Embedding Multiplications at a Linear Rate and its Applications

Alexander R. Block[*, †] Hemanta K. Maji[‡, †] Hai H. Nguyen[§, †]

April 30, 2018

Abstract

Consider the following embedding problem. Alice has input $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{F}^m$ and Bob has input $\mathbf{b} = (b_1, \ldots, b_m) \in \mathbb{F}^m$, where $\mathbb{F}$ is a finite field. The two parties want Bob to receive $\mathbf{c} = (c_1, \ldots, c_m)$ such that $c_i = a_i \cdot b_i$, for all $i \in \{1, \ldots, m\}$. Alice and Bob have access to an oracle that takes as input two elements $A, B \in \mathbb{K}$ from Alice and Bob, respectively, and outputs the product $C = A \cdot B \in \mathbb{K}$ to Bob, where $\mathbb{K}$ is a degree-n extension of the finite field $\mathbb{F}$. Alice and Bob want to perform only one call to this oracle and enable Bob to compute $\mathbf{c}$ without any additional communication. Given n, how large can m be?

More tersely: "How many multiplications over the base field can we perform using only one multiplication over an extension field?"

Block, Maji, and Nguyen (CRYPTO–2017) proposed this problem and their combinatorial solution achieved $m = n^{1-o(1)}$. Our paper presents an explicit embedding that achieves the optimal asymptotic bound $m = \Theta(n)$, where the constant in the asymptotic notation depends on the size of the base field $|\mathbb{F}|$. The construction of our proposed embedding relies on the toolkit provided by algebraic function fields.

Although the study of this embedding problem is of independent theoretical interest, we present a few representative applications to secure computation. We construct a linear number of oblivious transfers based on the computational hardness assumptions like the pseudorandomness of noisy Reed Solomon codewords with a constant computational overhead. This result enables the efficient secure evaluation of arithmetic circuits that use arithmetic gates over extension fields of the same base field. Next, we construct the first correlation extractor with a linear production rate and 1/2 resilience by composing our embedding with the correlation extractor of Block, Maji, and Nguyen (CRYPTO–2017).

[*]Department of Computer Science, Purdue University. block9@purdue.edu.

[†]The research effort is supported in part by an NSF CRII Award CNS–1566499, an NSF SMALL Award CNS–1618822, and an REU CNS–1724673.

[‡]Department of Computer Science, Purdue University. hmaji@purdue.edu.

[§]Department of Computer Science, Purdue University. nguye245@purdue.edu.

Contents

1 Introduction

Secure multi-party computation (MPC) allows mutually distrusting parties to compute securely over their private data. Typically, MPC protocols establish a basis to represent the computation and, subsequently, support arbitrary secure computation in that representation. For example, we can represent the computation as a circuit that uses boolean AND, and XOR gates, and represent the input, output, and the intermediate values of the computation in binary. Alternatively, we can represent the computation as a circuit that uses arithmetic MUL, and ADD gates over appropriate finite fields, and represent the input, output, and the intermediate values of the computation as elements from a finite field.

MPC protocols securely implement computations represented using binary gates using oblivious transfer (OT). The oblivious transfer functionality takes as input a pair of bits (x_0, x_1) from the sender and a choice bit b from the receiver, and outputs the bit x_b to the receiver. Parties perform m calls to the OT functionality to securely compute circuits that have (roughly) m AND gates (and an arbitrary number of XOR gates). We can emulate computations using arithmetic gates over large fields by implementing the MUL and ADD arithmetic gates using appropriate circuits.

On the other hand, using oblivious linear-function evaluation (OLE), a natural generalization of OT, MPC protocols implement computations represented using arithmetic gates. The OLE functionality takes as input a pair of field elements $(a, b) \in \mathbb{F}^2$ from the sender and an element $x \in \mathbb{F}$ from the receiver, and outputs the linear evaluation $z = a \cdot x + b$ to the receiver. Note that, for $x_0, x_1, b \in \mathbb{GF}[2]$, we have $x_b = (x_0+x_1)b+x_0$, i.e., OT is a particular instantiation of the OLE functionality. As in the setting of boolean circuits, parties perform m calls to the OLE functionality to securely compute circuits that have (roughly) m MUL gates.

Computationally secure protocols for the OLE functionality exist based on standard cryptographic hardness assumptions like the pseudorandomness of noisy Reed-Solomon codewords. The current state-of-the-art MPC protocols can securely compute arithmetic circuits by incurring a constant computational overhead [ADI+17]. However, based on this computational hardness assumptions, it is unknown whether we can securely evaluate boolean circuits with a constant computational overhead as well. Ideally, our objective should be to simultaneously support evaluation of circuits that incorporate arithmetic as well as boolean gates. For example, there are natural applications in privacy-preserving data mining where the circuits involve the simultaneous use of arithmetic gates and boolean range queries (represented by boolean circuits over an appropriate representation of the field elements). Our paper's primary technical contribution, among its other consequences, resolves this problem.

1.1 Multiplication Embedding Problem

This combinatorial embedding problem was originally introduced by Block, Maji, and Nguyen [BMN17] in the context of leakage-resilient MPC. Let $\mathbb{F}$ be a finite field. Alice has private input $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{F}^m$ and Bob has private input $\mathbf{b} = (b_1, \ldots, b_m) \in \mathbb{F}^m$. The two parties want Bob to receive the output $\mathbf{c} = (c_1, \ldots, c_m) \in \mathbb{F}^m$ such that $c_i = a_i \cdot b_i$, for all $i \in \{1, \ldots, m\}$.

Alice and Bob have access to an oracle that takes input $A \in \mathbb{K}$ from Alice and $B \in \mathbb{K}$ from Bob, where $\mathbb{K}$ is a degree-n extension of the field $\mathbb{F}$, and outputs $C = A \cdot B$ to Bob. Alice and Bob want to perform only one call to this oracle and enable Bob to compute $\mathbf{c}$. Note that Alice and Bob perform *no additional interactions*. Given a fixed value of n and a particular base field $\mathbb{F}$, how large can m be?

The prior work of Block et al. [BMN17] constructed an embedding that achieved $m = n^{1-o(1)}$ using techniques from additive combinatorics. This paper, using algebraic function fields, provides an asymptotically optimal $m = \Theta(n)$ construction. Section 1.2 summarizes our results and a few of its consequences for MPC.

1.2 Our Contributions

Given two vectors $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{F}^m$ and $\mathbf{b} = (b_1, \ldots, b_m) \in \mathbb{F}^m$, we represent their Schur product as the vector $\mathbf{a} * \mathbf{b} = (a_1 \cdot b_1, \ldots, a_m \cdot b_m)$. We prove the following theorem.

Theorem 1 (Embedding Theorem)**.** *Let $\mathbb{F}_q$ be a finite field of size q, a power of a prime. There exists constants $c_q^* \in \{1, 2, 3, 4, 6\}$, $c_q > 0$, and $n_0 \in \mathbb{N}$ such that for all $n \geqslant n_0$ where c_q^* divides n, there exist (linear) maps $E \colon \mathbb{F}_q^m \to \mathbb{K}$ and $D \colon \mathbb{K} \to \mathbb{F}_q^m$, where $\mathbb{K}$ is the degree-n extension of the field $\mathbb{F}_q$, such that the following constraints are satisfied.*

1. *We have $m \geqslant c_q n$, and*
2. *For all $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^m$, we have: $D\big(E(\mathbf{a}) \cdot E(\mathbf{b})\big) = \mathbf{a} * \mathbf{b}$.*

Intuitively, an oracle that implements one multiplication over a degree-n extension field $\mathbb{K}$ facilitates the computation of $m = \Theta(n)$ multiplications over the base field $\mathbb{F}$. For instance, assuming the base field $\mathbb{F} = \mathbb{GF}[2]$, our result shows that we can implement $m = \Theta(n)$ AND gates, which are equivalent to the MUL arithmetic gates over the $\mathbb{GF}[2]$, by performing only one call to the functionality that implements MUL over $\mathbb{K} = \mathbb{GF}[2^n]$. Section 1.3 presents a summary of the intuition that inspired our construction, and Section 2 provides the required technical background and Section 2.2 presents the proof of Theorem 1.

Applications to MPC. Recall that the OLE functionality over the field $\mathbb{K}$ takes as input (A, B) from the sender and X from the receiver, and outputs $Z = A \cdot X + B$ to the receiver. Essentially, OLE over the field $\mathbb{K}$ generates an additive secret share $(-B, Z)$ of the product $A \cdot X$. The embedding of Theorem 1 also helps Alice and Bob implement m independent OLEs over the base field $\mathbb{F}$, represented by the $\mathsf{OLE}(\mathbb{F})^m$ functionality, using one OLE over the extension field $\mathbb{K}$.

Corollary 2. *Let $\mathbb{F}$ be a finite field and $\mathbb{K}$ be a degree-n extension of $\mathbb{F}$. There exists a 2-party secure protocol for the $\mathsf{OLE}(\mathbb{F})^m$ functionality in the $\mathsf{OLE}(\mathbb{K})$-hybrid, where $m = \Theta(n)$, that performs only one call to the $\mathsf{OLE}(\mathbb{K})$ functionality.*

Section 3 provides the proof of this corollary in the semi-honest setting. Continuing our working example of $\mathbb{F} = \mathbb{GF}[2]$, we can implement $m = \Theta(n)$ independent OT functionalities by performing one call to the $\mathsf{OLE}(\mathbb{K})$ functionality.

Using Corollary 2 we can implement a linear number of OTs at a constant overhead based on the pseudorandomness of noisy Reed-Solomon codewords, which helps construct an OLE over large (but finite) fields. In fact, we can leverage efficient bilinear multiplication algorithms [CC87] that incur a constant overhead, to obtain the following result (see Appendix A).

Corollary 3. *Let $\mathbb{F}$ be a finite field and $\mathbb{K}$ be a degree-n extension of $\mathbb{F}$. Let $\mathbb{F}_1, \ldots, \mathbb{F}_k$ be finite fields such that $\mathbb{F}_i$ is a degree-n_i extension of the base field $\mathbb{F}$, for $i \in \{1, \ldots, k\}$. Let C be a circuit that uses m_i arithmetic gates over the field $\mathbb{F}_i$. If $m_1 n_1 + \cdots + m_k n_k \leqslant \Theta(n)$, then there exists a secure protocol for C in the $\mathsf{OLE}(\mathbb{K})$-hybrid that performs only one call to the $\mathsf{OLE}(\mathbb{K})$ functionality.*

Appendix A provides the outline of constant overhead secure computation of $\mathsf{OLE}(\mathbb{F}_i)$ by performing $\Theta(n_i)$ calls to the $\mathsf{OLE}(\mathbb{F})$ functionality, where $\mathbb{F}_i$ is a degree-n_i extension of the base field $\mathbb{F}$. We emphasize that Corollary 3 allows us the flexibility to generate the (randomized version of the) $\mathsf{OLE}(\mathbb{K})$ in an offline phase of the computation without the necessity to fix the representation of the computation itself.

Finally, using our embedding, instead of the embedding of [BMN17], we obtain the following result for correlation extractors (cf., [IKOS09] for an introduction).

Corollary 4. *For every $1/2 > \varepsilon > 0$, there exists an n-bit correlated private randomness such that, despite $t = (1/2 - \varepsilon)n$ bits of leakage, we can securely construct $m = \Theta(\varepsilon n)$ independent OTs from this leaky correlation.*

Section 4 presents the details of the definition of correlation extractors and the proof of this corollary.

1.3 Technical Overview

To illustrate the underlying idea of our embedding, we use the example where $|\mathbb{F}| = 3n/2$, where $\mathbb{K}$ is a degree-n extension of $\mathbb{F}$. Note that in this intuition the size of the base field implicitly bounds the degree of the extension field $\mathbb{K}$ that we can consider. Ideally, our objective is to obtain multiplication embeddings for small constant-size $\mathbb{F}$ for infinitely many n, which our theorem provides. Nevertheless, we feel that the intuition presented in the sequel assists the reading of the details of Section 2.

Assume that n is even and $m := (n/2 - 1)$. We arbitrarily enumerate the elements in $\mathbb{F}$

$$\mathbb{F} = \{f_{-m}, \ldots, f_{-2}, f_{-1}, f_1, f_2, \ldots, f_{n-1}\}$$

Suppose the field $\mathbb{K}$ is isomorphic to $\mathbb{F}[t]/\pi(t)$, where $\pi(t) \in \mathbb{F}[t]$ is an irreducible polynomial of degree n.

Recall that Alice and Bob have private inputs $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{F}^m$ and $\mathbf{b} = (b_1, \ldots, b_m) \in \mathbb{F}^m$. Alice constructs the unique polynomial $A(t) \in \mathbb{F}[t]/\pi(t)$ of degree $< m$ such that $A(f_{-i}) = a_i$, for all $i \in \{1, \ldots, m\}$ using Lagrange interpolation. Similarly, Bob constructs the unique polynomial $B(t) \in \mathbb{F}[t]/\pi(t)$ of degree $< m$ such that $B(f_{-i}) = b_i$, for all $i \in \{1, \ldots, m\}$.

Suppose the two parties have access to an oracle that multiplies two elements of $\mathbb{K}$ and outputs the result to Bob. Upon receiving the inputs $A(t)$ and $B(t)$ from Alice and Bob, respectively, which correspond to elements in $\mathbb{K}$, the oracle outputs the result $C(t) = A(t) \cdot B(t)$ to Bob.[1] Note that $C(t)$ is the convolution of the two polynomials $A(t)$ and $B(t)$. Moreover, it has the property that $C(f_{-i}) = a_i \cdot b_i$, for all $i \in \{1, \ldots, m\}$. So, Bob can evaluate the polynomial $C(t)$ at appropriate places to obtain $\mathbf{c} = \mathbf{a} * \mathbf{b}$.

Note that this protocol crucially relies on the fact that the field $\mathbb{F}$ has sufficiently many *places* $\{f_{-1}, \ldots, f_{-m}\}$ to enable the encoding of $a_1, \ldots, a_m$ as the *evaluation* of polynomials at those respective places. For constant-size fields $\mathbb{F}$, this intuition fails to scale to large values of n. So, we use the toolkit of algebraic function fields for a more generalized and formal treatment of these intuitive concepts and construct these multiplication embeddings for *every* base field $\mathbb{F}$.

2 Embedding Multiplications

Our goal is to embed m multiplications over $\mathbb{F}_q$ using a single multiplication over $\mathbb{F}_{q^n}$ such that $m = \Theta(n)$. To do so, we use algebraic function fields over $\mathbb{F}_q$ with appropriate parameters.

2.1 Preliminaries

We introduce the basics of algebraic function fields necessary for our construction. We follow the conventions of [Sti09, Cas10]. Let $\mathbb{F}_q$ be a finite field of q elements, where q is a power of prime.

Definition 1 (Algebraic Function Field)**.** *An* algebraic function field *(or function field for simplicity) $K/\mathbb{F}_q$ of one variable over $\mathbb{F}_q$ is an extension field $K \supseteq \mathbb{F}_q$ and a finite algebraic extension of $\mathbb{F}_q(x)$ for some element x which is transcendental over $\mathbb{F}_q$.*

We let $\widetilde{\mathbb{F}}_q$ denote the field of constants of $K/\mathbb{F}_q$. In the remainder of this paper, we only consider function fields $K/\mathbb{F}_q$ such that $\mathbb{F}_q = \widetilde{\mathbb{F}}_q$. For ease of presentation, we assume $\mathbb{F}_q$ to always be the field of constants and denote $K/\mathbb{F}_q$ by K. The simplest example of a function field is the *rational function field*. The function field K is called *rational* if $K = \mathbb{F}_q(x)$ for $x \in K$ which is transcendental over $\mathbb{F}_q$. Explicitly, the rational function field K is written as

$$K = \left\{ \frac{f(x)}{g(x)} \ : \ f, g \in \mathbb{F}_q[x], g \not\equiv 0 \right\}.$$

Definition 2 (Valuation Ring)**.** *A valuation ring of the function field K is a ring $\mathcal{O} \subseteq K$ such that*

- $\mathbb{F}_q \subsetneq \mathcal{O} \subsetneq K$*, and*
- *for every $z \in K$, either $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.*

[1] Note that this is exact polynomial multiplication because the degree of $A(t)$ and $B(t)$ are both $< m$. So, the degree of $C(t)$ is $< 2m - 1 = n$. This observation, intuitively, implies that "$\bmod \pi(t)$" does not affect $C(t)$.

Valuation rings are used to define a more general "point" of a function field, namely *places*.

Definition 3 (Places)**.** *A* place P *of* K *is the maximal ideal of some valuation ring* $\mathcal{O}$ *of* K*. We denote the set of all places of* K *by* $\mathbb{P}(K)$*.*

Places uniquely define their corresponding valuation rings, and valuation rings uniquely define their corresponding places. This is given by the following lemmas.

Imported Lemma 1 ([Cas10, Proposition 2.5])**.** *A valuation ring* $\mathcal{O}$ *of* K *is a local ring; that is, its only maximal ideal is* $P = \mathcal{O} \setminus \mathcal{O}^*$*, where* $\mathcal{O}^*$ *denotes the group of units of* $\mathcal{O}$*.*

Imported Lemma 2 ([Cas10, Proposition 2.8])**.** *Given* $P \in \mathbb{P}(K)$*, there is a unique valuation ring* $\mathcal{O}_P$ *such that* P *is its maximal ideal. This valuation ring is precisely*

$$\mathcal{O}_P = \{f \in K \ : \ f^{-1} \notin P\}.$$

These two imported lemma state that places and valuation rings are interchangeable. In fact, a place P is the principle ideal of its corresponding valuation ring $\mathcal{O}_P$.

Imported Lemma 3 ([Cas10, Proposition 2.9])**.** *Any valuation ring* $\mathcal{O}$ *of* K *is a principal ideal domain. Therefore any place* $P \in \mathbb{P}(K)$ *is a principle ideal and can be written in the form* $P = t_P\mathcal{O}_P$ *for some* $t_P \in P$*.*

Any $t_P \in P$ which satisfies $P = t_p\mathcal{O}_P$ is called a *uniformizing parameter* for P. Valuation rings give rise to valuation maps.

Definition 4 (Valuation Map)**.** *For any* $P \in \mathbb{P}(K)$ *with any uniformizing parameter* t_P*, define the function* $v_P \colon K \to \mathbb{Z} \cup \{\infty\}$ *by*

$$v_P(f) := \begin{cases} n & \text{if } 0 \neq f \in \mathcal{O}_P, \text{ and } f = t_P^n u, u \in \mathcal{O}_P^* \\ -n & \text{if } f \in K \setminus \mathcal{O}_P, \text{ and } f^{-1} = t_P^n u, u \in \mathcal{O}_P^* \\ \infty & \text{if } f = 0 \end{cases}$$

The value $v_P(f)$ *is the* valuation *of* f *at* P*.*

This map is well-defined since $\mathcal{O}_P$ is a valuation ring and by the following lemma.

Imported Lemma 4 ([Cas10, Proposition 2.12])**.** *For any* $P \in \mathbb{P}(K)$ *and uniformizing parameter* t_P *for* P*, every element* $0 \neq f \in \mathcal{O}_P$ *can be uniquely written as* $f = t_P^n u$ *for* $n \in \mathbb{N}$ *and* $u \in \mathcal{O}_P^*$*. Furthermore, for any* $0 \neq f \in \mathcal{O}_P$ *and any two uniformizing parameters* t_P *and* t'_P *of* P*, if* $f = t_P^n u = (t'_P)^{n'} u'$*, then* $n' = n$*.*

Note that Definition 4 gives an equivalent definition of a valuation ring $\mathcal{O}_P$ for place P.

Imported Theorem 1 ([Sti09, Theorem 1.1.13])**.** *For any* $P \in \mathbb{P}(K)$*, we have* $\mathcal{O}_P = \{z \in K \ : \ v_P(z) \geqslant 0\}$*.*

We can now define evaluation of a function at a place.

Definition 5 (Evaluation at a Place)**.** *For any $P \in \mathbb{P}(K)$, the* residue class field *of P is $K_P := \mathcal{O}_P/P$. The* evaluation *of $f \in \mathcal{O}_P$ at P is its residue class in K_P and is denoted by $f(P)$. For $f \notin \mathcal{O}_P$, its evaluation at P is defined to be $f(P) = \infty$.*

In other words, evaluation of a function f at place P yields the residue class of f in K_P. In fact, K_P is isomorphic to a finite field extension of $\mathbb{F}_q$, where the degree of the extension depends on the place P.

Imported Lemma 5 ([Cas10, Proposition 2.17])**.** *Let $P \in \mathbb{P}(K)$. Then $\mathbb{F}_q \subseteq \mathcal{O}_P$ and $\mathbb{F}_q \cap P = \{0\}$. Hence there is a canonical embedding of $\mathbb{F}_q$ into K_P, so $\mathbb{F}_q$ can be considered as a subfield of K_P. Furthermore the degree $|K_P\colon \mathbb{F}_q|$ of the field extension satisfies $|K_P\colon \mathbb{F}_q| \leqslant |K\colon \mathbb{F}_q(x)| < \infty$, for any $0 \neq x \in P$.*

In particular, if $|K_P\colon \mathbb{F}_q| = a$, then we have $K_P \cong \mathbb{F}_{q^a}$ and $f(P) \equiv \alpha \in \mathbb{F}_{q^a}$ for $f \in \mathcal{O}_P$. Imported Lemma 5 naturally defines the degree of a place P.

Definition 6 (Degree of a place)**.** *For every $P \in \mathbb{P}(K)$, the* degree *of P is* $\deg P := |K_P\colon \mathbb{F}_q|$.

We denote the set of all places of degree k by $\mathbb{P}^{(k)}(K)$. Note that the set $\mathbb{P}^{(1)}(K)$ is called the *set of rational places* (or rational points). Places are used to define the divisors of a function field K.

Definition 7 (Divisors)**.** *A* divisor *D of a function field K is a formal sum $D = \sum_{P\in\mathbb{P}(K)} m_P P$ where $m_P \in \mathbb{Z}$ and $m_P = 0$ except for a finite number of places $P \in \mathbb{P}(K)$. We define $\mathsf{Supp}(D) := \{P \in \mathbb{P}(K) : m_P \neq 0\}$ to be the* support *of divisor D. The set of all divisors of K is denoted* $\mathrm{Div}(K)$.

Note that from Definition 7, it is clear that every place $P \in \mathbb{P}(K)$ is also a divisor, namely $P = 1 \cdot P \in \mathrm{Div}(K)$. Such divisors are called *prime divisors*. Any divisor $D \in \mathrm{Div}(K)$ has corresponding degree depending on places $P \in \mathsf{Supp}(D)$.

Definition 8 (Degree of a Divisor)**.** *For any divisor $D = \sum_{P\in\mathbb{P}(K)} m_P P$, the* degree *of D is* $\deg D := \sum_{P\in\mathbb{P}(K)} m_P(\deg P) \in \mathbb{Z}$.

This definition is consistent with the degree of place P for the case where divisor D is also a place. We can naturally define the summation of two divisors.

Definition 9 (Sum of Divisors)**.** *Let $D = \sum_{P\in\mathbb{P}(K)} m_P P$ and $D' = \sum_{P\in\mathbb{P}(K)} n_P P$ be two divisors. Then $D + D' := \sum_{P\in\mathbb{P}(K)} (m_P + n_P)P$.*

We use Definition 9 to define a partial ordering of divisors.

Definition 10 (Divisor Partial Ordering)**.** *For divisors $D = \sum_{P\in\mathbb{P}(K)} m_P P$ and $D' = \sum_{P\in\mathbb{P}(K)} n_P P$, we say that $D \leqslant D'$ if $m_P \leqslant n_P$ for all $P \in \mathbb{P}(K)$. We say that a divisor D is* effective *(or positive) if $D \geqslant 0$.*

Every $f \in K \setminus \{0\}$ can be associated with a divisor by the following theorem.

Imported Theorem 2 ([Cas10, Theorem 2.32])**.** *Every $f \in K \setminus \{0\}$ has finitely many zeros and poles. That is, we have $v_P(f) = 0$ except for finitely many $P \in \mathbb{P}(K)$.*

We now define the divisor associated to $f \in K \setminus \{0\}$.

Definition 11 (Principal Divisors)**.** *For any $f \in K \setminus \{0\}$, the divisor*

$$(f) := \sum_{P \in \mathbb{P}(K)} v_P(f) P$$

is the principal divisor *associated to f. We let* $\mathrm{Prin}(K) := \{D \in \mathrm{Div}(K) \colon \exists f \in K \setminus \{0\},\ D = (f)\}$ *denote the set of principal divisors.*

Associating every nonzero function f with divisor (f) allows us to define the Riemann-Roch space.

Definition 12 (Riemann-Roch Space)**.** *For a divisor $G \in \mathrm{Div}(K)$, the* Riemann-Roch space *associated with G is defined as*

$$\mathscr{L}(G) := \{f \in K : (f) + G \geqslant 0\} \cup \{0\}.$$

Note that $\mathscr{L}(G)$ is a vector space over $\mathbb{F}_q$ for any $G \in \mathrm{Div}(K)$. We denote the dimension of $\mathscr{L}(G)$ over $\mathbb{F}_q$ by $\ell(G)$. In particular, the dimension of the Riemann-Roch space is bounded above and below by the degree of its divisor.

Imported Lemma 6 ([Cas10, Lemma 2.51])**.** *For any $G \in \mathrm{Div}(K)$, we have $\ell(G) \leqslant \deg G + 1$. In particular, if $\deg G < 0$, then $\ell(G) = 0$.*

Imported Theorem 3 (Riemann's Theorem [Cas10, Theorem 2.53])**.** *There exists $M \in \mathbb{Z}$ such that for all $D \in \mathrm{Div}(K)$, we have $\ell(D) \geqslant M + \deg D$.*

We now define the genus of the function field K.

Definition 13 (Genus)**.** *The* genus *of the function field K is defined as*

$$g(K) := \max_{D \in \mathrm{Div}(K)} \deg D - \ell(D) + 1 \in \mathbb{N}.$$

When clear from context, we let $g := g(K)$.

The genus always exists and is a non-negative integer by Imported Theorem 3. Next we define canonical divisors. First we need the following definition.

Definition 14 (Space of Differential Forms)**.** *The* space of differential forms $\Omega(K)$ *of K is the K-vector space generated by the symbols df, $f \in K$, such that*

- *$d(f+g) = df + dg$ for all $f, g \in K$,*
- *$d(fg) = f \cdot dg + df \cdot g$ for all $f, g \in K$,*
- *$df = 0$ for all $f \in \mathbb{F}_q$.*

Now we can associate a divisor to any $w \in \Omega(K) \setminus \{0\}$.

Definition 15 (Canonical Divisor)**.** *For any $w \in \Omega(K)\backslash\{0\}$, the* canonical divisor *associated to w is the divisor*

$$(w) := \sum_{P \in \mathbb{P}(K)} v_P(w)P.$$

Canonical divisors are well-defined by the following lemma.

Imported Lemma 7 ([Cas10, Proposition 2.62])**.** *For $w \in \Omega(K) \setminus \{0\}$, we have $v_P(w) = 0$ for all but a finite number of places $P \in \mathbb{P}(K)$.*

Next we state an important result about canonical divisors.

Imported Theorem 4 ([Cas10, Theorem 2.65])**.** *For any canonical divisor $W \in \mathrm{Div}(K)$, we have $\deg W = 2g - 2$ and $\ell(W) = g$.*

We have the tools in place to state the Riemann-Roch Theorem.

Imported Theorem 5 (Riemann-Roch Theorem [Sti09, Theorem 1.5.15])**.** *Let W be a canonical divisor of $K/\mathbb{F}_q$. Then for each divisor $A \in \mathrm{Div}(K)$,*

$$\ell(A) = \deg A + 1 - g + \ell(W - A).$$

The final ingredients for our construction are the following lemma and theorem. The lemma states that for large enough n, there always exists a prime divisor of degree n in K. The theorem states that there always exists a construction of a function field K such that the number of divisors of degree one is large.

Imported Lemma 8 ([BCS97, Lemma 18.21])**.** *Let $K/\mathbb{F}_q$ be an algebraic function field of one variable of genus g and let n be an integer satisfying $n \geqslant 2\log_q g + 6$. Then there exists a prime divisor of degree n of $K/\mathbb{F}_q$.*

Imported Theorem 6 (Garcia and Stichtenoth [GS95], [BCS97, Theorem 18.24])**.** *Let p be a power of prime, X_1 be an indeterminate over $\mathbb{F}_{p^2}$, and $K_1 := \mathbb{F}_{p^2}(X_1)$. For $i \geqslant 1$ let $K_{i+1} := K_i(Z_{i+1})$, where Z_{i+1} satisfies the Artin-Schreier equation $Z_{i+1}^p + Z_{i+1} = X_m^{p+1}$ and $X_i := Z_i/X_{i-1} \in K_i$ (for $i \geqslant 2$). Then K_i/F_{p^2} has genus g_i given by*

$$g_i = \begin{cases} p^i + p^{i-1} - p^{\frac{i+1}{2}} - 2p^{\frac{i-1}{2}} + 1 & \text{if } i \equiv 1 \bmod 2, \\ p^i + p^{i-1} - \frac{1}{2}p^{\frac{i}{2}+1} - \frac{3}{2}p^{\frac{i}{2}} - p^{\frac{i}{2}-1} + 1 & \text{if } i \equiv 0 \bmod 2, \end{cases}$$

and $|\mathbb{P}^{(1)}(K_i/\mathbb{F}_{p^2})| \geqslant (p^2 - 1)p^{i-1} + 2p \geqslant (p-1)g_i$.

2.2 Our Construction

In this section, we present our construction which satisfies the requirements of and proves Theorem 1. The following lemma will be used.

Lemma 1. *Let V be a subspace of dimension m of $\mathbb{F}_q^r$. Then there exists a linear mapping $\psi : \mathbb{F}_q^r \to \mathbb{F}_q^m$ such that ψ is a bijection from V to $\mathbb{F}_q^m$ and that $\psi(x) * \psi(y) = \psi(x * y)$ for every $x, y \in \mathbb{F}_q^r$.*

Proof. Let G be a generator matrix of V, then $V = u \cdot G$ for $u \in \mathbb{F}^m$ and for any $x \in \mathbb{F}^r$ there exists a unique $u \in \mathbb{F}^m$ such that $x = uG$. Let $s \subseteq [r]$ be a set of indices such that $G \setminus G_S$ still has full rank. For example, if $G = [I|P]$ in standard form, then $G_S = P$, and $S = \{m+1, m+2, \ldots, r\}$. Note that $|S| = r - m$. Let $G' = G \setminus G_S$ and $S' = [r] \setminus S$. We define $\psi(x) = x_{S'}$. It is easy to see that ψ is a linear map. Now, for any $x, y \in \mathbb{F}^r$, we have

$$\psi(x) * \psi(y) = x_{S'} * y_{S'} = (x * y)_{S'} = \psi(x * y)$$

Finally, ψ is a bijection from V to $\mathbb{F}^m$ since for any $x \in \mathbb{F}^r$ there exists a unique $u \in \mathbb{F}^m$ such that $x = uG$, and since G' has full rank. □

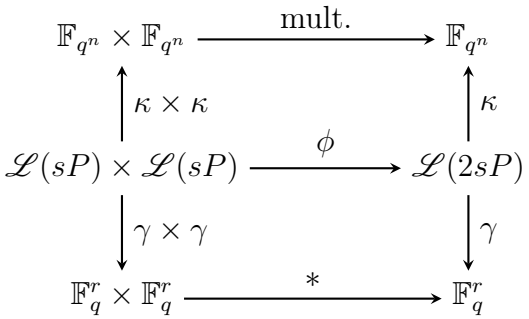

Figure 1: Commutative diagram for performing r pointwise multiplications (the Schur product) over $\mathbb{F}_q$ using one multiplication over $\mathbb{F}_{q^n}$. The map ϕ represents polynomial multiplication.

Proof of Theorem 1 . We consider two cases for the size q of the field: (1) q is an even power of a prime and $q \geqslant 49$, and (2) $q < 49$ or q is an odd power of a prime.

Case 1. Suppose $q \geqslant 49$ and q is an even power of a prime. In this case we choose $c_q^* = 1$. Let $K/\mathbb{F}_q$ be an algebraic function field of genus g. Let $n > 2\log_q g + 6$, let $s = \lfloor (n-1)/2 \rfloor$, and let P be a prime divisor of degree one of $K/\mathbb{F}_q$. By Imported Lemma 8 there exists a prime divisor Q of degree n. Consider the Riemann-Roch space

$$\mathscr{L}(2sP) = \{z \in K/\mathbb{F}_q \mid (z) + 2sP \geqslant 0\},$$

and the valuation ring of Q

$$\mathcal{O}_Q = \{z \in K/\mathbb{F}_q \mid v_Q(z) \geqslant 0\}.$$

The vector space $\mathscr{L}(2sP)$ is contained in $\mathcal{O}_Q$, which yields that the map $\kappa : \mathscr{L}(2sP) \to \mathbb{F}_{q^n}$ defined as $z \mapsto z(Q)$ is a ring homomorphism. The kernel of κ is $\mathscr{L}(2sP - Q)$, which has dimension 0 by Imported Lemma 6 since $\deg(2sP - Q) = 2s - n < 0$. This implies that κ is injective. Since $\mathscr{L}(sP) \subseteq \mathscr{L}(2sP)$, the restriction of the evaluation map $\kappa|_{\mathscr{L}(sP)}$ is a homomorphism from $\mathscr{L}(sP)$ to $\mathbb{F}_{q^n}$ and is injective.

Let $r > s$ and let $P_1, P_2, \ldots, P_r$ be distinct prime divisors of degree one other than P. Consider the evaluation map $\gamma : \mathscr{L}(sP) \to \mathbb{F}_q^r$ defined by

$$x \mapsto (x(P_1), x(P_2), \ldots, x(P_r)) .$$

Since $\deg(sP - \sum P_i) = s - r < 0$, the kernel of this mapping $\mathscr{L}(sP - \sum P_i)$ has dimension 0. Note that γ is a linear map, therefore by the rank-nullity theorem we have $\dim(ker(\gamma)) + \dim(\mathrm{Im}(\gamma)) = \dim(\mathscr{L}(sP))$. So $\dim(\mathrm{Im}(\gamma)) = \dim(\mathscr{L}(sP)) = s - g + 1$. Let $m = s - g + 1$ and $V = \mathrm{Im}(\gamma)$. Then V is a vector subspace of $\mathbb{F}_q^r$ of dimension m. By Lemma 1, there exists a bijection $\psi : V \to \mathbb{F}_q^m$ such that it preserves the point-wise product operation; that is, $\psi(x) * \psi(y) = \psi(x * y)$ for every $x, y \in V$.

We define $E : \mathbb{F}_q^m \to \mathbb{K}$ such that $E = \kappa \circ \gamma^{-1} \circ \psi^{-1}$, and $D : \mathrm{Im}(E) \cdot \mathrm{Im}(E) \to \mathbb{F}_q^m$ such that $D = \psi \circ \gamma \circ \kappa^{-1}$, where $\mathbb{K} = \mathbb{F}_{q^n}$. Note that $\mathrm{Im}(E) \cdot \mathrm{Im}(E) \subseteq \mathbb{K}$.

Claim 1. *The maps E and D are well-defined.*

Proof. The definitions of E and D have inversion of functions and the fact is that not all functions have inverse functions. So we need to prove that we can always do the inversions γ^{-1}, ψ^{-1}, and κ^{-1}. Since ψ is a bijection from from V to $\mathbb{F}_q^m$ and γ is also a bijection from $\mathscr{L}(sP)$ to V, the mapping E is well-defined. To show that D is well-defined, we need to show that for every $y \in \mathrm{Im}(E) \cdot \mathrm{Im}(E)$, there exists a unique $x \in \mathscr{L}(2sP)$ such that $y = \kappa(x)$. Because $y \in \mathrm{Im}(E) \cdot \mathrm{Im}(E)$, it must be the case that $y = u \cdot v$ for some $u, v \in \mathrm{Im}(E)$. Note κ is a bijection from $\mathscr{L}(sP)$ to $\mathrm{Im}(\kappa) = \mathrm{Im}(E)$, so we can define $x = \kappa^{-1}(u) \cdot \kappa^{-1}(v)$. Then $\kappa(x) = \kappa(\kappa^{-1}(u) \cdot \kappa^{-1}(v)) = \kappa(\kappa^{-1}(u \cdot v)) = u \cdot v = y$ and $x \in \mathscr{L}(sP) \cdot \mathscr{L}(sP)$. Since $\mathscr{L}(sP) \cdot \mathscr{L}(sP) \subseteq \mathscr{L}(2sP)$, we have $x \in \mathscr{L}(2sP)$. The uniqueness of x follows from the fact that κ is injective. □

Claim 2. *E and D are linear maps.*

This follows directly from the fact that ψ, κ, and γ are all linear maps. Next we will show that $D\big(E(\mathbf{a}) \cdot E(\mathbf{b})\big) = \mathbf{a} * \mathbf{b}$ for every $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^m$. Let $x, y \in \mathscr{L}(sP)$ such that $\mathbf{a} = \psi(x(P_1), x(P_2), \ldots, x(P_r)) = \psi(\gamma(x))$ and $\mathbf{b} = \psi(y(P_1), y(P_2), \ldots, y(P_r)) = \psi(\gamma(y))$ (such x and y always exist by properties of ψ and γ). Note that

$$\begin{aligned}
\gamma(x \cdot y) &= ((x \cdot y)(P_1), \ldots, (x \cdot y)(P_r)) \\
&= (x(P_1) \cdot y(P_1), \ldots, x(P_r) \cdot y(P_r)) \\
&= (x(P_1), \ldots, x(P_r)) * (y(P_1), \ldots, y(P_r)) \\
&= \gamma(x) * \gamma(y).
\end{aligned}$$

Therefore, we have

$$\begin{aligned}
D(E(\mathbf{a}) \cdot E(\mathbf{b})) &= D(\kappa(x) \cdot \kappa(y)) = D(\kappa(x \cdot y)) \\
&= \psi(\gamma(x \cdot y)) = \psi(\gamma(x) * \gamma(y)) \\
&= \psi(\gamma(x)) * \psi(\gamma(y)) = \mathbf{a} * \mathbf{b}.
\end{aligned}$$

Finally, since $s = \lfloor (n-1)/2 \rfloor$ and $g = \Theta(n)$, where the constant depends on $|\mathbb{F}_q|$, we have that $m = s - g + 1 = \Theta(n)$. This completes the proof of Case 1.

Case 2. Suppose $q < 49$ is a power of prime or q is an odd power of a prime. Then it suffices to choose $c_q^* = 6$ by the following observations.

1. If $q < 49$ and a power of a prime, then $q^6 \geqslant 49$.
2. If q is an odd power of a prime, then q^6 is an even power of a prime.

Figure 2 presents a more careful choice of c_q^*.

q													
	$q < 49$											$q \geqslant 49$	
	2	4	8	16	32	3	9	27	5	25	$q \geqslant 7$	$q = p^{2a+1}$	$q = p^{2a}$
c_q^*	6	3	2	2	2	4	2	2	4	2	2	2	1

Figure 2: Table for our choices of c_q^* for Theorem 1. The value of c_q^* is chosen minimally such that $q^{c_q^*}$ is an even power of a prime and $q^{c_q^*} \geqslant 49$.

Let $q^* := q^{c_q^*}$. Suppose n is sufficiently large, n is divisible by c_q^*, and $n/c_q^* > 2\log_{q^*} g + 6$. Now q^* is an even power of a prime and $q^* \geqslant 49$, so we are in Case 1 with the following parameters. Let $n^* := n/c^*$, let $K/\mathbb{F}_{q^*}$ be an algebraic function field of genus g, and let Q be a prime divisor of degree n^*. Divisor Q exists since $n^* > 2\log_{q^*} g + 6$. Let $s = \lfloor (n^* - 1)/2 \rfloor$ and set $m = s - g + 1$.

Notice for every $x \in \mathbb{F}_q$, it holds that $x \in \mathbb{F}_{q^*}$ since $\mathbb{F}_q$ is a subfield of $\mathbb{F}_{q^*}$. Now consider any $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^m$. Again we have $\mathbf{a}, \mathbf{b} \in \mathbb{F}_{q^*}^m$. We define the maps of case 1 with respect to q^* and n^*. In particular, we apply the algorithm from case 1 with appropriate changes to q and n. Concretely, let $\kappa \colon \mathscr{L}(2sP) \to \mathbb{F}_{(q^*)^{n^*}}$, let $\gamma \colon \mathscr{L}(sP) \to \mathbb{F}_{q^*}^r$, and let $V = \mathrm{Im}(\gamma)$. Let $\psi \colon V \to \mathbb{F}_{q^*}^m$ be a bijection defined by Lemma 1. Let $E = \kappa \circ \gamma^{-1} \circ \psi^{-1}$ and $D = \psi \circ \gamma \circ \kappa^{-1}$. Then we have

$$D(E(\mathbf{a}) \cdot E(\mathbf{b})) = \mathbf{a} * \mathbf{b}$$

as desired.

Finally, we have $s = \lfloor (n^* - 1)/2 \rfloor = \lfloor (n/c_q^* - 1)/2 \rfloor = \Theta(n)$ and $g = \Theta(n^*) = \Theta(n)$. Therefore $m = s - g + 1 = \Theta(n)$. This completes the proof of case 2. □

Remark. We note that the linear map D is defined on the set $\mathrm{Im}(E) \cdot \mathrm{Im}(E) = \{x \cdot y : x, y \in \mathrm{Im}(E)\}$. In particular, for our application we never evaluate D on input $x \notin \mathrm{Im}(E) \cdot \mathrm{Im}(E)$. When given such an input x, D can simply output 0, or any special symbol, say $\perp$.

2.3 Function Field Instantiation using Garcia-Stichtenoth Curves

For our embedding, we use appropriate Garcia-Stichtenoth curves to ensure there are enough places of degree one (rational places) and that there exists a prime divisor of degree n. Formally, we use Imported Theorem 6 and the following theorem.

Imported Theorem 7 (Garcia-Stichtenoth [GS96])**.** *For every q that is an even power of a prime and $q \geqslant 49$, there exists an infinite family of curves $\{C_u\}_{u\in\mathbb{N}}$ such that:*

1. *The number of rational places $\#C_u(\mathbb{F}_q) \geqslant q^{u/2}(\sqrt{q}-1)$, and*
2. *The genus of the curve $g(C_u) \leqslant q^{u/2}$.*

For Theorem 1, we want the following conditions to be satisfied.

1. The number of distinct degree one places is at least $r+1$
2. There exists a prime divisor of degree n.

Let $q \geqslant 49$ be an even power of a prime. Then for any $u \in \mathbb{N}$, we choose $n = q^{u/2}(\sqrt{q}-1) \in \mathbb{N}$ and consider the function field given by the curve C_u. By Imported Theorem 7, we have that the number of rational points $\#C_u(\mathbb{F}_q) \geqslant q^{u/2}(\sqrt{q}-1) = n$ and $g(C_u) \leqslant q^{u/2} = \frac{n}{\sqrt{q}-1}$. In particular, for $s = \left\lfloor \frac{n-1}{2} \right\rfloor$, we have $s < n$ and we can always choose r such that $s < r \leqslant n$. Setting $r = n-1$, we have that the map γ in the proof of Theorem 1 defines a suitable Goppa code [Gop81] over $\mathbb{F}_q$. With $r = n-1$, we in fact have that there are at least $r+1$ distinct prime divisors of degree one. Furthermore, since $g \leqslant \frac{n}{\sqrt{q}-1}$ we have

$$2\log_q g + 6 \leqslant 2\log_q\left(\frac{n}{\sqrt{q}-1}\right) + 6 < n.$$

So there exists a prime divisor of degree n by Imported Lemma 8. Finally we have

$$m = s - g + 1 \geqslant \left\lfloor \frac{n-1}{2} \right\rfloor - 2\log_q\left(\frac{n}{\sqrt{q}-1}\right) + 6 = \Theta(n).$$

Note that $g \geqslant 0$, so we also have $m \leqslant \left\lfloor \frac{n-1}{2} \right\rfloor + 6 = \Theta(n)$.

3 Realizing $\mathsf{OLE}(\mathbb{F})^m$ using one $\mathsf{ROLE}(\mathbb{K})$

In this section, we show how to securely realize m independent copies of $\mathsf{OLE}(\mathbb{F})$ using one sample of $\mathsf{ROLE}(\mathbb{K})$, for field $\mathbb{F} = \mathbb{F}_q$ and $\mathbb{K}$ a degree n extension field of $\mathbb{F}$. Intuitively, the $\mathsf{ROLE}(\mathbb{K})$ functionality is an inputless functionality that samples A, B, X uniformly and independently at random from $\mathbb{K}$, and output (A, B) to one party and (X, Z) to the other party. This secure realization is achieved by composing two steps. First, we securely realize one $\mathsf{OLE}(\mathbb{K})$ from one $\mathsf{ROLE}(\mathbb{K})$ using a standard protocol (cf. the randomized self-reducibility of the OLE functionality [WW06]). Then, we embed m copies of $\mathsf{OLE}(\mathbb{F})$ into one $\mathsf{OLE}(\mathbb{K})$. Formally, we have the following theorem.

Theorem 5 (Realizing multiple small OLE using one large ROLE)**.** *Let $\mathbb{F}$ be a field of size q, a power of a prime. Let $\mathbb{K}$ be a degree n extension field of $\mathbb{F}$. There exists a perfectly secure protocol for $\mathsf{OLE}(\mathbb{F})^m$ in the $\mathsf{ROLE}(\mathbb{K})$-hybrid that performs only one call to the $\mathsf{ROLE}(\mathbb{K})$ functionality and $m = \Theta(n)$.*

3.1 Preliminaries

We introduce the functionalities we are interested in.

Oblivious Linear-function Evaluation. For a field $(\mathbb{F}, +, \cdot)$, oblivious linear-function evaluation over $\mathbb{F}$, represented by $\mathsf{OLE}(\mathbb{F})$, is a two-party functionality that takes as input $(a, b) \in \mathbb{F}^2$ from Alice and $x \in \mathbb{F}$ from Bob and outputs $z = ax + b$ to Bob. In particular, OLE refers to the $\mathsf{OLE}(\mathbb{GF}[2])$ functionality.

Random Oblivious Linear-function Evaluation. For a field $(\mathbb{F}, +, \cdot)$, random oblivious linear-function evaluation over $\mathbb{F}$, represented by $\mathsf{ROLE}(\mathbb{F})$, is a correlation that samples $a, b, x \in \mathbb{F}$ uniformly and independently at random. It provides Alice the secret share $r_A = (a, b)$ and provides Bob the secret share $r_B = (x, z)$, where $z = ax + b$. In particular, ROLE refers to the $\mathsf{ROLE}(\mathbb{GF}[2])$ correlation.

3.2 Securely realizing $\mathsf{OLE}(\mathbb{K})$ using one $\mathsf{ROLE}(\mathbb{K})$

The protocol presented in Figure 3 is the standard protocol that implements the $\mathsf{OLE}(\mathbb{K})$ functionality in the $\mathsf{ROLE}(\mathbb{K})$-hybrid with perfect semi-honest security.

Pseudocode of the OLE protocol $\rho(\mathbb{K}, A^*, B^*, X^*)$

Given. Alice has $(\widetilde{A}_0, \widetilde{B}_0)$ and Bob has $(\widetilde{X}_0, \widetilde{Z}_0)$, where $\widetilde{A}_0, \widetilde{B}_0, \widetilde{X}_0$ are random elements in $\mathbb{K}$ and $\widetilde{Z}_0 = \widetilde{A}_0\widetilde{X}_0 + \widetilde{B}_0$.

Private Inputs. Alice has private input $(A^*, B^*) \in \mathbb{K}^2$ and Bob has $X^* \in \mathbb{K}$.

Hybrid. Parties are in $\mathsf{ROLE}(\mathbb{K})$-hybrid.

Interactive Protocol.

1. **First Round.** Bob sends $M = \widetilde{X}_0 - X^*$ to Alice.
2. **Second Round.** Alice sends $\alpha = \widetilde{A}_0 + A^*$ and $\beta = \widetilde{A}_0 M + B^* + \widetilde{B}_0$.

Output Computation. Bob outputs $Z^* = \alpha X^* + \beta - \widetilde{Z}_0$.

Figure 3: Perfectly secure protocol realizing $\mathsf{OLE}(\mathbb{K})$ in the $\mathsf{ROLE}(\mathbb{K})$ correlation hybrid.

3.3 Securely realizing $\mathsf{OLE}(\mathbb{F})^m$ from $\mathsf{OLE}(\mathbb{K})$

This section presents the realization of Corollary 2. Our goal is to embed m independent copies of $\mathsf{OLE}(\mathbb{F})$ into one $\mathsf{OLE}(\mathbb{K})$, where $m = \Theta(n)$. More concretely, suppose we are given an oracle that takes as input $A^*, B^* \in \mathbb{K}$ from Alice and $X^* \in \mathbb{K}$ from Bob, and outputs $Z^* = A^* \cdot X^* + B^*$ to Bob. Our aim is to implement the following functionality. Alice has inputs $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{F}_q^m$ and $\mathbf{b} = (b_1, \ldots, b_m) \in \mathbb{F}_q^m$, and Bob has input $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{F}_q^m$. We want Bob to obtain $\mathbf{z} = (z_1, \ldots, z_m)$, where $\mathbf{z} = \mathbf{a} * \mathbf{x} + \mathbf{b}$,

in other words, $z_i = a_i \cdot x_i + b_i$ for every $i \in [m]$. We show that the protocol presented in Figure 4 achieves $m = \Theta(n)$.

Given. Two linear maps E and D as in Theorem 1.

Private input. Alice has private inputs $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{F}_q^m$ and $\mathbf{b} = (b_1, \ldots, b_m) \in \mathbb{F}_q^m$. Bob has private input $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{F}_q^m$.

Hybrid. Parties are in the $\mathsf{OLE}(\mathbb{K})$-hybrid.

Private Input Construction.

1. Alice creates private inputs $A^* = E(\mathbf{a})$ and $B^* = E(\mathbf{b})$.
2. Bob creates private input $X^* = E(\mathbf{x})$.
3. Both parties invoke the $\mathsf{OLE}(\mathbb{K})$ functionality with respective Alice input (A^*, B^*) and Bob input X^*. Bob receives $Z^* = A^*X^* + B^* = E(\mathbf{a}) \cdot E(\mathbf{x}) + E(\mathbf{b})$.

Output Decoding. Bob outputs $\mathbf{z} = D(Z^*) = D(E(\mathbf{a}) \cdot E(\mathbf{x}) + E(\mathbf{b})) = \mathbf{a} * \mathbf{x} + \mathbf{b}$.

Figure 4: Protocol for embedding m copies of $\mathsf{OLE}(\mathbb{F})$ into one $\mathsf{OLE}(\mathbb{K})$, where $\mathbb{K}$ is a degree n extension field of $\mathbb{F}$.

Figure 4 is the protocol which realizes Corollary 2. We argue the correctness of the protocol. In the protocol, Alice creates $A^* = E(\mathbf{a})$ and $B^* = E(\mathbf{b})$, and Bob creates $X^* = E(\mathbf{x})$. Calling the $\mathsf{OLE}(\mathbb{K})$ functionality, Bob receives $Z^* = A^* \cdot X^* + B^*$. In particular, Bob receives $Z^* = E(\mathbf{a}) \cdot E(\mathbf{x}) + E(\mathbf{b})$. Then Bob computes $D(Z^*)$. Since D is a linear map and by Theorem 1, we have $m = \Theta(n)$ and the following.

$$\begin{aligned} D(Z^*) &= D\left(E(\mathbf{a}) \cdot E(\mathbf{x}) + E(\mathbf{b})\right) \\ &= D\left(E(\mathbf{a}) \cdot E(\mathbf{x})\right) + D(E(\mathbf{b})) \\ &= \mathbf{a} * \mathbf{x} + \mathbf{b} \end{aligned}$$

3.4 Realization of $\mathsf{OLE}(\mathbb{F})^m$ in the $\mathsf{ROLE}(\mathbb{K})$-hybrid

The protocol which realizes Theorem 5 is the parallel composition of the protocols presented in Figure 3 and Figure 4 (Corollary 2). The composition of these protocols in parallel gives an optimal two-round protocol for realizing $\mathsf{OLE}(\mathbb{F})^m$ in the $\mathsf{ROLE}(\mathbb{K})$-hybrid with perfect security and $m = \Theta(n)$ by Theorem 1, as desired.

4 Linear Production Correlation Extractors in the High Resilience Setting

This section provides the necessary background of correlation extractors and proves Corollary 4. In particular, Corollary 4 is achieved by the construction of a suitable correlation extractor. A *correlation extractor*, or *correlation* in short, is a joint distribution (R_A, R_B) which samples shares (r_A, r_B) according to the distribution and sends secret share r_A to Alice and r_B to Bob. Correlations are given to parties in an offline preprocessing phase. Parties then use their respective secret shares in an online phase in an interactive protocol to securely compute an intended functionality. Correlation extractors take *leaky* shares of correlations and distill them into *fresh* randomness to be used to securely compute the intended functionality. Formally, we define a correlation extractor below.

Definition 16 (Correlation Extractor)**.** *Let (R_A, R_B) be a correlated private randomness such that the secret share size of each party is n'-bits. An (n', m, t, ε)-*correlation extractor for (R_A, R_B) *is a two-party interactive protocol in the $(R_A, R_B)^{[t]}$ hybrid that securely implements the OT^m functionality against information-theoretic semi-honest adversaries with ε-simulation error.*

Using this definition we restate Corollary 4 as follows.

Theorem 6 (Half Resilience, Linear Production Correlation Extractor)**.** *For all constants $0 < \delta < g \leqslant 1/2$, there exists a correlation (R_A, R_B), where each party gets n-bit secret shares, such that there exists a two-round (n', m, t, ε)-correlation extractor for (R_A, R_B), where $m = \Theta(n')$, $t = (1/2 - g)n'$, and $\varepsilon = 2^{-(g-\delta)n'/2}$.*

The construction of this correlation extractor achieves linear production $m = \Theta(n)$ and $1/2$ leakage resilience by composing our embedding (Theorem 1, Corollary 2) with the correlation extractor of Block, Maji, and Nguyen [BMN17]. Prior correlation extractors either achieved sub-linear production, (significantly) less than $1/2$ resilience, or were not round-optimal.

4.1 Preliminaries

We introduce some useful functionalities and correlations.

Oblivious Transfer. Oblivious transfer, represented by OT, is a two-party functionality that takes as input $(x_0, x_1) \in \{0,1\}^2$ from Alice and $b \in \{0,1\}$ from Bob and outputs x_b to Bob.

Random Oblivious Transfer Correlation. Random oblivious transfer, represented by ROT, is a correlation that samples x_0, x_1, b uniformly and independently at random. It provides Alice the secret share $r_A = (x_0, x_1)$ and provides Bob the secret share $r_B = (b, x_b)$.

Recall also the **Oblivious Linear-function Evaluation** and **Random Oblivious Linear-function Evaluation** functionalities from Section 3.1. We denote $\mathsf{ROLE}(\mathbb{GF}[2])$ by ROLE. Note that ROT and ROLE are identical (functionally equivalent) correlations.

Inner-product Correlation. For a field $(\mathbb{F}, +, \cdot)$ and $n' \in \mathbb{N}$, inner-product correlation over $\mathbb{F}$ of size n', represented by $\mathsf{IP}\left(\mathbb{F}^{n'}\right)$, is a correlation that samples random

$r_A = (x_0, \ldots, x_{n'-1}) \in \mathbb{F}^{n'}$ and $r_B = (y_0, \ldots, y_{n'-1}) \in \mathbb{F}^{n'}$ subject to the constraint that $x_0 + y_0 = \sum_{i=1}^{n'-1} x_i y_i$. The secret shares of Alice and Bob are, respectively, r_A and r_B.

Toeplitz Matrix Distribution. Given a field $\mathbb{F}$, the distribution $\mathbb{T}_{(k,n')}$ represents a uniform distribution over all matrices of the form $[I_{k\times k} \| P_{k\times n'-k}]$, where $I_{k\times k}$ is the identity matrix and $P_{k\times n'-k}$ is a Toeplitz matrix with each entry in $\mathbb{F}$. $\mathbb{T}_{\perp,(k,n')}$ is the uniform distribution over all matrices of the form $[P_{n'-k\times k} \| I_{n'-k\times n'-k}]$, where $I_{'n-k\times n'-k}$ is the identity matrix and $P_{n'-k\times k}$ is a Toeplitz matrix with each entry in $\mathbb{F}$.

For $m \in \mathbb{N}$, the functionality $\mathcal{F}^m$ represents the functionality that implements m independent copies of any functionality/correlation $\mathcal{F}$.

The following unpredictability lemma is needed to prove security of the correlation extractor of Theorem 6.

Imported Lemma 9 (Unpredictability Lemma [BMN17]). *Let $\mathcal{G} \in \left\{\mathbb{T}_{(k,\eta+1)}, \mathbb{T}_{\perp,(k,\eta+1)}\right\}$. Consider the following game between an honest challenger and an adversary:*

1. *$\mathcal{H}$ samples $m_{[\eta]} \sim U_{\mathbb{K}^\eta}$.*
2. *$\mathcal{A}$ sends a leakage function $\mathcal{L}\colon \mathbb{K}^\eta \to \{0,1\}^t$.*
3. *$\mathcal{H}$ sends $\mathcal{L}\left(m_{[\eta]}\right)$ to $\mathcal{A}$.*
4. *$\mathcal{H}$ samples $x_{[k]} \sim U_{\mathbb{K}^k}$, $G \sim \mathcal{G}$, and computes $y_{\{0\}\cup[n]} = x \cdot G + (0, m_{[\eta]})$. $\mathcal{H}$ sends $(y_{[\eta]}, G)$ to $\mathcal{A}$. $\mathcal{H}$ picks $b \xleftarrow{\$} \{0,1\}$. If $b = 0$, then she sends $\mathsf{chal} = y_0$ to $\mathcal{A}$; otherwise (if $b = 1$) then she sends $\mathsf{chal} = u \sim U_{\mathbb{K}}$ to $\mathcal{A}$.*
5. *$\mathcal{A}$ replies with an element $\tilde{b} \in \{0,1\}$.*

The adversary $\mathcal{A}$ wins the game if $b = \tilde{b}$. For any $\mathcal{A}$, the advantage of the adversary is $\leqslant \frac{1}{2}\sqrt{\frac{|\mathbb{K}|2^t}{|\mathbb{K}|^k}}$.

4.2 Extracting one ROLE from a Leaky Inner Product Correlation

Conceptually, Theorem 6 follows from the construction of two protocols. In this section, we describe the first protocol. Informally, this protocol takes leaky shares of the inner-product correlation over $\mathbb{K}$, the protocol securely extracts one random sample of $\mathsf{ROLE}(\mathbb{K})$. For completeness we restate the protocol from [BMN17] in Figure 5.

As noted in [BMN17], the security of Figure 5 follows from Imported Lemma 9 over fields. For full details, see Appendix A of [BMN17]. In particular, the protocol of Figure 5 is resilient to $t = (1/2 - g)n'$ bits of leakage, for any $g \in (0, 1/2]$. Here, $\mathbb{K}$ is a degree n extension of some suitably chosen base field $\mathbb{F}$ of size q, and η is an appropriately chosen constant.

4.3 Extracting m copies of OLE $(\mathbb{F})$ from one ROLE $(\mathbb{K})$

This section presents the second protocol required to construct Theorem 6. Previously, [BMN17] presented a construction which embedded m copies of $\mathsf{OLE}(\mathbb{F})$ into a single $\mathsf{OLE}(\mathbb{K})$,

Pseudocode of the extraction protocol $\pi(\mathbb{K}, \eta)$.

Given. Alice has $(X_0, X_1, \ldots, X_\eta)$ and Bob has $(Y_0, Y_1, \ldots, Y_\eta)$ such that $X_0 + Y_0 = \sum_{i=1}^{\eta} X_i Y_i$, where $X_0, \ldots, X_\eta, Y_0, \ldots, Y_\eta \in \mathbb{K}$. For ease of presentation assume that η is odd and set $w = (\eta+1)/2$. An adversarial party can obtain arbitrary t-bit leakage on the share of the other party.

Interactive Protocol.

1. **First Round.** Bob sample a random generator matrix G from the distribution $\mathbb{T}_{w\times(\eta+1)}$ such that its elements are in $\mathbb{K}$. Let $\mathcal{C}$ be the code generated by G, and $\mathcal{C}^\perp$ be its dual code. Let H be the generator matrix for the code $\mathcal{C}^\perp$. If the first column of H is $0^{\eta+1-w}$ (i.e., all zeros), then abort the protocol. Bob picks a random codeword $(\widetilde{X}_0, \widetilde{X}_1, \ldots, \widetilde{X}_\eta) \in \mathcal{C}^\perp$ and calculates $M_{[\eta]} = Y_{[\eta]} - \widetilde{X}_{[\eta]}$.

   Bob sends $M_{[\eta]}$ and G to Alice.

2. **Second Round.** Alice samples a random codeword $(\widetilde{A}_0, \widetilde{A}_1, \ldots, \widetilde{A}_\eta) \in \mathcal{C}$ and a random field element $\widetilde{B}_0 \in \mathbb{K}$. Alice computes $\alpha_{[\eta]} = X_{[\eta]} + \widetilde{A}_{[\eta]}$ and $\beta = \left\langle X_{[\eta]}, M_{[\eta]} \right\rangle - \widetilde{B}_0 - X_0$.

   Alice sends $\alpha_{[\eta]}$ and β to Bob.

Output Computation. Alice outputs $(\widetilde{A}_0, \widetilde{B}_0)$ and Bob outputs $(\widetilde{X}_0, \widetilde{Z}_0)$, where $\widetilde{Z}_0 = -\left\langle \alpha_{[\eta]}, \widetilde{X}_{[\eta]} \right\rangle - \beta + Y_0$.

Figure 5: Protocol to securely extract one random sample of the $\mathsf{ROLE}(\mathbb{K})$ functionality from the leaky $\mathsf{IP}(\mathbb{K}^{\eta+1})^{[t]}$ correlation.

with $m = n^{1-o(1)}$ and $\mathbb{K}$ a degree n extension field of $\mathbb{F}$. Here we present our $m = \Theta(n)$ solution.

This protocol is exactly the parallel composition of the protocols presented in Figure 3 and Figure 4; i.e., the result of Theorem 5. The result follows by choosing the appropriate settings. In particular, given q, η, and n', we set the degree of extension $n = \frac{n'}{(\eta+1)\lg q}$. So $m = \Theta(n) = \Theta(n')$.

4.4 Realizing Theorem 6

The realization of Theorem 6 is the parallel composition of the protocols of Figure 5, Figure 3, and Figure 4 with the following setting. We take $(R_A, R_B) = \mathsf{IP}\left(\mathbb{GF}\left[2^{\delta n'}\right]^{1/\delta}\right)$, where n' and δ are given, $\eta := \frac{1}{\delta} - 1$, and $n := \frac{n'}{(\eta+1)}$. Note n here corresponds to the n in Corollary 4.

The protocol of Figure 5 is a perfectly secure semi-honest protocol for extracting one $\mathsf{ROLE}\left(\mathbb{GF}\left[2^{\delta n'}\right]\right)$ in the $\left(\mathsf{IP}\left(\mathbb{GF}\left[2^{\delta n'}\right]^{1/\delta}\right)\right)^{[t]}$-hybrid which is resilient to $t = (1/2 - g)n'$ bits

of leakage, for all $0 < \delta < g \leqslant 1/2$. Then the parallel composition of protocols Figure 3 and Figure 4 is a perfectly secure semi-honest protocol for realizing m copies of $\mathsf{OLE}(\mathbb{GF}[2])$ in the $\mathsf{ROLE}\left(\mathbb{GF}\left[2^{\delta n'}\right]\right)$-hybrid, and $m = \Theta(n') = \Theta(n)$. This proves Theorem 6, and thus Corollary 4.

4.5 Comparison with Prior Works

Correlation extractors were introduced by Ishai, Kushilevitz, Ostrovsky, and Sahai [IKOS09] as a natural generalization of privacy amplification and randomness extraction. Since the initial feasibility result of [IKOS09], there have been significant qualitative and quantitative improvement in correlation extractor constructions. Figure 6 summarizes the current state-of-the-art of correlation extractors.

	Correlation Description	Message Complexity	Number of OTs Produced ($m/2$)	Number of Leakage bits (t)	Simulation Error (ε)
IKOS [IKOS09]	$\mathsf{ROT}^{n/2}$	4	$\Theta(n)$	$\Theta(n)$	$2^{-\Theta(n)}$
GIMS [GIMS15]	$\mathsf{ROT}^{n/2}$	2	$n/\operatorname{poly}\lg n$	$(1/4 - g)n$	$2^{-gn/m}$
	$\mathsf{IP}\left(\mathbb{K}^{n/\lg\lvert\mathbb{K}\rvert}\right)$	2	1	$(1/2 - g)n$	2^{-gn}
BMN [BMN17]	$\mathsf{IP}\left(\mathbb{K}^{n/\lg\lvert\mathbb{K}\rvert}\right)$	2	$n^{1-o(1)}$	$(1/2 - g)n$	2^{-gn}
BGMN [BGMN18]	$\mathsf{ROT}^{n/2}$	2	$\Theta(n)$	$\Theta(n)$	$2^{-\Theta(n)}$
	$\mathsf{ROLE}\left(\mathbb{F}\right)^{n/2\lg\lvert\mathbb{F}\rvert}$	2	$\Theta(n)$	$\Theta(n)$	$2^{-\Theta(n)}$
Our Results	$\mathsf{IP}\left(\mathbb{K}^{n/\lg\lvert\mathbb{K}\rvert}\right)$	2	$\Theta(n)$	$(1/2 - g)n$	2^{-gn}

Figure 6: A qualitative summary of prior relevant works in correlation extractors and a comparison to our correlation extractor construction. Here $\mathbb{K}$ is a finite field and $\mathbb{F}$ is a finite field of constant size. The $\mathsf{IP}(\mathbb{K}^s)$ is a correlation that samples random $r_A = (u_1, \ldots, u_s) \in \mathbb{K}^s$ and $r_B = (v_1, \ldots, v_s) \in \mathbb{K}^s$ such that $u_1 v_1 + \cdots + u_s v_s = 0$. All correlations have been normalized so that each party gets an n-bit secret share.

Prior to our work, the BGMN correlation extractors [BGMN18] achieve the best qualitative and quantitative parameters. For example, starting with $n/2$ independent samples of the ROT correlation, they construct the first round-optimal correlation extractor that produces $m = \Theta(n)$ secure ROT samples despite $t = (1/4 - \varepsilon)n$ bits of leakage, for any $\varepsilon > 0$. Note that any correlation extractor for $n/2$ ROT samples can have at most $t = n/4$ resilience [IMSW14].

Our correlation extractor is also round optimal. However, the BMN [BMN17] correlation extractor and our correlation extractor has resilience in the range $t \in [1/4, 1/2)$. Intuitively, our correlation extractor is ideal where high resilience is necessary. Our correlation extractor needs a large correlation, for example, the inner-product correlation over large fields. Contrast this with the case of BGMN extractor that uses multiple samples of the ROT correlation. To achieve $t = (1/2 - \varepsilon)n$ resilience, where $\varepsilon \in (0, 1/4]$, we use the inner-product correlation over fields of size (roughly) $2^{n\varepsilon}$. Using the multiplication embedding in Theorem 1, our work demonstrates the feasibility of extracting $m = \Theta(n\varepsilon)$ independent ROT samples when the fractional resilience is in the range $t/n \in [1/4, 1/2)$.

References

[ABBR15] Kevin Atighehchi, Stéphane Ballet, Alexis Bonnecaze, and Robert Rolland. On chudnovsky-based arithmetic algorithms in finite fields. *CoRR*, abs/1510.00090, 2015. 24

[ADI+17] Benny Applebaum, Ivan Damgård, Yuval Ishai, Michael Nielsen, and Lior Zichron. Secure arithmetic computation with constant computational overhead. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part I*, volume 10401 of *LNCS*, pages 223–254. Springer, Heidelberg, August 2017. 1

[BBBT17] Stéphane Ballet, Nicolas Baudru, Alexis Bonnecaze, and Mila Tukumuli. On the construction of the asymmetric chudnovsky multiplication algorithm in finite fields without derivated evaluation. *Comptes Rendus Mathematique*, 355(7):729 – 733, 2017. 24

[BBT13] Stéphane Ballet, Alexis Bonnecaze, and Mila Tukumuli. On the construction of elliptic chudnovsky-type algorithms for multiplication in large extensions of finite fields. March 2013. 24

[BCS97] Peter Bürgisser, Michael Clausen, and Mohammad Amin Shokrollahi. *Algebraic complexity theory*. Grundlehren der mathematischen Wissenschaften ; 315. Springer, Berlin ; New York, 1997. 8, 21

[BGMN18] Alexander R. Block, Divya Gupta, Hemanta K. Maji, and Hai H. Nguyen. Secure computation using leaky correlations (asymptotically optimal constructions). Cryptology ePrint Archive, Report 2018/372, 2018. https://eprint.iacr.org/2018/372. 18

[BMN17] Alexander R. Block, Hemanta K. Maji, and Hai H. Nguyen. Secure computation based on leaky correlations: High resilience setting. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part II*, volume 10402 of *LNCS*, pages 3–32. Springer, Heidelberg, August 2017. 1, 2, 3, 15, 16, 18

[BPR16] Stéphane Ballet, Julia Pieltant, and Matthieu Rambaud. On some bounds for symmetric tensor rank of multiplication in finite fields. *CoRR*, abs/1601.00126, 2016. 24

[BR04] S. Ballet and R. Rolland. Multiplication algorithm in a finite field and tensor rank of the multiplication. *Journal of Algebra*, 272(1):173 – 185, 2004. 24

[Cas10] Ignacio Cascudo. *On asymptotically good strongly multiplicative linear secret sharing*. PhD thesis, Tesis doctoral, Universidad de Oviedo, 2010. 4, 5, 6, 7, 8

[CC87] David V Chudnovsky and Gregory V Chudnovsky. Algebraic complexities and algebraic curves over finite fields. *Proceedings of the National Academy of Sciences*, 84(7):1739–1743, 1987. 3, 21, 24

[Cha12] Jean Chaumine. *Multiplication in small finite fields using elliptic curves*, pages 343–350. 2012. 24

[CÖ10] Murat Cenk and Ferruh Özbudak. On multiplication in finite fields. *Journal of Complexity*, 26(2):172–186, 2010. 24

[GIMS15] Divya Gupta, Yuval Ishai, Hemanta K. Maji, and Amit Sahai. Secure computation from leaky correlated randomness. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 701–720. Springer, Heidelberg, August 2015. 18

[Gop81] Valerii Denisovich Goppa. Codes on algebraic curves. In *Soviet Math. Dokl*, pages 170–172, 1981. 12

[GS95] Arnaldo Garcia and Henning Stichtenoth. A tower of artin-schreier extensions of function fields attaining the drinfeld-vladut bound. *Inventiones mathematicae*, 121(1):211–222, December 1995. 8, 24

[GS96] Arnaldo Garcia and Henning Stichtenoth. On the asymptotic behaviour of some towers of function fields over finite fields. *Journal of Number Theory*, 61(2):248–273, 1996. 12, 24

[IKOS09] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Extracting correlations. In *50th FOCS*, pages 261–270. IEEE Computer Society Press, October 2009. 3, 18

[IMSW14] Yuval Ishai, Hemanta K. Maji, Amit Sahai, and Jürg Wullschleger. Single-use ot combiners with near-optimal resilience. In *2014 IEEE International Symposium on Information Theory, Honolulu, HI, USA, June 29 - July 4, 2014*, pages 1544–1548. IEEE, 2014. 18

[Ran12] Hugues Randriambololona. Bilinear complexity of algebras and the chudnovsky–chudnovsky interpolation method. *Journal of Complexity*, 28(4):489–517, 2012. 24

[Sti09] Henning Stichtenoth. *Algebraic Function Fields and Codes*. Graduate Texts in Mathematics, 254. 2nd ed.. edition, 2009. 4, 5, 8

[STV92] Ie Shparlinski, MA Tsfasman, and SG Vladut. Curves with many points and multiplication in finite-fields. *Lecture Notes In Mathematics*, 1518:145–169, 1992. 24

[WW06] Stefan Wolf and Jürg Wullschleger. Oblivious transfer is symmetric. In Serge Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 222–232. Springer, Heidelberg, May / June 2006. 12

A Chudnovsky-Chudnovsky Bilinear Multiplication

We discuss the reverse problems of Theorem 1 and Theorem 5. We assume familiarity with Section 2. First we consider the problem of computing one large field multiplications using many small field multiplications. This is given by the following theorem.

Theorem 7 (Field Extension Multiplication via Pointwise Base Field Multiplication)**.** *Let $\mathbb{F}$ be a finite field of size q, a power of a prime. For sufficiently large n, there exists a constant $c' > 0$ and (linear) maps $E' \colon \mathbb{K} \to \mathbb{F}^m$ and $D' \colon \mathbb{F}^m \to \mathbb{K}$, where $\mathbb{K}$ is the degree-n extension of the field $\mathbb{F}$, such that the following constraints are satisfied.*

1. *We have $m \geqslant c'n$, and*
2. *For all $A, B \in \mathbb{K}$, the following identity holds*

$$D'\left(E'(A) * E'(B)\right) = A \cdot B$$

where "$*$" is pointwise multiplication over $\mathbb{F}^m$.

Note that since the maps E' and D' are linear, the following holds.

Corollary 8. *For all $A, B, C \in \mathbb{K}$, we have*

$$D'\big(E'(A) * E'(B) + E'(C)\big) = D'\big(E'(A) * E'(B)\big) + D'\big(E'(C)\big).$$

Theorem 7 follows from the results of Chudnovsky-Chudnovsk [CC87]. In particular, they show that the rank of bilinear multiplication is $\Theta(n)$.

Imported Theorem 8 (Chudnovsky and Chudnovsky [BCS97, Theorem 18.20])**.** *For every power of a prime q there exists a constant c_q such that $R(\mathbb{F}_{q^n}/\mathbb{F}_q) \leqslant c_q n$, where R is the rank of the $\mathbb{F}_q$-bilinear map that is multiplication over $\mathbb{F}_{q^n}$.*

The theorem states that if $\mathbb{K}$ is a degree n extension of $\mathbb{F}_q$, then the bilinear complexity of multiplication over $\mathbb{K}$ is $\Theta(n)$. This result is due to the Chudnovsky-Chudnovsky interpolation algorithm and the result of Garcia and Stichtenoth found in Imported Theorem 7.

Imported Lemma 10 (Chudnovsky-Chudnovsky Interpolation Algorithm [BCS97, Proposition 18.22])**.** *Let $K/\mathbb{F}_q$ be an algebraic function field of one variable of genus g, $n \geqslant 2\log_q g + 6$, and assume that there exist at least $4g + 2n$ prime divisors of degree one of $K/\mathbb{F}_q$. Then we have $R(\mathbb{F}_{q^n}/\mathbb{F}_q) \leqslant 3g + 2n - 1$.*

This lemma gives rise to the commutative diagram of Figure 7 which defines the interpolation method. This interpolation method implements multiplication over $\mathbb{F}_{q^n}$ using r' pointwise multiplications over $\mathbb{F}_q^{r'}$. This gives that $r' = 3g + 2n - 1 = \Theta(n)$. Setting $m = r'$ and setting E' and D' according to the interpolation algorithm directly yields Theorem 7. Concretely, we have the maps E' and D' defined as follows.

$$E' := \kappa' \circ (\gamma')^{-1} \qquad\qquad D' := \gamma' \circ (\kappa')^{-1}$$

Note both κ' and γ' are linear maps, so E' and D' are also linear maps.

Given E' and D' of Theorem 7, we compute the reverse problem of Theorem 5. That is, we can use multiple small ROLE to realize one large OLE.

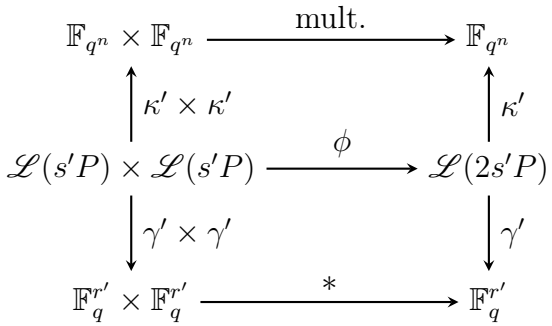

Figure 7: Chudnovsky-Chudnovsky interpolation algorithm for performing multiplication over $\mathbb{F}_{q^n}$ using r' pointwise multiplications over $\mathbb{F}_q^{r'}$, where $r' = \Theta(n)$ and $s' = n + 2g - 1$.

Theorem 9 (Realizing one large OLE using multiple small ROLE)**.** *Let $\mathbb{F}$ be a field of size q, a power of a prime. Let $\mathbb{K}$ be a degree n extension field of $\mathbb{F}$. There exists a perfectly secure protocol for $\mathsf{OLE}(\mathbb{K})$ in the $\mathsf{ROLE}(\mathbb{F})^m$-hybrid that performs only one call to the $\mathsf{ROLE}(\mathbb{F})^m$ functionality and $m = \Theta(n)$.*

To realize Theorem 9, we compose two steps in parallel. First we securely realize $\mathsf{OLE}(\mathbb{F})^m$ from $\mathsf{ROLE}(\mathbb{F})^m$ using a standard protocol. Then we use m copies of $\mathsf{OLE}(\mathbb{F})$ to implement a single $\mathsf{OLE}(\mathbb{K})$.

A.1 Securely realizing $\mathsf{OLE}(\mathbb{F})^m$ using $\mathsf{ROLE}(\mathbb{F})^m$

The protocol presented in Figure 8 is an extension of the standard protocol that implements the $\mathsf{OLE}(\mathbb{F})$ functionality in the $\mathsf{ROLE}(\mathbb{F})$-hybrid with perfect semi-honest security. In particular, it is the m parallel composition of the $\mathsf{OLE}(\mathbb{F})$ functionality in the $\mathsf{ROLE}(\mathbb{F})$-hybrid.

Pseudocode of the $\mathsf{OLE}(\mathbb{F})^m$ protocol

Given. Alice has $(\mathbf{a}', \mathbf{b}')$ and Bob has $(\mathbf{x}', \mathbf{z}')$, where $\mathbf{a}', \mathbf{b}', \mathbf{x}'$ are random elements in $\mathbb{F}^m$ and $\mathbf{z}' = \mathbf{a}' * \mathbf{x}' + \mathbf{b}'$.

Private Inputs. Alice has private input $(\mathbf{a}^*, \mathbf{b}^*) \in \mathbb{F}^{2m}$ and Bob has $\mathbf{x}^* \in \mathbb{F}^m$.

Hybrid. Parties are in $\mathsf{ROLE}(\mathbb{F})^m$-hybrid.

Interactive Protocol.

1. **First Round.** Bob sends $\mathbf{m} = \mathbf{x}' - \mathbf{x}^*$ to Alice.
2. **Second Round.** Alice sends $\boldsymbol{\alpha} = \mathbf{a}' + \mathbf{a}^*$ and $\boldsymbol{\beta} = \mathbf{a}' * \mathbf{m} + \mathbf{b}^* + \mathbf{b}'$.

Output Computation. Bob outputs $\mathbf{z}^* = \boldsymbol{\alpha} * \mathbf{x}^* + \boldsymbol{\beta} - \mathbf{z}'$.

Figure 8: Perfectly secure protocol realizing $\mathsf{OLE}(\mathbb{F})^m$ in the $\mathsf{ROLE}(\mathbb{F})^m$ correlation hybrid.

A.2 Securely realizing $\mathsf{OLE}(\mathbb{K})$ from $\mathsf{OLE}(\mathbb{F})^m$

The goal is to use m copies of $\mathsf{OLE}(\mathbb{F})$ to compute one $\mathsf{OLE}(\mathbb{K})$, where $m = \Theta(n)$. Concretely, suppose we are given an oracle which takes as input $\mathbf{a}, \mathbf{b} \in \mathbb{F}^m$ from Alice and $\mathbf{x} \in \mathbb{F}^m$ from Bob, and outputs $\mathbf{z} = \mathbf{a} * \mathbf{x} + \mathbf{b}$ to Bob. Our aim is to implement the following functionality. Alice has private inputs $A \in \mathbb{K}$ and $B \in \mathbb{K}$, and Bob has input $X \in \mathbb{K}$. We want Bob to obtain $Z = AX + B \in \mathbb{K}$. We show that if Alice and Bob use the protocol presented in Figure 9, we can achieve $m = \Theta(n)$. More formally, we have the following lemma.

Lemma 2 (Performing one large OLE using multiple small OLE)**.** *Let $\mathbb{K}$ be an extension field of $\mathbb{F}$ of degree n. There exists a perfectly secure protocol for $\mathsf{OLE}(\mathbb{K})$ in the $\mathsf{OLE}(\mathbb{F})^m$-hybrid that performs only one call to the $\mathsf{OLE}(\mathbb{F})^m$ functionality and $m = \Theta(n)$.*

Given. Two linear maps E' and D' as in Theorem 7.

Private input. Alice has private inputs $A \in \mathbb{K}$ and $B \in \mathbb{K}$. Bob has private input $X \in \mathbb{K}$.

Hybrid. Parties are in the $\mathsf{OLE}(\mathbb{F})^m$-hybrid.

Private Input Construction.

1. Alice creates private inputs $\mathbf{a} = E'(A)$ and $\mathbf{b} = E'(B)$.
2. Bob creates private inputs $\mathbf{x} = E'(X)$.
3. Both parties invoke the the $\mathsf{OLE}(\mathbb{F})^m$ functionality with respective Alice input $(\mathbf{a}, \mathbf{b})$ and Bob input $\mathbf{x}$. Bob receives $\mathbf{z} = \mathbf{a} * \mathbf{x} + \mathbf{b} = E'(A) * E'(X) + E'(B)$.

Output Decoding. Bob outputs $Z = D'(\mathbf{z}) = D'\big(E'(\mathbf{a}) * E'(\mathbf{x}) + E'(\mathbf{b})\big) = AX + B$.

Figure 9: Protocol for computing one $\mathsf{OLE}(\mathbb{K})$ using m copies of $\mathsf{OLE}(\mathbb{F})$, where $\mathbb{K}$ is a degree n extension field of $\mathbb{F}$.

Figure 9 realizes Lemma 2. In the protocol, Alice creates $\mathbf{a} = E'(A)$ and $\mathbf{b} = E'(B)$, and Bob creates $\mathbf{x} = E'(X)$. Calling the $\mathsf{OLE}(\mathbb{F})^m$ functionality, Bob receives $\mathbf{z} = \mathbf{a} * \mathbf{x} + \mathbf{b}$. In particular, he receives $\mathbf{z} = E'(A) * E'(X) + E'(B)$. Bob then computes $D'(\mathbf{z})$. Since D' is a linear map and by Theorem 7, we have the following.

$$\begin{aligned} D'(\mathbf{z}) &= D'\big(E'(A) * E'(X) + E'(B)\big) \\ &= D'\big(E'(A) * E'(X)\big) + D'\big(E'(B)\big) \\ &= AX + B \end{aligned}$$

A.3 Proof of Theorem 9

The protocol which satisfies Theorem 9 is the parallel composition of the protocols presented in Figure 8 and Figure 9 (Lemma 2). The composition of these protocols in parallel gives

an optimal two-round protocol for realizing $\mathsf{OLE}(\mathbb{K})$ in the $\mathsf{ROLE}(\mathbb{F})^m$-hybrid with perfect security and $m = \Theta(n)$ by Theorem 7, as desired.

A.4 Prior Work

Chudnovsky-Chudnovsky [CC87] gave the first feasibility result on the bilinear complexity of multiplication, showing $\Theta(n)$ multiplications in $\mathbb{F}_q$ suffice to perform one multiplication over $\mathbb{F}_{q^n}$. Since then there have been several works on explicit constructions and variants of the bilinear multiplication algorithms and improved the bounds on the bilinear complexity.

The works of [STV92, GS95, GS96] discuss the construction of appropriate function fields such that there is sufficient number of rational points for interpolation. Improvement on the bounds for the bilinear complexity of multiplication and generalizations of the Chudnovsky-Chudnovsky method appear in [BR04, Ran12, BPR16, BBBT17]. Explicit construction of multiplication algorithms are discussed in [CÖ10, ABBR15, BBBT17], and in the particular case of function fields over elliptic curves in [Cha12, BBT13].