Secure Computation with Constant Communication Overhead using Multiplication Embeddings

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

Abstract

Secure multi-party computation (MPC) allows mutually distrusting parties to compute securely over their private data. The hardness of MPC, essentially, lies in performing secure multiplications over suitable algebras. Parties use diverse cryptographic resources, like computational hardness assumptions or physical resources, to securely compute these multiplications.

There are several cryptographic resources that help securely compute one multiplication over a large finite field, say $\mathbb{GF}[2^n]$, with linear communication complexity. For example, the computational hardness assumption like noisy Reed-Solomon codewords are pseudorandom. However, it is not known if we can securely compute, say, a linear number of AND-gates from such resources, i.e., a linear number of multiplications over the base field $\mathbb{GF}[2]$. Before our work, we could only perform $o(n)$ secure AND-evaluations. This example highlights the general inefficiency of multiplying over the base field using one multiplication over the extension field. Our objective is to remove this hurdle and enable secure computation of boolean circuits while incurring a constant communication overhead based on more diverse cryptographic resources.

Technically, we construct a perfectly secure protocol that realizes a linear number of multiplication gates over the base field using one multiplication gate over a degree-n extension field. This construction relies on the toolkit provided by algebraic function fields.

Using this construction, we obtain the following results. If we can perform one multiplication over $\mathbb{GF}[2^n]$ with linear communication using a particular cryptographic resource, then we can also evaluate linear-size boolean circuits with linear communication using the same cryptographic resource. In particular, we provide the first construction that computes a linear number of oblivious transfers with linear communication complexity from the computational hardness assumptions like noisy Reed-Solomon codewords are pseudorandom, or arithmetic-analogues of LPN-style assumptions. Next, we highlight the potential of our result for other applications to MPC by constructing the first correlation extractor that has $1/2$ resilience and produces a linear number of oblivious transfers.

[*]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 [Yao82, GMW87] (MPC) allows mutually distrusting parties to compute securely over their private data. Even when parties follow the protocols honestly, but are curious to find additional information about other parties' private inputs, most functionalities cannot be securely computed [Kil88, IL89, Kus89, Bea89]. So, we rely on diverse forms of cryptographic resources to help parties perform computations over their private data. These cryptographic resources can either be computational hardness assumptions [GMW87, IPS08] or physical resources like noisy channels [CK88, Kil91, BMM99, Kil00], correlated private randomness [Kil00, WW06], trusted resources [CLOS02, IPS08, IPS09], and tamper-proof hardware [Kat07, CGS08, MS08, DNW08].

In this paper, for the simplicity of exposition of the key ideas, we consider 2-party secure computation against honest-but-curious adversaries. Suppose two parties are interested in securely computing a boolean circuit C that uses AND, and XOR, and represent the input, output, and the intermediate values of the computation in binary. Parties can use the oblivious transfer (OT) functionality to securely compute C (with perfect security and linear communication complexity) using the GMW protocol [GMW87]. The OT 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 m AND gates (and an arbitrary number of XOR gates) with $\Theta(m)$ communication complexity. In this work, we consider secure computation protocols that have communication complexity proportional to the size of the circuit C.[1]

Parties can also compute arithmetic circuits that use MUL and ADD gates over large fields by emulating the arithmetic gates using finite fields. In particular, using efficient bilinear multiplication algorithms [CC87], parties can securely compute one multiplication over the finite field $\mathbb{GF}[2^n]$ by performing m OT calls and linear communication complexity, where $n = \Theta(m)$. In general, using m OT calls, parties can securely compute any circuit C that has m_i arithmetic gates over $\mathbb{GF}[2^{n_i}]$, for $i \in \mathbb{N}$, such that $\sum_i m_i \cdot n_i = \Theta(m)$, which measures the *size of* C. Intuitively, the size of the arithmetic circuit C refers to the cumulative size of representing the elements of the (multiplication) gates in the circuit.

Summarizing this discussion, we conclude that m OT calls help the parties securely compute arithmetic circuits (over characteristic 2 fields) of size $\Theta(m)$ with communication complexity $\Theta(m)$. Several cryptographic resources can implement the m instances of the OT functionality using a linear communication complexity. For example, there are instantiations based on polynomial-stretch local pseudorandom generators [IKOS08], the Phi-hiding assumption [IKOS09], LWE [DHRW16], DDH-hard groups [BGI17], and noisy channels [IKO+11]. By composing these protocols, parties can use the corresponding cryptographic resources and securely compute linear-size circuits using only linear communication.

On the other hand, there are cryptographic resources that directly enable secure multiplication over a large extension field using communication that is proportional to the size of the field. For example, consider the constructions based on Paillier encryption [Pai99, DJ01, Gil99], LWE [LPR10, DPSZ12], pseudorandomness of noisy random Reed-Solomon

[1] Network latency considerations typically motivate the study of MPC protocols with linear communication complexity.

codewords [NP06, IPS09], and arithmetic analogues well-studied cryptographic assumptions [ADI+17]. The key functionality in this context is a generalization of the OT functionality, namely the Oblivious Linear-function Evaluation [WW06] (OLE) over a field $\mathbb{K}$, say $\mathbb{K} = \mathbb{GF}[2^n]$. The OLE functionality takes as input a pair of field elements $(A, B) \in \mathbb{K}^2$ from the sender and an element $X \in \mathbb{K}$ 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. Using (the generalization of) the GMW protocol, parties can compute one multiplication over $\mathbb{K}$ with $\Theta(\lg |\mathbb{K}|)$ communication complexity. Note that the circuit with one MUL gate (over $\mathbb{K}$) has size $\lg |\mathbb{K}|$, so the communication complexity of the protocol is linear in the circuit size. However, using OLE over $\mathbb{K} = \mathbb{GF}[2^n]$, *can we securely compute boolean circuits such that the communication complexity is linear in the circuit size?*

The question motivated above with the illustrative example of $\mathbb{K} = \mathbb{GF}[2^n]$ and $\mathbb{F} = \mathbb{GF}[2]$ generalizes to any $\mathbb{K}$ that is an extension field of a constant-size base field $\mathbb{F}$. Before our work, the best solution securely evaluated size $m = o(n)$ boolean circuits using $\Theta(n) = \omega(m)$ communication complexity from one OLE over $\mathbb{GF}[2^n]$ (refer to Section 1.3 for the state-of-the-art construction). We present the first solution that securely evaluates size $m = \Theta(n)$ boolean circuits using one OLE over $\mathbb{GF}[2^n]$ and, thus, has communication complexity linear in the circuit size. Additionally, we found secure computation of size-m boolean circuits using linear communication from more diverse cryptographic resources. Because, any cryptographic resource that securely implements OLE over $\mathbb{K}$ with a linear communication complexity, also enables the secure computation of linear-size boolean circuits with a linear communication complexity. In particular, we provide the first linear communication protocols for m OTs from cryptographic hardness assumptions like the pseudorandomness of noisy Reed-Solomon codewords [NP06, IPS09] and arithmetic analogues of well-studied cryptographic assumptions [ADI+17].

1.1 Multiplication Embedding Problem

Our approach to the MPC problem begins with the following combinatorial embedding problem, which 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.

Concurrent and Independent Work. Recently, in concurrent and independent work,[2] Cascudo et al. [CCXY18] also studied this embedding problem as reverse multiplication-friendly embeddings (RMFE), and provide a constant-rate construction. They use this result to achieve new amortization results in MPC.

1.2 Our Contributions

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

Consequences for 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 $\mathbb{K}$.

Theorem 2. *Let $\mathbb{F}$ be a finite field, and $\mathbb{K}$ be a degree-n extension of $\mathbb{F}$. There exists a 2-party semi-honest 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 (and no additional communication).*

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 Theorem 2, we can implement a linear number of OTs at a constant communication overhead based on computational hardness assumptions like the pseudorandomness of noisy Reed-Solomon codewords [NP06, IPS09] and arithmetic analogues of well-studied

[2] Our work appears on the eprint as [BMN18].

cryptographic assumptions [ADI+17], which help construct an OLE over large (but finite) fields. In general, if a cryptographic resource supports the generation of one OLE over $\mathbb{K}$ using $\Theta(\lg|\mathbb{K}|)$ communication complexity, then the following result also applies to it.

Corollary 3. *There exists a computationally secure protocol implementing m OTs using $\Theta(m)$ communication based on (any of) the following computational hardness assumptions.*

1. *Pseudorandomness of noisy random Reed-Solomon codewords [NP06, IPS09],*
2. *Arithmetic analogues of "LPN-style assumptions" and the existence of polynomial-stretch local arithmetic PRG [ADI+17]*

In fact, we can leverage efficient bilinear multiplication algorithms [CC87] that incur a constant communication overhead, to obtain the following result (see Appendix A).

Corollary 4. *Let $\mathbb{F}$ be a finite field, and $\mathbb{K}$ be a degree-n extension of $\mathbb{F}$. Let $\mathbb{F}_1, \ldots, \mathbb{F}_k$ are 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 $m_1n_1 + \cdots + m_kn_k \leqslant \Theta(n)$, 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 4 allows 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. We only fix the base field $\mathbb{F}$ and an upper-bound n estimating the size of the circuit C.

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

Corollary 5. *For every $1/2 \geqslant \varepsilon > 0$, 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 $|\mathbb{F}| = 3n/2$, and $\mathbb{K}$ 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 $\mathbf{a} = (a_1, \dots, a_m) \in \mathbb{F}^m$ and $\mathbf{b} = (b_1, \dots, b_m) \in \mathbb{F}^m$. 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 $i \in \{1, \dots, m\}$ 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 $i \in \{1, \dots, m\}$.

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.[3] 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 $i \in \{1, \dots, m\}$. 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* $\{f_{-1}, \dots, f_{-m}\}$ to enable the encoding of $a_1, \dots, a_m$ 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 $\mathbb{F}$.

Prior Best Construction.[4] [BMN17] showed that $(\lg |\mathbb{F}|)^{1-o(1)}$ OTs could be embedded into one OLE over $\mathbb{F}$ if $\mathbb{F}$ has characteristic 2. Overall, this construction yields $s(\log s)^{-o(1)}$ OTs from one OLE over $\mathbb{K}$, where $s = \lg |\mathbb{K}|$.

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

[3] 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 $C(t)$.

[4] We only consider works that appear publicly before our work appears on the eprint as [BMN18].

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 $z^{-1} \in \mathcal{O}$.*

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* $\operatorname{Prin}(K) := \{D \in \operatorname{Div}(K) \colon \exists f \in K \setminus \{0\},\ D = (f)\}$ *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* $G \in \operatorname{Div}(K)$*, 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 $G \in \operatorname{Div}(K)$. 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 by the degree of its divisor.

Imported Lemma 6 ([Cas10, Lemma 2.51]). *For any* $G \in \operatorname{Div}(K)$*, 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* $D \in \operatorname{Div}(K)$*, 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*

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

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* $w \in \Omega(K) \setminus \{0\}$, *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 that proves Theorem 1. We shall use the following lemmas.

Imported Lemma 9 ([Cas10, Lemma 2.51])**.** *Let $K/\mathbb{F}_q$ be an algebraic function field. For any $G \in \mathrm{Div}(K)$, we have $\ell(G) \leqslant \deg G + 1$. In particular, if $\deg G < 0$, then $\ell(G) = 0$. Here $\ell(G) := \dim(\mathscr{L}(G))$.*

Imported Lemma 10 ([BCS97, Lemma 18.21])**.** *Let $K/\mathbb{F}_q$ be an algebraic function field of one variable of genus g and degree at least n satisfying $n \geqslant 2\log_q g + 6$. Then there exists a prime divisor of degree n of $K/\mathbb{F}_q$.*

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 $x \in V$ there exists a unique $u \in \mathbb{F}^m$ such that $x = uG$, and since G' has full rank. $\square$

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.

$$\begin{tikzcd}
\mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \arrow[r, "\text{mult.}"] & \mathbb{F}_{q^n} \\
\mathscr{L}(sP) \times \mathscr{L}(sP) \arrow[r, "\phi"] \arrow[u, "\kappa \times \kappa"] \arrow[d, "\gamma \times \gamma"] & \mathscr{L}(2sP) \arrow[u, "\kappa"] \arrow[d, "\gamma"] \\
\mathbb{F}_q^r \times \mathbb{F}_q^r \arrow[r, "*"] & \mathbb{F}_q^r
\end{tikzcd}$$

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 $n \geqslant \max\{2\log_q g + 6, 6g\}$, $s = \lfloor (n-1)/2 \rfloor$, and P be a prime divisor of degree one of $K/\mathbb{F}_q$. By Imported Lemma 10 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 $\mathcal{O}_Q = \{z \in K/\mathbb{F}_q \mid v_Q(z) \geqslant 0\}$ of Q. 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 9 (since $\deg(2sP - Q) = 2s - n < 0$). This implies that κ is injective. Since $\mathscr{L}(sP) \subseteq \mathscr{L}(2sP)$, the evaluation map κ restricted to $\mathscr{L}(sP)$, represented by $\kappa|_{\mathscr{L}(sP)}$, 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 $\gamma : \mathscr{L}(2sP) \to \mathbb{F}_q^r$ 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 $\gamma|_{\mathscr{L}(sP)}$ is $\mathscr{L}(sP - \sum P_i)$, which has dimension 0. Note that γ is a linear map, therefore by the rank-nullity theorem we have $\dim(\ker(\gamma|_{\mathscr{L}(sP)}))+ \dim(\mathrm{Im}(\gamma|_{\mathscr{L}(sP)})) = \dim(\mathscr{L}(sP))$. So $\dim(\mathrm{Im}(\gamma|_{\mathscr{L}(sP)})) = \dim(\mathscr{L}(sP)) = s - g + 1$ since $\deg(sP) = s > 2g - 1$. Let $m = s - g + 1$ and $V = \mathrm{Im}(\gamma|_{\mathscr{L}(sP)})$. 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 $D : \mathrm{Im}(\kappa) \subseteq \mathbb{F}_{q^n} \to \mathbb{F}_q^m$ such that $D = \psi \circ \gamma \circ \kappa^{-1}$, where $\mathbb{K} = \mathbb{F}_{q^n}$.

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 perform 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. Next, since κ is injective it is a bijection from $\mathscr{L}(2sP)$ to $\mathrm{Im}(\kappa)$. Thus, the mapping D is also well-defined. □

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 $(x \cdot y) \in \mathscr{L}(2sP)$ because $\mathscr{L}(sP) \cdot \mathscr{L}(sP) \subseteq \mathscr{L}(2sP)$, so γ has the following property.

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

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 $6g \leqslant n$, 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 Figure 1 presents how to choose c_q^* such that $q^{c_q^*}$ is an even power of a prime and is at least 49.

Let $q^* := q^{c_q^*}$. Suppose that n is sufficiently large and is divisible by c_q^*, and that $n/c_q^* \geqslant \max\{2 \log_{q^*} g + 6, 6g\}$. Now q^* is an even power of a prime and $q^* \geqslant 49$, so we are in Case 1 with the following parameters. Let $n^* := n/c_q^*$, 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 $n^* \geqslant 2 \log_{q^*} g + 6$. Let $s = \lfloor (n^* - 1)/2 \rfloor$ and set $m = s - g + 1$.

	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 1: 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 $q^{c_q^*} \geqslant 49$.

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 $\gamma\colon \mathscr{L}(2sP) \to \mathbb{F}_{q^*}^r$, and let $V = \mathrm{Im}(\gamma|_{\mathscr{L}(sP)})$. 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 $D = \psi \circ \gamma \circ \kappa^{-1}$. Consequently, we have

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

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, we have $m = s - g + 1 = \Theta(n)$. This completes the proof of case 2. $\square$

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 have the following theorem.

Imported Theorem 7 (Garcia-Stichtenoth [GS96])**.** *For every q that is an even power of a prime, 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, clearly $n \geqslant 6g$ and since $g \leqslant \frac{n}{\sqrt{q}-1}$ we have

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

So there exists a prime divisor of degree n by Imported Lemma 10. 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 $m \leqslant \lfloor\frac{n-1}{2}\rfloor + 6 = \Theta(n)$.

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

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

Theorem 6 (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 $\mathsf{OLE}\left(\mathbb{F}\right)^m$ in the $\mathsf{ROLE}\big(\mathbb{K}\big)$-hybrid that performs only one call to the $\mathsf{ROLE}\big(\mathbb{K}\big)$ functionality, $m = \Theta(n)$, and has communication complexity* $3\lg|\mathbb{K}|$.

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 $\mathsf{OLE}\left(\mathbb{F}\right)$, 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 $\mathsf{OLE}\left(\mathbb{GF}\left[2\right]\right)$ functionality.

Random Oblivious Linear-function Evaluation. For a field $(\mathbb{F}, +, \cdot)$, random oblivious linear-function evaluation over $\mathbb{F}$, represented by $\mathsf{ROLE}\big(\mathbb{F}\big)$, 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 $\mathsf{ROLE}\big(\mathbb{GF}\left[2\right]\big)$ correlation.

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

The protocol presented in Figure 2 is the standard protocol that implements the $\mathsf{OLE}\left(\mathbb{K}\right)$ functionality in the $\mathsf{ROLE}\big(\mathbb{K}\big)$-hybrid with perfect semi-honest security (cf. [WW06]).

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

3.3 Securely realizing $\mathsf{OLE}\left(\mathbb{F}\right)^m$ using one $\mathsf{OLE}\left(\mathbb{K}\right)$

This section presents the realization of Theorem 2. Our goal is to embed m independent copies of $\mathsf{OLE}\left(\mathbb{F}\right)$ into one $\mathsf{OLE}\left(\mathbb{K}\right)$, 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 $i \in [m]$. To do that, we extend our multiplication embedding with addition using a standard technique like in [GIMS15, BMN17]. We define a randomized encoding function E_2 needed for our protocol as the following.

Definition of the (randomized) encoding function E_2

$E_2 : \mathbb{F}_q^m \to \mathbb{F}_{q^n}$. $E_2(\mathbf{b})$ returns a random $B \in \mathrm{Im}(\kappa) \subseteq \mathbb{F}_{q^n}$ such that $D(B) = \mathbf{b}$, that is, $\psi(\gamma(\kappa^{-1}(B))) = \mathbf{b}$.

We show that the protocol presented in Figure 3 achieves $m = \Theta(n)$.

Figure 3 is the protocol which realizes Theorem 2. We argue the correctness of the protocol by showing that $D(Z^*) = \mathbf{a} * \mathbf{x} + \mathbf{b}$. In the protocol, Alice creates $A^* = E(\mathbf{a})$ and $B^* = E_2(\mathbf{b})$, and Bob creates $X^* = E(\mathbf{x})$. Calling the $\mathsf{OLE}\left(\mathbb{K}\right)$ functionality, Bob receives $Z^* = A^* \cdot X^* + B^*$. In particular, Bob receives $Z^* = E(\mathbf{a}) \cdot E(\mathbf{x}) + E_2(\mathbf{b})$. Then Bob computes $D(Z^*)$. Since D is a linear map and by Theorem 1, we have $m = \Theta(n)$ and the following.

$$D(Z^*) = D\left(E(\mathbf{a}) \cdot E(\mathbf{x}) + E_2(\mathbf{b})\right) = D\left(E(\mathbf{a}) \cdot E(\mathbf{x})\right) + D(E_2(\mathbf{b})) = \mathbf{a} * \mathbf{x} + \mathbf{b}$$

We provide the security arguments for our protocol in Appendix B. It relies on the observation that $E(\mathbf{a}) \cdot E(\mathbf{x}) + E_2(\mathbf{b})$ is uniformly distributed over the set

$$\{Z \colon Z \in \mathrm{Im}(\kappa) \text{ and } D(Z) = \mathbf{z}\},$$

where $\mathbf{z} = \mathbf{a} * \mathbf{b} + \mathbf{c}$.

Given. Linear maps E and D as in Theorem 1, and the linear map E_2 defined above.

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 $B^* = E_2(\mathbf{b})$.
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 $Z^* = A^*X^* + B^* = E(\mathbf{a}) \cdot E(\mathbf{x}) + E_2(\mathbf{b})$.

Output Decoding. Bob outputs $\mathbf{z} = D(Z^*) = D(E(\mathbf{a}) \cdot E(\mathbf{x}) + E_2(\mathbf{b}))$.

Figure 3: 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 $\mathbb{F}$.

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

The protocol that realizes Theorem 6 is the parallel composition of the protocols presented in Figure 2 and Figure 3 (Theorem 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 5. In particular, Corollary 5 is achieved by the construction of a suitable correlation extractor. A *correlated private randomness*, 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 [IKOS09])**.** *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 m copies of the OT functionality against information-theoretic semi-honest adversaries with ε-simulation error.*

Using this definition we restate Corollary 5 as follows.

Theorem 7 (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, Theorem 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.

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 $\mathsf{ROLE}\big(\mathbb{GF}[2]\big)$ by ROLE. Note that ROT and ROLE are identical (functionally equivalent) correlations.

Inner-product Correlation. For a field $(\mathbb{K}, +, \cdot)$ and $n' \in \mathbb{N}$, inner-product correlation over $\mathbb{K}$ of size n', represented by $\mathsf{IP}\big(\mathbb{K}^{n'}\big)$, is a correlation that samples random $r_A = (x_0, \dots, x_{n'-1}) \in \mathbb{K}^{n'}$ and $r_B = (y_0, \dots, y_{n'-1}) \in \mathbb{K}^{n'}$ 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.

4.2 Realizing Theorem 7

The realization of Theorem 7 is the parallel composition of two protocols. First, we utilize the BMN [BMN17] $\mathsf{ROLE}\big(\mathbb{K}\big)$ extraction protocol. Informally, the BMN extraction protocol takes leaky shares of the inner-product correlation over the field $\mathbb{K}$, and securely extracts one sample of $\mathsf{ROLE}\big(\mathbb{K}\big)$. In particular, the BMN extraction protocol is resilient to $t = (1/2 - g)n'$ bits of leakage, for any $g \in (0, 1/2]$.

Second, we utilize our new embedding protocol of Theorem 6 which produces m copies of $\mathsf{OLE}\,(\mathbb{F})$ from one $\mathsf{ROLE}\big(\mathbb{K}\big)$, and compose it in parallel with the BMN extraction protocol for $\mathsf{ROLE}\big(\mathbb{K}\big)$. Previously, the BMN embedding achieved $m = (n')^{1-o(1)}$ production, whereas with Theorem 6 we achieve $m = \Theta(n')$ production with the following parameters. We take $\mathbb{F} = \mathbb{GF}[2]$ and $\mathbb{K} = \mathbb{GF}[2^{\delta n'}]$, where n' and δ are given, $\eta := \frac{1}{\delta} - 1$, and $n := \frac{n'}{(\eta+1)}$. In particular, $\mathbb{K}$ is a degree-n extension of $\mathbb{F}$, and n here corresponds to the n of Corollary 5. So $m = \Theta(n') = \Theta(n)$. We then take $(R_A, R_B) = \mathsf{IP}\big(\mathbb{K}^{1/\delta}\big)$ to be the input correlation for the BMN extraction protocol.

The BMN extraction protocol is a perfectly secure semi-honest protocol for extracting one $\mathsf{ROLE}\big(\mathbb{GF}[2^{\delta n'}]\big)$ in the $\big(\mathsf{IP}\big(\mathbb{GF}[2^{\delta n'}]^{1/\delta}\big)\big)^{[t]}$-hybrid which is resilient to $t = (1/2 - g)n'$ bits of leakage, for all $0 < \delta < g \leqslant 1/2$ (cf. Theorem 1, [BMN17]). Then the parallel composition of protocols Figure 2 and Figure 3 is a perfectly secure semi-honest protocol for realizing m

copies of $\mathsf{OLE}\left(\mathbb{GF}[2]\right)$ in the $\mathsf{ROLE}\left(\mathbb{GF}[2^{\delta n'}]\right)$-hybrid, and $m = \Theta(n') = \Theta(n)$. This proves Theorem 7, and thus Corollary 5.

4.3 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 4 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	$\Theta(n)$	$\Theta(n)$	$2^{-\Theta(n)}$
	$\mathsf{ROLE}(\mathbb{F})^{n/2\lg\lvert\mathbb{F}\rvert}$	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 4: 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 $\mathsf{IP}\left(\mathbb{K}^s\right)$ 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 $u_1v_1 + \cdots + u_sv_s = 0$. All correlations have been normalized so that each party gets an n-bit secret share. The parameter g is defined as the gap to leakage resilience s.t. $t \geqslant 0$.

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 $t/n \in [1/4, 1/2)$. 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. URL: http://arxiv.org/abs/1510.00090, arXiv:1510.00090. 26

[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. 2, 4

[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. URL: http://www.sciencedirect.com/science/article/pii/S1631073X17301577, doi:https://doi.org/10.1016/j.crma.2017.06.002. 26

[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. 26

[BCS97] Peter Bürgisser, Michael Clausen, and Mohammad Amin Shokrollahi. *Algebraic complexity theory*. Grundlehren der mathematischen Wissenschaften ; 315. Springer, Berlin ; New York, 1997. 9, 10, 23

[Bea89] Donald Beaver. Perfect privacy for two-party protocols. In Joan Feigenbaum and Michael Merritt, editors, *Proceedings of DIMACS Workshop on Distributed Computing and Cryptography*, volume 2, pages 65–77. American Mathematical Society, 1989. 1

[BGI17] Elette Boyle, Niv Gilboa, and Yuval Ishai. Group-based secure computation: Optimizing rounds, communication, and computation. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Part II*, volume 10211 of *LNCS*, pages 163–193. Springer, Heidelberg, May 2017. 1

[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. 17

[BMM99] Amos Beimel, Tal Malkin, and Silvio Micali. The all-or-nothing nature of two-party secure computation. In Michael J. Wiener, editor, *CRYPTO'99*, volume 1666 of *LNCS*, pages 80–97. Springer, Heidelberg, August 1999. 1

[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. 2, 4, 5, 14, 16, 17

[BMN18] Alexander R. Block, Hemanta K. Maji, and Hai H. Nguyen. Embedding multiplications at a linear rate and its applications. Cryptology ePrint Archive, Report 2018/395, 2018. https://eprint.iacr.org/2018/395. 3, 5

[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. URL: http://arxiv.org/abs/1601.00126, arXiv:1601.00126. 26

[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. URL: http://www.sciencedirect.com/science/article/pii/S0021869303006951, doi:https://doi.org/10.1016/j.jalgebra.2003.09.031. 26

[Cas10] Ignacio Cascudo. *On asymptotically good strongly multiplicative linear secret sharing*. PhD thesis, Tesis doctoral, Universidad de Oviedo, 2010. 5, 6, 7, 8, 9, 10

[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. 1, 4, 23, 26

[CCXY18] Ignacio Cascudo, Ronald Cramer, Chaoping Xing, and Chen Yuan. Amortized complexity of information-theoretically secure mpc revisited. Cryptology ePrint Archive, Report 2018/429, 2018. https://eprint.iacr.org/2018/429. 3

[CGS08] Nishanth Chandran, Vipul Goyal, and Amit Sahai. New constructions for UC secure computation using tamper-proof hardware. In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 545–562. Springer, Heidelberg, April 2008. 1

[Cha12] Jean Chaumine. *Multiplication in small finite fields using elliptic curves*, pages 343–350. 2012. URL: https://www.worldscientific.com/doi/abs/10.1142/9789812793430_0018, arXiv:https://www.worldscientific.com/doi/pdf/10.1142/9789812793430_0018, doi:10.1142/9789812793430_0018. 26

[CK88] Claude Crépeau and Joe Kilian. Achieving oblivious transfer using weakened security assumptions (extended abstract). In *29th FOCS*, pages 42–52. IEEE Computer Society Press, October 1988. 1

[CLOS02] Ran Canetti, Yehuda Lindell, Rafail Ostrovsky, and Amit Sahai. Universally composable two-party and multi-party secure computation. In *34th ACM STOC*, pages 494–503. ACM Press, May 2002. 1

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

[DHRW16] Yevgeniy Dodis, Shai Halevi, Ron D. Rothblum, and Daniel Wichs. Spooky encryption and its applications. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part III*, volume 9816 of *LNCS*, pages 93–122. Springer, Heidelberg, August 2016. doi:10.1007/978-3-662-53015-3_4. 1

[DJ01] Ivan Damgård and Mats Jurik. A generalisation, a simplification and some applications of Paillier's probabilistic public-key system. In Kwangjo Kim, editor, *PKC 2001*, volume 1992 of *LNCS*, pages 119–136. Springer, Heidelberg, February 2001. 1

[DNW08] Ivan Damgård, Jesper Buus Nielsen, and Daniel Wichs. Isolated proofs of knowledge and isolated zero knowledge. In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 509–526. Springer, Heidelberg, April 2008. 1

[DPSZ12] Ivan Damgård, Valerio Pastro, Nigel P. Smart, and Sarah Zakarias. Multiparty computation from somewhat homomorphic encryption. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 643–662. Springer, Heidelberg, August 2012. 1

[Gil99] Niv Gilboa. Two party RSA key generation. In Michael J. Wiener, editor, *CRYPTO'99*, volume 1666 of *LNCS*, pages 116–129. Springer, Heidelberg, August 1999. 1

[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. doi:10.1007/978-3-662-48000-7_34. 14, 17

[GMW87] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or A completeness theorem for protocols with honest majority. In Alfred Aho, editor, *19th ACM STOC*, pages 218–229. ACM Press, May 1987. 1

[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. 9, 26

[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, 26

[IKO+11] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Manoj Prabhakaran, Amit Sahai, and Jürg Wullschleger. Constant-rate oblivious transfer from noisy channels. In Phillip Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 667–684. Springer, Heidelberg, August 2011. 1

[IKOS08] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Cryptography with constant computational overhead. In Richard E. Ladner and Cynthia Dwork, editors, *40th ACM STOC*, pages 433–442. ACM Press, May 2008. 1

[IKOS09] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Extracting correlations. In *50th FOCS*, pages 261–270. IEEE Computer Society Press, October 2009. 1, 4, 15, 17

[IL89] Russell Impagliazzo and Michael Luby. One-way functions are essential for complexity based cryptography (extended abstract). In *30th FOCS*, pages 230–235. IEEE Computer Society Press, October / November 1989. 1

[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. URL: http://dx.doi.org/10.1109/ISIT.2014.6875092, doi:10.1109/ISIT.2014.6875092. 17

[IPS08] Yuval Ishai, Manoj Prabhakaran, and Amit Sahai. Founding cryptography on oblivious transfer - efficiently. In David Wagner, editor, *CRYPTO 2008*, volume 5157 of *LNCS*, pages 572–591. Springer, Heidelberg, August 2008. 1

[IPS09] Yuval Ishai, Manoj Prabhakaran, and Amit Sahai. Secure arithmetic computation with no honest majority. In Omer Reingold, editor, *TCC 2009*, volume 5444 of *LNCS*, pages 294–314. Springer, Heidelberg, March 2009. 1, 2, 3, 4

[Kat07] Jonathan Katz. Universally composable multi-party computation using tamper-proof hardware. In Moni Naor, editor, *EUROCRYPT 2007*, volume 4515 of *LNCS*, pages 115–128. Springer, Heidelberg, May 2007. 1

[Kil88] Joe Kilian. Founding cryptography on oblivious transfer. In *20th ACM STOC*, pages 20–31. ACM Press, May 1988. 1

[Kil91] Joe Kilian. A general completeness theorem for two-party games. In *23rd ACM STOC*, pages 553–560. ACM Press, May 1991. 1

[Kil00] Joe Kilian. More general completeness theorems for secure two-party computation. In *32nd ACM STOC*, pages 316–324. ACM Press, May 2000. 1

[Kus89] Eyal Kushilevitz. Privacy and communication complexity. In *30th FOCS*, pages 416–421. IEEE Computer Society Press, October / November 1989. 1

[LPR10] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 1–23. Springer, Heidelberg, May 2010. 1

[MS08] Tal Moran and Gil Segev. David and goliath commitments: UC computation for asymmetric parties using tamper-proof hardware. In Nigel P. Smart, editor, *Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings*, volume 4965 of *Lecture Notes in Computer Science*, pages 527–544. Springer, 2008. URL: http://dx.doi.org/10.1007/978-3-540-78967-3_30, doi:10.1007/978-3-540-78967-3_30. 1

[NP06] Moni Naor and Benny Pinkas. Oblivious polynomial evaluation. *SIAM Journal on Computing*, 35(5):1254–1281, 2006. 2, 3, 4

[Pai99] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In Jacques Stern, editor, *EUROCRYPT'99*, volume 1592 of *LNCS*, pages 223–238. Springer, Heidelberg, May 1999. 1

[Ran12] Hugues Randriambololona. Bilinear complexity of algebras and the chudnovsky–chudnovsky interpolation method. *Journal of Complexity*, 28(4):489–517, 2012. 26

[Sti09] Henning Stichtenoth. *Algebraic Function Fields and Codes*. Graduate Texts in Mathematics, 254. 2nd ed.. edition, 2009. 5, 7, 9

[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. 26

[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. 1, 2, 13

[Yao82] Andrew Chi-Chih Yao. Protocols for secure computations (extended abstract). In *23rd FOCS*, pages 160–164. IEEE Computer Society Press, November 1982. 1

A Chudnovsky-Chudnovsky Bilinear Multiplication

We discuss the reverse problems of Theorem 1 and Theorem 6. 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 8 (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 9. *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 8 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 6.

Imported Lemma 11 (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 5 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 8. 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 8, we compute the reverse problem of Theorem 6. That is, we can use multiple small ROLE to realize one large OLE.

$$\begin{tikzcd}
\mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \arrow[r, "\text{mult.}"] & \mathbb{F}_{q^n} \\
\mathscr{L}(s'P) \times \mathscr{L}(s'P) \arrow[r, "\phi"] \arrow[u, "\kappa' \times \kappa'"] \arrow[d, "\gamma' \times \gamma'"] & \mathscr{L}(2s'P) \arrow[u, "\kappa'"] \arrow[d, "\gamma'"] \\
\mathbb{F}_q^{r'} \times \mathbb{F}_q^{r'} \arrow[r, "*"] & \mathbb{F}_q^{r'}
\end{tikzcd}$$

Figure 5: 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 10 (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, $m = \Theta(n)$, and has communication complexity $3m \lg |\mathbb{F}|$.*

To realize Theorem 10, 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 6 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 6: 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 7, 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 8.

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 7: 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 7 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 8, 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 10

The protocol which satisfies Theorem 10 is the parallel composition of the protocols presented in Figure 6 and Figure 7 (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 8, 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].

B Security Arguments for the protocol in Figure 3

Note that Alice does not receive any message, so the simulation of semi-honest corrupt Alice is trivial.

Consider the case that Bob is semi-honest corrupt. In this case, the simulator receives $\mathbf{x}$ from the environment, sends $\mathbf{x}$ to the external functionality, and receives $\mathbf{z}$ as output. It samples $Z^* = E_2(\mathbf{z})$, and sends $(X^* = E(\mathbf{x}), Z^*, \mathbf{z})$ as the view of Bob to the environment.

We shall show that this simulation is perfect. Note that $E(\mathbf{a}) \cdot E(\mathbf{x}) \in \mathrm{Im}(\kappa)$. Observe that $E_2(\mathbf{b})$ is a uniform distribution over a coset of $E_2(0^m)$. Now, $E(\mathbf{a}) \cdot E(\mathbf{x}) + E_2(\mathbf{b})$ is a uniform distribution over the coset

$$\{Z \colon Z \in \mathrm{Im}(\kappa) \text{ and } D(Z) = \mathbf{z}\},$$

where $\mathbf{z} = \mathbf{a} * \mathbf{x} + \mathbf{b}$. That is, the distribution of $E(\mathbf{a}) \cdot E(\mathbf{x}) + E_2(\mathbf{b})$ is identical to the distribution of $E_2(\mathbf{z})$.