Strongly Multiplicative Ramp Schemes From High Degree Rational Points On Curves

Hao Chen[1], Ronald Cramer[2], Robbert de Haan[3], and Ignacio Cascudo Pueyo[4]

[1] Software Engineering Institute, East China Normal University, Shanghai 20062, China. EMAIL: haochen@sei.ecnu.edu.cn.

[2] CWI, Amsterdam & Mathematical Institute, Leiden University, The Netherlands. URL: http://www.cwi.nl/∼cramer.

[3] CWI, Amsterdam, The Netherlands. URL: http://www.cwi.nl/∼haan.

[4] Department of Mathematics, University of Oviedo, Spain. EMAIL: icascudo@orion.ciencias.uniovi.es.

Abstract. In this work we introduce a novel paradigm for the construction of ramp schemes with strong multiplication that allows the secret to be chosen in an extension field, whereas the shares lie in a base field. When applied to the setting of Shamir's scheme, for example, this leads to a ramp scheme with strong multiplication from which protocols can be constructed for atomic secure multiplication with communication equal to a linear number of field elements in the size of the network.

This is also achieved by the results from Cramer, Damgaard and de Haan from EUROCRYPT 2007. However, our new ramp scheme has an improved privacy bound that is essentially optimal and leads to a significant mathematical simplification of the earlier results on atomic secure multiplication.

As a result, by considering high degree rational points on algebraic curves, this can now be generalized to algebraic geometric ramp schemes with strong multiplication over a constant size field, which in turn leads to low communication atomic secure multiplication where the base field can now be taken constant, as opposed to earlier work.

1 Introduction

Recent constructions of ramp schemes with (strong) multiplication [2, 3] play a crucial role in advances in the communication efficiency of secure multi-party computation [2–4] and, quite surprisingly, of constant rate zero knowledge proofs for circuit satisfiability [9]. The constructions of these dedicated ramp schemes rely on the theory of error correcting codes as well as arithmetic geometry,

[1] Hao Chen's research has been supported by NSFC grants 90607005 and 60433050.

[2] Ronald Cramer's research has been partially supported by NWO VICI.

[3] Robbert de Haan's research has been partially funded by the Dutch BSIK/BRICKS project PDC1.

[4] Ignacio Cascudo Pueyo's research has been partially supported by MEC of Spain, project MTM 2004-08115-C04-01 and FPU grant AP2005-0836.

and allow for the field of definition to be fixed, while offering almost optimal corruption tolerance. This is to be contrasted with Shamir's scheme, where the field size is linear in the size of the network.

In this work we introduce a novel paradigm for the construction of ramp schemes with strong multiplication [5] that allows the secret to be chosen in an extension field, whereas the shares lie in a base field. Our paradigm is based on selection of certain suitable rational subcodes of error correcting codes defined over extension fields.

Applied to the setting of Shamir's scheme, for example, this comes down to choosing random polynomials f subject to the constraints that $f(0)$ is equal to the secret s lying in an extension field L, while the shares $f(P)$ lie in a subfield K. In particular, this appears to be a novel way of turning Shamir's scheme into a ramp scheme with strong multiplication. When applied to the setting of Shamir's scheme, for example, this leads to a ramp scheme with strong multiplication from which protocols can be constructed for atomic secure multiplication with communication equal to a linear number of field elements in the size of the network. This is also achieved by the results from Cramer, Damgaard and de Haan from EUROCRYPT 2007. However, our new ramp scheme has an improved privacy bound (an additive factor linear in the degree of the field extension) that is essentially optimal and it leads to a significant mathematical simplification of the earlier results on atomic secret multiplication.

As a result, by considering high degree rational points on algebraic curves, this can now be generalized to algebraic geometric ramp schemes with strong multiplication over a constant size field, which in turn leads to low communication atomic secure multiplication where the base field can now be taken constant, as opposed to earlier work. This introduces a second scheme with strong multiplication over a constant-sized field, where the previous known such scheme due to Chen and Cramer [2] could be used to perform multiple multiplications in parallel at the cost of one.

For both these algebraic geometric schemes we additionally propose new general zero-error multiparty computation protocols secure against a malicious adversary, with corruption tolerance $t = \Omega(n)$, and where each multiplication in the protocol requires communication of $O(n^3)$ base field elements to perform a multiplication involving up to $\Omega(n)$ base field elements. This matches the communication cost of the low-cost protocol for the special case presented in [4], but requires the use of more involved techniques due to the lack of structure in these general schemes.

2 Prior Work

We first formally define the concept of ramp scheme, which is essentially a non-perfect secret sharing scheme. Ramp schemes are useful because they can achieve a high information rate, i.e., the size of the shares can be much smaller than the size of the secret. We then proceed with a brief reiteration of two strongly multiplicative variants of such ramp schemes, which were presented in [7] and

[4]. Both of these ramp schemes are ideal and have a high information rate. In particular they involve secret vectors that consist of k field elements while producing shares that consist of a single field element.

2.1 Ramp Schemes

Let $\mathbb{P} = \{p_1, \ldots, p_n\}$ be a set of players and $\mathcal{A}$ and Γ be two subsets of $2^{\mathbb{P}}$ such that $\Gamma \cap \mathcal{A} = \emptyset$. We define a ramp scheme over the field $\mathbb{F}_q$ as follows.

Let a $d \times e$ matrix M over $\mathbb{F}_q$ and a mapping $\phi : \{1, \ldots, d\} \to \{1, \ldots, n\}$ be given. Given a subset A of $\mathbb{P}$ we denote by M_A the set of the rows M_j of M such that $\phi(j) \in A$.

Definition 1 *The matrix M defines a* ramp scheme *if the following two conditions hold:*

1. *For any $A \in \mathcal{A}$, and any k elements $w_1, \ldots, w_k \in \mathbb{F}_q$, there exists a vector $\boldsymbol{v} \in KerM_A$ such that its first k coordinates are $w_1, \ldots, w_k$.*
2. *For any $B \in \Gamma$, the i^{th} unit vector $\boldsymbol{\epsilon}_i \in \mathbb{F}_q^e$ is in the image of M_B^T for all $i \in \{1, \ldots, k\}$.*

We say that $\mathcal{A}$ and Γ are the adversary structure and access structure of the scheme, respectively.

To share a secret vector $(s_1, \ldots, s_k)$ with the scheme above, a dealer chooses a random vector $\boldsymbol{v} \in \mathbb{F}_q^e$ such that its first k coordinates are $(s_1, \ldots, s_k)$ and sends to player p_j the elements $M_i v$ for which $\phi(i) = j$. Condition 1 implies that any set of players in the adversary structure can get no information about the secrets, while condition 2 ensures that any set of players in the access structure can reconstruct the secret vector using their shares. Note that the definition in [4] specifies a special case of this definition, where the access and adversary structure are defined by two (different) thresholds.

In the following, let $\odot : \mathbb{F}_q^k \times \mathbb{F}_q^k \to \mathbb{F}_q^k$ be a symmetric non-degenerate bilinear map. We define multiplication of secret shared vectors $\boldsymbol{s}, \boldsymbol{t} \in \mathbb{F}_q^k$ to be via this map, which we denote by $\boldsymbol{s} \odot \boldsymbol{t}$.

Definition 2 *A ramp scheme is* multiplicative *if for any $i \in \{1, \ldots, k\}$, there exist $\lambda_1^{(i)}, \ldots, \lambda_d^{(i)} \in \mathbb{F}_q$ such that for any two secret vectors $\boldsymbol{s}$ and $\boldsymbol{t}$ with sets of shares $(a_1, \ldots, a_d)$ and $(b_1, \ldots, b_d)$, we have that $(\boldsymbol{s} \odot \boldsymbol{t})_i = \sum_{j=1}^{d} \lambda_j^{(i)} a_j b_j$.*

Definition 3 *A ramp scheme is* strongly multiplicative *if it is multiplicative on any subset of players for which the complement is in the adversary structure. In other words, given any $A \in \mathcal{A}$, for any $i \in \{1, \ldots, k\}$ and any j so that $\phi(j) \in \bar{A}$ there exists a $\lambda_j^{(i)}$ in $\mathbb{F}_q$ such that for every two secret vectors $\boldsymbol{s}$ and $\boldsymbol{t}$ with sets of shares $(a_1, \ldots, a_d)$ and $(b_1, \ldots, b_d)$, we have that $(\boldsymbol{s} \odot \boldsymbol{t})_i = \sum_{j:\phi(j) \in \bar{A}} \lambda_j^{(i)} a_j b_j$.*

2.2 Parallel Secure Computation

The first ramp scheme we discuss is due to Franklin and Yung [7]. It has the advantage that, at the price of an additive factor k in the corruption tolerance, we can perform multiplication for k elements in parallel at the cost of a single multiplication.

The ramp scheme works as follows. Let t and k be such that $t+k-1 < n/2$ and assume that the finite field $\mathbb{F}_q$ is such that $|\mathbb{F}_q| \geq n+k$. Let the sets $\{x_1, \dots, x_n\}$ and $\{e_1, \dots, e_k\}$ be two disjoint sets of distinct elements from $\mathbb{F}_q$. Now for a vector $a = (u_1, \dots, u_k)$ of secret elements from $\mathbb{F}_q$, we select a random polynomial $f(X) \in \mathbb{F}_q[X]$ of degree at most $t+k-1$ such that $f(e_j) = u_j$ for $j = 1, 2, \dots, k$ and define the shares to be $a_j = f(x_j)$ for $j = 1, 2, \dots, n$.

Clearly, $t+k$ shares or more jointly determine f and hence the secret vector a, so the access structure includes all player sets of size at least $t+k$. As to privacy, it is a straightforward consequence of Lagrange-interpolation that t or fewer shares jointly give no information on the secret vector, so the adversary structure includes all player sets of size at most t. We can sum these properties up by calling the resulting scheme a $(t, t+k)$*-ramp scheme*, with secrets of length k.

Assume that we additionally performed this sharing with a polynomial $g(X)$ for a secret vector $b = (v_1, \dots, v_k)$. Since for $j = 1, 2, \dots, k$ it holds that $(fg)(e_j) = u_j v_j$ and furthermore $(fg)(x_i) = f(x_i)g(x_i)$ for $i = 1, 2, \dots, n$, it follows from Lagrange's interpolation theorem that the scheme is multiplicative. Therefore, we can use the generic method described in [4] to bootstrap a protocol for parallel multiplication from this scheme. For additional details, see [7] or [4].

2.3 Extension Field Multiplication

The other relevant ramp scheme can be found in [4]. With this ramp scheme it is possible to perform multiplications in a finite field using only communication and operations over a subfield, reducing the communication cost of every single multiplication by a multiplicative factor. For the technique to be used it is required that the finite field has a sufficiently large extension degree k over a subfield. Furthermore, the corruption tolerance needs to be decreased by an additive factor $2k$.

The scheme works as follows. Let t and k be such that $t + 2k - 2 < n/2$. A finite field $\mathbb{F}_{q^k} = \mathbb{F}_q(\alpha)$ is selected such that $|\mathbb{F}_q| > n$. Let $x_1, \dots, x_n$ be distinct non-zero elements from $\mathbb{F}_q$, let $a = u_0 + u_1\alpha + \ldots + u_{k-1}\alpha^{k-1} \in \mathbb{F}_{q^k}$ be a secret element and define $u(X) = u_0 + u_1 X + \ldots + u_{k-1}X^{k-1} \in \mathbb{F}_q[X]$. Choose a random polynomial $r(X) \in \mathbb{F}_q[X]$ of degree at most $t-1$ and define $f(X) = u(X) + r(X) \cdot X^{2k-1} \in \mathbb{F}_q[X]$.

Clearly, since f has degree $t+2k-2$, it is clear that $t+2k-1$ shares or more jointly determine f and hence the secret vector a. As to privacy, let $u'(X) \in \mathbb{F}_q[X]$ of degree at most $k-1$ be arbitrary and let $r'(X)$ be the polynomial that evaluates to $r(x_i) + (u(x_i) - u'(x_i))/x_i^{2k-1}$ for t points x_i. Then the polynomial $f'(X) = u'(X) + r'(X) \cdot X^{2k-1}$ is consistent with the evaluation of f in these t

points, but the secret corresponds with $u'(X)$ here. So it is a $(t, t+2k-1)$-ramp scheme, with secrets of length k.

Now, when we multiply two such polynomials $f(X) = u(X) + r(X) \cdot X^{2k-1}$ and $g(X) = v(X) + r'(X) \cdot X^{2k-1}$, the product polynomial fg has as its first $2k-1$ coefficients homogeneous sums $s_k = \sum_{i+j=k} u_i v_j$ of coefficients in $u(X)$ and $v(X)$. It is shown in [4] that this suffices for calculating the coefficients of the secret product in $\mathbb{F}_{q^k}$ via linear functions on the local products of the shares. Therefore, this scheme is also multiplicative and can be used to perform the secure multiplication over $\mathbb{F}_{q^k}$ using shares in $\mathbb{F}_q$. For additional details see [4].

Note that in order to share a secret of length k, the scheme introduces a gap between the privacy and reconstruction thresholds of size $2k-1$, whereas the scheme due to Franklin and Yung only requires a gap of size k. In Section 3 we introduce an improved version of this scheme that matches the latter thresholds.

3 An Initial Observation

A closer examination of the scheme in [4] shows that it uses a secret sharing polynomial that has a fixed k-size gap between the lower degree coefficients that relate to the secret and the higher degree coefficients that introduce randomness. In fact, this explains the disparity between the parameters of the schemes described in Sections 2.2 and 2.3.

The observation described in this section allows to remove this disparity and leads to a scheme with tight parameters that is additionally much easier to describe than the scheme from Section 2.3, while it achieves the same effect. Due to its more natural structure, it additionally generalizes over algebraic geometric curves as demonstrated in Section 4. This leads to low communication atomic secure multiplication protocols where the base field can now be taken constant as opposed to linear in the number of players as required by the approach in [4].

The proposed scheme is based on the following theorem, which generalizes Lagrange's interpolation theorem to a setting where the evaluation points are taken from different extension fields of a perfect base field K while the secret sharing polynomial is taken from $K[X]$. The idea is that the evaluation points get assigned different weights, depending on the extension degree of the smallest extension field of K in which they occur.

Theorem 1 *Let K be a perfect field, and let $\overline{K}$ denote an algebraic closure of K. Fix distinct $a_1, \ldots, a_l \in \overline{K}$ such that there is no pair a_i, a_j $(i \neq j)$ where a_j is a Galois-conjugate (over K) of a_i. For $i = 1, \ldots, l$, let n_i denote $[K(a_i) : K]$, the degree of $K(a_i)$ over K as a field extension, and let N denote $\sum_{i=1}^{l} [K(a_i) : K]$. Then, for each $b_1, \ldots, b_l$ with $b_i \in K(a_i)$ $(i = 1, \ldots, l)$, there exists a unique polynomial $f(X) \in K[X]$ such that deg $(f) < N$ and $f(a_i) = b_i$, $i = 1, \ldots, l$.*

Proof. Let $K[X]_{<N}$ denote the polynomials in $K[X]$ of degree smaller than N. Consider the map

$$\phi : K[X]_{<N} \longrightarrow \bigoplus_{i=1}^{l} K(a_i), f \mapsto (f(a_1), \ldots, f(a_l)).$$

We want to show that ϕ is an isomorphism of K-vector spaces. Since the dimensions on both sides are equal, it is sufficient to argue that ϕ is injective. Indeed, suppose g maps to 0. Then, for $i = 1, \ldots, l$, $g(a_i) = 0$. Since $g \in K[X]$, g must be a multiple of the minimal polynomial h of a_i in $K[x]$. The Galois-conjugates of a_i are the roots of h and hence they are roots of g. Because the field is perfect, h is separable, i.e. all the roots of h are different, and the number of these roots is equal to n_i, so the number of conjugates of a_i is n_i. Note that a_i and a_j are not Galois conjugates for any i, j so g has at least $\sum_{i=1}^{l} n_i = N$ zeroes in $\overline{K}$. Thus, viewing g as an element of $\overline{K}[X]$, we conclude that $g \equiv 0$. △

The new scheme works as follows. Let t and k be such that $t + k - 1 < n/2$. A finite field $\mathbb{F}_{q^k} = \mathbb{F}_q[\alpha]$ is selected such that $|\mathbb{F}_q| \geq n$. Let $x_1, \ldots, x_n$ be distinct (not necessarily non-zero) elements from $\mathbb{F}_q$ and select $e \in \mathbb{F}_{q^k}$ such that $[\mathbb{F}_q(e) : \mathbb{F}_q] = k$. The secret sharing is now performed as follows. For a secret element $a \in \mathbb{F}_{q^k}$, we choose a random polynomial $f(X) \in \mathbb{F}_q[X]$ of degree at most $t+k-1$ such that $f(e) = a$. The shares are again $f(x_1), f(x_2), \ldots, f(x_n)$.

Theorem 2 *The previous scheme has $(t+k)$-reconstruction and t-privacy.*

Proof. Reconstruction: Given the value of f in $t+k$ points $x_{i_1}, \ldots, x_{i_{t+k}}$, we can apply the previous theorem with $l = t + k$, $a_j = x_{i_j}$ (so $n_j = 1$ and $N = t + k$), to see that these shares determine the polynomial and hence the secret.

Privacy: Given the value of f in t points $x_{i_1}, \ldots, x_{i_t}$ take in the previous theorem $l = t + 1$, $a_j = x_{i_j}$ for $j = 1, \ldots, l-1$ and $a_l = e$. Then $n_j = 1$ for $j = 1, \ldots, l-1$ and $n_l = k$, so $N = t + k$. The theorem shows that for every possible choice of the secret $a \in \mathbb{F}_{q^k}$, there exists a unique polynomial of degree less than $t + k$ such that $f(e) = a$ and f evaluates to the known values in $x_{i_1}, \ldots, x_{i_t}$. △

3.1 Multi-Party Computation Secure Against an Eavesdropping Adversary

We can now use this scheme to perform secure multi-party computation of elements in $\mathbb{F}_{q^k}$ using communication and operations over the base field $\mathbb{F}_q$. In particular, when $k = O(n)$, this results in a secure multiplication protocol for which $O(n^2)$ field elements in $\mathbb{F}_q$ need to be communicated, while the multiplication is between elements in $\mathbb{F}_{q^k}$. This corresponds with a communication of only $O(n)$ field elements in $\mathbb{F}_{q^k}$.

The secure multiplication works as follows. Assume that $t + k - 1 < n/2$ and that secrets $a \in \mathbb{F}_{q^k}$ and $b \in \mathbb{F}_{q^k}$ have been secret shared, resulting in shares $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$. Due to Theorem 1 applied to the product polynomial fg there exist constants $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{F}_{q^k}$ such that $f(e)g(e) = \sum_{i=1}^{n} \lambda_i f(x_i) g(x_i)$. Writing this out over the basis $\{1, \alpha, \ldots, \alpha^{k-1}\}$ we find coefficients $\lambda_i^{(j)} \in \mathbb{F}_q$ such that $\pi_j(f(e)g(e)) = \sum_{i=1}^{n} \lambda_i^{(j)} f(x_i) g(x_i)$, where π_j is the map that maps an element $\sum_{j=0}^{k-1} w_{j+1} \alpha^j$ to the coefficient w_j. Now every player p_i reshares the element $\sum_{j=0}^{k-1} \lambda_i^{(j+1)} f(x_i) g(x_i) \alpha^j$, and it is easy to see that due to the linearity of the scheme the players can then locally sum up their new shares to obtain a share in $f(e)g(e)$.

4 Algebraic Geometric Ramp Schemes

Algebraic geometric ramp schemes were first proposed in [2] and later in [3], although the latter scheme is not multiplicative. Here we present a new algebraic geometric ramp scheme, which can be seen as a generalization of the scheme in [4], in the sense that it also allows to perform multiplication over a finite field based on operations in a subfield.

Applying some of the algebraic geometric coding techniques of [2] and using the curves introduced by García and Stichtenoth [8], we can for instance obtain families of curves from which we can define strongly multiplicative ramp schemes with corruption tolerance t with $(1/3-\epsilon)n < t < n/3$ for any $\epsilon > 0$ over constant-sized fields. In particular this implies that we can work with fixed-size shares, i.e., schemes where the share size is independent of the number of players, which was impossible to achieve with the scheme from [4].

We next describe the ramp scheme of [2] and introduce our new algebraic geometric ramp scheme where the dealer uses a high degree rational point on the curve to allocate the secret. Furthermore, we provide proofs that demonstrate both schemes are (strongly) multiplicative given a large enough number of participating players and additionally show how to compute the coefficients corresponding with the (strong) multiplication property.

4.1 Preliminaries

A very nice overview of most of the algebraic geometry theory that is required to describe the results in this paper can be found in [2]. Here we briefly reiterate the key ingredients and in addition introduce the notion of differential form.

Let $\mathbb{F}_q$ be a finite field with algebraic closure $\overline{\mathbb{F}}_q$ and let $\mathcal{C}$ be an absolutely irreducible, projective smooth curve defined over $\mathbb{F}_q$ with genus g. The function field $\overline{\mathbb{F}}_q(\mathcal{C})$ contains elements, called rational functions, which can be seen as maps from the curve $\mathcal{C}$ to $\overline{\mathbb{F}}_q$. The non-zero rational functions have the property that they can have at most a finite number of poles and zeroes, where the number of poles equals the number of zeroes when both are counted with the correct multiplicities.

A divisor is a formal sum $D = \sum_{P \in \mathcal{C}} a_P \cdot P$ with $a_P \in \mathbb{Z}$ for which the support $supp(D)$, i.e., the set of points P for which a_P is nonzero, is finite. Given two divisors $D = \sum_{P \in \mathcal{C}} a_P \cdot P$ and $D' = \sum_{P \in \mathcal{C}} a'_P \cdot P$, we say that $D \geq D'$ if $a_P \geq a'_P$ for all the points P on the curve. The degree of a divisor $D = \sum_{P \in \mathcal{C}} a_P \cdot P$ is the sum of its coefficients, i.e., $deg(D) = \sum_{P \in \mathcal{C}} a_P$.

Every rational function $f \in \overline{\mathbb{F}}_q(\mathcal{C})$ defines a divisor $(f) = \sum_{P \in \mathcal{C}} \nu_P(f) \cdot P$, where ν_P can be seen as a function that counts the number of zeroes or poles of

f with the correct multiplicity for every point P. Clearly, $deg(f) = 0$ for every $f \in \overline{\mathbb{F}}_q(\mathcal{C})$.

The set $\Omega(\mathcal{C})$ contains all rational differential forms on $\mathcal{C}$.[5] Every differential form $\eta \in \Omega(\mathcal{C})$ defines a divisor (η), where every pair of such differential forms $\eta, \eta' \in \Omega(\mathcal{C})$ gives rise to linearly equivalent divisors, i.e., $(\eta') = (\eta) + (f)$ for some $f \in \overline{\mathbb{F}}_q(\mathcal{C})$. Any such divisor K defined by a differential form is called a *canonical divisor*. For any canonical divisor K, we have that $deg(K) = 2g - 2$.

The residue maps $Res_P : \Omega(\mathcal{C}) \to \overline{\mathbb{F}}_q$ assign to every differential form $\eta \in \Omega(\mathcal{C})$ an evaluation in the point $P \in \mathcal{C}$, where $Res_P(\eta) = 0$ if η does not have a pole in P and $Res_P(\eta) \neq 0$ if η has a pole in P of multiplicity one. As with divisors based on rational functions, the multiplicity of a zero or pole in η can be read off from the coefficient at P in the formal divisor sum $(\eta) = \sum_{P \in \mathcal{C}} a_P \cdot P$. Furthermore, the Residue Theorem states that for any $\eta \in \Omega(\mathcal{C})$ we have that $\sum_{P \in \mathcal{C}} Res_P(\eta) = 0$.

For any divisor D, the corresponding Riemann-Roch space $L(D)$ is defined by $L(D) = \{f \in \overline{\mathbb{F}}_q(\mathcal{C}) \mid (f) + D \geq 0\}$. This is a vector space over $\overline{\mathbb{F}}_q$ and its dimension is denoted $\ell(D)$. For any canonical divisor K we have $\ell(K) = g$, and for any divisor D with $deg(D) < 0$ we have that $\ell(D) = 0$. More generally, the Riemann-Roch Theorem states that for any divisor D we have that $\ell(D) = \ell(K - D) + deg(D) - g + 1$. This implies in particular that $\ell(D) = deg(D) - g + 1$ when $deg(D) > 2g - 2$.

Similarly, we can for any divisor D define the space $\Omega(D)$ by

$$\Omega(D) = \{\omega \in \Omega(\mathcal{C})\backslash\{0\} \mid (\omega) + D \geq 0\} \cup \{0\}.$$

There exists an isomorphism $L(K + D) \simeq \Omega(D)$ via the map $f \mapsto f\eta$, where $(\eta) = K$, which allows us to apply the Riemann-Roch Theorem to calculate the dimension of $\Omega(D)$.

An $\mathbb{F}_q$-rational point on $\mathcal{C}$ is a point that can be represented using coordinates in $\mathbb{F}_q$. An $\mathbb{F}_q$-rational divisor is a divisor for which the support is invariant under the Galois group $Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. Note that such a divisor can have support outside of the $\mathbb{F}_q$-rational points on $\mathcal{C}$. The Riemann-Roch space of an $\mathbb{F}_q$-rational divisor admits a basis defined over $\mathbb{F}_q$, and we can consider the $\mathbb{F}_q$-linear span of this basis. We refer to functions in such an $\mathbb{F}_q$-linear span as $\mathbb{F}_q$-rational functions. Similarly, we can define the subset of $\mathbb{F}_q$-rational differential forms in a set $\Omega(\mathcal{C})$. In the sequel all rational functions and differential forms are $\mathbb{F}_q$-rational, unless otherwise specified.

4.2 Interpolation in Riemann-Roch spaces

The following result is the algebraic geometry counterpart of Theorem 1 corresponding with an arbitrary algebraic curve C.

[5] Rather than formally defining differential forms here, we restrict the description to an overview of their relevant properties. For a formal description of differential forms, the interested reader is referred to [11].

THEOREM 3 *Let $P_1, \dots, P_l$ be points on the curve C such that P_i and P_j are not conjugate for any $i \neq j$. For $i = 1, \dots, l$ let n_i be the smallest number such that P_i is $\mathbb{F}_{q^{n_i}}$-rational and define $N = \sum_{i=1}^{l} n_i$. Let G be a rational divisor such that supp $G \bigcap \{P_1, \dots, P_l\} = \emptyset$. Then:*

1. *If $N \geq deg(G) + 1$, for any $(y_1, \dots, y_l)$ with $y_i \in \mathbb{F}_{q^{n_i}}$ there exists* at most *one $f \in L(G)$ such that $f(P_i) = y_i$ for all $i = 1, \dots, l$*
2. *If $N \leq deg(G) - 2g + 1$, for any $(y_1, \dots, y_l)$ with $y_i \in \mathbb{F}_{q^{n_i}}$ there exists* at least *one $f \in L(G)$ such that $f(P_i) = y_i$ for all $i = 1, \dots, l$. Furthermore, the number of such rational functions is the same for any $(y_1, \dots, y_l)$.*

PROOF. Let $\phi : L(G) \to \bigoplus_{i=1}^{l} \mathbb{F}_{q^{n_i}}$, defined by $f \mapsto (f(P_1), \dots, f(P_l))$. For $i = 1, \dots, l$, let $P_i^{(0)} = P_i, \ \dots, \ P_i^{(n_i-1)}$ be the n_i conjugates of P_i under the Frobenius automorphism over $\mathbb{F}_q$. Observe that $\sum_{j=0}^{n_i-1} P_i^{(j)}$ is a rational point, as any element of the group $Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ permutes the conjugates of P_i. Call $A = G - \sum_{i=1}^{n}(\sum_{j=0}^{n_i-1} P_i^{(j)})$. Then $Ker(\phi) = L(A)$. Observe that $deg(A) = deg(G) - N$. Then

1. If $N \geq deg(G) + 1$, $deg(A) < 0$ and $\ell(A) = 0$. Hence ϕ is injective, which proves the property.
2. If $N \leq deg(G) - 2g + 1$, then $deg(A) \geq 2g - 1$ and we can invoke Riemann-Roch theorem to conclude that $l(A) = deg(A) - g + 1 = deg(G) - N - g + 1 = l(G) - N$. We know that $dim(Im\phi) = dim(L(G)) - dim(Ker\phi) = l(G) - l(A) = N$. Therefore ϕ is surjective.

△

4.3 An Algebraic Geometric Ramp Scheme with Parallel Multiplication [2]

Let $D = \{Q_1, \dots, Q_k, P_1, \dots, P_n\}$ be a set of $\mathbb{F}_q$-rational points on the curve $\mathcal{C}$ and G be an $\mathbb{F}_q$-rational divisor of degree $2g + t + k - 1$ with support disjoint from D. Note that since G can have support outside the $\mathbb{F}_q$-rational points, it is possible to include all $\mathbb{F}_q$-rational points on $\mathcal{C}$ in D. Every point P_i corresponds to a player p_i and every point Q_j corresponds to the j^{th} position of a secret vector, as follows. To share the secret vector $(s_1, \dots, s_k) \in \mathbb{F}_q^k$ the dealer takes a random rational function $f \in L(G)$ such that $f(Q_i) = s_i$ for all $i = 1, \dots, k$ and sends player p_i the value $f(P_i) \in \mathbb{F}_q$ as his share.

The scheme described above fits into the formal matricial definition of ramp scheme given in Section 2.1, which is useful for the following sections. Let $\{f_1, \dots, f_u\}$ be a basis of $L(G)$ such that $f_i(Q_j) = 1$ if $i = j$ and $f_i(Q_j) = 0$ if $i \neq j$, for $i = \{1, \dots, u\}$ and $j = \{1, \dots, k\}$. It is easy to see that we can always choose such a basis due to Theorem 3. Indeed, we have that $k < deg(G) - 2g + 1 = t + k + 1$ so the theorem ensures the existence of such f_i for $i = 1, \dots, k$. Now simply take $\{f_{k+1}, \dots, f_u\}$ as a basis of $L(G - \sum_{i=1}^{k} Q_i)$, which has dimension $u - k$ according to the Riemann-Roch Theorem.

Next, define the matrix M whose (i,j) entry is $f_j(P_i)$. If we take a vector $\boldsymbol{v} = (s_1, \ldots, s_k, r_{k+1}, \ldots, r_n)$ and multiply any row of M_i by $\boldsymbol{v}$, we obtain the value $g(P_i)$, where $g = \sum_{j=1}^{k} s_j f_j + \sum_{j=k+1}^{n} r_j f_j$. It holds that $g(Q_i) = s_i$ for any $i = 1, \ldots, k$.

Theorem 4 *The description above defines a ramp scheme with t-privacy and $(2g+t+k)$-reconstruction.*

Proof. It can be easily seen as a special case of Theorem 3 that any rational function in $L(G)$ is uniquely determined by its evaluations in $deg(G)+1$ rational points (this is exactly Lemma 1 of [2]). In our case, $deg(G) = 2g+t+k-1$ so any $2g+t+k$ players can reconstruct the rational function and thus the secret vector.

Next we prove privacy. Let A be any set of t players. We only need to argue that for any secret vector $\boldsymbol{s} = (s_1, \ldots, s_k) \in \mathbb{F}_q^k$ there exists a rational function f such that $f(Q_i) = s_i$ and the evaluation of f in the points corresponding to the players in A is zero. Theorem 3 shows us that this is true because $t + k = deg(G) - 2g + 1$.

△

4.4 A New Algebraic Geometric Ramp Scheme with Extension Field Multiplication

Let $D = \{P_1, \ldots, P_n\}$ again be a set of $\mathbb{F}_q$-rational points on the curve $\mathcal{C}$ such that $supp(G) \bigcap D = \emptyset$, and additionally let Q be a point on the curve outside the support of G that is $\mathbb{F}_{q^k}$-rational and not $\mathbb{F}_{q^d}$-rational for any integer $d < k$.

Let $\{e_1, e_2, \ldots, e_k\}$ be a basis of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$. To share the secret vector $(s_1, \ldots, s_k)$, the dealer selects a random rational function $f \in L(G)$ such that $f(Q) = s_1 e_1 + \ldots + s_k e_k \in \mathbb{F}_{q^k}$, and sends player p_i the value $f(P_i) \in \mathbb{F}_q$ as his share.

We can also represent this ramp scheme by a matrix. In this case we take a basis $\{f_1, \ldots, f_u\}$ of $L(G)$ such that $f_i(Q) = e_i$ for $i = 1, \ldots, k$ and $f_i(Q) = 0$ for $i = k+1, \ldots, n$. It can again be shown that such a basis exists using Theorem 3. We have only one point of degree k and $k \leq deg(G) - 2g + 1$, so we know such f_i exist for $i = 1, \ldots, k$, and we can take $\{f_{k+1}, \ldots, f_u\}$ a basis of $L(G - Q - \sum_{i=1}^{k-1} Q_i)$, where $Q_1, Q_2, \ldots, Q_{k-1}$ are the conjugate points of Q under the Frobenius automorphism over $\mathbb{F}_q$.

Let M be the matrix M whose (i,j) entry is $f_j(P_i)$. As before, if we take a vector $\boldsymbol{v} = (s_1, \ldots, s_k, r_{k+1}, \ldots, r_n)$ and multiply any row of M_i by $\boldsymbol{v}$, we obtain the value $g(P_i)$, where $g = \sum_{j=1}^{k} s_j f_j + \sum_{j=k+1}^{n} r_j f_j$ and it holds that $g(Q) = \sum_{i=1}^{k} s_i e_i$.

Theorem 5 *The description above defines a ramp scheme with t-privacy and $(2g+t+k)$-reconstruction.*

Proof. As before, both properties are a direct consequence of Theorem 3.

△

4.5 Multiplication

Both of the schemes thus described introduce their own form of multiplication. For the parallel multiplication scheme, given two vectors $\boldsymbol{s} = (s_1, s_2, \ldots, s_k)$ and $\boldsymbol{t} = (t_1, t_2, \ldots, t_k)$, we can define the product $\boldsymbol{s} \odot \boldsymbol{t} = (s_1 t_1, s_2 t_2, \ldots, s_k t_k)$.

For the extension field multiplication scheme, given any two vectors $\boldsymbol{s} = (s_1, s_2, \ldots, s_k)$ and $\boldsymbol{t} = (t_1, t_2, \ldots, t_k)$, representing the elements $s = s_1 e_1 + s_2 e_2 + \ldots + s_k e_k \in \mathbb{F}_{q^k}$ and $t = t_1 e_1 + t_2 e_2 + \ldots + t_k e_k \in \mathbb{F}_{q^k}$, the product of these two elements in the field $\mathbb{F}_{q^k}$ is some element $u = u_1 e_1 + u_2 e_2 + \ldots + u_k e_k \in \mathbb{F}_{q^k}$ for some $u_i \in \mathbb{F}_q$. We can therefore define the product of $\boldsymbol{s}$ and $\boldsymbol{t}$ as $\boldsymbol{s} \odot \boldsymbol{t} = (u_1, u_2, \ldots, u_k)$.

We next prove that, given enough players, the two schemes are multiplicative and strongly multiplicative with regard to their respective multiplications.

Theorem 6 *The parallel multiplication scheme is multiplicative when $n \geq 2t + 4g + 2k - 1$ and strongly multiplicative when $n \geq 3t + 4g + 2k - 1$.*

Proof. We need to show that for any $i = 1, \ldots, k$ there are coefficients $\lambda_1^{(i)}, \ldots, \lambda_n^{(i)}$ such that for any $f, g \in L(G)$, $f(Q_i)g(Q_i) = \sum_{j=1}^{n} \lambda_j^{(i)} f(P_j)g(P_j)$. Note that if f and g are in $L(G)$ their product is in the space $L(2G)$.

According to Theorem 3 we have that if $deg(2G) + 1 \leq n$ the mapping $\phi : L(2G) \to \bigoplus_{j=1}^{n} \mathbb{F}_q$ defined by $h \mapsto (h(P_1), \ldots, h(P_n))$ is linear and injective, so it has an inverse and it is also linear. Furthermore, the maps $\psi_i : L(2G) \to \mathbb{F}_q$ defined by $h \mapsto h(Q_i)$ are also linear for any $i \in \{1, \ldots, k\}$. So the composition of ϕ^{-1} and any ψ_i is linear. Therefore $fg(Q_i)$ is a linear combination of $f(P_j)g(P_j)$ for any f and g in $L(G)$. Finally observe that the condition $deg(2G) + 1 \leq n$ holds whenever $4g + 2t + 2k - 1 \leq n$. △

Similar to the simpler finite field setting the coefficients $\lambda_j^{(i)}$ can be explicitly determined. We now describe how to obtain these using the Residue Theorem (see [11]).

Determining the coefficients $\boldsymbol{\lambda_j^{(i)}}$. A consequence of the Residue Theorem is that for any function φ in $L(2G)$ and any differential ω in $\Omega(Q_i + \sum_{j=1}^{n} P_j - 2G)$ the relation $0 = \sum_{j=1}^{n} res_{P_j}(\varphi\omega) + res_{Q_i}(\varphi\omega) = \sum_{j=1}^{n} \varphi(P_j) res_{P_j}(\omega) + \varphi(Q_i) res_{Q_i}(\omega)$ holds. Therefore, if there exists a nonzero element ω in $\Omega(Q_i + \sum_{j=1}^{n} P_j - 2G)$, applying the theorem for the rational function fg gives a linear relation between the values $fg(Q_i)$ and $fg(P_j)$ for $j = 1, \ldots, n$ for some coefficients which do not depend on f and g. If we can additionally ensure that the coefficient $res_{Q_i}(\omega)$ is non-zero, then we have a relation of the form $fg(Q_i) = \sum_{j=1}^{n} -\frac{res_{P_j}(\omega)}{res_{Q_i}(\omega)} fg(P_j)$. Thus, $\lambda_j^{(i)} = -\frac{res_{P_j}(\omega)}{res_{Q_i}(\omega)}$ and we are done.

It is a known fact that we can define an isomorphism of $\mathbb{F}_q$-vector spaces $\phi : L(K + Q_i + \sum_{j=1}^{n} P_j - 2G) \to \Omega(Q_i + \sum_{j=1}^{n} P_j - 2G)$ defined by $\phi(h) = h\eta$ where K is a canonical divisor and η is a differential such that $div(\eta) = K$. It suffices to find an element h in $L(K + Q_i + \sum_{j=1}^{n} P_j - 2G)$ with a first order pole in Q_i. Hence, we have to show that there exists an element in the difference of the spaces $L(K + Q_i + \sum_{j=1}^{n} P_j - 2G)$ and $L(K + \sum_{j=1}^{n} P_j - 2G)$. Applying the Riemann-Roch theorem for $n \geq 2t + 4g + 2k - 1$ shows us that the dimensions of these spaces differ and the result follows.

Theorem 7 *The extension field multiplication scheme is multiplicative when $n \geq 2t + 4g + 2k - 1$ and strongly multiplicative when $n \geq 3t + 4g + 2k - 1$.*

Proof. Now we need to show that for any $i = 1, \ldots, k$ there exist coefficients $\lambda_1^{(i)}, \ldots, \lambda_n^{(i)}$ in $\mathbb{F}_q$ such that for any $f, g \in L(G)$, $\pi_i(f(Q)g(Q)) = \sum_{j=1}^{n} \lambda_j^{(i)} f(P_j)g(P_j)$. An argument similar to that in Theorem 6 shows that, for $n \geq 2t + 4g + 2k - 1$, there exist elements $r_j \in \mathbb{F}_{q^k}$ such that $f(Q)g(Q) = \sum_{j=1}^{n} r_j f(P_j)g(P_j)$. Now, note that $r_j = \sum_{i=1}^{k} \lambda_j^{(i)} e_i$, which gives us the desired result. △

5 Multi-Party Computation Secure Against An Active Adversary

In the sequel we present the techniques that can be used to construct multi-party computation protocols secure against an active adversary for the algebraic geometric ramp schemes presented earlier. Due to the lack of structure in these schemes compared to the simpler polynomial-based approaches we need to introduce some new techniques here. Most of these techniques revolve around the construction of some specialized variants of VSS, which are then employed to ensure that the players honestly participate in the protocol.

6 A VSS Protocol for the Algebraic Geometric Schemes

When the number of players is sufficiently large, we can perform efficient reconstruction of the secret in the presence of corrupted shares. This is due to the strong relation between our schemes and Goppa error correction codes [11]. In both schemes, the set of possible share vectors forms a Goppa code over $\mathbb{F}_q$ of length n (the number of players) with minimum distance larger than or equal to $n - deg(G)$. We know that a code with minimum distance d allows for reconstruction of a codeword in the presence of t errors, provided that $2t + 1 \leq d$. Furthermore, it is known how to efficiently correct such errors for Goppa codes. We have the following property:

Property 1 *Assume that a honest dealer shares a secret vector with one of the algebraic geometric ramp schemes in the previous section. If $n \geq 3t + 2g + k$, honest players can efficiently reconstruct the secret vector even when up to t corrupted players provide incorrect shares.*

Note that this bound is weaker than that required for strong multiplicativity for any of the two schemes in Section 4.

We now describe the general procedure used to verifiably secret share a vector with a ramp scheme. Recall that in the usual definition of a verifiable secret sharing (VSS), the VSS ensures that at the end of the sharing either all honest players hold consistent shares in a value s or the dealer is disqualified. Additionally, when the dealer is not disqualified, it is guaranteed that the players can uniquely reconstruct the secret s by pooling their shares in s, even when some of the dishonest players provide an incorrect share. We follow this standard definition of VSS, except that we allow the secret to be a vector.

6.1 Definitions and Notation

We need to introduce some new notation. Given an $\mathbb{F}_q$-vector space V with base $\{v_1, \ldots, v_u\}$, consider the tensor product $V \otimes V$. The elements in the space $V \otimes V$ are formal sums $\sum_{i,j} a_{ij}(v_i \otimes v_j)$ with $a_{ij} \in \mathbb{F}_q$. The symmetric tensor $S^2(V)$ is defined to be the subspace consisting of all the elements in $V \otimes V$ such that $a_{ij} = a_{ji}$ for all $i, j \in \{1, \ldots, u\}$.

We define now the space $S^2(L(G))$. Given an element F in this space, we can evaluate it in any pair (P, Q) of points on the curve, where if $F = \sum_{i,j} a_{ij}(f_i \otimes f_j)$ we have $F(P, Q) = \sum_{i,j} a_{ij}(f_i(P)f_j(Q))$. Now, if P_i is the point corresponding to the player p_i, we define F_i to be the rational function in $L(G)$ such that $F_i(P) = F(P_i, P)$.

For the parallel multiplication scheme from Section 4.3 we define F_0 to be the rational function defined by $F_0(P) = F(Q_1, P)$. Furthermore, for the extension field multiplication scheme from Section 4.4, let F_0 be the rational function defined as follows. Take the function $F_0'(Y) = F(Q, Y) = \sum_{i,j} a_{ij} f_i(Q) f_j(Y)$ in the variable Y that runs over the points on the curve. Note that the coefficients $a_{ij} f_i(Q)$ belong to $\mathbb{F}_{q^k}$. Now we can define the rational function $F_0 = \sum_{i,j} \pi_1(a_{ij} f_i(Q)) f_j$, where the function π_1 is the projection function that has been described in Section 3.1. We now have the following symmetry property, which is easily verified.

Proposition 1 *We have that $F_i(P_j) = F_j(P_i)$ and $F_i(Q_1) = F_0(P_i)$ for the parallel multiplication scheme (respectively, $\pi_1(F_i(Q)) = F_0(P_i)$ for the extension field multiplication scheme) for any $F \in S^2(L(G))$ and $i, j \in \{1, \ldots, n\}$.*

6.2 The VSS Scheme

Conceptually, the rational function F_0 plays the same role in the VSS as the secret sharing polynomial does for Shamir's scheme. We now describe how to perform the VSS for the two algebraic geometric schemes.

First, given a secret vector $(s_1, s_2, \ldots, s_k)$ and a divisor D (for our purposes D is always G or $2G$) we define the set $S_{(s_1,\ldots,s_k)}(D) = \{f \in L(D) : f(Q_l) = s_l \; \forall l = 1, \ldots, k\}$ for the parallel multiplication scheme and $S_{(s_1,\ldots,s_k)}(D) = \{f \in L(D) : f(Q) = s_1e_1 + s_2e_2 + \cdots + s_ke_k\}$ for the extension field multiplication scheme. The set $S_{(s_1,\ldots,s_k)}(D)$ forms the sets of rational functions from which F_0 can be drawn when the secret vector is $(s_1, \ldots, s_k)$.

Let us also define $\mathcal{S}_{(s_1,\ldots,s_k)}(D) = \{F \in S^2(L(D)) : F_0 \in S_{(s_1,\ldots,s_k)}(D)\}$ for any of both schemes. If the dealer now wants to VSS a vector $(s_1, s_2, \ldots, s_k)$ he must first select a uniformly random element F in $\mathcal{S}_{(s_1,\ldots,s_k)}(G)$ and then send player p_i the rational function $F_i \in L(G)$ for $i = 1, 2, \ldots, n$. After this the players execute a number of steps to ensure the consistency of the data that they received from the dealer. These steps are very similar to those for the Shamir-based VSS described in [5] and we do not enumerate them here. The value $F_i(Q_1) = F(P_i, Q_1) = F_0(P_i)$ (respectively $\pi_1(F_i(Q)) = F_0(P_i)$) should be seen as player $p_i's$ share in the parallel multiplication scheme (respectively the extension field multiplication scheme).

We next prove that this VSS scheme can always be applied and that it provides privacy in the presence of any adversary controlling up to t players. Unique reconstruction of the secret for the honest players follows from an argument similar to that for the Shamir-based VSS scheme and is omitted here.

For the privacy statement, we first assume without loss of generality that the rational share functions F_i that adversarial players receive are all zero. For any subset $B \subset \{P_1, \ldots, P_n\}$ with $|B| = e \leq t$, we define the sets $W_B(D) = \{f \in L(D) : f(P_j) = 0 \ \forall j \in B\}$ and $\mathcal{W}_B(D) = \{F \in S^2(L(D)) : F_j = 0 \ \forall j \in B\}$ respectively denoting the potential secret sharing functions and rational share functions corresponding to this assumption. Note that in particular when $e = 0$, we have $W_B(D) = L(D)$ and $\mathcal{W}_B(D) = S^2(L(D))$.

For the privacy statement to hold, we mainly need to prove that we have $|\mathcal{S}_{(s_1,\ldots,s_k)}(G) \cap \mathcal{W}_B(G)| = |\mathcal{S}_{(s'_1,\ldots,s'_k)}(G) \cap \mathcal{W}_B(G)|$ for any two secret vectors $(s_1, \ldots, s_k)$ and $(s'_1, \ldots, s'_k)$. To prove that the VSS can always be applied we need to prove that $|\mathcal{S}_{(s_1,\ldots,s_k)}(G)| > 0$ for any secret vector $(s_1, \ldots, s_k)$. Both statements can be deduced from the following theorem:

Theorem 8 *For any adversary set B and any secret vector $(s_1, \ldots, s_k)$, the mapping $\mathcal{S}_{(s_1,\ldots,s_k)}(G) \cap \mathcal{W}_B(G) \rightarrow S_{(s_1,\ldots,s_k)}(G) \cap W_B(G)$ given by $F \mapsto F_0$ is surjective.*

Proof. We here give the proof for the parallel multiplication scheme. The proof for the extension field multiplication scheme is very similar and therefore omitted here.

Let f be an element of $S_{(s_1,\ldots,s_k)}(G) \cap W_B(G)$. If $s_1 \neq 0$ then take $F = \frac{1}{s_1}(f \otimes f)$. We have that $F_j = \frac{1}{s_1} f(P_j) f = 0$ for any player $p_j \in B$ because $f \in W_B(G)$, so $F \in \mathcal{W}_B(G)$. Moreover $F_0 = \frac{1}{s_1} f(Q_1) f = f$.

If $s_1 = 0$ then select an $h \in L(G)$ such that $h(Q_1) = 1$ and $h(P_j) = 0$ for all $j \in B$. Such h exists due to the privacy properties of the parallel multiplication scheme described in Section 4.3. Now define $F = f \otimes h + h \otimes f$. We have $F_0 = h(Q_1) f + f(Q_1) h = f$ and $F_j = h(P_j) f + f(P_j) h = 0 \ \forall \ P_j \in B$. This completes the proof. $\triangle$

If we take $B = \emptyset$, Theorem 8 implies that we can always VSS a secret vector since it was already clear from Sections 4.3 and 4.4 that we can always secret share a secret vector. As for the privacy property, observe that as a consequence of the surjectivity of the mapping, for any set B in the adversary structure and any secret vector $(s_1, \dots, s_k)$ we know that $\mathcal{S}_{(s_1,\dots,s_k)}(G) \cap \mathcal{W}_B(G)$ is non-empty. Now, given the secret vectors $(s_1, \dots, s_k)$ and $(s'_1, \dots, s'_k)$, take any element F in $\mathcal{S}_{(s'_1-s_1,\dots,s'_k-s_k)}(G) \cap \mathcal{W}_B(G)$. We have that addition by the function F induces a bijective mapping between the sets $\mathcal{S}_{(s_1,\dots,s_k)}(G) \cap \mathcal{W}_B(G)$ and $\mathcal{S}_{(s'_1,\dots,s'_k)}(G) \cap \mathcal{W}_B(G)$.

It can be seen, using Property 1 and the proof for the consistency checks in [5], that the VSS protocol additionally guarantees consistency between the shares of the honest players whenever $n \geq 3t + 2g + k$.

7 Low Complexity MPC for Algebraic Geometric Ramp Schemes

In this section we demonstrate multi-party computation protocols secure against an active adversary based on the algebraic geometric ramp schemes from Section 4, where we assume that n is sufficiently large so that we can perform efficient reconstruction of the secret vectors for rational functions in $L(2G)$ and we are also able to perform VSS over $L(2G)$. Concretely, this is ensured when $n \geq 4t + 4g + 2k - 1$.

The protocols in this section require the communication of $O(n^3)$ field elements while operating on vectors consisting of k elements, which matches that attained for the special case detailed in [4]. However, since we lack the convenient structure that the polynomials provided in [4], we required some new specialized forms of VSS to ensure that the players honestly follow the protocol. Below, we provide the details of the special types of VSS that we require.

7.1 Tailored VSS

It is possible to place some restrictions on the randomly selected element $F \in S^2(L(2G))$ that is used for the VSS in order to ensure to the players that the VSS'ed secret vector is of a special form. Here two types of structural restrictions are relevant for our results; one where some positions in the secret vector are fixed to zero and one where all positions in the secret vector contain the same value. We also look at the combination of these two types, where all-zero vectors replace the secret vectors. This particular variant is used to a create a "one-time-pad" that is used to securely verify the equality of the secret vectors in two secret sharings, and is invoked in a slightly different manner as explained below.

We additionally note the following about the special types of VSS before providing the details in the following sections. In Section 7.2, whenever the secret vector is non-zero, the special types of VSS are used to generate rational functions in $L(G)$. On the other hand, when the special VSS is used to generate a one-time-pad, the resulting rational functions are in $L(2G)$. Note that, since $L(G) \subset L(2G)$, we can use a basis for $L(2G)$ of the form $f_1, f_2, \dots, f_{u'}$, where the rational functions $f_1, f_2, \dots, f_u$ form the selected basis for $L(G)$. Note also that $S^2(L(G))$ can be embedded in $S^2(L(2G))$ in the natural way.

Fixing zeros and producing repetition The restriction is imposed as follows for the case where we introduce zero's in the vector such that the first position of the vector remains non-zero. Let $I \subset \{1, \ldots, k\}$ be a set consisting of positions in the vector that should be zero. Let $\{u_v\}$ be a base of $L(2G)$ of the appropriate form as described in Sections 4.3 and 4.4 and $V_I(2G) \subset L(2G)$ be spanned by $\{u_v\}_{v \notin I}$. Then $V_I(2G)$ consists of all functions of $L(2G)$ which are zero in Q_j for $j \in I$. Analogously define $\mathcal{V}_I(2G) = \{F \in S^2(L(2G)) : F_j(Q_l) = 0\ \forall j = 0, \ldots, n,\ l \in I\}$, which can be seen as a bivariate version of this set. If we now VSS using elements in $\mathcal{V}_I(2G)$ not only does the secret rational function belong to $V_I(2G)$, but so do all rational functions that are received as shares by the players.

We need a similar kind of restriction for the generation of one-time-pads in $L(2G)$ by a certain player p_i, except that in this case we will require that all the elements of $V_I(2G)$ have their first coordinate equal to zero. Therefore given an $F \in \mathcal{V}_I(2G)$, we have that $F_0 = 0$ and this cannot be used as a one-time-pad due to it's lack of randomness. We propose to use the rational function F_i that player p_i receives as his share instead, where the evaluations $F_j(P_i) = F_i(P_j)$ of the players p_j act as the shares in F_i.[6] It remains to show that we can always VSS a random but restricted rational function F_i in this way, and that this procedure does not leak additional useful information to the adversary. The first property is a consequence of the following theorem.

Theorem 9 *Let B be a set in the adversary structure. The mapping $\mathcal{V}_I(2G) \cap \mathcal{W}_B(2G) \to V_I(2G) \cap W_B(2G)$ given by $F \mapsto F_i$ is surjective.*

The proof is very similar to that of Theorem 8 and omitted here due to space considerations. As a consequence of this theorem, given any rational function $f \in V_I(2G)$ there exists at least one $F \in \mathcal{V}_I(2G)$ such that $F_i = f$. Moreover, the VSS does not add new information to the adversary about F_i, as shown in the following theorem.

Theorem 10 *Let B be a set in the adversary structure and F any uniformly randomly selected element of $\mathcal{V}_I(2G)$ under the restrictions given above. Then, the values $(F_j)_{j \in B}$ add no further information about F_i to the information given by $F_i(P_j)$.*

Proof. It suffices to prove that for every rational function $f \in V_I(2G)$ such that $f(P_j) = 0$ for all $j \in B$, we can find an F in $\mathcal{V}_I(2G)$ such that $F_j = 0$ for all j in B and $F_i = f$. This is again a consequence of Theorem 9. △

The repetitive type of structural restriction is only needed for the parallel multiplication scheme and consist of the following. A player wants to VSS a vector $(s, s, \ldots, s)$ of k equal elements in such a way that the coefficients of the

[6] This is not known to be possible in the space $L(G)$ as defined here, but any encompassing space $L(G')$ of larger dimension with $supp(G') \cap D = \emptyset$ suffices. In particular this can be done in the space $L(2G)$.

rational share functions F_1, F_2 and F_n at the basis elements $f_1, \ldots, f_k$ are also equal.

Let us define the sets $\mathcal{R}_s(D) = \{F \in S^2(L(D)) : F_0(Q_1) = \cdots = F_0(Q_k) = s$ and $F_j(Q_1) = \cdots = F_j(Q_k)\ \forall j = 0, \ldots, n\}$ and $R_s(D) = \{f \in L(D) : f(Q_1) = \cdots = f(Q_k) = s\}$. Privacy and existence can, similar to before, be deduced from the following theorem.

Theorem 11 *The mapping $\mathcal{R}_s(G) \cap \mathcal{W}_B(G) \to R_s(G) \cap W_B(G)$ given by $F \mapsto F_0$ is surjective for any $s \in \mathbb{F}_q$.*

We omit the proof, as it is very similar to that of Theorems 8 and 9.

Creating a default sharing for $(\boldsymbol{\lambda_i^{(1)}, \lambda_i^{(2)}, \ldots, \lambda_i^{(k)}})$ Consider the vector $\boldsymbol{\lambda_i} = (\lambda_i^{(1)}, \lambda_i^{(2)}, \ldots, \lambda_i^{(k)})$. We here create a default ramp sharing of this (public) vector that is used later on. To do so, we take the rational function $\lambda_i = \sum_{j=1}^{k} \lambda_i^{(j)} f_j \in L(G)$, such that the share of player p_j is $\lambda_i(P_j)$. Note that in the parallel multiplication scheme $\lambda_i(Q_\ell) = \lambda_i^{(\ell)}$, while in the extension field multiplication scheme $\lambda_i(Q) = \sum_{l=1}^{k} \lambda_i^{(\ell)} e_\ell$. This sharing is later used to create VSS'ed shares in the vector $(\lambda_i^{(1)} y, \lambda_i^{(2)} y, \ldots, \lambda_i^{(k)} y)$ in the space $L(2G)$ from a VSS of y in the space $L(G)$.

7.2 The MPC Protocols Secure Against an Active Adversary

As usual, addition and multiplication with a constant can be performed locally by the players. Therefore, the main focus is on the initialization, secure multiplication and reconstruction parts of the protocol. During the multiplication part of the protocol, the special types of VSS that were introduced in Section 7.1 are used to force the dishonest players to follow the protocol honestly. Due to this, the protocol can basically be seen as an application of the protocol secure against an eavesdropping adversary enhanced with checking information that ensures that players perform the correct steps. We now present the details of the main protocol parts.

Initialization The dealer verifiably secret shares $\boldsymbol{s}, \boldsymbol{t} \in \mathbb{F}_q^k$ using uniformly random elements $F \in \mathcal{S}_{\boldsymbol{s}}$, $G \in \mathcal{S}_{\boldsymbol{t}}$, resulting in rational functions $f_i := F_i$ and $g_i := G_i$ for every player p_i and secret sharing functions $f_0 := F_0$ and $g_0 := G_0$. For the parallel multiplication scheme we denote $f_{i0} := f_i(Q_1)$ and $g_{i0} := g_i(Q_1)$ and similarly for the extension field multiplication scheme we denote $f_{i0} := \pi_1(f_i(Q))$ and $g_{i0} := \pi_1(g_i(Q))$ for $i, j = 1, 2, \ldots, n$.

Using this notation it is to be understood that f_{i0} is the actual share of player p_i in the scheme based on F and similarly for the g_{i0} and G. Furthermore, for both schemes we denote $f_{ij} := f_i(P_j)$ and $g_{ij} := g_i(P_j)$ for $i, j = 1, 2, \ldots, n$, where the share f_{ij} can be seen as the share of player p_i in the rational function F_j held by player p_j. We also use this convention of using lower case letters to denote the shares and rational functions for the other VSSes introduced in the protocols below.

Multiplication The following two protocols describe the main parts of the multiplication protocol for the parallel multiplication scheme. After proving their properties, we then sketch the changes required for the extension field multiplication scheme. The general structure of the multiplication protocol is as follows. First, every player p_i simultaneously:

1. Reshares the product $a_i b_i$ of his shares a_i and b_i in the VSS of the secret vectors that are to be multiplied in a special format depending on the scheme involved.
2. Reshares his contribution $\boldsymbol{\lambda_i} a_i b_i = (\lambda_i^{(1)} a_i b_i, \lambda_i^{(2)} a_i b_i, \ldots, \lambda_i^{(k)} a_i b_i)$ in the output of the multiplication, where the validity of this resharing is verified using the special resharing created in the previous step.

After this the players can add up their shares in the contributions $\boldsymbol{\lambda_i} a_i b_i$ of the players to obtain shares in the product $\boldsymbol{s} \odot \boldsymbol{t} = \sum_{i=1}^{n} \boldsymbol{\lambda_i} a_i b_i$. Below these subprotocols are listed for the respective secret sharing schemes.

Protocol 1: (Parallel multiplication) Resharing the input of player p_i
Input: Two VSSes with elements $F, G \in S^2(L(G))$.
Output: A VSS with $D \in_R \mathcal{R}_s(G)$ with $s = f_{i0} g_{i0}$ or a disqualification for player p_i.
Protocol:

1. Player p_i VSSes $D \in_R \mathcal{R}_s(G)$.
2. Player p_i VSSes $S \in_R \mathcal{V}_{\{1\}}(2G)$.
3. The players publicly verify that $s - d_0(Q_1) + s_{i0} = 0$. If not, player p_i is disqualified.

Protocol 2: (Parallel multiplication) Computing contribution player p_i
Input: A VSS with $D \in \mathcal{R}_s(G)$.
Output: A VSS with $H^i \in_R \mathcal{S}_{(\boldsymbol{\lambda_i} s)}(G)$ or a disqualification for player p_i.
Protocol:

1. The players locally generate shares λ_j in the default sharing of $\boldsymbol{\lambda_i}$.
2. Player p_i VSSes $H^i \in_R \mathcal{S}_{(\boldsymbol{\lambda_i} s)}(G)$.
3. Player p_i VSSes $T \in_R \mathcal{V}_{\{1,2,\ldots,k\}}(2G)$.
4. The players verify that $[\lambda_0 d_0 - h_0^i + t_i](Q_\ell) = 0$ for $\ell = 1, 2, \ldots, k$. If not, player p_i is disqualified.

We now prove that Protocol 1 is private and correct. Since the privacy and correctness proofs for the other protocols are very similar, these are omitted.

Theorem 12 *At the end of Protocol* 1*, either player p_i has been disqualified, or the output is a sharing of the correct form.*

Proof. The main claim to be verified is that $d_0(Q_\ell) = f_i(Q_1) g_i(Q_1)$ for $j = 1, 2, \ldots, k$ if player p_i is not disqualified at the end of the protocol. We have $f_i(Q_1) g_i(Q_1) - d_0(Q_1) + s_i(Q_1) = 0$ iff $f_i(Q_1) g_i(Q_1) = d_0(Q_1)$.

Due to the applications of VSS, every player p_j holds a value $[f_ig_i - d_0 + s_i](P_j)$ in the rational function $[f_ig_i - d_0 + s_i]$. The rational function $[f_ig_i - d_0 + s_i]$ and the evaluations held by the players now define a ramp sharing scheme over $L(2G)$ and from our assumptions on the number of players, we know that the players can efficiently and correctly reconstruct the value $[f_ig_i - d_0 + s_i](Q_1)$ from the pooling of their shares. Due to the special VSS structure used for S, the claim now follows. $\triangle$

THEOREM 13 *If player p_i is honest, pooling the shares $f_{ij}g_{ij} - d_0(P_j) + s_{ij}$ leaks no additional information on f_ig_i or d_0.*

PROOF. Due to the privacy properties of the secret sharing scheme we can first assume wlog that the shares $(d_j)_{j\in A}$, $(f_{ij}g_{ij})_{j\in A}$, $(s_{ij})_{j\in A}$ of the adversary in the three sharings are all equal to zero. The adversary knows a priori that $f_ig_i \in L(2G) \cap W_B(2G)$, $s_i \in V_{\{1\}}(2G) \cap W_B(2G)$ and $d_0 \in R_s(G) \cap W_B(G)$ for some s he does not know. He also knows that $f_ig_i - d_0 \in V_{\{1\}}(2G) \cap W_B(2G)$. We must prove that pooling the shares, and therefore learning the rational function $h = f_ig_i - d_0 + s_i$, adds no further information to this knowledge.

To do so we prove that for any $d \in R_s(G) \cap W_B(G)$, and $f, g \in L(G)$ such that $fg \in L(2G) \cap W_B(2G)$ and $fg(Q_1) = i(Q_1)$, there exist $F, G \in S^2(L(G))$, $I \in \mathcal{R}_s(G) \cap W_B(G)$ and $S \in \mathcal{V}_{\{1\}}(2G) \cap \mathcal{W}_B(2G)$, such that $s_{i0} = 0$, $f_i = f$, $g_i = g$, $d_0 = d$ and $f_ig_i - d_0 + s_i = h$. As a particular case of Theorem 8 we can see that there exist $F, G \in S^2(L(G))$ and $D \in \mathcal{R}_s(G) \cap \mathcal{W}_B(G)$ such that $f_i = f$, $f_i = g$, $d_0 = d$. Finally take $z = h - f_ig_i + d_0$ which is a rational function in $V_{\{1\}}(2G) \cap W_B(2G)$. As a consequence of Theorem 9 we can show that there exists $S \in \mathcal{V}_{\{1\}}(2G) \cap \mathcal{W}_B(2G)$ with $s_i = z$ and that completes the proof.

$\triangle$

We now briefly describe the adjustments that need to be made to the protocols above in order to obtain equally efficient secure protocols for the extension field multiplication. The most important modification is that whereas in the previously listed protocols every player p_i VSSes the product s of his local shares using an element in $\mathcal{R}_s(G)$, for the extension field multiplication scheme the VSS needs to use an element in $\mathcal{S}_{(s,0,\ldots,0)}$. The reason for this is that in the second protocol this allows multiplication with the public sharing for $\boldsymbol{\lambda_i}$ in order to locally create a VSS of $\boldsymbol{\lambda_i}s$ in $L(2G)$, similar to what is done in Protocol 2. The second change, which is also required due to the differing structures of the two schemes, is that in the second scheme the coefficients of the secret vector are accessed via the projection maps $\pi_1, \pi_2, \ldots, \pi_k$, which requires small adjustments in the final verification steps of the two protocols.

Share construction Every player p_j locally sums his rational function shares H_j^i, resulting in a rational function share $H_j = \sum_{i=1}^n H_j^i$ in the product $\boldsymbol{s} \odot \boldsymbol{t}$.

7.3 Complexity Analysis of the Multiplication Protocol

During the multiplication protocol every player performs a constant number of VSSes, where every VSS requires $O(n^2)$ communication. Therefore, the multiplication part requires $O(n^3)$ communication for k elements.

References

1. G. R. Blakley and C. Meadows. Security of ramp schemes. In *Proceedings CRYPTO '85*, volume 196, pages 242–269. Springer Verlag LNCS, 1985.
2. H. Chen and R. Cramer. Algebraic geometric secret sharing schemes and secure multi-party computation over small fields. In *Proceedings of 26th Annual IACR CRYPTO*, volume 4117, pages 516–531, Santa Barbara, Ca., USA, August 2006. Springer Verlag LNCS.
3. H. Chen, R. Cramer, S. Goldwasser, R. de Haan, and V. Vaikuntanathan. Secure computation from random error correcting codes. In *Proceedings of 26th Annual IACR EUROCRYPT 2007*, volume 4515, pages 291–310. Springer Verlag LNCS, 2007.
4. R. Cramer, I. Damgaard, and R. de Haan. Atomic secure multi-party multiplication with low communication. In *Proceedings of EUROCRYPT 2007*, volume 4515, pages 329–346. Springer Verlag LNCS, 2007.
5. R. Cramer, I. Damgaard, and U. Maurer. General secure multi-party computation from any linear secret sharing scheme. In *Proceedings of EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 316–334. Springer Verlag, 2000.
6. R. Cramer, V. Daza, I. Gracia, J. Jiménez Urroz, G. Leander, J. Martí-Farré, and C. Padró. On codes, matroids and secure multi-party computation from linear secret sharing schemes. In *Proceedings of CRYPTO 2005*, volume 3621 of *LNCS*, pages 327–343. Springer-Verlag, 2005.
7. M. Franklin and M. Yung. Communication complexity of secure computation. In *Proceedings of STOC 1992*, pages 699–710. ACM Press, 1992.
8. A. García and H. Stichtenoth. On the asymptotic behavior of some towers of function fields over finite fields. *J. Number Theory*, 61:248–273, 1996.
9. Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai. Zero-knowledge from secure multiparty computation. In *Proceedings of STOC 2007*, pages 21–30. ACM Press, 2007.
10. A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.
11. M. A. Tsfasman and S. G. Vlăduţ. *Algebraic-Geometric Codes.* Kluwer, 1991.