# Algebraic Geometric Secret Sharing Schemes and Secure Multi-Party Computations over Small Fields*

Hao Chen[1] and Ronald Cramer[2,3]

[1] Department of Computing and Information Technology, School of Information Science and Engineering, Fudan University, Shanghai, China
`chenhao@fudan.edu.cn`
[2] CWI, Amsterdam, The Netherlands
`cramer@cwi.nl`
[3] Mathematical Institute, Leiden University, The Netherlands

**Abstract.** We introduce algebraic geometric techniques in secret sharing and in secure multi-party computation (MPC) in particular. The main result is a linear secret sharing scheme (LSSS) defined over a finite field $\mathbb{F}_q$, with the following properties.

1. It is *ideal*. The number of players $n$ can be *as large as* $\#C(\mathbb{F}_q)$, where $C$ is an algebraic curve $C$ of genus $g$ defined over $\mathbb{F}_q$.
2. It is *quasi-threshold*: it is $t$-rejecting and $t+1+2g$-accepting, but not necessarily $t+1$-accepting. It is thus in particular a ramp scheme. High information rate can be achieved.
3. It has *strong multiplication* with respect to the $t$-threshold adversary structure, if $t < \frac{1}{3}n - \frac{4}{3}g$. This is a multi-linear algebraic property on an LSSS facilitating zero-error multi-party multiplication, unconditionally secure against corruption by an active $t$-adversary.
4. The finite field $\mathbb{F}_q$ can be *dramatically smaller than* $n$. This is by using algebraic curves with many $\mathbb{F}_q$-rational points. For example, for each small enough $\epsilon$, there is a finite field $\mathbb{F}_q$ such that for infinitely many $n$ there is an LSSS over $\mathbb{F}_q$ with strong multiplication satisfying $(\frac{1}{3} - \epsilon)n \leq t < \frac{1}{3}n$.
5. Shamir's scheme, which requires $n > q$ and which has strong multiplication for $t < \frac{1}{3}n$, is a special case by taking $g = 0$.

Now consider the classical ("BGW") scenario of MPC unconditionally secure (with zero error probability) against an active $t$-adversary with $t < \frac{1}{3}n$, in a synchronous $n$-player network with secure channels. By known results it now follows that there exist MPC protocols in this scenario, achieving the same communication complexities in terms of the number of field elements exchanged in the network compared with known Shamir-based solutions. However, in return for decreasing corruption tolerance by a small $\epsilon$-fraction, $q$ may be dramatically smaller than $n$. This tolerance decrease is unavoidable due to properties of MDS codes. The techniques extend to other models of MPC. Results on less specialized LSSS can be obtained from more general coding theory arguments.

* The authors independently submitted similar results to CRYPTO 2006 [5, 8]. This paper is the result of merging those two papers.

## 1 Introduction

This paper introduces the use of algebraic geometric techniques in secret sharing and in secure multi-party computation (MPC) in particular. MPC concerns the problem of a network of players who wish to compute an agreed function on respective private inputs in a secure way, i.e., guaranteeing correctness of the result and privacy of their respective inputs, even if some players are corrupted by an adversary.

Let $\mathcal{A}_{t,n}$ denote the $t$-threshold adversary structure on the players $\{1,\dots,n\}$, i.e., it consists of all subsets of size at most $t$. Similarly, let $\Gamma_{r,n}$ denote the threshold access structure consisting of all subsets of size at least $r$. For a linear secret sharing scheme (LSSS) $\mathcal{M}$ on $n$ players, let $\Gamma(\mathcal{M})$ denote the sets accepted by $\mathcal{M}$, and let $\mathcal{A}(\mathcal{M})$ denote the sets rejected by $\mathcal{M}$. Let $\mathbb{F}_q$ be a finite field, and let $C$ be a smooth projective absolutely irreducible curve defined over $\mathbb{F}_q$, and let $g$ denote its genus. The number of $\mathbb{F}_q$-rational points on $C$ is denoted $\#C(\mathbb{F}_q)$.

We show that for any integer $n$ with $1 < n < \#C(\mathbb{F}_q)$ and any integer $t$ with $1 \leq t < n - 2g$ there exists an LSSS $\mathcal{M}$ over $\mathbb{F}_q$ with the following properties.

1. It is an *ideal* scheme on $n$ players; the secret as well as each share consists of a single field element.
2. It is *quasi-threshold* (with a $2g$ gap). This means that $\mathcal{A}_{t,n} \subset \mathcal{A}(\mathcal{M})$ and $\Gamma_{r,n} \subset \Gamma(\mathcal{M})$ where $r = t + 1 + 2g$. It it thus in particular a ramp scheme. We also show how high information rate can be achieved.
3. It has *strong multiplication* [15] with respect to the $\mathcal{A}_{t,n}$ adversary structure provided that $t < \frac{1}{3}n - \frac{4}{3}g$.
   This is a specialized multi-linear algebraic property known to facilitate zero-error multi-party multiplication, unconditionally secure against active corruptions (see [15, 14]). See Section 2 for the definition.
   It is also known to linearize in general the problem of recovery of the secret in the presence of corrupted shares [10].
4. Shamir's scheme, which requires $n > q$ and which has strong multiplication for $t < \frac{n}{3}$, is a special case of our scheme by taking $g = 0$. However, by taking $g > 0$ and by selecting suitable curves, $q$ can be *dramatically smaller than the number of players* $n$, as elaborated below.

Consider the model of a synchronous network with pair-wise secure channels. It is a classical result due Ben-Or, Goldwasser and Wigderson [1] and Chaum, Crépeau and Damgaard [4] that efficient MPC unconditionally secure (*with zero error probability* [1]) against an active adversary bound by the threshold condition that fewer than a 1/3-fraction of the players are corrupted is possible in this model. An active adversary is one who may arbitrarily influence and coordinate the behavior of the corrupted parties. The actual protocols make intricate use of Shamir's scheme.

Cramer, Damgaard and Maurer [15] show how to "efficiently bootstrap" MPC protocols from general LSSS, thereby providing means for dealing with general (i.e., "non-threshold") adversaries. The adversary structure capturing the resulting MPC's resilience is related to the access structure of the LSSS. Interestingly, these techniques will be used here for achieving security against a threshold adversary. Indeed, in the model we consider here, the properties of the proposed LSSS are for instance sufficient for the construction of an efficient (additively homomorphic) verifiable secret sharing scheme (VSS). [1] This is a fundamental primitive in MPC, as general MPC secure against an active adversary is essentially about performing secure arithmetic on VSS-ed secret values. The scheme is unconditionally secure (with zero error probability) against an active $t$-adversary. This is by requiring $t < \frac{1}{3}n - \frac{2}{3}g$: this renders the scheme $n-2t$-accepting, which is needed to enforce error-freeness of the VSS. The strong multiplication property is immaterial in this case. The number of field elements exchanged is the same as in the VSS from [1] or as in later variations, except that the field over which it is defined can be much smaller than the number of players $n$. Shamir-based solutions require $n > q$. The price to be paid is that that the corruption tolerance is decreased by an (arbitrarily) small (constant) fraction of $n$.

An LSSS per se is not known to be sufficient for efficient MPC, even though, as said, additively homomorphic VSS as such can be constructed from it. This does of course enable secure computation of addition, or more generally, linear functionals. However, secure multiplication is only known to be possible if the underlying LSSS in addition satisfies certain multi-linear algebraic properties, such as the multiplication property or the strong multiplication property. In the particular "perfect, zero-error" MPC scenario considered here, the strong multiplication property is essential. It will enable the claimed MPC over small fields, just as with the VSS discussed above.

Note that there exists an efficient transformation that maps relevant LSSS to equivalent LSSS that additionally satisfy the multiplication property [15], increasing the share size by only a multiplicative factor of two. However, it is important to note that no efficient transformation at all is known for the case of strong multiplication.

LSSS that satisfy the multiplication property rather than the strong multiplication property can in particular be used as basis for MPC secure against a *passive* adversary or against an active one but with non-zero yet negligible error probabilities. Moreover, if the model is augmented with a *broadcast primitive*, an *active adversary* can be tolerated who corrupts fewer than a *1/2-fraction* of the players, at the cost of introducing non-zero yet negligible error probabilities [32]. For VSS it is required that the underlying LSSS is $n-t$-accepting and for secure multiplication the LSSS is required to satisfy the multiplication property. Using

[1] Briefly, this strengthens a secret sharing scheme so as to withstand an active adversary who may corrupt part of the network, possibly including the dealer: it is a scheme that uses an interactive protocol to force even a possibly corrupted dealer to distribute shares consistent with the secret sharing scheme, that offers privacy to an honest dealer, and that offers unambiguous reconstruction of the secret.

the LSSS introduced here, both are satisfied if $t < \frac{1}{2}n - 2g$. More details and extended results can be found in [16, 7].

In general, LSSS with strong multiplication admit an algorithm to recover the secret in the presence of corrupted shares. This algorithm is efficient if the secret sharing scheme itself is efficient to begin with. This follows from the results in [10] where it is shown that strong multiplication linearizes this "decoding problem," by means of a generalization of ideas taken from the Berlekamp-Welch algorithm. For completeness we include in this paper a description of the general procedure from [10] as it applies to our algebraic geometric secret sharing schemes, even though in the present case it also follows by efficient decoding algorithms for algebraic geometry codes.

The quasi-threshold property of our scheme is sufficient for our purposes, but it is also unavoidable. Indeed, threshold linear secret sharing schemes are equivalent to maximum distance separable codes (MDS). For such codes it is well-known that $q \geq \max\{t, n-t+1\}$ if $0 < t < n-1$, which gives for example a $2q/3$ lower bound when $t$ is approximately $n/3$. Worse, the Main Conjecture for MDS codes implies $q \geq n-2$. Since VSS in the scenario we consider here requires an LSSS that is $t$-rejecting and $n-2t$-accepting, the setting $n = 3t+1$ would mean that the LSSS is required to be $t$-rejecting and $t+1$-accepting. In other words, it would be a threshold scheme, and the MDS argument above applies. Similar reasoning applies to different scenarios of MPC.

Some remarks on ramp schemes are in order. An $(a, b)$-ramp scheme is in some sense as a threshold secret sharing scheme. It is $a$-rejecting (no information) and $b$-accepting (full information). However, $b > a+1$ is allowed. This means that for sets whose size is between $a$ and $b$ anything might happen, including partial information. Ramp schemes may have higher information rate than secret sharing schemes; the size of a secret may be larger than the size of a share. It seems that all known *linear* ramp schemes required relatively large fields of definition, just as ordinary threshold secret sharing schemes. So it seems that our results may also be viewed as bearing on the theory of ramp schemes per se. We also show how to achieve high information rate, see Section 4. Finally, we also indicate in this paper how general coding theory arguments combined with (extensions of) known relationships between coding and secret sharing allow for a discussion of the ramp schemes claimed above (neglecting strong multiplication) without explicit reference to the algebraic geometric framework.

Mathematically, our construction is inspired by Goppa's algebraic geometric error correcting codes [23]. In particular, shares are defined by evaluating a function on the points of a curve, where the function is chosen from an appropriate Riemann-Roch space. However, several issues that are immaterial for coding theory play a role in the present context and indeed influence the definition, the analysis and the choice of parameters of the new scheme presented here. Shamir's scheme may be viewed as the genus 0 case.

Earlier work on secret sharing and secure computation that relies on techniques from algebraic number theory and/or algebraic geometry includes [17, 13, 12, 9]. Earlier applications of algebraic curves to other areas in information theoretically secure cryptography include those to authentication codes (see e.g. [2, 38, 26, 39]), and cover-free families and broadcast exclusion [25]. In general, algebraic geometry plays an increasingly important role in combinatorics, theoretical computer science and applied mathematics.

Before quantifying the possible advantages and trade-offs of the new scheme, note that trade-offs between communication complexity and corruption tolerance have been studied before. Indeed, Franklin and Yung [19] have shown that with a lower but still linear (in $n$) corruption bound, the same computation can be performed on many different inputs for the price of one such computation in the standard, classical case. Recently [11] it has been shown that a single, stand-alone secure multiplication can be performed with linear instead of quadratic communication (in $n$). Nevertheless, these results rely in an essential way on secret sharing techniques over a field of size at least $n$.

Let $N_q(g)$ denote the maximal number of $\mathbb{F}_q$-rational points on a genus $g$ curve $C$ defined over $\mathbb{F}_q$. The Hasse-Weil bound states that $q+1-2g\sqrt{q} \leq N_q(g) \leq q+1+2g\sqrt{q}$. Note that if $C$ is a plane curve then the bound becomes $q+1-(d-1)(d-2)\sqrt{q} \leq N_q(g) \leq q+1+(d-1)(d-2)\sqrt{q}$. However, curves in higher dimensional spaces can have many more points.

The theoretical upper bound is an additional $2g\sqrt{q}$ players compared to using Shamir's scheme in secure computation, while lowering the maximal tolerable number of corrupted players by an additive factor at most $4g/3$.

Viewed from a different angle, and using the García-Stichtenoth curves [21], a family of non-plane curves with many rational points and celebrated for their optimal ratio between genus and number of rational points, one can achieve the following asymptotic bound. For each $\epsilon$ with $0 < \epsilon < \frac{1}{6}$, there is a finite field $\mathbb{F}_q$ such that for infinitely many $n$ there exists a scheme with strong multiplication and with $(\frac{1}{3} - \epsilon) \cdot n \leq t < \frac{1}{3} \cdot n$. In particular all sets of size at least $n - 2t$ are accepted. This example is detailed at the end of this paper, together with other examples.

Note that there exists theoretically efficient constructions of the curves of García and Stichtenoth. Efficient construction means here that one can also efficiently work with the relevant Riemann-Roch spaces. There are a host of classes of curves with many rational points known from coding theory that allow for efficient construction. We do not further address computational issues here. This is deferred to the full version.

The results in this paper focus on application to error-free unconditionally secure MPC in the secure channels model, with synchronous communication and in the presence of an active adversary. The results can be adapted to other models of MPC or just to plain secret sharing or ramp schemes, e.g., in the context of secure and private storage. In ongoing work generalizations to higher dimensional varieties are studied [6] as well as the case of MPC in the broadcast model [7].

## 2 Preliminaries

This section contains some basic definitions and conventions about linear secret sharing and about algebraic curves over finite fields, as well as some relevant facts. The definitions concerning linear secret sharing below are slight adaptations of definitions from [15].

An adversary structure $\mathcal{A}$ on a finite player set $\mathcal{U}$ is a collection of subsets of $\mathcal{U}$ with the property that $A' \in \mathcal{A}$ and $A \subset A'$ implies $A \in \mathcal{A}$. An adversary structure is $Q3$ if for all $A, A', A'' \in \mathcal{A}$ it holds that $A \cup A' \cup A''$ is a proper subset of $\mathcal{U}$. $\mathcal{A}_{t,n}$ is the adversary structure consisting of all sets $A \subset \mathcal{U}$ of size at most $t$. The access structure $\Gamma_{r,n}$ consists of all sets $B \subset \mathcal{U}$ of size at least $r$.

A linear secret sharing scheme (LSSS) $\mathcal{M}$ over $\mathbb{F}_q$ on the player set $\mathcal{U}$ is given by a positive integer $e$, a sequence $V_1, \dots, V_n$ of subspaces of the $e$-dimensional $\mathbb{F}_q$-vector space $\mathbb{F}_q^e$, and a non-zero vector $u \in \mathbb{F}_q^e$. Let $V_A$ denote $\sum_{i \in A} V_i$, the $\mathbb{F}_q$-subspace spanned by all the $V_i$ with $i \in A$. The access structure $\Gamma(\mathcal{M})$ of $\mathcal{M}$ consists of all sets $B \subset \mathcal{U}$ with $u \in V_B$. We set $u = (1, 0, \dots, 0) \in \mathbb{F}^e$, without loss of generality. The structure $\mathcal{A}(\mathcal{M})$ consists of the sets $A \subset \mathcal{U}$ with $A \notin \Gamma(\mathcal{M})$. An LSSS as defined here is essentially a monotone span program [24]. An LSSS $\mathcal{M}$ is said to reject a given adversary structure $\mathcal{A}$ defined on $\mathcal{U}$ if $\mathcal{A} \subset \mathcal{A}(\mathcal{M})$. If $B$ is a non-empty set with $B \subset \mathcal{U}$, then $\mathcal{M}_B$ denotes the LSSS on the player set $B$ given by restricting to those $V_i$ with $i \in B$. An ideal LSSS is one in which all $V_i$ have dimension 1 and where for each $i$ there is $B$ in $\Gamma(\mathcal{M})$ that is minimal with respect to inclusion and for which $i \in B$.

Secret sharing based on an LSSS works in essence as follows. Suppose that bases for the $V_i$'s are fixed. Let $s \in \mathbb{F}_q$ be a "secret value." Choose a random linear map $\phi : \mathbb{F}_q^e \to \mathbb{F}_q$ subject to $\phi(u) = s$, and give $\phi_{|V_i}$ to player $i$, i.e., the action of $\phi$ on each of the chosen basis vectors of $V_i$. It holds that $\{\phi_{|V_i}\}_{i \in A}$ determines the secret $s$ uniquely if and only if $A \in \Gamma(\mathcal{M})$, and $\{\phi_{|V_i}\}_{i \in A}$ gives no information about $s$ in all other cases, i.e., when $A \in \mathcal{A}(\mathcal{M})$. Note that by basic linear algebra $A \in \mathcal{A}(\mathcal{M})$ if and only if there exists a linear map $\kappa : \mathbb{F}_q^e \to \mathbb{F}_q$ such that $\kappa$ vanishes on $V_A$, i.e., $\kappa_{|V_A} \equiv 0$, but $\kappa(u) = 1$.

For elements $x, \in \mathbb{F}_q^e$, let $(x_1, \dots, x_e)$, $(y_1, \dots, y_e)$ denote their respective coordinate vectors with respect to the standard basis. $x \otimes y$ denotes the vector with coordinates $(\dots, x_i \cdot y, \dots) \in \mathbb{F}_q^{e^2}$. Let $\widehat{V}_i$ denote the subspace $V_i \otimes V_i \subset \mathbb{F}_q^{e^2}$, i.e., the $\mathbb{F}_q$-vector space spanned by all elements of the form $x \otimes y$ with $x, y \in V_i$. $\widehat{V}_B$ denotes $\mathbb{F}_q \langle \{\widehat{V}_i\}_{i \in B} \rangle$, and $\widehat{u}$ denotes $u \otimes u$. For given LSSS $\mathcal{M}$, the LSSS $\hat{\mathcal{M}}$ be defined by the tuple $(\mathbb{F}_q, \widehat{V}_1, \dots, \widehat{V}_n, \widehat{v})$. $\mathcal{M}$ is said to have the multiplication property if $\widehat{u} \in V_{\mathcal{U}}$. $\mathcal{M}$ has the strong multiplication property with respect to an adversary structure $\mathcal{A}$ (on $\mathcal{U}$) if the following holds.

1. $\mathcal{M}$ rejects the adversary structure $\mathcal{A}$.
2. For all $B \subset \mathcal{U}$ with $B = \mathcal{U} \setminus A$ for some $A \in \mathcal{A}$, $\widehat{\mathcal{M}_B}$ has multiplication.

It is not hard to see that strong multiplication implies that if $A, A' \in \mathcal{A}$, then $\mathcal{U} \setminus A \cup A' \in \Gamma(\mathcal{M})$. Thus, in particular, in order for an LSSS to have strong multiplication with respect to an adversary structure $\mathcal{A}$, it must be so that $\mathcal{A}$ is $Q3$.[2]

It can be shown that for all finite fields $\mathbb{F}_q$ and for all $Q3$ adversary structures $\mathcal{A}$ there is an LSSS with strong multiplication. In general, however, the dimension may be very large. The standard example for an ideal LSSS is Shamir's scheme. If $t < n/3$ in this scheme, it has strong multiplication with respect to $\mathcal{A}_{t,n}$. Note that $\Gamma(\mathcal{M}) = \Gamma_{t+1,n}$ and that it requires $q > n$.

In analogy to Shamir's scheme, in the case of an ideal LSSS it is sufficient to prove that "for each set $A \in \mathcal{A}$, the pair-wise local products of two vectors of shares belonging to the set $B = \mathcal{U} \setminus A$ jointly uniquely determine the product of the secrets." This is then by linear combination as a consequence. These facts are used implicitly when arguing about strong multiplication in the sequel.

As an aside we mention that it is known [15] how to efficiently enforce the multiplication property on all relevant LSSS; the dimension only goes up by a multiplicative factor 2. In the much more demanding case of strong multiplication the general question whether it can always be efficiently enforced on all relevant LSSS is completely open.

As indicated earlier in this paper, using the techniques from [15] one can construct efficient MPC protocols for the MPC scenario we consider in this paper from an LSSS that satisfies strong multiplication with respect to a $Q3$ adversary structure $\mathcal{A}$. Note that in the present paper we are using a slightly generalized definition of the adversary structure of an LSSS and what it means to satisfy strong multiplication with respect to it: in [15] the adversary structure is always $\mathcal{A}(\mathcal{M})$, and strong multiplication is always defined with respect to that structure only. In the present paper we have refined these notions, and allow for the definition to apply to an adversary structure $\mathcal{A}$ contained in $\mathcal{A}(\mathcal{M})$. This does not make any essential difference. [3]

We now give a quick overview of basics on algebraic geometry. In Section 3 we briefly point out how part of our result (i.e, neglecting strong multiplication) can be appreciated if one accepts some general results about algebraic geometric error correcting codes and (an extension of) a known connection between codes and secret sharing.

Let $C$ be a smooth, projective, absolutely irreducible curve defined over $\mathbb{F}_q$, and let $g$ denote the genus of $C$. Let $\overline{\mathbb{F}}_q$ denote the algebraic closure of $\mathbb{F}_q$. A plane such curve can be represented by some polynomial $F[X, Y] \in \mathbb{F}_q[X, Y]$ that is irreducible in $\overline{\mathbb{F}}_q[X, Y]$. The affine part of the curve is defined as the set of points $P \in \overline{\mathbb{F}}_q^2$ such that $F(P) = 0$. By taking its projective closure, which amounts to introducing an extra variable, homogenizing the polynomial

[2] In [10] it is shown how strong multiplication enables efficient error correction.

[3] For zero-error VSS from LSSS the condition that $\mathcal{A}$ is $Q3$ and that for all $A, A' \in \mathcal{A}$, $\mathcal{U} \setminus A \cup A' \in \Gamma(\mathcal{M})$ must be explicitly made. In case of strong multiplication this condition is implied, as pointed out.

and considering the zeroes in the two-dimensional projective space $\mathbb{P}^2(\overline{\mathbb{F}}_q)$, one obtains the entire curve. More generally, curves defined over $\mathbb{F}_q$ is the "set of zeroes" in $\mathbb{P}^m(\overline{\mathbb{F}}_q)$ of a homogeneous ideal $I \subset \mathbb{F}_q[X_0, \ldots, X_m]$, where $I$ is such that its function field has transcendence degree 1 over the ground field, i.e., it is a one dimensional variety. Smoothness concerns not simultaneously vanishing partial (formal) derivatives.

$\overline{\mathbb{F}}_q(C)$ denotes the function field of the curve. Very briefly, it consists of all fractions of polynomials $a, b \in \overline{\mathbb{F}}_q[X_0, \ldots, X_m]$, $b \notin I$, such that both are homogeneous of the same degree, under the equivalence relation that $a/b \equiv a'/b'$ if $ab' \equiv a'b \bmod I$. The elements can be viewed as maps from the curve to $\overline{\mathbb{F}}_q$, and they have at most a finite number of poles and zeroes, unless it is the zero function. Their "multiplicities add up to zero."

Since $C$ is smooth at each point $P \in C$ by assumption, the local ring $\mathcal{O}_P(C)$ of functions $f \in \overline{\mathbb{F}}_q(C)$ that are well-defined at $P$ (equivalently, the ones that do not have a pole at $P$) is a discrete valuation ring. Thus, at each $P \in C$, there exists $t \in \overline{\mathbb{F}}_q(C)$ (a uniformizing parameter) such that $t(P) = 0$ and each $f \in \mathcal{O}_P(C)$ can be uniquely written as $f = u \cdot t^{\nu_P(f)}$. Here, $u \in \mathcal{O}_P(C)$ is a unit (i.e.,$u(P) \neq 0$), and $\nu_P(f)$ is a non-negative integer. This valuation $\nu_P$ extends to all of $\overline{\mathbb{F}}_q(C)$, by defining $\nu_P(f) = -\nu_P(1/f)$ if $f$ has a pole at $P$.

A divisor is a formal sum $\sum_{P \in C} m_p \cdot (P)$ with integer coefficients $m_p$ taken over all points $P$ of the curve $C$. Divisors are required to have finite support, i.e., they are zero except possibly at finitely many points. The divisor of $f \in \mathbb{F}_q(C)$ is defined as $\text{div}(f) = \sum_{P \in C} \nu_P(f) \cdot (P)$. It holds that deg $\text{div}(f) = 0$. The degree $\deg D$ of a divisor $D$ is the sum $\sum_{P \in C} m_P \in \mathbb{Z}$ of its coefficients $m_P$.

The Riemann-Roch space associated with a divisor $D$ is defined as $\mathcal{L}(D) = \{f \in \overline{\mathbb{F}}_q(C) | \text{div}(f) + D \geq 0\} \cup \{0\}$. This is an $\overline{\mathbb{F}}_q$-vector space. The (partial) ordering "$\geq$" refers to the comparison of integer vectors and declaring one larger than the other if this holds coordinate-wise. Its dimension is denoted $\ell(D)$. This dimension is equal to 0 if $\deg D < 0$. The Riemann-Roch Theorem is concerned with the dimensions of those spaces. It says that $\ell(D) - \ell(K - D) = \deg D + 1 - g$. Here $K$ is a canonical divisor. These are the divisors $K$ of degree $2g - 2$ and $\ell(K) = g$. It follows immediately that $\ell(D) = \deg D + 1 - g$ if $\deg D$ is large enough, i.e., at least $2g - 1$. This consequence suffices for the purposes in this paper.

An $\mathbb{F}_q$-rational point on $C$ is one whose projective coordinates can be chosen in $\mathbb{F}_q$. Rational point shall mean $\mathbb{F}_q$-rational point. Note that non-plane curves can in principle harbor many more rational points than plane curves.

The divisors on $C$ defined over $\mathbb{F}_q$ (or $\mathbb{F}_q$-rational divisors) are those that are invariant under the Galois group $\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. This includes the divisors whose support consists of rational points only. In this paper all divisors are rational.

If $D$ is rational, then $\mathcal{L}(D)$ admits a basis defined over $\mathbb{F}_q$. *In this paper $\mathcal{L}(D)$ is tacitly restricted to the $\mathbb{F}_q$-part of $\mathcal{L}$, i.e., the $\mathbb{F}_q$-linear span of such* *basis, or equivalently, the subspace of $\mathcal{L}(D)$ fixed under $Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. This has $q^{\ell(D)}$ elements. As a consequence of this convention, if $P \in C$ is rational and if $f \in \mathcal{L}(D)$, then $f(P) \in \mathbb{F}_q$.*

For introductions to algebraic geometry, see for instance [20, 27], or or textbooks that place special emphasis on curves over $\mathbb{F}_q$ such as [37, 36]. For an accessible, high level overview of the technicalities sketched above see for instance [28].

## 3 Main Result

As before, let $C$ be a smooth projective absolutely irreducible curve defined over $\mathbb{F}_q$, and let $g$ denote its genus.

Let

$$Q, P_0, P_1, \ldots, P_n$$

be any distinct rational points on $C$, possibly exhausting all rational points of $C$. Let $t$ be any fixed integer with $1 \leq t < n - 2g$. The divisor $D$ is defined as

$$D = (2g + t) \cdot (Q).$$

Thus, it has support $Q$ and degree $2g + t$.[4]

The claimed LSSS $\mathcal{M}$ works as follows.

Let $s \in \mathbb{F}_q$ be a secret value.

Select

$$f \in \mathcal{L}(D)$$

at random, subject to the constraint

$$f(P_0) = s.$$

There is always at least one such $f$, since $\mathcal{L}(D)$ contains in particular the constant functions. By the convention made earlier on, the choice of $f$ is restricted to the $\mathbb{F}_q$-part of $\mathcal{L}(D)$, which is a vector space over $\mathbb{F}_q$ of dimension $g + t + 1$. So the random choice of $f$ conditioned on the secret $s$ consumes $g + t$ random field elements from $\mathbb{F}_q$.

Now define

$$f(P_1) = s_1 \in \mathbb{F}_q, \ldots, f(P_n) = s_n \in \mathbb{F}_q$$

as the shares. By definition of the divisor $D$ and by the definition of the space $\mathcal{L}(D)$, the functions $f \in \mathcal{L}(D)$ only have a pole in $Q$. Thus the values $f(P_i)$ are always well-defined.

[4] Any other divisor of that degree would do as well. However, with a small support of $D$ the maximum value of $n$ is greater.

The construction above may be viewed as a combination of Goppa's algebraic-geometry error correcting codes [23] and Massey's construction of linear secret sharing schemes from error-correcting codes [29, 30]. The latter result allows to study privacy and reconstruction in terms of properties of the underlying linear codes and their duals. More precisely, one observes that their respective minimum distances imply bounds on the parameters of a ramp scheme. This can be combined with known properties of algebraic-geometric codes to obtain bounds on privacy and reconstruction as we give below. Nevertheless, a slight generalization of the results of Massey is needed to be able to analyze our high information rate ramp scheme from Section 4. We have, however, chosen a self-contained presentation whose details can all be directly understood from the corollary of Riemann-Roch we stated before. Moreover, in order to prove the strong multiplication property as we do it is essential to be able to address the explicit structure of our secret sharing scheme.

LEMMA 1 *Let $E$ be a divisor on $C$ that is defined over $\mathbb{F}_q$, and suppose that $\ell(E) > 0$. Then each $f \in \mathcal{L}(E)$ is uniquely determined by evaluations of $f$ on any $degE + 1$ rational points on $C$ outside the support of $E$.*

PROOF. This is a standard argument. First note that for each $f \in \mathcal{L}(E)$ and for each rational point $P$ on the curve outside the support of $E$ the value $f(P)$ is well-defined, as $f$ certainly has no poles there. This follows from the definition of $\mathcal{L}(E)$.

Write $d$ for the degree of $E$, and consider rational points $Q_1, \ldots, Q_{d+1}$ on the curve, outside the support of $E$. The map

$$\phi : \mathcal{L}(E) \longrightarrow \mathbb{F}_q^{d+1},$$

$$f \mapsto (f(Q_1), \ldots, f(Q_{d+1}))$$

is an injective linear map of $\mathbb{F}_q$-vector spaces. Indeed, if $f, h \in \mathcal{L}(E)$ and $\phi(f) = \phi(h)$, then $f - h \in \mathcal{L}(E - (Q_1 + \ldots + Q_{d+1})) \subset \mathcal{L}(E)$. Here it is used that the support of $E$ is disjoint from the $Q_i$'s. The degree of the divisor $E - (Q_1 + \ldots + Q_{d+1})$ is negative, so $f = h$.

Note that, just as with Lagrange interpolation by polynomials, this interpolation is linear in the following sense. If $Q_0$ is a rational point on the curve different from the $Q_i$'s and outside the support of $E$, then there are coefficients $\lambda_i \in \mathbb{F}_q$ such that for all $f \in \mathcal{L}(E)$

$$f(Q_0) = \sum_{i=1}^{d+1} \lambda_i \cdot f(Q_i).$$

Concretely, since $\phi$ is injective, there exists a surjective linear map

$$\chi : \mathbb{F}_q^{d+1} \longrightarrow \mathcal{L}(E)$$

such that $\chi \circ \phi$ is the identity on $\mathcal{L}(E)$. So

$$f = \chi(f(Q_1), \ldots, f(Q_{d+1})),$$

and

$$f(Q_0) = \chi_0 \circ \chi(f(Q_1), \ldots, f(Q_{d+1}),$$

where the linear map $\chi_0$ is defined as

$$\chi_0 : \mathcal{L}(E) \longrightarrow \mathbb{F}_q$$
$$f \mapsto f(Q_0).$$

△

PROPOSITION 1 $\mathcal{A}(\mathcal{M})$ *consists of all sets* $A \subset \{1, \ldots, n\}$ *such that*

$$\ell(D - (P_0 + \sum_{i \in A} P_i)) < \ell(D - (\sum_{i \in A} P_i)).$$

*Equivalently,* $\Gamma(\mathcal{M})$ *consists of all sets* $B \subset \{1, \ldots, n\}$ *such that*

$$\ell(D - (P_0 + \sum_{i \in B} P_i)) = \ell(D - (\sum_{i \in B} P_i)).$$

PROOF. Clearly, $A \in \mathcal{A}$ if and only if there exists $k \in \mathcal{L}(D)$ such that $k(P_i) = 0$ for all $i \in A$ and $k(P_0) = 1$. This is a general fact about linear secret sharing schemes, which is easily proved by linear algebra.

It holds generally that $\mathcal{L}(F) \subset \mathcal{L}(F')$ if $F \leq F'$. This follows immediately from the definitions. Since the support of $D$ is disjoint from the $P_i$'s, it therefore holds that

$$\mathcal{L}(D - (P_0 + \sum_{i \in A} P_i)) \subset \mathcal{L}(D - (\sum_{i \in A} P_i)) \subset \mathcal{L}(D).$$

All functions $k'$ in the difference

$$\mathcal{L}(D - (\sum_{i \in A} P_i)) \setminus \mathcal{L}(D - (P_0 + \sum_{i \in A} P_i)),$$

if any, satisfy $k' \in \mathcal{L}(D)$, $k'(P_0) \neq 0$, and $k'(P_i) = 0$ for all $i \in A$. By normalizing at $P_0$, the desired function $k$ is obtained. Clearly, the difference between those spaces is non-empty if and only if their dimensions differ. △

COROLLARY 1 $\mathcal{A}_{t,n} \subset \mathcal{A}(\mathcal{M})$.

PROOF. If $|A| = t$, then

$$\deg(D - (P_0 + \sum_{i \in A} P_i)) = 2g - 1,$$

$$\deg(D - (\sum_{i \in A} P_i)) = 2g.$$

Therefore,

$$g = \ell(D - (P_0 + \sum_{i \in A} P_i)) < g + 1 = \ell(D - (\sum_{i \in A} P_i)).$$

△

COROLLARY 2 $\Gamma_{2g+t+1,n} \subset \Gamma(\mathcal{M})$.

PROOF. First note that by definition $n \geq 2g+t+1$. If $B \subset \{1,\ldots,n\}$ is a set of size $2g+t+1$, then $\ell(D - \sum_{i\in B} P_i) = 0$, since the argument is a divisor of negative degree. Thus, $0 = \ell(D - (P_0 + \sum_{i\in B} P_i) \leq \ell(D - \sum_{i\in B} P_i) = 0$ $\triangle$

PROPOSITION 2 *$\mathcal{M}$ has strong multiplication with respect to $\mathcal{A}_{t,n}$ if $3t < n-4g$. $\mathcal{M}$ has multiplication if $2t < n-4g$.*

PROOF. We only treat the strong multiplication case. Let $f, h \in \mathcal{L}(D)$. Using the basic fact that $\mathrm{div}(fh) = \mathrm{div} f + \mathrm{div} h$, it follows that

$$0 \leq (\mathrm{div} f + D) + (\mathrm{div} h + D) = \mathrm{div}(fh) + 2D.$$

Hence

$$f \cdot h \in \mathcal{L}(2D).$$

Thus M has strong multiplication if

$$n - t > \deg(2D) = 4g + 2t,$$

as follows by application of Lemma 1. Indeed, let $B$ be any set with $B \subset \{1,\ldots,n\}$ and $|B| = 4g+2t+1$. Define linear maps

$$\hat{\phi}_0 : \mathcal{L}(2D) \longrightarrow \mathbb{F}_q$$

$$\hat{f} \mapsto \hat{f}(P_0),$$

and

$$\hat{\phi} : \mathcal{L}(2D) \longrightarrow \mathbb{F}_q^{4g+2t+1}$$

$$\hat{f} \mapsto (\hat{f}(P_i))_{i\in B},$$

and

$$\hat{\chi} : \mathbb{F}_q^{4g+2t+1} \longrightarrow \mathcal{L}(2D)$$

such that $\hat{\chi} \circ \hat{\phi}$ is the identity on $\mathcal{L}(2D)$.

Then, for all $f, h \in \mathcal{L}(D)$, it holds that

$$s \cdot s' = \hat{\phi}_0 \circ \hat{\chi}((s_i \cdot s_i')_{i\in B}),$$

where

$$s = f(P_0), s' = h(P_0), \text{ and for all } i \in B, s_i = f(P_i), s_i' = h(P_i).$$

$\triangle$

An alternative proof of the strong multiplication property can be based on the observation that this LSSS has strong multiplication with respect to an adversary structure $\mathcal{A} \subset \mathcal{A}(\mathcal{M})$ if for all $A \in \mathcal{A}$ it holds that

$$\ell(2D - (P_0 + \sum_{i \in B} P_i)) = \ell(2D - (\sum_{i \in B} P_i)),$$

where $B = \{1, \ldots, n\} \setminus A$.

For completeness we show how strong multiplication linearizes the problem of recovering the secret in the presence of corrupted shared. It is a special case of the more general technique given in [10]. But also note that known techniques for decoding algebraic-geometry codes apply here. In any case, assume $t < (n - 4g)/3$. Let $u = (f(P_1), \ldots, f(P_n))$ be a share vector for the secret $s = f(P_0)$, with $f \in \mathcal{L}(D)$. Let $e \in \mathbb{F}_q^n$ be a vector of Hamming-weight at most $t$, i.e., its number of nonzero coordinates is at most $t$. For any $P \in \{P_1, \ldots, P_n\}$ write $c = u + e \in \mathbb{F}_q^n$, and write $c(P)$ for the coordinate of $c$ "that corresponds to $P$." Now solve the following linear equation system $\forall P \in \{P_1, \ldots, P_n\} \ : \ h(P) = c(P) \cdot k(P)$, $k(P_0) = 1$, where $h \in \mathcal{L}(2D), k \in \mathcal{L}(D)$. These are $n+1$ equations in $(3g + 2t + 1) + (g + t + 1) = 4g + 3t + 2$ variables. There always exists a solution, and each solution $(h, k) \in \mathcal{L}(2D) \times \mathcal{L}(D)$ satisfies $h(P_0) = s$. This system of linear equations can be efficiently set up if the underlying curve supports efficient algorithms.

Some final remarks about the basic construction are in order. Often one may re-define $D$ so that one extra player is supported. Indeed, by using the Weak Approximation Theorem (see [36]) an equivalent $D'$ can be found whose support really lies in an extension field, thereby making all rational points available for players. There is an alternative approach to "winning points" in which all of the points in the support of any (positive divisor) $D$ can be used as extra players. This involves redefining the embedding of $\mathcal{L}(D)$ by scaling at each point in the support of $D$ with an appropriate power of a uniformizing parameter at that point.

## 4 Construction of Ramp Schemes with Large Information Rate

Instead of taking a single point $P_0$, consider taking a sequence of distinct points $P_0^1, \ldots, P_0^\ell$, disjoint from $Q$ and $P_1, \ldots, P_n$ and where $2g + t + \ell \leq n$. It is not hard to show, by arguments virtually identical to the ones used before, that if ones takes $2g + t + \ell - 1$ instead of $2g + t$ as the degree of $D$, then the secrets may in fact be chosen arbitrarily from $\mathbb{F}_q^\ell$ instead of $\mathbb{F}_q$. The share size doesn't change. Thus it is a $(t, 2g + t + \ell, n)$-ramp scheme where each share is in $\mathbb{F}_q$, but where the secret can be chosen in $\mathbb{F}_q^\ell$. Strong multiplication and efficient error recovery can also be appropriately carried over to this variation.

## 5 Achievable Parameters

Below concrete numerical examples are given, using well-known classes of curves. The genus 0 case of our construction collapses to Shamir's scheme. As a first example with an advantage compared to known technique, consider elliptic curves, i.e., $g = 1$. It is well-known that $N_q(1) = q+1+\lfloor 2\sqrt{q}\rfloor$, unless a certain condition on $q$ and the characteristic of $p$ of $\mathbb{F}_q$ holds,[5] in which case this maximum number is just one less. Compared to using Shamir's scheme in secure computation, our scheme supports, over the same finite field $\mathbb{F}_q$, an additional $2\sqrt{q} - 1$ players. The maximal level of corruption tolerance is decreased by at most an additive factor of 2 (just 1 if the number of players $n$ is such that $n - 1$ is not divisible by 3).

Here is one example based on higher genus curves. Consider the Hermitian curves $X^{\sqrt{q}+1} + Y^{\sqrt{q}+1} = Z^{\sqrt{q}+1}$ over $\mathbb{F}_q$, where $q$ is a square. These well-known curves hit the Hasse-Weil upper bound. The genus of such curves is equal to $\frac{1}{2}(q - \sqrt{q})$, and their number of $\mathbb{F}_q$-rational points is $q\sqrt{q} + 1$.

For example, working over $\mathbb{F}_{64}$, more than 500 players are supported and more than 130 corruptions are tolerated. In comparison, in Shamir's scheme $q$ would be greater than 500 (instead of 64), but almost 40 more corruptions could be tolerated.

Finally, the well-known (non-plane) curves of García and Stichtenoth [21] from coding theory, prove useful here as well. Let $q$ be a square. Then there is a family of curves $\{C_m\}_{m\in\mathbb{Z}_{>0}}$ defined over $\mathbb{F}_q$ such that

$$\#C_m(\mathbb{F}_q) \geq (q - \sqrt{q})\sqrt{q}^{m-1} \text{ and } g(C_m) \leq \sqrt{q}^m.$$

So the ratio here is

$$\frac{g(C_m)}{\#C_m(\mathbb{F}_q))} \leq \frac{1}{\sqrt{q}-1}.$$

Consider a finite field $\mathbb{F}_q$ with $q$ a square. Let $t$ be chosen maximal such that

$$t < (\frac{1}{3} - c) \cdot n,$$

where $c = \frac{4}{3(\sqrt{q}-1)} < \frac{1}{3}$. This means that $q \geq 49$. It follows that for each $\epsilon$ with $0 < \epsilon < \frac{1}{6}$, there is a finite field $\mathbb{F}_q$ such that for infinitely many $n$ there exists a scheme with strong multiplication and with $(\frac{1}{3} - \epsilon) \cdot n \leq t < \frac{1}{3} \cdot n$. Note that in particular all sets of size at least $n - 2t$ are accepted.

Note that there exists theoretically efficient constructions of the curves of García and Stichtenoth. Efficient construction means here that one can also efficiently work with the relevant Riemann-Roch spaces. There are a host of classes of curves with many rational points known from coding theory that allow for efficient construction. We do not further address computational issues here. This is deferred to future work. See also a table with known values of $N_q(g)$, see [22].

[5] $p$ divides $\lfloor 2\sqrt{q}\rfloor$ and $\mathbb{F}_q$ is an extension of degree at least 3 over $\mathbb{F}_p$

## 6 Acknowledgements

Ronald Cramer makes the following acknowledgments. Thanks to Ivan Damgaard, Iwan Duursma, Bas Edixhoven, Serge Fehr, Gerard van der Geer, Maribel González Vasco, Robbert de Haan, Javier Herranz, Martin Hirt, Robin de Jong, Keith Martin, Hendrik Lenstra, Carles Padró, Victor Shoup, Douglas Stinson and Chaoping Xing for useful discussions, inspiration, and suggestions. Special thanks to Hendrik Lenstra for encouraging study of secret sharing from the point of view of algebraic geometry in the first place. Hao Chen's work was supported by National Natural Science Foundation Distinguished Young Scholar Grant 10225106 and by Grant 60542006 (NNSF, China).

## References

1. M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. Proceedings of STOC 1988, ACM Press, pp. 1–10.
2. J. Bierbrauer. Universal Hashing and Geometric Codes. Designs, Codes and Cryptography, vol. 11, pp. 207–221, 1997.
3. G. R. Blakley. Safeguarding cryptographic keys. Proceedings of National Computer Conference '79, volume 48 of AFIPS Proceedings, pp. 313–317, 1979.
4. D. Chaum, C. Crépeau, and I. Damgaard. Multi-party unconditionally secure protocols. Proceedings STOC 1988, ACM Press, pp. 11–19.
5. H. Chen. Linear secret sharing from algebraic-geometric codes. Merged with [8].
6. H. Chen, R. Cramer, C. Ding, and C. Xing. Secret sharing and secure multi-party compuation from projective algebraic subsets. Work in progress.
7. H. Chen, R. Cramer, S. Goldwasser, V. Vaikuntanathan, R. de Haan. Threshold MPC in the Rabin-Ben Or broadcast model unconditionally secure against corrupt minorities based on general error correcting codes. Work in progress.
8. R. Cramer. Algebraic geometric secret sharing and secure computation over small fields. Merged with [5].
9. R. Cramer, S. Fehr, and M. Stam. Blackbox secret sharing from primitive sets in algebraic number fields. Proceedings of CRYPTO 2005, volume 3621 of LNCS, pp. 344–360, Springer-Verlag, 2005.
10. R. Cramer, V. Daza, I. Gracia, J. Jimenez Urroz, G. Leander, J. Martí-Farré, and C. Padró. On codes, matroids and secure multi-party computation from linear secret sharing schemes. Proceedings of CRYPTO 2005, volume 3621 of LNCS, pp. 327–343, Springer-Verlag, 2005.
11. R. Cramer and R. de Haan. Atomic Secure Multi-Party Multiplication with Low Communication. Manuscript, 2004.
12. R. Cramer, S. Fehr, Y. Ishai, and E. Kushilevitz. Efficient multi-party computation over rings. Proceedings of EUROCRYPT 2003, volume 2656 of LNCS, pp. 596–613, Springer-Verlag, 2003.
13. R. Cramer and S. Fehr. Optimal black-box secret sharing over arbitrary Abelian groups. Proceedings of CRYPTO 2002, volume 2442 of LNCS, pp. 272–287, Springer-Verlag, 2002.
14. R. Cramer, I. Damgaard, and S. Dziembowski. On the complexity of verifiable secret sharing and multi-party computation. Proceedings of STOC 2000, ACM Press, pp. 325–334, 2000.

15. R. Cramer, I. Damgaard, and U. Maurer. General secure multi-party computation from any linear secret sharing scheme. Proceedings of EUROCRYPT 2000, volume 1807 of LNCS, pp. 316–334, Springer-Verlag, 2000.
16. R. Cramer, I. Damgaard, S. Dziembowski, M. Hirt, and T. Rabin. Efficient multiparty computations secure against an adaptive adversary. In Proceedings of EUROCRYPT 1999, volume 1592, Springer-Verlag, 1999.
17. Y. Desmedt and Y. Frankel. Homomorphic zero-knowledge threshold schemes over any finite abelian group. SIAM Journal of Discrete Mathematics, 7 (1994), pp. 667-679.
18. R. J. McEliece and D. V. Sarvate. On sharing secrets and Reed-Solomon codes. Comm. of the ACM, 22(11), November 1979, pp. 612–613.
19. M. Franklin and M. Yung. Communication complexity of secure computation. Proceedings of STOC 1992, ACM Press.
20. W. Fulton. Algebraic Curves. Advanced Book Classics, Addission-Wesley.
21. A. García and H. Stichtenoth. On the asymptotic behavior of some towers of function fields over finite fields. J. Number Theory, vol. 61, pp. 248–273, 1996.
22. G. van der Geer and M. van der Vlugt. Tables of curves with many points Mathematics of Computation 69 (2000), 797-810. See also `www.science.uva.nl/~geer` for regular updates.
23. V.D. Goppa. Codes on algebraic curves. Soviet Math. Dokl. 24: 170–172, 1981.
24. M. Karchmer and A. Wigderson. On span programs. Proceedings of the Eigth Annual Structure in Complexity Theory Conference, pp. 102–111, IEEE, 1993.
25. R. Kumar, S. Rajagopalan, and A. Sahai. Coding constructions for blacklisting problems without computational assumptions. Proceedings of CRYPTO 1999, Springer-Verlag, pp. 609–623, 1999.
26. K. Y. Lam, H. X. Wang, and C. Xing. Constructions of authentication codes from algebraic curves over finite fields. IEEE Transactions in Information Theory, Vol. 46, 886-892, 2000.
27. S. Lang. Algebra. Addison-Wesley, 1997.
28. J.H. van Lint. Introduction to Coding Theory. GTM, Springer Verlag.
29. J. L. Massey. Minimal codewords and secret sharing. Proceedings of the 6-th Joint Swedish-Russian Workshop on Information Theory Molle, Sweden, August 1993, pp. 269–279.
30. J. L. Massey. Some applications of coding theory in cryptography. Codes and Ciphers: Cryptography and Coding IV, 1995, pp. 33–47.
31. H. Niederreiter, H. Wang, and C. Xing. Function fields over finite fields and their application to cryptography. In: A. García and H. Stichtenoth (Ed.). Topics in geometry, coding theory and cryptography, Springer Verlag, to appear (2006).
32. T. Rabin and M. Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority. In Proc. ACM STOC 1989, pages 73–85, 1989.
33. A. Shamir. How to share a secret. Comm. of the ACM, 22(11):612–613, 1979.
34. J. Silverman. The Arithmetic of Elliptic Curves. GTM, Springer Verlag.
35. K.W. Shum, I. Aleshnikov, V.P. Kumar, H. Stichtenoth, V. Deolaikar. A low-complexity algorithm for the construction of algebraic-geometric codes better than the Gilbert-Varshamov bound. IEEE Trans. IT 47 (2001), no. 6, 2225–2241.
36. H. Stichtenoth. Algebraic function fields and codes. Springer Verlag, 1993.
37. M. Tsfasman and S. Vladuts. Algebraic-geometric codes. Kluwer, 1991.
38. S. Vladuts. A note on authentication codes from algebraic geometry. IEEE Transactions in Information Theory 44, no. 3, pp. 1342–1345, 1998.
39. C. Xing. Authentication codes and algebraic curves. Proceedings of the 3rd European Congress of Mathematics, Bikhauser, Vol.2, pp. 239-244, 2001.