t-1} = a^t$. The desired result follows. △

PROPOSITION 2. *Let $k = \mathbb{F}_q$ and assume that a prime $r$ does not divide $q - 1$.*

1. *If $A$ is a Jacobian variety over $k$, then $|A(k)[r^t]| \le r^{gt}$ for every $t \ge 1$.*
2. *If $m \ge 2$ is an integer, then $|A(k)[m]| \le (dm)^g$, where $d = \gcd(m, q - 1)$.*

PROOF. Part 1 is the direct result of Proposition 1 and Lemma 2. To prove Part 2, we factorize $m$ into the product $\prod_p p^{s_p} \times \prod_\ell \ell^{s_\ell}$ of prime powers, where $d = \prod_p p^{s_p}$ is a factor of $q - 1$ and $\prod_\ell \ell^{s_\ell} = m/d$. By Part 1 and the following isomorphism $A(k)[m] \simeq \prod_p A(k)[p^{s_p}] \times \prod_\ell A(k)[\ell^{s_\ell}]$, we have $|A(k)[m]| = |\prod_p A(k)[p^{s_p}]| \times \prod_\ell |A(k)[\ell^{s_\ell}]| \le d^{2g} \times (m/d)^g = (dm)^g$. △

Theorem 1(iii), Lemma 2, and Proposition 2 now imply Theorem 2.

## 4 Riemann Roch Systems of Equations

Let $F/\mathbb{F}_q$ be an algebraic function field.

Definition 3. Let $L \in \mathbb{Z}_{>0}$ and let $Y_i \in \mathrm{Cl}(F)$, $d_i \in \mathbb{Z} \setminus \{0\}$ for $i = 1, \ldots, L$. The *Riemann-Roch system of equations* in the indeterminate $X$ is the system $\{\ell(d_i X + Y_i) = 0\}_{i=1}^{L}$ determined by these data. A solution is some $[G] \in \mathrm{Cl}(F)$ which satisfies all equations when substituted for $X$.

It is often more convenient to define systems over $\mathrm{Div}(F)$ rather than $\mathrm{Cl}(F)$. The idea of using Riemann-Roch systems of equations was already present in some papers, e.g. [36], [39], [40]. However, those systems are less general, namely they have $d_i = \pm 1$ for all $i$.[3] The following theorem shows that a solution of degree $s$ exists if a certain numerical condition is satisfied that involves the class number, the number $A_{r_i}$ of effective divisors of degree $r_i$ and the cardinality of the $d_i$-torsion subgroups of the degree-zero divisor class group, where the $d_i$ are determined by the system and the $r_i$ are determined by $s$ and the $d_i$.

Theorem 6. *Consider the Riemann-Roch system* $\{\ell(d_i X + Y_i) = 0\}_{i=1}^{L}$. *Write* $s_i = \deg Y_i$ *for* $i = 1, \ldots, L$. *Denote by* $A_r$ *the number of effective divisors of degree* $r$ *in Div*$(F)$ *for* $r \geq 0$, *and* $0$ *for* $r < 0$. *Let* $s \in \mathbb{Z}$ *and define* $r_i = d_i s + s_i$ *for* $i = 1, \ldots, L$. *If* $h > \sum_{i=1}^{L} A_{r_i} \cdot |\mathcal{J}_F[d_i]|$, *then the Riemann-Roch system has a solution* $[G] \in Cl_s(F)$.

Proof. Let $S$ be the set $\{1 \leq i \leq L : \ r_i \geq 0\}$. For each $i \in S$, we argue as follows. Define the maps $\phi_i : \mathrm{Cl}_s(F) \to \mathrm{Cl}_{d_i s}(F), \quad X \mapsto d_i X$ and $\psi_i : \mathrm{Cl}_{d_i s}(F) \to \mathrm{Cl}_{r_i}(F), \quad X' \mapsto X' + Y_i$. Then $\psi_i$ is an injection and each image under $\phi_i$ has exactly $|\mathcal{J}_F[d_i]|$ pre-images. Write $\sigma_i = \psi_i \circ \phi_i$. Then, for any element $Z \in \mathrm{Cl}^+_{r_i}(F)$, $|\sigma_i^{-1}(Z)| \leq |\mathcal{J}_F[d_i]|$. Hence, $|\sigma_i^{-1}(\mathrm{Cl}^+_{r_i}(F))| \leq A_{r_i} \cdot |\mathcal{J}_F[d_i]|$. Thus, $\bigcup_{i \in S} \sigma_i^{-1}(\mathrm{Cl}^+_{r_i}(F))| \leq \sum_{i \in S} A_{r_i} \cdot |\mathcal{J}_F[d_i]|$. Since by hypothesis we have $|\mathrm{Cl}_s(F)| = h > \sum_{i=1}^{L} A_{r_i} \cdot |\mathcal{J}_F[d_i]| = \sum_{i \in S} A_{r_i} \cdot |\mathcal{J}_F[d_i]|$, there is an element $[G] \in \mathrm{Cl}_s(F) \setminus \bigcup_{i \in S} \sigma_i^{-1}(\mathrm{Cl}^+_{r_i}(F))$. Since $\sigma_i([G]) \in \mathrm{Cl}_{r_i}(F)$ but $\sigma_i([G]) \notin \mathrm{Cl}^+_{r_i}(F)$, it follows that $\ell(\sigma_i([G])) = 0$ for $i \in S$, i.e., $[G]$ is a solution of the system $\{\ell(d_i X + Y_i + T_i) = 0\}_{i \in S}$. Finally $[G]$ is also a solution of $\{\ell(d_i X + Y_i) = 0\}_{i \notin S}$, because $\deg(d_i[G] + Y_i) = r_i < 0$ for all $i \notin S$. △

Remark 2. ("Solving by taking any divisor $X$ of large enough degree")

(i) If $r_i < 0$ for all $i = 1, \ldots, L$, then the inequality in Theorem 6 is automatically satisfied and hence the Riemann-Roch system always has a solution.
(ii) For instance, in [7], it was simply assumed that $r_i < 0$ to obtain $(n, t, d, n-t)$-arithmetic secret sharing schemes. But this does not always give the best results. In particular, in Section 5, we will show how we can employ Theorem 6 to get improvements, *especially for small finite fields*.

[3] In [33], the case $d_i = 2$ was considered but their result must be corrected for torsion.

## 5 Application to Arithmetic Secret Sharing

We first recall the results of [7], cast in a novel, technical framework.[4] This will make it possible to state our main quantitative results on arithmetic secret sharing in transparent language, which also facilitates easy comparison with earlier work. Let $k, n$ be integers with $k, n \geq 1$. Consider the $\mathbb{F}_q$-vector space $\mathbb{F}_q^k \times \mathbb{F}_q^n$, where $\mathbb{F}_q$ is an arbitrary finite field.

Definition 4. *The $\mathbb{F}_q$-vector space morphism $\pi_0 : \mathbb{F}_q^k \times \mathbb{F}_q^n \to \mathbb{F}_q^k$ is defined by the projection $(s_1, \ldots, s_k, c_1, \ldots, c_n) \mapsto (s_1, \ldots, s_k)$. For each $i \in \{1, \ldots, n\}$, the $\mathbb{F}_q$-vector space morphism $\pi_i : \mathbb{F}_q^k \times \mathbb{F}_q^n \to \mathbb{F}_q$ is defined by the projection $(s_1, \ldots, s_k, c_1, \ldots, c_n) \mapsto c_i$. For $\emptyset \neq A \subset \{1, \ldots, n\}$, the $\mathbb{F}_q$-vector space morphism $\pi_A : \mathbb{F}_q^k \times \mathbb{F}_q^n \to \mathbb{F}_q^{|A|}$ is defined by the projection $(s_1, \ldots, s_k, c_1, \ldots, c_n) \mapsto (c_i)_{i \in A}$. For $\mathbf{v} \in \mathbb{F}_q^k \times \mathbb{F}_q^n$, it is sometimes convenient to denote $\pi_0(\mathbf{v}) \in \mathbb{F}_q^k$ by $\mathbf{v}_0$ and $\pi_A(\mathbf{v}) \in \mathbb{F}_q^{|A|}$ by $\mathbf{v}_A$. We write $\mathcal{I}^* = \{1, \ldots, n\}$. It is also sometimes convenient to refer to $\mathbf{v}_0$ as the* secret-component *of $\mathbf{v}$ and to $\mathbf{v}_{\mathcal{I}^*}$ as its* shares-component*.*

Definition 5. *An $n$-code for $\mathbb{F}_q^k$ (over $\mathbb{F}_q$) is an $\mathbb{F}_q$-vector space $C \subset \mathbb{F}_q^k \times \mathbb{F}_q^n$ such that $\pi_0(C) = \mathbb{F}_q^k$ and $(\operatorname{Ker} \pi_{\mathcal{I}^*}) \cap C \subset (\operatorname{Ker} \pi_0) \cap C$. For $\mathbf{c} \in C$, $\mathbf{c}_0 \in \mathbb{F}_q^k$ is the* secret *and $\mathbf{c}_{\mathcal{I}^*} \in \mathbb{F}_q^n$ the* shares*.*

The first condition means that, in $C$, the secret can take any value in $\mathbb{F}_q^k$. More precisely, for a uniformly random vector $\mathbf{c} \in C$, the secret $\mathbf{c}_0$ is uniformly random in $\mathbb{F}_q^k$. This follows from the fact that the projection $(\pi_0)_{|C}$ is regular (since it is a surjective $\mathbb{F}_q$-vector space morphism). The second condition means that the shares uniquely determine the secret. Indeed, the shares do not always determine the secret uniquely if and only if there are $\mathbf{c}, \mathbf{c}' \in C$ such that their shares coincide but not their secrets. Therefore, by linearity, the shares determine the secret uniquely if and only if the shares being zero implies the secret being zero. Moreover this condition implies that $k \leq n$. Note that an $n$-code with the stronger condition $(\operatorname{Ker} \pi_{\mathcal{I}^*}) \cap C = (\operatorname{Ker} \pi_0) \cap C$ is a $k$-dimensional error correcting code of length $n$.

Definition 6 ($r$-reconstructing). *An $n$-code $C$ for $\mathbb{F}_q^k$ is* $r$-reconstructing *($1 \leq r \leq n$) if $(\operatorname{Ker} \pi_A) \cap C \subset (\operatorname{Ker} \pi_0) \cap C$ for each $A \subset \mathcal{I}^*$ with $|A| = r$.*

In other words, $r$-reconstructing means that any $r$ shares uniquely determine the secret. Note that $r \leq n$ by definition of an $n$-code.

Definition 7 ($t$-Disconnected). *An $n$-code $C$ for $\mathbb{F}_q^k$ is* $t$-disconnected *if $t = 0$ or else if $1 \leq t < n$, the projection $\pi_{0,A} : C \longrightarrow \mathbb{F}_q^k \times \pi_A(C)$, $\mathbf{c} \mapsto (\pi_0(\mathbf{c}), \pi_A(\mathbf{c}))$ is surjective for each $A \subset \mathcal{I}^*$ with $|A| = t$. If, additionally, $\pi_A(C) = \mathbb{F}_q^t$, we say $C$ is* $t$-uniform*.*

[4] This is a special case of the notion of an *(arithmetic) codex* that we introduced in an invited talk at EUROCRYPT'11 and, earlier, at the IPAM workshop on Information-Theoretic Cryptography.

If $t > 0$, then $t$-disconnectedness means the following. Let $A \subset \mathcal{I}^*$ with $|A| = t$. Then, for uniformly randomly $\mathbf{c} \in C$, the secret $\mathbf{c}_0$ is independently distributed from the $t$ shares $\mathbf{c}_A$. Indeed, for the same reason that the secret $\mathbf{c}_0$ is uniformly random in $\mathbb{F}_q^k$, it holds that $(\mathbf{c}_0, \mathbf{c}_A)$ is uniformly random in $\mathbb{F}_q^k \times \pi_A(C)$. Since the uniform distribution on the Cartesian-product of two finite sets corresponds to the uniform distribution on one set, and independently, the uniform distribution on the other, the claim follows. Uniformity means that, in addition, $\mathbf{c}_A$ is uniformly random in $\mathbb{F}_q^t$.

Definition 8 (Generator of an $n$-Code). *A* generator $(k_0, \sigma)$ *of an $n$-code $C$ consists of a positive integer $k_0$ and a surjective $\mathbb{F}_q$-vector space morphism $\sigma : \mathbb{F}_q^k \times \mathbb{F}_q^{k_0} \longrightarrow C$, such that $\pi_0(\sigma(\mathbf{s}, \mathbf{z})) = \mathbf{s}$ for all $(\mathbf{s}, \mathbf{z}) \in \mathbb{F}_q^k \times \mathbb{F}_q^{k_0}$.*

In particular, a generator selects an element of $C$ with a prescribed secret. We can always assume $k_0 \leq n$. Note that a generator can be represented by a matrix defined by the columns (or rows, depending on one's view) $\sigma(\mathbf{e}_1, \mathbf{0}), \ldots, \sigma(\mathbf{e}_k, \mathbf{0})$, $\sigma(\mathbf{0}, \mathbf{e}'_1), \ldots, \sigma(\mathbf{0}, \mathbf{e}'_{k_0})$, where the $\mathbf{e}_i$'s are the standard unit-vectors in $\mathbb{F}_q^k$, and the $\mathbf{e}'_j$'s are the standard unit-vectors in $\mathbb{F}_q^{k_0}$. Given such a matrix-representation, selecting a uniformly random $\mathbf{c} \in C$ such that its secret equals some prescribed value, can be done efficiently. By elementary linear algebra, this also holds for $r$-reconstruction of a secret. Similarly, a generator can be computed efficiently from a basis of $C$.

Definition 9 (Powers of an $n$-Code). *Let $m \in \mathbb{Z}_{>0}$. For $\mathbf{x}, \mathbf{x}' \in \mathbb{F}_q^m$, their* product $\mathbf{x} * \mathbf{x}' \in \mathbb{F}_q^m$ *is defined as $(x_1 x'_1, \ldots, x_m x'_m)$. Let $d$ be a positive integer. If $C$ is an $n$-code for $\mathbb{F}_q^k$, then $C^{*d} \subset \mathbb{F}_q^k \times \mathbb{F}_q^n$ is the $\mathbb{F}_q$-linear subspace generated by all terms of the form $\mathbf{c}^{(1)} * \ldots * \mathbf{c}^{(d)}$ with $\mathbf{c}^{(1)}, \ldots, \mathbf{c}^{(d)} \in C$. For $d = 2$, we use the abbreviation $\widehat{C} := C^{*2}$.*

Remark 3 (Powering Need Not Preserve $n$-Code). *Suppose $C \subset \mathbb{F}_q^k \times \mathbb{F}_q^n$ is an $n$-code for $\mathbb{F}_q^k$. It follows immediately that the secret-component in $C^{*d}$ takes any value in $\mathbb{F}_q^k$. However, the shares-component in $C^{*d}$* need not *determine the secret-component uniquely. Thus, $C^{*d}$* need not be an *$n$*-code for $\mathbb{F}_q^k$.

Remark 4. *Let $C$ be an $n$-code for $\mathbb{F}_q^k$ and let $(k_0, \sigma)$ be a generator. For an integer $d \geq 2$, suppose $C^{*d}$ is an $n$-code. If $d = 2$, then it is easy to see that $\widehat{C}$ is generated by the vectors $\mathbf{x} * \mathbf{y} \in \mathbb{F}_q^k \times \mathbb{F}_q^n$, where $\mathbf{x}, \mathbf{y}$ range over all pairs of vectors selected from $\sigma(\mathbf{e}_1, \mathbf{0}), \ldots, \sigma(\mathbf{e}_k, \mathbf{0}), \sigma(\mathbf{0}, \mathbf{e}'_1), \ldots, \sigma(\mathbf{0}, \mathbf{e}'_{k_0})$. Since, for $i = 1, \ldots, k$, the vector $\sigma(\mathbf{e}_i, \mathbf{0}) * \sigma(\mathbf{e}_i, \mathbf{0})$ has the $i$-th unit vector as its secret-component, a generator for $\widehat{C}$ can be efficiently constructed from $(k_0, \sigma)$. This generalizes to $d > 2$ in a straightforward way.*

Definition 10 (Arithmetic secret sharing scheme).
*An $(n, t, d, r)$-*arithmetic secret sharing scheme for $\mathbb{F}_q^k$ (over $\mathbb{F}_q$) *is an $n$-code $C$ for $\mathbb{F}_q^k$ such that $t \geq 1$, $d \geq 2$, $C$ is $t$-disconnected, $C^{*d}$ is in fact an $n$-code for $\mathbb{F}_q^k$, and $C^{*d}$ is $r$-reconstructing. $C$ has* uniformity *if, in addition, it is $t$-uniform.*

For example, the case $k = 1$, $d = 2$, $n = 3t + 1$, $r = n - t$, $q > n$ obtained from Shamir's secret sharing scheme (taking into account that degrees sum up when taking products of polynomials) corresponds to the secret sharing scheme used in [2,6]. The properties are easily proved using Lagrange's Interpolation Theorem. The generalization to $k > 1$ of this Shamir-based approach is due to [15]. The abstract notion is due to [10], where also constructions for $d = 2$ were given based on general linear secret sharing. See also [7,8,9]. On the other hand the following limitations are easy to establish.

PROPOSITION 3. *Let $C$ be an $(n, t, d, r)$-arithmetic secret sharing scheme for $\mathbb{F}_q^k$ over $\mathbb{F}_q$. As a linear secret sharing scheme for $\mathbb{F}_q^k$ over $\mathbb{F}_q$, $C$ has $t$-privacy and $(r - (d-1)t)$-reconstruction. Hence, $dt + k \leq r$. Particularly, if $k = 1$, $d = 2$, $r = n - t$, then $3t + 1 \leq n$.*

Stronger bounds are also known [5]. We note that arithmetic secret sharing schemes enjoy *efficient recovery of the secret in the presence of faulty shares.* The theorem below is a generalization of a result from [12].

THEOREM 7. *Let $i, j$ be integers with $1 \leq i < j$. Suppose $C$ and $C^{*j}$ are $n$-codes for $\mathbb{F}_q^k$. If the $n$-code $C^{*i}$ is $t$-disconnected and if $C^{*j}$ has $(n-t)$-reconstruction, then, given a generator for $C$, there is an efficient algorithm for the $n$-code $C^{*(j-i)}$ that, on input $\tilde{\mathbf{a}} := \mathbf{c}_{\mathcal{I}^*} + \mathbf{e} \in \mathbb{F}_q^n$ (faulty shares) with $\mathbf{c} \in C^{*(j-i)}$ and $\mathbf{e} \in \mathbb{F}_q^n$ of Hamming-weight at most $t$, outputs $\mathbf{c}_0 \in \mathbb{F}_q^k$ (correct secret).*

PROOF. Note that if $C$ and $C^{*j}$ are an $n$-codes, then so is $C^{*j'}$ for any $j'$ with $1 \leq j' \leq j$. Let $\mathbf{c} \in C^{*(j-i)}$. Let $(\mathbf{0}, \mathbf{e}) \in \mathbb{F}_q^k \times \mathbb{F}_q^n$ such that $\mathbf{e}$ has Hamming-weight at most $t$. Define $\tilde{\mathbf{c}} = \mathbf{c} + (\mathbf{0}, \mathbf{e})$ and let $\tilde{\mathbf{a}} = \tilde{\mathbf{c}}_{\mathcal{I}^*} = \mathbf{c}_{\mathcal{I}^*} + \mathbf{e}$. Write $\mathbf{u} = (1, \ldots, 1) \in \mathbb{F}_q^k$. Consider the system of equations $\{\tilde{\mathbf{a}} * \mathbf{x}_{\mathcal{I}^*} = \mathbf{y}_{\mathcal{I}^*},\ \mathbf{x}_0 = \mathbf{u},\ \mathbf{x} \in C^{*i},\ \mathbf{y} \in C^{*j}\}$, in the unknowns $\mathbf{x}, \mathbf{y}$. Note that this is in fact a *linear* system of equations (taking into account that, of course, membership of a subspace can be captured by a linear system of equations). We prove now that, first, this system has *some* solution $(\mathbf{x}, \mathbf{y})$, and that, second, *any* solution $(\mathbf{x}, \mathbf{y})$ satisfies $\mathbf{c}_0 = \mathbf{y}_0$. Efficiency then follows by linear algebra, in combination with the fact that a generator for $C$ is given and that generators for the higher powers can be constructed efficiently from it. First, define $A \subset \{1, \ldots, n\}$ as the set of all $i$ with $e_i \neq 0$. Since $C^{*i}$ is $t-$disconnected, there is $\mathbf{z} \in C^{*i}$ such that $\mathbf{z}_0 = \mathbf{u}$ and $\mathbf{z}_A = \mathbf{0}$. Then $\mathbf{x} := \mathbf{z}$, $\mathbf{y} := \mathbf{c} * \mathbf{z}$ is a solution. Second, let $(\mathbf{x}, \mathbf{y})$ be any solution. Then, for at least $n - |A| \geq n - t$ indices within $\mathcal{I}^*$ it holds that the vectors $\mathbf{c} * \mathbf{x} \in C^{*j}$ and $\mathbf{y} \in C^{*j}$ coincide. Since $C^{*j}$ has $(n-t)$-reconstruction and since $\mathbf{x}_0 = \mathbf{u}$, the claim follows. △

We briefly sketch two well-known applications. First, consider an $(n, t, 2, n)$-arithmetic secret sharing scheme $C$ for $\mathbb{F}_q^k$ over $\mathbb{F}_q$. Such a scheme can be used to reduce $n$-party secure multiplication to secure addition in the case of a *honest-but-curious adversary*, at the cost of one round of interaction. From the definition, it follows there is an $\mathbb{F}_q$-vector space morphism $\psi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^k$ such that,

for all $\mathbf{c}, \mathbf{c}' \in C$, $\psi(c_1 c'_1, \ldots, c_n c'_n) = \mathbf{c}_0 * \mathbf{c}'_0$. The reduction works as follows.[5] Let $\mathbf{c}_{\mathcal{I}^*}, \mathbf{c}'_{\mathcal{I}^*} \in \mathbb{F}_q^n$ be secret-sharings, with respective secrets $\mathbf{c}_0, \mathbf{c}'_0 \in \mathbb{F}_q^k$ $(\mathbf{c}, \mathbf{c}' \in C)$. Using a generator for $C$, player $P_i$ secret-shares $(\lambda_{i1} c_i c'_i, \ldots, \lambda_{ik} c_i c'_i) \in \mathbb{F}_q^k$, where the coefficient vector is the "$i$-th row of the matrix representing $\psi$ in the standard basis" $(i = 1, \ldots, n)$. Next, player $P_j$ sums the $n$ received shares $(j = 1, \ldots, n)$. This gives a secret-sharing of $\mathbf{c}_0 * \mathbf{c}'_0$ according to $C$ (see e.g. [9]). This generalizes Shamir-based solutions from [2,6,15] (see also [10]).

Second, consider an $(n, t, 2, n-t)$-arithmetic secret sharing scheme $C$ for $\mathbb{F}_q^k$ over $\mathbb{F}_q$. Such a scheme can be used for "zero-knowledge verification of secret multiplications." In a nutshell, the main idea is as follows. Suppose a prover puts forward commitments to secrets $\mathbf{x}_0, \mathbf{y}_0, \mathbf{z}_0 \in \mathbb{F}_q^k$, and claims that $\mathbf{x}_0 * \mathbf{y}_0 = \mathbf{z}_0$. To prove his claim, he gives ("coordinate-wise") commitments to random $\mathbf{x}, \mathbf{y} \in C$ where the respective secrets are the $\mathbf{x}_0, \mathbf{y}_0$ from the input, and a ("coordinate-wise") commitment to a random $z \in C^{*2}$ where the secret is the $\mathbf{z}_0 \in \mathbb{F}_q^k$ from the input. If the commitment scheme is $\mathbb{F}_q$-linear, then it is easy to enforce that indeed $\mathbf{x}, \mathbf{y} \in C$ and $\mathbf{z} \in C^{*2}$, and that the respective secrets are indeed the ones from the input. Now, if $\mathbf{z} = \mathbf{x} * \mathbf{y}$ (as an honest prover would choose), then indeed $\mathbf{x}_0 * \mathbf{y}_0 = \mathbf{z}_0$. In this case, inspection of any $t$ "share-triples" $(x_i, y_i, z_i)$ gives no information on the "secret-triple" $(\mathbf{x}_0, \mathbf{y}_0, \mathbf{x}_0\mathbf{y}_0)$. Yet, $z_i = x_i y_i$ for each of those $t$ share-triples. On the other hand, suppose $\mathbf{z}_0 \neq \mathbf{x}_0 * \mathbf{y}_0$. Then there are at most $n - t - 1$ share-triples $(x_i, y_i, z_i)$ such that $z_i = x_i y_i$, and hence there are at least $t + 1$ share-triples for which an inconsistency could show up. These facts together give a handle to checking that $\mathbf{z}_0 = \mathbf{x}_0\mathbf{y}_0$ in several different application scenarios, most notably perfect information-theoretically secure general multi-party computation, in the case of a *malicious adversary*. See [11] for an application with $d > 2$. The procedure above is essentially from [10] (which was inspired by ideas from [2,6]).

We are now ready to state the asymptotical results from [7] in full generality.[6] Let $F/\mathbb{F}_q$ be an algebraic function field (in one variable, with $\mathbb{F}_q$ as field of constants). Let $g$ denote the genus of $F$. Let $k, t, n \in \mathbb{Z}$ with $n > 1$, $1 \leq t \leq n$, $1 \leq k \leq n$. Suppose $Q_1, \ldots, Q_k, P_1, \ldots, P_n \in \mathbb{P}^{(1)}(F)$ are *pairwise distinct* $\mathbb{F}_q$-rational places. Write $Q = \sum_{j=1}^{k} Q_j \in \mathrm{Div}(F)$ and $D = Q + \sum_{i=1}^{n} P_i \in \mathrm{Div}(F)$. Let $G \in \mathrm{Div}(F)$ be such that $\mathrm{supp}\, D \cap \mathrm{supp}\, G = \emptyset$, i.e, they have disjoint support. Consider the AG-code

$$C(G; D) = \{(f(Q_1), \ldots, f(Q_k), f(P_1), \ldots, f(P_n)) \mid f \in \mathcal{L}(G)\} \subset \mathbb{F}_q^k \times \mathbb{F}_q^n.$$

THEOREM 8. *(from [7]). Let $t \geq 1, d \geq 2$. Let $C = C(G; D)$ with $\deg G \geq 2g + t + k - 1$. If $n > 2dg + (d+1)t + dk - d$, then $C$ is an $(n, t, d, n-t)$-arithmetic sharing scheme for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ with uniformity.*

THEOREM 9. *(from [7]). Fix $d \geq 2$ and a finite field $\mathbb{F}_q$. Suppose $A(q) > 2d$, where $A(q)$ is Ihara's constant. Then there is an infinite family of $(n, t, d, n-t)$-arithmetic secret sharing schemes for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ with uniformity such that $n$*

[5] This "local share-multiplication plus re-sharing" simplification in the case of Shamir's scheme has been attributed to Michael Rabin

[6] In fact, we state a version that is proved by exactly the same arguments as in [7].

*is unbounded, $k = \Omega(n)$ and $t = \Omega(n)$. Moreover, for every scheme $C$ in the family, a generator for $C$ is poly$(n)$-time computable and $C^{*i}$ has poly$(n)$-time reconstruction of a secret in the presence of $t$ faulty shares ($i = 1, \ldots, d-1$).*

Since $A(q) = \sqrt{q} - 1$ if $q$ is a square, it holds that $A(q) > 2d$ if $q$ is a square with $q > (2d+1)^2$. Also, by Serre's Theorem, $A(q) > c \log q$ for some absolute constant $c > 0$. Therefore, $A(q) > 2d$ if $q$ is (very) large.[7] The asymptotical result from [7] plays an important communication-saving role in *two-party cryptography*, see [23,24,18,22,13,21]. Often, the point is that terms in the communication analysis which would otherwise be logarithmic can be made constant using the [7] results. Note that [22,21] also use the efficient error correction. We will now apply our results on the torsion-limit in combination with appropriate Riemann-Roch systems in order to relax the condition $A(q) > 2d$ considerably. As a result, we attain the result of [7] but this time over *nearly all finite fields*.

THEOREM 10. *Let $t \geq 1, d \geq 2$. Define $\mathcal{I}^* = \{1, \ldots, n\}$. For $A \subset \mathcal{I}^*$ with $A \neq \emptyset$, define $P_A = \sum_{j \in A} P_j \in \mathrm{Div}(F)$. Let $K \in \mathrm{Div}(F)$ be a canonical divisor. If the system $\{\ell(dX - D + P_A + Q) = 0,\ \ell(K - X + P_A + Q) = 0\}_{A \subset \mathcal{I}^*, |A| = t}$ is solvable, then there is a solution $G \in \mathrm{Div}(F)$ such that $C(G; D)$ is an $(n, t, d, n-t)$-arithmetic secret sharing scheme for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ (with uniformity).*

PROOF. First note that if the system is solvable, then the Weak Approximation Theorem guarantees that we can take a solution $G \in \mathrm{Div}(F)$ such that $\mathrm{supp}\ G \cap \mathrm{supp}\ D = \emptyset$. We claim that the condition that $\ell(K - G + P_A + Q) = 0$ for $A \subset \mathcal{I}^*$ with $|A| = t$ implies $t$-disconnection and uniformity on the code. Write $A = \{i_1, \ldots, i_t\}$. Consider the map $\phi : \mathcal{L}(G) \to \mathbb{F}_q^{k+t}$ given by $f \mapsto (f(Q_1), \ldots, f(Q_k), f(P_{i_1}), \ldots, f(P_{i_t}))$. Its kernel is $\mathcal{L}(G - Q - P_A)$. Consequently $\dim(\mathrm{Im}\ \phi) = \ell(G) - \ell(G - Q - P_A) = \ell(K - G) - \ell(K - G + Q + P_A) + \deg(Q + P_A)$, where the second equality follows by application of the Riemann-Roch theorem to $G$ and to $G - Q - P_A$. Hence, $\ell(K - G) \leq \ell(K - G + Q + P_A) = 0$, where the inequality follows from the fact that $Q, P_A \geq 0$ and where the equality holds by assumption. Therefore, $\ell(K - G) = 0$ and $\dim(\mathrm{Im}\ \phi) = \deg(Q + P_A) = k + t$. We conclude that $\phi$ is surjective and this proves the claim. Finally we prove $(n-t)$-reconstruction in $C^{*d}$. Let $B = \{i_1, \ldots, i_{n-t}\}$ for distinct indices $i_1, \ldots, i_{n-t} \in \mathcal{I}^*$. Since $f_1, \ldots, f_d \in \mathcal{L}(G)$ implies $\prod_{i=1}^d f_i \in \mathcal{L}(dG)$, it is sufficient to prove that, for all $f \in \mathcal{L}(dG)$, the following holds: if the condition $f(P_i) = 0$ holds for all $i \in B$, then $f(Q_j) = 0$ for all $j \in \{1, \ldots, k\}$. Since $P_B = D - Q - P_A$ for some $A \subset \mathcal{I}^*$ with $|A| = t$, it holds that $\mathcal{L}(dG - P_B) = \mathcal{L}(dG - D + P_A + Q)$, which by assumption has dimension 0. Hence, $f \in \mathcal{L}(dG - P_B) = \{0\}$, and $f = 0$. $\triangle$

And now as a corollary of Theorems 6 and 10 we get the following:

COROLLARY 2. *Let $F/\mathbb{F}_q$ be an algebraic function field. Let $d, k, t, n \in \mathbb{Z}$ with $d \geq 2$, $n > 1$ and $1 \leq t < n$. Suppose $Q_1, \ldots, Q_k, P_1, \ldots, P_n \in \mathbb{P}^{(1)}(F)$ are pairwise distinct. If there is $s \in \mathbb{Z}$ such that $h > \binom{n}{t}(A_{r_1} + A_{r_2}|\mathcal{J}_F[d]|)$ where $r_1 := 2g - s + t + k - 2$ and $r_2 := ds - n + t$, then there exists an $(n, t, d, n-t)$-arithmetic secret sharing scheme for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ with uniformity.*

[7] The best known estimate for $c$ is currently about $\frac{1}{96}$.

MAIN THEOREM 1. *Let $\mathbb{F}_q$ be a finite field and $d \in \mathbb{Z}_{\geq 2}$. If there exists $0 < A \leq A(q)$ such that $A > 1 + J_d(q, A)$, then there is an infinite family of $(n, t, d, n-t)$-arithmetic secret sharing schemes for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ with $t$-uniformity where $n$ is unbounded, $k = \Omega(n)$ and $t = \Omega(n)$.*

This will follow from the more precise statement in Theorem 11 below. Combining Main Theorem 1 with Theorem 3 we obtain, in the special case $d = 2$:

MAIN THEOREM 2. *For $q = 8, 9$ and for all prime powers $q \geq 16$ there is an infinite family of $(n, t, 2, n-t)$-arithmetic secret sharing schemes for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ with $t$-uniformity where $n$ is unbounded, $k = \Omega(n)$ and $t = \Omega(n)$.*

As to efficiency, when given a divisor that is a solution to these Riemann-Roch systems, it is efficient to compute a generator for the scheme $C$ defined by this divisor. However, solving Riemann-Roch systems efficiently in full generality is subject of further research. In particular, for our strongest results to follow it is not known at present how to efficiently compute a generator. But of course, there exists a poly$(n)$-size description of generators, so overall, there is efficiency as before, but now in the weaker model where such description is given as advice.

More precisely, we have the following result (for $d > 2$ there is a similar analysis).

THEOREM 11. *Let $\mathbb{F}_q$ be a finite field. Suppose $\kappa \in [0, \frac{1}{3})$ and $\tau \in (0, 1]$ and $0 < A \leq A(q)$ are real number such that $A > \frac{1+\kappa}{1-3\kappa}(1 + J_2(q, A))$ and*

$$\tau + \frac{H_2(\tau)}{\log q} < \frac{1}{3}\left(1 - 3\kappa - \frac{(1 + J_2(q, A))(1 + \kappa)}{A}\right)$$

*Then there is an infinite family of $(n, t, 2, n-t)$-arithmetic secret sharing schemes for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ with uniformity where $n$ is unbounded, $k = \lfloor \kappa n \rfloor + 1$ and $t = \lfloor \tau n \rfloor$.*

The proof of this fact relies on showing that the conditions in Corollary 2 are satisfied asymptotically for a family of function field with Ihara's limit $A$, if the requirements of Theorem 11 are met. It is easy to show why Theorem 11 implies Main Theorem 2: if $0 < A \leq A(q)$ is such that $A > 1 + J_2(q, A)$ we can always select $\kappa \in (0, \frac{1}{3})$ and $\tau \in (0, 1]$ satisfying the conditions in Theorem 11. Note that in order to obtain the result in Main Theorem 2 we require $\kappa > 0$.

We prove Theorem 11 formally below, but give here an an indication of how one would bound asymptotically each parameter in the inequality of Corollary 2. Of course $|\mathcal{J}_F[2]|$ is dealt with asymptotically with the torsion limit $J_2(q, A)$ which we have introduced in this paper. Stirling's Formula gives an asymptotical bound for the binomial coefficients $\binom{n}{t}$ when $t$ is some fixed fraction of $n$. Finally the quotients $A_r/h$ can be bounded by means of algebraic geometric techniques which have been used before in the code theoretic literature, for instance [25], [28], [39], [40]. We state now an upper bound of this type.

PROPOSITION 4. *Let $F/\mathbb{F}_q$ be a function field with $g \geq 1$. Then, for any $r \in \mathbb{Z}$ with $0 \leq r \leq g - 1$, $A_r/h \leq \frac{g}{q^{g-r-1}(\sqrt{q}-1)^2}$.*

PROOF. For $i \geq 2g-1$, $A_i = \frac{h}{q-1}(q^{i+1-g}-1)$ (see Lemma 5.1.4 and Corollary 5.1.11 in [34]). This has been exploited in Lemma 3 (ii) from [28], to show that

$$\sum_{i=0}^{g-2} A_i T^i + \sum_{i=0}^{g-1} q^{g-1-i} A_i T^{2g-2-i} = \frac{L(T) - hT^g}{(1-T)(1-qT)}$$

where $L(T)$ is the $L$-polynomial associated to the zeta function of $F$.

The claim from Proposition 4 can be derived from a relation that is obtained by taking the limit as $T$ tends to $1/q$ on both sides of the equation above, where l'Hôpital's Rule is applied on the right hand side, then finding an expression for $L'(1/q)$ (using the Functional Equation for $L$-polynomials and the fact that $L(1) = h$) and substituting that back in. This is similar to the proof of Proposition 2.5 (in the case $s = 0$) in [40].

△

PROOF OF THEOREM 11. Fix any $A, \kappa, \tau$ satisfying the conditions of the statement. Let $\mathcal{F} = \{F_m\}_{m>0}$ be an infinite family of algebraic function fields over $\mathbb{F}_q$ with $g(F_m) \to \infty$ such that $A(\mathcal{F}) \geq A$ and $J := J_2(\mathcal{F}) = J_2(q, A)$. Define $g_m = g(F_m)$, $h_m = h(F_m)$, $j_m = \log_q(|\mathcal{J}(F_m)[2]|)$. Let $n_m = \lfloor \frac{1}{1+\kappa}(N(F_m)-1) \rfloor$ and $k_m = \lfloor \kappa n_m \rfloor + 1$. Note $n_m + k_m \leq N(F_m)$ so we can pick $n_m + k_m$ distinct rational points in $F_m$. We set $t_m = \lfloor \tau n_m \rfloor$. We choose $d_m = \lfloor \delta g_m \rfloor$ where $\delta = 1 + \frac{A-1-J}{3}$. Define $(r_1)_m = 2g_m - d_m + t_m + k_m - 2$ and $(r_2)_m = 2d_m - n_m + t_m$. For $m$ large enough we want to verify that we can apply Corollary 2 to $F_m$. We already noted we can take $n_m + k_m$ distinct points in $\mathbb{P}^{(1)}(F_m)$ so we now need to verify the condition

$$h_m > \binom{n_m}{t_m} (A_{(r_1)_m} + A_{(r_2)_m} |\mathcal{J}_{F_m}[2]|).$$

We will use Proposition 4. It is easy to see that $0 \leq (r_1)_m, (r_2)_m \leq g_m$ for large enough $m$ for our selection of the parameters. Thus,

$$A_{(r_i)_m} \leq \frac{g_m h_m}{q^{g_m - (r_i)_m - 1}(\sqrt{q}-1)^2}$$

for large enough $m$ and $i = 1, 2$. Consequently it is sufficient to show that

$$\binom{n_m}{t_m} \frac{g_m q^{t_m}}{q^{g_m-1}(\sqrt{q}-1)^2} \left( q^{(r_1)_m - t_m} + q^{(r_2)_m - t_m} |\mathcal{J}_{F_m}[2]| \right) < 1$$

which is equivalent, taking logarithms, to

$$\log_q \binom{n_m}{t_m} + \log_q \left( \frac{g_m q^{t_m}}{q^{g_m-1}(\sqrt{q}-1)^2} \right) + \log_q \left( q^{(r_1)_m - t_m} + q^{(r_2)_m - t_m} |\mathcal{J}_{F_m}[2]| \right) < 0. \tag{1}$$

Take $\epsilon \in \mathbb{R}_{>0}$ such that $\tau + \frac{H_2(\tau)}{\log q} < \frac{1}{3}\left(1 - 3\kappa - \frac{(1+J)(1+\kappa)}{3A} - 3\epsilon\right)$, which exists by hypothesis. For large enough $m$, by definition of $J$, $j_m < (J+\epsilon)g_m$. Moreover

by definition of $A$ we have $(A-\epsilon)g_m < n_m + k_m \leq Ag_m$ for large enough $m$. Note that this implies $\frac{1}{1+\kappa}(A-\epsilon)g_m \leq n_m \leq \frac{1}{1+\kappa}Ag_m$ and $k_m \leq \frac{\kappa}{1+\kappa}Ag_m + 1$. We have the following observations: First, since $t_m \leq \tau n_m$, from Stirling's Formula $\binom{n_m}{t_m} \leq 2^{H_2(\tau)n_m}$, and hence $\log_q \binom{n_m}{t_m} \leq \frac{H_2(\tau)}{\log q} n_m \leq \frac{H_2(\tau)}{(1+\kappa)\log q} Ag_m$. Second, we have

$$\log_q \left( q^{(r_1)_m - t_m} + |\mathcal{J}(\mathbb{F}_m)[2]| q^{(r_2)_m - t_m} \right) \leq$$

$$\log_q 2 + max\{2g_m - d_m + k_m - 2, 2d_m - n_m + j_m\}.$$

Now for large enough $m$, the following two inequalities hold:

$$2g_m - d_m + k_m - 2 \leq \left(2 - \delta + \frac{\kappa}{1+\kappa}A\right) g_m = \left(1 + \frac{1}{3}(1+J) + \frac{2\kappa - 1}{3(1+\kappa)}A\right) g_m,$$

$$\begin{aligned} 2d_m - n_m + j_m &\leq \left(2\delta - \frac{1}{1+\kappa}(A-\epsilon) + (J+\epsilon)\right) g_m \\ &\leq \left(1 + \frac{1}{3}(1+J) + \frac{2\kappa-1}{3(1+\kappa)}A + 2\epsilon\right) g_m. \end{aligned}$$

Finally, for large enough $m$, using elementary calculus and noticing $t_m \leq \tau n_m$ we get

$$\log_q \left( \frac{g_m q^{t_m}}{q^{g_m - 1}(\sqrt{q}-1)^2} \right) \leq \left( \frac{\tau}{1+\kappa}A - 1 + \epsilon \right) g_m.$$

Putting all these observations together we obtain that the left part of Equation 1 is at most

$$\begin{aligned} &\frac{H_2(\tau)}{(1+\kappa)\log q} Ag_m + \left( \frac{\tau}{1+\kappa}A - 1 + \epsilon \right) g_m + \\ &\log_q 2 + \left(1 + \frac{1}{3}(1+J) + \frac{2\kappa-1}{3(1+\kappa)}A + 2\epsilon\right) g_m. \end{aligned}$$

Now using $\tau + \frac{H_2(\tau)}{\log q} < \frac{1}{3}\left(1 - 3\kappa - \frac{(1+J)(1+\kappa)}{3A} - 3\epsilon\right)$ one can see that this expression is at most $\log_q 2 - \frac{\kappa}{3(1+\kappa)}Ag_m$ and this is clearly smaller than 0 for large enough $m$. Therefore, we can apply Corollary 2 to $F_m$, for each $m > M_0$ (for some constant $M_0$), and we have an $(n_m,\ t_m\ ,2\ ,n_m - t_m)$-arithmetic secret sharing scheme for $\mathbb{F}_q^{k_m}$ over $\mathbb{F}_q$ with uniformity, with $k_m = \lfloor \kappa n_m \rfloor + 1$ and $t_m = \lfloor \tau n_m \rfloor$. Since $N(F_m)$ tends to $\infty$ as $m$ tends to $\infty$ (because $A(\mathcal{F}) \geq A > 0$) then the set $\mathcal{M} = \{n_m\}_{m \geq M_0}$ is infinite. This concludes the proof. △

Finally, using our paradigm we also improve the explicit lower bounds for the parameter $\widehat{\tau}(q)$ from [7] and [4] for all $q$ with $q \leq 81$ and $q$ square, as well as for all $q$ with $q \leq 9$. Recall $\widehat{\tau}(q)$ is defined as the maximum value of $3t/(n-1)$ which can be obtained asymptotically (when $n$ tends to infinity) when $t$, $n$ are subject to the condition that an $(n, t, 2, n-t)$-arithmetic secret sharing for $\mathbb{F}_q$ over $\mathbb{F}_q$ exists (no uniformity required here). The new bounds are shown in the upper row of Table 1. All the new bounds marked with a star (*) are obtained by applying

Theorem 11 in the case $\kappa = 0$ and using the upper bounds given in Theorem 1 for the torsion limits. To obtain the rest of the new upper bounds, for each $q$, we apply the field descent technique in [4] to $\mathbb{F}_{q^2}$(in the special case of $\mathbb{F}_9$, even though Theorem 11 can be applied directly, as remarked in Main Theorem 2, it is better to apply Theorem 11 to $\mathbb{F}_{81}$ and then use the descent technique). These are compared with the previous bounds: the ones obtained in [7] (marked also with the symbol (*)), and the rest, which were obtained in [4] by means of the aforementioned field descent technique.

**Table 1.** Lower bounds for $\widehat{\tau}(q)$

| $q$ | 2 | 3 | 4 | 5 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|
| New bounds | 0.034 | 0.057 | 0.104 | 0.107 | 0.149 | 0.173(*) | 0.173 |
| Previous bounds | 0.028 | 0.056 | 0.086 | 0.093 | 0.111 | 0.143 | 0.167 |

| $q$ | 16 | 25 | 49 | 64 | 81 |
|---|---|---|---|---|---|
| New bounds | 0.298(*) | 0.323(*) | 0.448(*) | 0.520(*) | 0.520(*) |
| Previous bounds | 0.244 | 0.278 | 0.333(*) | 0.429(*) | 0.500(*) |

**Acknowledgments.** We are grateful for valuable contributions to the refinements on the bounds for the torsion-limit in Theorem 1. Bas Edixhoven and Hendrik Lenstra suggested the generic approach we used in its second part. Alp Bassa and Peter Beelen confirmed our hope that stronger bounds should be attainable from certain *specific* recursive towers, by contributing the proof of its third part. We also thank Hendrik for many helpful discussions, and for his encouragement since the paper was first circulated in the Fall of 2009. Part of this research was done when Cascudo was with University of Oviedo, partially supported by Spanish MEC project MTM2010-18370-C04-01. Cramer's research was supported by his NWO VICI project *Mathematical Foundations of Secure Computation*. Xing's research is partially supported by the Singapore National Research Foundation Competitive Research Program grant NRF-CRP2-2007-03 and the Singapore Ministry of Education under Research Grant T208B2206.

## References

1. Bassa, A., Garcia, A., Stichtenoth, H.: A new tower over cubic finite fields. Moscow Mathematical Journal 8(3), 401–418 (2008)
2. Ben-Or, M., Goldwasser, S., Wigderson, A.: Completeness theorems for non-cryptographic fault-tolerant distributed computation. In: Proceedings of STOC 1988, pp. 1–10. ACM Press, New York (1988)
3. Bezerra, J., Garcia, A., Stichtenoth, H.: An explicit tower of function fields over cubic finite fields and Zink's lower bound. J. Reine Angew. Math. 589, 159–199 (2005)
4. Cascudo, I., Chen, H., Cramer, R., Xing, C.: Asymptotically Good Ideal Linear Secret Sharing with Strong Multiplication over *Any* Finite Field. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 466–486. Springer, Heidelberg (2009)

5. Cascudo, I., Cramer, R., Xing, C.: Upper Bounds on Asymptotic Optimal Corruption Tolerance in Strongly Multiplicative Linear Secret Sharing (2009) (manuscript)
6. Chaum, D., Crépeau, C., Damgaard, I.: Multi-party unconditionally secure protocols. In: Proceedings of STOC 1988, pp. 11–19. ACM Press, New York (1988)
7. Chen, H., Cramer, R.: Algebraic Geometric Secret Sharing Schemes and Secure Multi-Party Computations over Small Fields. In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 516–531. Springer, Heidelberg (2006)
8. Chen, H., Cramer, R., Goldwasser, S., de Haan, R., Vaikuntanathan, V.: Secure Computation from Random Error Correcting Codes. In: Naor, M. (ed.) EUROCRYPT 2007. LNCS, vol. 4515, pp. 329–346. Springer, Heidelberg (2007)
9. Chen, H., Cramer, R., de Haan, R., Cascudo Pueyo, I.: Strongly multiplicative ramp schemes from high degree rational points on curves. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 451–470. Springer, Heidelberg (2008)
10. Cramer, R., Damgaard, I., Maurer, U.: General secure multi-party computation from any linear secret sharing scheme. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, p. 316. Springer, Heidelberg (2000)
11. Cramer, R., Damgaard, I., Pastro, V.: On the Amortized Complexity of Zero Knowledge Protocols for Multiplicative Relations (2010) (manuscript)
12. Cramer, R., Daza, V., Gracia, I., Jiménez Urroz, J., Leander, G., Martí-Farré, J., Padró, C.: On codes, matroids and secure multi-party computation from linear secret sharing schemes. IEEE Transactions on Information Theory 54, 2644–2657 (2008); Earlier version: CRYPTO 2005
13. Damgaard, I., Ishai, Y., Krøigaard, M.: Perfectly Secure Multiparty Computation and the Computational Overhead of Cryptography. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 445–465. Springer, Heidelberg (2010)
14. Duursma, I., Mak, K.-H.: On lower bounds for the Ihara constants A(2) and A(3). preprint (2011), http://arxiv.org/abs/1102.4127
15. Franklin, M., Yung, M.: Communication Complexity of Secure Computation. In: ACM STOC 1992, pp. 699–710
16. Garcia, A., Stichtenoth, H.: A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlăduţ bound. Invent. Math. 121, 211–222 (1995)
17. Garcia, A., Stichtenoth, H.: On the asymptotic behavior of some towers of function fields over finite fields. J. Number Theory 61, 248–273 (1996)
18. Harnik, D., Ishai, Y., Kushilevitz, E., Nielsen, J.: OT-Combiners via Secure Computation. In: Canetti, R. (ed.) TCC 2008. LNCS, vol. 4948, pp. 393–411. Springer, Heidelberg (2008)
19. Hirschfeld, J.W.P., Korchmáros, G., Torres, F.: Algebraic Curves of Finite Fields. Princeton Series in Applied Mathematics (2008)
20. Ihara, Y.: Some remarks on the number of rational points of algebraic curves over finite fields. J. Fac. Sci. Tokyo 28(3), 721–724 (1981)
21. Ishai, Y., Kushilevitz, E., Ostrovsky, R., Prabhakaran, M., Sahai, A., Wullschleger, J.: Constant-rate OT from Noisy Channels. These proceedings, CRYPTO (2011)
22. Ishai, Y., Kushilevitz, E., Ostrovsky, R., Sahai, A.: Extracting Correlations. In: Proc. 50th IEEE FOCS, pp. 261–270 (2009)
23. Ishai, Y., Kushilevitz, E., Ostrovsky, R., Sahai, A.: Zero-knowledge from secure multiparty computation. In: Proceedings of 39th STOC, San Diego, Ca., USA, pp. 21–30 (2007)
24. Ishai, Y., Prabhakaran, M., Sahai, A.: Founding Cryptography on Oblivious Transfer-Efficiently. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 572–591. Springer, Heidelberg (2008)

25. Lachaud, G., Martin-Deschamps, M.: Deschamps Nombre de points des jacobiennes sur un corps fini. Acta Arith. 56, 329–340 (1990)
26. Milne, J.S.: Abelian Varities. Online Lecture Notes (2009)
27. Mumford, D.: Abelian Varieties. Oxford University Press, Oxford (1970)
28. Niederreiter, H., Xing, C.: Low-Discrepancy Sequences and Global Function Fields with Many Rational Places. Finite Fields and Their Applications 2, 241–273 (1996)
29. Niederreiter, H., Xing, C.: Rational points on curves over finite fields-theory and applications, Cambridge (2000)
30. Rosen, M.: Number Theory in Function Fields. GTM, Springer (2001)
31. Serre, J.-P.: Rational points on curves over finite fields. Harvard University, Cambridge (1985)
32. Shamir, A.: How to share a secret. Comm. of the ACM 22(11), 612–613 (1979)
33. Shparlinski, I., Tsfasman, M., Vlăduţ, S.: Curves with many points and multiplication in finite fields. Lecture Notes in Math., vol. 1518, pp. 145–169. Springer, Berlin (1992)
34. Stichtenoth, H.: Algebraic function fields and codes. Springer, Heidelberg (1993) (new edition: 2009)
35. Tsfasman, M., Vlăduţ, S.: Modular curves, Shimura curves, and Goppa codes, better than Varshamov Gilbert bound. Math. Nachr. 109, 21–28 (1982)
36. Vlăduţ, S.G.: An exhaustion bound for algebro-geometric modular codes. Probl. Inf. Transm. 23, 22–34 (1987)
37. Vlăduţ, S.G., Drinfeld, V.G.: Number of points of an algebraic curves. Funct. Anal. Appl. 17, 53–54 (1983)
38. Weil, A.: Variétés Abéliennes et Courbes Algébriques. Hermann, Paris (1948)
39. Xing, C.: Algebraic geometry codes with asymptotic parameters better than the Gilbert-Varshamov and the Tsfasman-Vlăduţ-Zink bounds. IEEE Trans. on Inf. Theory 47(1), 347–352 (2001)
40. Xing, C.: Goppa Geometric Codes Achieving the Gilbert-Varshamov Bound. IEEE Trans. on Inf. Theory 51(1), 259–264 (2005)
41. Xing, C., Ling, Y.S.: Algebraic curves with many points over the binary field. J. Algebra 311, 775–780 (2007)
42. Zink, T.: Degeneration of Shimura surface and a problem in coding theory. In: Budach, L. (ed.) FCT 1985. LNCS, vol. 199, pp. 503–511. Springer, Heidelberg (1985)