Secure Computation using Leaky Correlations (Asymptotically Optimal Constructions)

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

April 29, 2018

Abstract

Most secure computation protocols can be effortlessly adapted to offload a significant fraction of their computationally and cryptographically expensive components to an offline phase so that the parties can run a fast online phase and perform their intended computation securely. During this offline phase, parties generate private shares of a sample generated from a particular joint distribution, referred to as the *correlation*. These shares, however, are susceptible to leakage attacks by adversarial parties, which can compromise the security of the entire secure computation protocol. The objective, therefore, is to preserve the security of the honest party despite the leakage performed by the adversary on her share.

Prior solutions, starting with n-bit leaky shares, either used 4 messages or enabled the secure computation of only sub-linear size circuits. Our work presents the first 2-message secure computation protocol for 2-party functionalities that have $\Theta(n)$ circuit-size despite $\Theta(n)$-bits of leakage, a qualitatively optimal result. We compose a suitable 2-message secure computation protocol in parallel with our new 2-message *correlation extractor*. Correlation extractors, introduced by Ishai, Kushilevitz, Ostrovsky, and Sahai (FOCS–2009) as a natural generalization of privacy amplification and randomness extraction, recover "fresh" correlations from the leaky ones, which are subsequently used by other cryptographic protocols. We construct the first 2-message correlation extractor that produces $\Theta(n)$-bit fresh correlations even after $\Theta(n)$-bit leakage.

Our principal technical contribution, which is of potential independent interest, is the construction of a family of multiplication-friendly linear secret sharing schemes that is simultaneously a family of small-bias distributions. We construct this family by randomly "twisting then permuting" appropriate Algebraic Geometry codes over constant-size fields.

[*]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.
[‡]Microsoft Research, Bangalore, India. t-digu@microsoft.com
[§]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. Secure computation of most functionalities requires expensive public-key primitives such as oblivious transfer even in the semi-honest setting.[1] We can effortlessly adjust most of these existing secure computation protocols so that they offload a significant fraction of their complex operations to an offline preprocessing phase. Subsequently, during an online phase, parties can implement extremely fast secure computation protocols.

For instance, in the two-party setting, we envision this offline phase as a secure implementation of a *trusted dealer* who generates private albeit correlated shares (r_A, r_B) for the Alice and Bob, respectively, sampled from an appropriate joint distribution (R_A, R_B), referred to as a *correlation*. This versatile framework allows the implementation of this trusted dealer using computational hardness assumptions, secure hardware, trusted hardware, or physical processes. Further, this offline phase is independent of the final functionality that is securely computed, as well as the private inputs of the parties to the functionality.

A particularly useful correlation is the *random oblivious transfer correlation*, represented by ROT. One sample of this correlation generates three random bits x_0, x_1, b and provides private shares $r_A = (x_0, x_1)$ to Alice, and $r_B = (b, x_b)$ to Bob. Note that Alice does not know the choice bit b, and Bob does not know the other bit x_{1-b}. Let $\mathcal{F}$ be the class of functionalities that admit 2-message secure computation protocols in the ROT-hybrid. Note that $\mathcal{F}$ includes the powerful class of functions that have a decomposable randomized encoding [AIK04, IK02, App17]. Alice and Bob can compute the required ROTs in the offline phase. Then, they can compute *any* functionality from this class using 2-messages, a protocol exhibiting optimal message complexity[2] and (essentially) optimal efficiency in the usage of cryptographic resources.

However, the private share of the honest party is susceptible to leakage attacks by an adversary, both during the generation of the shares and the duration of storing the shares. We emphasize that the leakage need not necessarily reveal individual bits of the honest party's share. The leakage can be on the entire share and encode crucial global information that can potentially jeopardize the security of the secure computation protocol. This concern naturally leads to the following fundamental question.

"Can we preserve the security and efficiency of the secure computation during the online phase despite the adversarial leakage on the honest party's shares?"

Using the class $\mathcal{F}$ of functionalities (defined above) as a yardstick, let us determine the primary hurdle towards a positive resolution of this question. In the sequel, $\mathcal{F}_m \subset \mathcal{F}$ is the set of all two-party functionalities that have a 2-message protocol in ROT^m-hybrid, i.e., parties start with m independent samples from the ROT correlation. In the leaky correlation setting, our objective is to design an (asymptotically) optimal secure computation protocol for $\mathcal{F}_m$. That is, starting with leaky correlations (of size n), we want to compute any $F \in \mathcal{F}_m$ such that $m = \Theta(n)$ via a 2-message protocol despite $t = \Theta(n)$ bits of leakage. We note

[1] A semi-honest adversary follows the prescribed protocol but is curious to find additional information.

[2] Message complexity refers to the number of messages exchanged between Alice and Bob.

that this task is equivalent to the task of constructing a secure computation protocol for the particular functionality ROT^m that also belongs to $\mathcal{F}_m$. This observation follows from the parallel composition of the secure protocol implementing the functionality ROT^m from leaky correlations with 2-message protocol for F in the ROT^m-hybrid. To summarize, our overall objective of designing optimal secure computation protocols from leaky ROT correlations reduces to the following equivalent goal.

"Construct a 2-message protocol to compute ROT^m securely, where $m = \Theta(n)$, from the leaky $\mathsf{ROT}^{n/2}$ correlation in spite of $t = \Theta(n)$ bits of leakage."

Note that in the $\mathsf{ROT}^{n/2}$-hybrid, both parties have private share of size n bits. The above problem is identical to *correlation extractors* introduced in the seminal work of Ishai, Kushilevitz, Ostrovsky, and Sahai [IKOS09].

Correlation Extractors. Ishai et al. [IKOS09] introduced the notion of correlation extractor as an interactive protocol that takes a leaky correlation as input and outputs a new correlation that is secure. Prior correlation extractors either used four messages [IKOS09] or had a sub-linear production [GIMS15, BMN17], i.e., $m = o(n)$. We construct the first 2-message correlation extractor that has a linear production and leakage resilience, that is, $m = \Theta(n)$ and $t = \Theta(n)$. Note that even computationally secure protocol can use the output of the correlation extractor in the online phase. Section 1.1 formally defines the notion of correlation extractors, and we present our main contributions in Section 1.2.

1.1 Correlation Extractors and Security Model

We consider the standard model of Ishai et al. [IKOS09] for correlation extractors, which is also used by subsequent works. We consider 2-party semi-honest secure computation in the preprocessing model. In the preprocessing step, a trusted dealer draws a sample of shares (r_A, r_B) from the joint distribution of correlated private randomness (R_A, R_B). The dealer provides the secret share r_A to Alice and r_B to Bob. Moreover, the adversarial party can perform arbitrary t-bits of leakage on the secret share of the honest party at the end of the preprocessing step. We represent this leaky correlation hybrid as $(R_A, R_B)^{[t]}$.[3]

Definition 1 (Correlation Extractor)**.** *Let (R_A, R_B) be a correlated private randomness such that the secret share 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 $\mathsf{ROT}^{m/2}$ functionality against information-theoretic semi-honest adversaries with ε simulation error.*

Note that the size of the secret shares output by the correlation extractor is m. We emphasize that no leakage occurs during the execution of the correlation extractor protocol.

[3] That is, the functionality samples secret shares (r_A, r_B) according to the correlation (R_A, R_B). The adversarial party sends a t-bit leakage function $\mathcal{L}$ to the functionality and receives the leakage $\mathcal{L}(r_A, r_B)$ from the functionality. The functionality sends r_A to Alice and r_B to Bob. Note that the adversary does not need to know its secret share to construct the leakage function because the leakage function gets the secret shares of both parties as input.

The t-bit leakage cumulatively accounts for all the leakage before the beginning of the online phase.

For brevity, in this work, we shall use the term "correlation extractor for (X, Y)" to refer to a correlation extractor that takes multiple samples of the correlation (X, Y) as input (such that the total size of the secret share of each party is n-bits), and outputs $\mathsf{ROT}^{m/2}$. We shall always normalize so that the total length of the input shares is n-bits.

1.2 Our Contribution

Recall that $\mathcal{F}_m \subset \mathcal{F}$ is the set of all two-party functionalities that have a 2-message protocol in ROT^m-hybrid. We prove the following results.

Theorem 1 (Asymptotically Optimal Secure Computation from Leaky Correlations)**.** *There exists a correlation (R_A, R_B) that produces n-bit secret share such that for all $F \in \mathcal{F}_{m/2}$ there exists a 2-message secure computation protocol for F in the leaky $(R_A, R_B)^{[t]}$ hybrid, where $m = \Theta(n)$ and $t = \Theta(n)$, with exponentially low simulation error.*

The crucial ingredient of Theorem 1 is our new 2-message (n, m, t, ε)-correlation extractor for $\mathsf{ROT}^{n/2}$. We compose the 2-message secure computation protocol for functionalities[4] in $\mathcal{F}_{m/2}$ in the $\mathsf{ROT}^{m/2}$-hybrid with our correlation extractor. Our work presents the first 2-message correlation extractor that has a linear production and a linear leakage resilience (along with exponentially low insecurity).

Theorem 2 (Asymptotically Optimal Correlation Extractor for ROT)**.** *There exists a 2-message (n, m, t, ε)-correlation extractor for $\mathsf{ROT}^{n/2}$ such that $m = \Theta(n)$, $t = \Theta(n)$, and $\varepsilon = \exp(-\Theta(n))$.*

The technical heart of the correlation extractor of Theorem 2 is another correlation extractor (see Theorem 3) for a generalization of the ROT correlation. For any finite field $\mathbb{F}$, the *random oblivious linear-function evaluation* correlation over $\mathbb{F}$ [WW06], represented by $\mathsf{ROLE}(\mathbb{F})$, samples random $a, b, x \in \mathbb{F}$ and defines $r_A = (a, b)$ and $r_B = (x, z)$, where $z = ax + b$. Note that, for $\mathbb{F} = \mathbb{GF}[2]$, we have $(x_0 + x_1)b + x_0 = x_b$; therefore, the $\mathsf{ROLE}(\mathbb{GF}[2])$ correlation is identical to the ROT correlation. One share of the $\mathsf{ROLE}(\mathbb{F})$ correlation has secret share size $2\lg|\mathbb{F}|$. In particular, the correlation $\mathsf{ROLE}(\mathbb{F})^{n/2\lg|\mathbb{F}|}$ provides each party with $n/2\lg|\mathbb{F}|$ independent samples from the $\mathsf{ROLE}(\mathbb{F})$ correlation and the secret share size of each party is n-bits for suitable constant sized field $\mathbb{F}$.

Theorem 3 (Asymptotically Optimal Correlation Extractor for $\mathsf{ROLE}(\mathbb{F})$)**.** *There exists a 2-message (n, m, t, ε)-correlation extractor for $\mathsf{ROLE}(\mathbb{F})^{n/2\lg|\mathbb{F}|}$ such that $m = \Theta(n)$, $t = \Theta(n)$, and $\varepsilon = \exp(-\Theta(n))$.*

In Figure 5, we present our correlation extractor that outputs fresh samples from the same $\mathsf{ROLE}(\mathbb{F})$ correlation. Finally, our construction obtains multiple ROT samples from *each* output $\mathsf{ROLE}(\mathbb{F})$ sample using the OT embedding technique of [BMN17].

Figure 1 positions our contribution vis-à-vis the previous state-of-the-art. In particular, it highlights the fact that our result simultaneously achieves the best qualitative parameters.

[4]We use $\mathcal{F}_{m/2}$ instead of $\mathcal{F}_m$ to be consistent with definition of correlation extractors (Definition 1).

	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}
Our Result	$\mathsf{ROT}^{n/2}$	2	$\Theta(n)$	$\Theta(n)$	$2^{-\Theta(n)}$
	$\mathsf{ROLE}\left(\mathbb{F}\right)^{n/2\lg\lvert\mathbb{F}\rvert}$	2	$\Theta(n)$	$\Theta(n)$	$2^{-\Theta(n)}$

Figure 1: 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 $u_1v_1 + \cdots + u_sv_s = 0$. All correlations have been normalized so that each party gets an n-bit secret share.

Next, we discuss the concrete performance numbers we obtain for Theorem 3 and Theorem 2. For more details and numerical comparison with prior works [IKOS09, GIMS15, BMN17], refer to Section 6.

Performance of Correlation Extractors for $\mathsf{ROLE}(\mathbb{F})$ (Theorem 3). Our correlation extractor for $\mathsf{ROLE}(\mathbb{F})$ relies on the existence of suitable Algebraic Geometry codes[5] over the finite field $\mathbb{F}$, such that $|\mathbb{F}|$ is an even power of a prime and $|\mathbb{F}| \geqslant 49$. We shall use $\mathbb{F}$ that is a finite field with characteristic 2.[6] As the size of the field $\mathbb{F}$ increases, the "quality" of the Algebraic Geometry codes get better. However, the efficiency of the BMN OT embedding protocol [BMN17] used to obtain the output ROT in our construction decreases with increasing $|\mathbb{F}|$. For example, with $\mathbb{F} = \mathbb{GF}[2^{14}]$ we achieve the highest production rate $m/n = 16.32\%$ if the fractional leakage rate is $t/n = 1\%$. Figure 8 in Section 6 summarizes these tradeoffs for various choices of the finite field $\mathbb{F}$.

Performance of Correlation Extractors for ROT (Theorem 2). We know extremely efficient algorithms that use multiplications over $\mathbb{GF}[2]$ to emulate multiplications over any $\mathbb{GF}[2^s]$ [CC87, CÖ10a]. For example, we can use 15 multiplications over $\mathbb{GF}[2]$ to emulate one multiplication over $\mathbb{GF}[2^6]$. Therefore, we can use 15 samples of $\mathsf{ROLE}(\mathbb{GF}[2])$ to perform one $\mathsf{ROLE}(\mathbb{GF}[2^6])$ with perfect semi-honest security. Note that, by applying this protocol, the share sizes reduce by a factor of $6/15$. In general, using this technique, we can convert the leaky ROLE (equivalently, ROT) correlation, into a leaky $\mathsf{ROLE}(\mathbb{F})$ correlation, where $\mathbb{F}$ is a finite field of characteristic 2, by incurring a slight multiplicative loss in the share size. Now, we can apply the correlation extractor for $\mathsf{ROLE}(\mathbb{F})$ discussed above. By optimizing the choice of the field $\mathbb{F}$ (in our case $\mathbb{F} = \mathbb{GF}[2^{10}]$), we can construct a 2-message correlation extractor for ROT that has fractional leakage resilience to $t/n = 1\%$ and achieves

[5] Once the parameters of the Algebraic Geometry code is fixed, it is a one-time investment to construct to construct its generator matrix.

[6] The $\mathsf{ROLE}(\mathbb{F})$ correlation over the field $\mathbb{F}$ of characteristic 2 has a natural bit-representation for its secret shares.

production rate of $m/n = 4.20\%$ (see Figure 9, Section 6). This is several orders of magnitude better than the production and resilience of the IKOS correlation extractor and uses less number of messages.[7]

High Leakage Resilience Setting. Ishai et al. [IMSW14] showed that $t < n/4$ is necessary to extract even one new sample of ROT from the leaky $\mathsf{ROLE}\,(\mathbb{F})^{n/2\lg\mathbb{F}}$ correlation. Our construction, when instantiated with a suitably large constant-size field $\mathbb{F}$, demonstrates that if $t \leqslant (1/4 - g)n$ then we can extract $\Theta(n)$ new samples of the ROT correlation. The prior construction of [GIMS15] only achieves a sub-linear production by using sub-sampling techniques.

Theorem 4 (Near Optimal Resilience with Linear Production)**.** *For every $g \in (0, 1/4]$, there exists a finite field $\mathbb{F}$ with characteristic 2 and a 2-message (n, m, t, ε)-correlation extractor for $(R_A, R_B) = \mathsf{ROLE}\,(\mathbb{F})^{n/2\lg\mathbb{F}}$, where $t = (1/4 - g)n$, $m = \Theta(n)$, and $\varepsilon = \exp(-\Theta(n))$.*

The production $m = \Theta(n)$ relies on the constant g, the gap to optimal fractional resilience. Appendix F proves this result. Section 6 shows that we can achieve linear production even for fractional resilience $t = 0.22n$ using $|\mathbb{F}| = 2^{10}$.

Correlation Extractors for Arbitrary Correlations. Similar to the construction of IKOS, we can also use our construction to construct a correlation extractor from *any* correlation and output samples of *any* correlation; albeit it is not round optimal anymore. However, our construction achieves overall better production and resilience than the IKOS construction because our correlation extractor for ROT has higher production and resilience. Figure 2 outlines a comparison of these two correlation extractor construction for the general case.

1.3 Other Prior Relevant Works

Figure 1 already provides the summary of the current state-of-the-art in correlation extractors. In this section, we summarize works related to combiners; extractors where the adversary is restricted to leaking individual bits of the honest party's secret share. The study of OT combiners was initiated by Harnik et al. [HKN+05]. Since then, there has been work on several variants and extensions of OT combiners [HIKN08, IPS08, MP06, MPW07, PW08]. Recently, Ishai et al. [IMSW14] constructed OT combiners with nearly optimal leakage resilience. Among these works, the most relevant to our paper are the ones by Meier, Przydatek, and Wullschleger [MPW07] and Przydatek, and Wullschleger [PW08]. They use Reed-Solomon codes to construct two-message error-tolerant[8] combiners that produce fresh ROLEs over large fields[9] from ROLEs over the same field. Using multiplication friendly secret sharing schemes based on Algebraic Geometry Codes introduced by Chen and Cramer [CC06],

[7] Even optimistic estimates of the parameters m/n and t/n for the IKOS construction are in the order of 10^{-6}.

[8] An *erroneous sample* from a correlation is a sample (r_A, r_B) that is not in the support of the distribution (R_A, R_B), i.e., it is an incorrect sample. An error-tolerant combiner is a combiner that is secure even if a few of the input samples are erroneous.

[9] The size of the fields increases with n, the size of the secret shares produced by the preprocessing step.

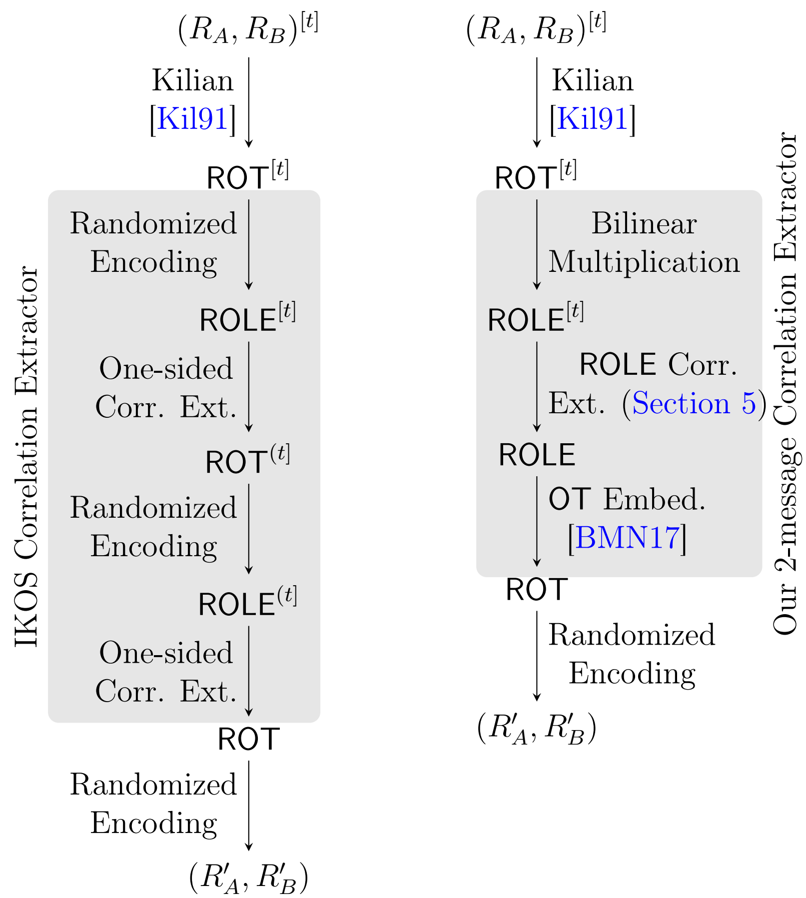

Figure 2: Correlation extractors in the general setting: Extracting arbitrary correlations from arbitrary correlations. Expanded IKOS [IKOS09] correlation extractor to enable efficiency comparison with our correlation extractor of Figure 5. In this figure, to reduce cumbersome notations, it is implicit that there are *multiple samples* of the correlations. The ROLE correlations are over suitable constant size fields. The superscript "$(t]$" represents that the correlation is secure against adversarial leakage of only one party.

a similar construction works over ROLEs over fields with appropriate constant size. We emphasize that this construction is *insecure* if an adversary can perform even 1-bit leakage on the whole secret of the other party. We rely of a family of linear codes instead of a particular choice of the linear code to circumvent this bottleneck. Section 1.4 provides the principal technical ideas underlying our correlation extractor construction.

In the malicious setting, the feasibility result on malicious-secure combiners for ROT is reported in [IPS08]. Recently, Cascudo et al. construct a malicious-secure combiner with high resilience, but $m = 1$ [CDFR17]. The case of malicious-secure correlation extractors remains entirely unexplored.

1.4 Technical Overview

In this section, we provide a high-level summary of the technical ideas underlying the construction of our new correlation extractor. For illustrative purposes, suppose $\mathbb{F}$ is a constant size field with characteristic 2, say $\mathbb{F} = \mathbb{GF}[2^6]$. We fix $(R_A, R_B) = \mathsf{ROLE}(\mathbb{F})^{n/2\lg|\mathbb{F}|}$. Note that each party receives n-bit shares. Suppose we are in the leaky correlation hybrid $(R_A, R_B)^{[t]}$. Our goal is to construct a 2-message correlation extractor that securely computes a sample from the correlation $\mathsf{ROLE}(\mathbb{F})^{m/2\lg|\mathbb{F}|}$.

This correlation extractor relies on the existence of a family of linear codes over $\mathbb{F}$ with suitable properties that we define below. For this discussion, let us assume that $s \in \mathbb{N}$ is the block-length of the codes. Let $\mathcal{J}$ be an index set, and we denote the family of linear codes with block-length s as follows.

$$\mathcal{C} = \{C_j : j \in \mathcal{J}\}$$

This family of code $\mathcal{C}$ needs to have the following properties.

1. **Multiplication Friendly Good Codes.** Each code $C_j \subseteq \mathbb{F}^s$ in the family $\mathcal{C}$ is a *good code*. That is, the rate and distance of every code C_j is $\Theta(s)$. Further, there exists a linear code D_j such that the Schur-product[10] of the codes $C_j * C_j$ is a sub-code of the code D_j, and the distance of D_j is also $\Theta(s)$. Such codes, for instance, are used to perform the multiplication of two secrets by multiplying their respective secret shares in secure computation protocols, hence the name.

2. **Small Bias Family.** Intuitively, a small bias family defines a pseudorandom distribution for linear tests. Let $S = (S_1, \ldots, S_s) \in \mathbb{F}^s$ and its corresponding linear test is defined as $L_S(x_1, \ldots, x_s) := S_1x_1 + \cdots + S_sx_s$. Consider the distribution D of $L_S(c)$ for randomly sampled codeword $c \in C_j$ and an index $j \in \mathcal{J}$. If $\mathcal{C}$ is a family of ρ-biased distributions, then the distribution D has statistical distance at most ρ from the output of $L_S(u)$ for random element $u \in \mathbb{F}^s$. For brevity, we say that the family $\mathcal{C}$ "*ρ-fools* the linear test L_S."

   An interesting property of any linear code $C \subseteq \mathbb{F}^s$ is the following. A random codeword $c \in C$ can 0-fool every linear test L_S such that S is *not* a codeword in the dual of C. However, if S is a codeword in the dual of the code C, then definitely the linear test L_S is not fooled.

   So, a randomly chosen codeword from one fixed linear code cannot fool *all* linear tests. However, when we consider an appropriate family of linear codes, then a randomly chosen codeword from a randomly chosen code in this family can fool *every* linear test.

The construction of such a family of codes over small finite fields $\mathbb{F}$ is of potential independent interest. Our starting point is an explicit Algebraic Geometry code $C \subseteq \mathbb{F}^s$ that is multiplication friendly [GS96]. Given one such code C, we randomly "twist then permute" the code to define the family $\mathcal{C}$. We emphasize that the production of our correlation extractor relies on the bias being small. So, it is extremely crucial to construct a family with extremely small bias. Next, we describe our "twist then permute" operation.

[10] Consider a linear code $C \subseteq \mathbb{F}^s$. Let $c = (c_1, \ldots, c_s)$ and $c' = (c'_1, \ldots, c'_s)$ be two codewords in the code C. We define $c * c' = (c_1c'_1, \ldots, c_sc'_s) \in \mathbb{F}^s$. The Schur-product $C * C$ is defined to be the set of all $c * c'$ such that $c, c' \in C$.

Twist then Permute. Suppose $C \subseteq \mathbb{F}^s$ is a linear code. Pick any $\lambda = (\lambda_1, \ldots, \lambda_s) \in (\mathbb{F}^*)^s$. Note that we do not include $0 \in \mathbb{F}$ in any of the coordinates. A λ-twist of the code C is defined as the following linear code

$$C_\lambda := \{(\lambda_1 c_1, \ldots, \lambda_s c_s) \colon (c_1, \ldots, c_s) \in C\}$$

Let $\pi \colon \{1, \ldots, s\} \to \{1, \ldots, s\}$ be a permutation. The π-permutation of the λ-twist of C is defined as the following linear code

$$C_{\pi,\lambda} := \{\left(\lambda_{\pi(1)} c_{\pi(1)}, \ldots, \lambda_{\pi(s)} c_{\pi(s)}\right) : (c_1, \ldots, c_s) \in C\}$$

Define $\mathcal{J}$ as the set of all (π, λ) such that $\lambda \in (\mathbb{F}^*)^s$ and π is a permutation over the set $\{1, \ldots, s\}$. Note that for our particular choice of C, the code $C_{\pi,\lambda}$ continues to be multiplication friendly good code. A key observation towards demonstrating that $\mathcal{C}$ is a family of small bias distributions is that the following two distributions are identical (see Claim 2).

1. Fix $S \in \mathbb{F}^s$. The output distribution of the linear test L_S on a random codeword $c \in C_j$, for a random index $j \in \mathcal{J}$.
2. Let $T \in \mathbb{F}^s$ be a random element of the same weight as S.[11] The output distribution of the linear test L_T on a random codeword $c \in C$.

Based on this observation, we can calculate the bias of the family of our codes. Note that there are a total of $\binom{s}{w}(q-1)^w$ elements in $\mathbb{F}^s$ that have weight w. Let A_w denote the number of codewords in the dual of C that have weight w. Our family of codes $\mathcal{C}$ fools the linear test L_S with $\rho = A_w \cdot \binom{s}{w}^{-1} (q-1)^{-w}$, where w is the weight of $S \in \mathbb{F}^s$.

We obtain precise asymptotic bounds on the weight enumerator $\{A_w \colon w \in \{0, 1, \ldots, s\}\}$ of the dual of the code C to estimate the bias ρ. This precise bound translates into higher production m, higher resilience t, and exponentially low simulation error ε of our correlation extractor.

We remark that if C has a small dual-distance, then the bias cannot be small. So, the restriction that the dual distance of C is linear in the block-length is a manifestation of ensuring the small-bias property.

Remark. The performance of the code C supersedes the elementary Gilbert-Varshamov bound. These Algebraic Geometry codes are one of the few codes in mathematics and computer science where explicit constructions have significantly better quality than elementary randomized constructions. So, elementary randomization techniques are unlikely to produce any (qualitatively) better parameters for this approach, given that the estimations of the weight enumerator in this work are asymptotically optimal. Therefore, finding *better techniques* to construct the family of multiplication friendly good codes that is also a family of small-bias distributions is the research direction that has the potential to reduce the bias. This reduction in the bias can further improve the production and leakage resilience of our correlation extractors.

[11] The weight of $S \in \mathbb{F}^s$ is defined as the number of non-zero elements in S.

2 Preliminaries

Symbolic Notations. We denote random variables by capital letters, for example X, and the values taken by small letters, for example $X = x$. For a positive integer n, we write $[n]$ and $[-n]$ to denote the sets $\{1, \dots, n\}$ and $\{-n, \dots, -1\}$, respectively. Let $\mathcal{S}_n$ be the set of all permutations $\pi : [n] \to [n]$. We consider the field $\mathbb{F} = \mathbb{GF}[q]$, where $q = p^a$, for a positive integer a and prime p. For any $c = (c_1, \dots, c_\eta) \in \mathbb{F}^\eta$, define the function $\mathsf{wt}(c)$ as the cardinality of the set $\{i : c_i \neq 0\}$. For any two $x, y \in \mathbb{F}^\eta$, let $x * y$ represent the point-wise product of x and y. That is, $x * y = (x_1y_1, x_2y_2, \dots, x_\eta y_\eta) \in \mathbb{F}^\eta$. For a set Y, U_Y denotes the uniform distribution on the set Y.

2.1 Correlation Extractors

We denote the functionality of 2-choose-1 bit Oblivious Transfer as OT and Oblivious Linear-function Evaluation over a field $\mathbb{F}$ as $\mathsf{OLE}(\mathbb{F})$. Also, we denote the Random Oblivious Transfer Correlation as ROT and Random Oblivious Linear-function Evaluation over field $\mathbb{F}$ as $\mathsf{ROLE}(\mathbb{F})$. When $\mathbb{F} = \mathbb{GF}[2]$, we denote $\mathsf{ROLE}(\mathbb{F})$ by ROLE. For completeness, we define these formally in Appendix A.

Let η be such that $2\eta \lg |\mathbb{F}| = n$. In this work, we consider the setting when Alice and Bob start with η samples of the $\mathsf{ROLE}(\mathbb{F})$ correlation and the adversary performs t bits of leakage. We give a secure protocol for extracting multiple secure OTs in this hybrid. Below we define such an correlation extractor formally using initial $\mathsf{ROLE}(\mathbb{F})$ correlations.

Leakage model. We define our leakage model for $\mathsf{ROLE}(\mathbb{F})$ correlations as follows:

1. **η-Random OLE correlation generation phase.** Alice gets $r_A = \{(a_i, b_i)\}_{i \in [\eta]} \in \mathbb{F}^{2\eta}$ and Bob gets $r_B = \{(x_i, z_i)\}_{i \in [\eta]} \in \mathbb{F}^{2\eta}$ such that for all $i \in [\eta]$, a_i, b_i, x_i is uniformly random and $z_i = a_i x_i + b_i$. Note that the size of secret share of each party is n bits.

2. **Corruption and leakage phase.** A semi-honest adversary corrupts either the sender and sends a leakage function $L : \mathbb{F}^\eta \to \{0,1\}^t$ and gets back $L(x_{[\eta]})$. Or, it corrupts the receiver and sends a leakage function $L : \mathbb{F}^\eta \to \{0,1\}^t$ and gets back $L(a_{[\eta]})$. Note that w.l.o.g. any leakage on the sender (resp., receiver) can be seen as a leakage on $a_{[\eta]}$ (resp., $x_{[\eta]}$).

We denote by (R_A, R_B) the above correlated randomness and by $(R_A, R_B)^{[t]}$ its t-leaky version. Recall the definition for (n, m, t, ε)-correlation extractor (see Definition 1, Section 1.1). Below, we give the correctness and security requirements.

The *correctness* condition says that the receiver's output is correct in all $m/2$ instances of ROT. The *privacy* requirement says the following: Let $(s_0^{(i)}, s_1^{(i)})$ and $(c^{(i)}, z^{(i)})$ be the output shares of Alice and Bob, respectively, in the i^{th} ROT instance. Then a corrupt sender (resp., receiver) cannot distinguish between $\{c^{(i)}\}_{i \in [m/2]}$ (resp., $\left\{s_{1-c^{(i)}}^{(i)}\right\}_{i \in [m/2]}$) and $r \xleftarrow{\$} \{0,1\}^{m/2}$ with advantage more than ε. The *leakage rate* is defined as t/n and the *production rate* is defined as m/n.

Our main sub-protocol for Theorem 3 shall take $\mathsf{ROLE}(\mathbb{F})$ as initial correlations and produces secure $\mathsf{ROLE}(\mathbb{F})$. Towards this, we define a $\mathsf{ROLE}(\mathbb{F})$-to-$\mathsf{ROLE}(\mathbb{F})$ extractor formally below.

Definition 2 ($(\eta,\gamma,t,\varepsilon)$-$\mathsf{ROLE}(\mathbb{F})$-to-$\mathsf{ROLE}(\mathbb{F})$ extractor)**.** *Let $(R_A, R_B) = (\mathsf{ROLE}(\mathbb{F}))^\eta$ be correlated randomness. An $(\eta,\gamma,t,\varepsilon)$-$\mathsf{ROLE}(\mathbb{F})$-to-$\mathsf{ROLE}(\mathbb{F})$ extractor is a two-party interactive protocol in the $(R_A, R_B)^{[t]}$ hybrid that securely implements the $(\mathsf{ROLE}(\mathbb{F}))^\gamma$ functionality against information-theoretic semi-honest adversaries with ε simulation error.*

Let $(u_i, v_i) \in \mathbb{F}^2$ and $(r_i, z_i) \in \mathbb{F}^2$ be the shares of Alice and Bob, respectively, in the i^{th} output ROLE instance. The *correctness* condition says that the receiver's output is correct in all γ instances of ROLE, i.e., $z_i = u_i r_i + v_i$ for all $i \in [\gamma]$. The *privacy* requirement says the following: A corrupt sender (resp., receiver) cannot distinguish between $\{r_i\}_{i\in[\gamma]}$ (resp., $\{u_i\}_{i\in[\gamma]}$) and $U_{\mathbb{F}^\gamma}$ with advantage more than ε.

2.2 Fourier Analysis over Fields

We follow the conventions of [Rao07]. To begin discussion of Fourier analysis, let η be any positive integer and let $\mathbb{F}$ be any finite field. We define the *inner product* of two complex functions.

Definition 3 (Inner Product)**.** *Let $f, g \colon \mathbb{F}^\eta \to \mathbb{C}$. We define the* inner product *of f and g as*

$$\langle f, g\rangle := \mathop{\mathbb{E}}_{x \xleftarrow{\$} \mathbb{F}^\eta}\left[f(x)\cdot \overline{g(x)}\right] = \frac{1}{|\mathbb{F}|^\eta}\sum_{x\in\mathbb{F}^\eta} f(x)\cdot\overline{g(x)},$$

where $\overline{g(x)}$ is the complex conjugate of $g(x)$.

Next, we define general *character functions* for both $\mathbb{F}$ and $\mathbb{F}^\eta$.

Definition 4 (General Character Functions)**.** *Let $\psi\colon \mathbb{F}\to\mathbb{C}^*$ be a group homomorphism from the additive group $\mathbb{F}$ and the multiplicative group $\mathbb{C}^*$. Then we say that ψ is a* character function *of $\mathbb{F}$.*

Let $\chi\colon \mathbb{F}^\eta\times\mathbb{F}^\eta \to \mathbb{C}^*$ be a bilinear, non-degenerate, and symmetric map defined as $\chi(x,y) = \psi(x\cdot y) = \psi(\sum_i x_i y_i)$. Then, for any $S\in\mathbb{F}^\eta$, the function $\chi(S,\cdot) := \chi_S(\cdot)$ is a character function *of $\mathbb{F}^\eta$.*

Given χ, we have the *Fourier Transformation.*

Definition 5 (Fourier Transformation)**.** *For any $S\in\mathbb{F}^\eta$, let $f\colon\mathbb{F}^\eta\to\mathbb{C}$ and χ_S be a character function. We define the map $\widehat{f}\colon\mathbb{F}^\eta\to\mathbb{C}$ as $\widehat{f}(S) := \langle f,\chi_S\rangle$. We say that $\widehat{f}(S)$ is a* Fourier Coefficient *of f at S and the linear map $f\mapsto\widehat{f}$ is the* Fourier Transformation of *f.*

Note that this transformation is an invertible linear map. The Fourier inversion formula is given by the following lemma.

Lemma 1 (Fourier Inversion)**.** *For any function $f\colon\mathbb{F}^\eta\to\mathbb{C}$, we can write $f(x) = \sum_{S\in\mathbb{F}^\eta}\widehat{f}(S)\chi_S(x)$.*

For completeness, we provide the relevant proofs related to Fourier analysis over fields in Appendix B.

2.3 Distributions and Min-Entropy

For a probability distribution X over a sample space U, entropy of $x \in X$ is defined as $H_X(x) = -\lg \Pr[X = x]$. The min-entropy of X, represented by $\mathbf{H}_\infty(X)$, is defined to be $\min_{x \in \mathsf{Supp}(X)} H_X(x)$. The binary entropy function, denoted by $\mathbf{h_2}(x) = -x \lg x - (1-x)\lg(1-x)$ for every $x \in (0,1)$.

Given a joint distribution (X, Y) over sample space $U \times V$, the marginal distribution Y is a distribution over sample space V such that, for any $y \in V$, the probability assigned to y is $\sum_{x \in U} \Pr[X = x, Y = y]$. The conditional distribution $(X|y)$ represents the distribution over sample space U such that the probability of $x \in U$ is $\Pr[X = x | Y = y]$. The average min-entropy [DORS08], represented by $\widetilde{\mathbf{H}}_\infty(X|Y)$, is defined to be $-\lg \mathbb{E}_{y \sim Y}[2^{-\mathbf{H}_\infty(X|y)}]$.

Lemma 2 ([DORS08])**.** *If $\mathbf{H}_\infty(X) \geqslant k$ and L is an arbitrary ℓ-bit leakage on X, then $\widetilde{\mathbf{H}}_\infty(X|L) \geqslant k - \ell$.*

Lemma 3 (Fourier Coefficients of a Min-Entropy Distribution)**.** *Let $X \colon \mathbb{F}^\eta \to \mathbb{R}$ be a min-entropy source such that $\mathbf{H}_\infty(X) \geqslant k$. Then*

$$\sum_S |\widehat{X}(S)|^2 \leqslant \frac{1}{|\mathbb{F}|^\eta \, 2^k}$$

We provide the proof of Lemma 3 in Appendix B.

2.4 Family of Small-Bias Distributions

Definition 6 (Bias of a Distribution)**.** *Let X be a distribution over $\mathbb{F}^\eta$. Then the* bias *of X with respect to $S \in \mathbb{F}^\eta$ is defined as $\mathsf{Bias}_S(X) := |\mathbb{F}|^\eta \cdot |\widehat{X}(S)|$.*

Dodis and Smith [DS05] defined small-bias distribution family for distributions over $\{0,1\}^\eta$. We generalize it naturally for distributions over $\mathbb{F}^\eta$.

Definition 7 (Small-bias distribution family)**.** *A family of distributions $\mathcal{F} = \{F_1, F_2, \cdots, F_k\}$ over sample space $\mathbb{F}^\eta$ is called a ρ^2-biased family if for every non-zero vector $S \in \mathbb{F}^\eta$ following holds.*

$$\mathop{\mathbb{E}}_{i \xleftarrow{\$} [k]} \mathsf{Bias}_S(F_i)^2 \leqslant \rho^2$$

Following extraction lemma was proven in previous works over $\{0,1\}^\eta$.

Lemma 4 ([NN90, AR94, GW97, DS05])**.** *Let $\mathcal{F} = \{F_1, \ldots, F_\mu\}$ be ρ^2-biased family of distributions over the sample space $\{0,1\}^\eta$. Let (M, L) be a joint distribution such that the marginal distribution M is over $\{0,1\}^\eta$ and $\widetilde{\mathbf{H}}_\infty(M|L) \geqslant m$. Then, the following holds: Let J be a uniform distribution over $[\mu]$.*

$$\mathrm{SD}\left(\, (F_J \oplus M, L, J) \, , \, \left(U_{\{0,1\}^\eta}, L, J\right) \, \right) \leqslant \frac{\rho}{2} \left(\frac{2^\eta}{2^m} \right)^{1/2}$$

A natural generalization of above lemma for distributions over $\mathbb{F}^\eta$ gives the following.

Theorem 5 (Min-entropy extraction via masking with small-bias distributions)**.** *Let $\mathcal{F} = \{F_1, \ldots, F_\mu\}$ be a ρ^2-biased family of distributions over the sample space $\mathbb{F}^\eta$ for field $\mathbb{F}$ of size q. Let (M, L) be a joint distribution such that the marginal distribution M is over $\mathbb{F}^\eta$ and $\widetilde{\mathbf{H}}_\infty(M|L) \geqslant m$. Then, the following holds: Let J be a uniform distribution over $[\mu]$.*

$$\mathrm{SD}\left(\ (F_J \oplus M, L, J) \ , \ (U_{\mathbb{F}^\eta}, L, J) \ \right) \leqslant \frac{\rho}{2} \left(\frac{|\mathbb{F}|^\eta}{2^m} \right)^{1/2}$$

For completeness, we give the proof of the above in Appendix G.

2.5 Distribution over Linear Codes

Let $C = [\eta, \kappa, d, d^\perp, d^{(2)}]_\mathbb{F}$ be a linear code over $\mathbb{F}$ with generator matrix $G \in \mathbb{F}^{\kappa \times \eta}$. We also use C to denote the uniform distribution over codewords generated by G. For any $\pi \in \mathcal{S}_\eta$, define $G_\pi = \pi(G)$ as the generator matrix obtained by permuting the columns of G under π.

The **dual code** of C, represented by $C^\perp$, is the set of all codewords that are orthogonal to every codeword in C. That is, for any $c^\perp \in C^\perp$, it holds that $\langle c, c^\perp \rangle = 0$ for all $c \in C$. Let $H \in \mathbb{F}^{(\eta-\kappa)\times\eta}$ be a generator matrix of $C^\perp$. The distance of $C^\perp$ is $d^\perp$.

The **Schur product code** of C, represented by $C^{(2)}$, is the set of all codewords obtained as a Schur product of codewords in C. That is, $C^{(2)} = C * C := \{c * c' \colon c, c' \in C\} \subseteq \mathbb{F}^\eta$, where $c * c'$ denotes the coordinate-wise product of c and c'. The distance of $C^{(2)}$ is $d^{(2)}$.

3 Family of Small-bias distributions with erasure recovery

In this section, we give our construction of the family of small-bias distributions $\{C_j\}_{j \in \mathcal{J}}$ such that each C_j is a linear code and $C_j * C_j$ supports erasure recovery. We formally define the requirements for this family of distributions in Property 1. Next, our construction of such a family is formally described in Figure 3. We prove our construction satisfies Property 1 in Theorem 6.

Property 1. *A family of linear code distributions $\mathcal{C} = \{C_j \colon j \in \mathcal{J}\}$ over $\mathbb{F}^{\eta^*}$ satisfy this property with parameters δ and γ if the following conditions hold.*

1. $2^{-\delta}$***-bias family of distributions****. For any $0^{\eta^*} \neq S \in \mathbb{F}^{\eta^*}$, the following holds for $\rho^2 = 2^{-\delta}$.*

$$\mathop{\mathbb{E}}_{j \xleftarrow{\$} \mathcal{J}} \left[\mathsf{Bias}_S(C_j)^2 \right] \leqslant \rho^2 = \frac{1}{2^\delta}$$

2. γ***-erasure recovery in Schur Product****. For all $j \in \mathcal{J}$, the Schur product code of C_j, that is $C_j * C_j = C_j^{(2)}$, supports erasure recovery the first γ coordinates. Moreover, the first γ-coordinates of C_j and $C_j^{(2)}$ are linearly independent of each other.*

3.1 Our Construction

Family of small-bias distributions with erasure recovery in the product distribution:

Fix a linear code $C = [\eta^*, \kappa, d, d^\perp, d^{(2)}]_\mathbb{F}$ with generator matrix $G \in \mathbb{F}^{\kappa\times\eta^*}$, where $|\mathbb{F}| = q$ and $\kappa \geqslant d^{(2)}$. Let γ be a fixed natural number (to be determined later during parameter setting in Appendix E and Section 6) such that $C * C$ supports γ-erasure recovery. We construct the family of small-bias distributions $\{C_{\pi,\lambda} \colon \pi \in \mathcal{S}_{\eta^*},\ \lambda \in (\mathbb{F}^*)^{\eta^*}\}$ over $\mathbb{F}^{\eta^*}$ as follows.

1. Let $\lambda \in (\mathbb{F}^*)^{\eta^*}$. Define $G_\lambda = [\lambda_1 G_1, \ldots, \lambda_{\eta^*} G_{\eta^*}] \in \mathbb{F}^{\kappa\times\eta^*}$, where G_i is the i^{th} column of G and $\lambda_i G_i$ the multiplication of G_i by $\lambda_i \in \mathbb{F}^*$.
2. Let $\pi \in \mathcal{S}_{\eta^*}$. Define $G_{\pi,\lambda} = \pi(G_\lambda) \in \mathbb{F}^{\kappa\times\eta^*}$, where $\pi(G_\lambda)$ is the permutation of the columns of G_λ according to permutation π. Then $C_{\pi,\lambda}$ is the uniform distribution over the linear code generated by $G_{\pi,\lambda}$.

$(\mathsf{Enc}, \mathsf{Dec})$ for $C_{\pi,\lambda}$: Let $(\mathsf{Enc}_C, \mathsf{Dec}_C)$ be the Encoder and Decoder for the linear code C.

- $\mathsf{Enc}(m)$: Compute $c = (c_1, \ldots, c_{\eta^*}) = \mathsf{Enc}_C(m)$. Compute $c * \lambda = (\lambda_1 c_1, \ldots, \lambda_{\eta^*} c_{\eta^*})$. Output $\pi(c * \lambda)$.
- $\mathsf{Dec}(x)$: Compute $c' = (c'_1, \ldots, c'_{\eta^*}) = \pi^{-1}(x)$. Compute $c' * \lambda' = (\lambda_1^{-1} c'_1, \ldots, \lambda_{\eta^*}^{-1} c'_{\eta^*})$. Output $\mathsf{Dec}_C(c' * \lambda')$.

$(\mathsf{Enc}, \mathsf{Dec})$ for $(C_{\pi,\lambda} * C_{\pi,\lambda})$: Let $(\mathsf{Enc}_{C^{(2)}}, \mathsf{Dec}_{C^{(2)}})$ be the Encoder and Decoder for the linear code $C^{(2)} = C * C$.

- $\mathsf{Enc}(m)$: Compute $c = (c_1, \ldots, c_{\eta^*}) = \mathsf{Enc}_{C^{(2)}}(m)$. Compute $c * \lambda * \lambda = (\lambda_1^2 c_1, \ldots, \lambda_{\eta^*}^2 c_{\eta^*})$. Output $\pi(c * \lambda * \lambda)$.
- $\mathsf{Dec}(x)$: Compute $c' = (c'_1, \ldots, c'_{\eta^*}) = \pi^{-1}(x)$. Compute $c' * \lambda' * \lambda' = (\lambda_1^{-2} c'_1, \ldots, \lambda_{\eta^*}^{-2} c'_{\eta^*})$. Output $\mathsf{Dec}_{C^{(2)}}(c' * \lambda' * \lambda')$.

Figure 3: Our Construction of a Family of Small Bias Linear Code Distributions.

Theorem 6. *The family of linear code distributions $\{C_{\pi,\lambda} \colon \pi \in \mathcal{S}_{\eta^*},\ \lambda \in (\mathbb{F}^*)^{\eta^*}\}$ over $\mathbb{F}^{\eta^*}$ given in Figure 3 satisfies Property 1 for any $\gamma < d^{(2)}$, where $d^{(2)}$ is the distance of the Schur product code of $C^{(2)}$, and*

$$\delta = \left(d^\perp + \frac{\eta^*}{\sqrt{q}-1} - 1\right)\left(\lg(q-1) - \mathbf{h_2}\left(\frac{1}{q+1}\right)\right) - \frac{\eta^*}{\sqrt{q}-1}\lg q$$

where $\mathbf{h_2}$ denotes the binary entropy function.

Proof. We first prove erasure recovery followed by the small-bias property.

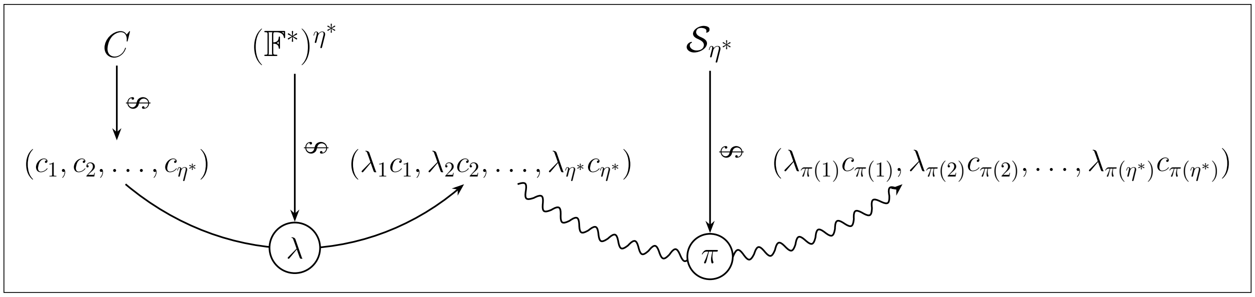

Figure 4: A pictorial outline of our "twist then permute" operation.

γ-erasure recovery in Schur Product code. First we note that permuting or reordering the columns of a generator matrix does not change its distance, distance of the Schur product, or its capability of erasure recovery (as long as we know the mapping of new columns vis-à-vis old columns). Let $\mathcal{I}_\gamma = \{i_1, \ldots, i_\gamma\}$ be the indices of the erased coordinates of codeword in $C^{(2)}_{\pi,\lambda}$. Hence to show erasure recovery of the coordinates $\mathcal{I}_\gamma$ of a codeword of $C^{(2)}_{\pi,\lambda}$, it suffices to show erasure recovery of the γ erased coordinates $\mathcal{J}_\gamma = \{j_1, \ldots, j_\gamma\}$ of a codeword of $C^{(2)}_\lambda$, where C_λ is the uniform codespace generated by G_λ, and $\pi(j_k) = i_k$ for every $k \in [\gamma]$.

Note that since $\gamma < d^{(2)}$, the code $C^{(2)}$ supports erasure recovery of *any* γ coordinates. Thus it suffices to show that this implies that $C^{(2)}_\lambda$ also supports the erasure recovery of *any* γ coordinates. Note that since $\lambda \in (\mathbb{F}^*)^{\eta^*}$, multiplication of the columns of G according to λ does not change its distance or distance of the Schur product. Then we do the following to perform erasure recovery of γ coordinates in $C^{(2)}_\lambda$. Let $c^{(2)} \in C^{(2)}_\lambda$ be a codeword with erased coordinate $\mathcal{J}_\gamma = \{j_1, \ldots, j_\gamma\}$, and let $\mathcal{J}_\eta = \{j'_1, \ldots, j'_\eta\}$ be the coordinates of $c^{(2)}$ that have not been erased. For every $j \in \mathcal{J}_\eta$, compute $c_j = (\lambda_j^{-1})^2 c_j^{(2)}$. Then the vector $(c_j)_{j \in \mathcal{J}_\eta}$ is a codeword of $C^{(2)}$ with coordinates c_i erased for $i \in \mathcal{J}_\gamma$. Since $C^{(2)}$ has γ erasure recovery, we can recover the c_i for $i \in \mathcal{J}_\gamma$. Once recovered, for every $i \in \mathcal{J}_\gamma$, compute $c_i^{(2)} = \lambda_i^2 c_i$. This produces the γ erased coordinates of $c^{(2)}$ in $C^{(2)}_\lambda$. Finally, one can map the $c_i^{(2)}$ for $i \in \mathcal{J}_\gamma$ to the coordinates $\mathcal{I}_\gamma$ using π, recovering the erasures in $C^{(2)}_{\pi,\lambda}$.

$2^{-\delta}$-bias family of distributions. Let $C, C_\lambda, C_{\pi,\lambda}$ be the uniform distribution over the linear codes generated by $G, G_\lambda, G_{\pi,\lambda}$, respectively. Recall that $d^\perp$ is the dual distance for C. Note that $C_\lambda, C_{\pi,\lambda}$ have dual-distance $d^\perp$ as well. Let $\eta^* = \eta + \gamma$. Since $\mathsf{Bias}_S(C_{\pi,\lambda}) = |\mathbb{F}|^{\eta^*} |\widehat{C_{\pi,\lambda}}|$ for every $S \in \mathbb{F}^{\eta^*}$, it suffices to show that

$$\mathop{\mathbb{E}}_{\pi,\lambda}\left[\widehat{C_{\pi,\lambda}}(S)^2\right] \leqslant \frac{1}{|\mathbb{F}|^{2\eta^*} \cdot 2^\delta}.$$

To begin, we first give an equivalent definition of $C_{\pi,\lambda}$:

$$C_{\pi,\lambda} := \{\pi(\lambda_1 c_1, \ldots, \lambda_{\eta^*} c_{\eta^*}) \mid (c_1, \ldots, c_{\eta^*}) \in C\}.$$

Next, given any $S \in \mathbb{F}^{\eta^*}$, define

$$\mathcal{S}(S) := \{\pi(\lambda_1 S_1, \ldots, \lambda_{\eta^*} S_{\eta^*}) \in \mathbb{F}^{\eta^*} \mid \forall \pi \in \mathcal{S}_{\eta^*} \wedge \lambda \in (\mathbb{F}^*)^{\eta^*}\}$$

Note that $\mathcal{S}(S)$ is equivalently characterized as

$$\mathcal{S}(S) = \{T = (T_1, \dots, T_{\eta^*}) \in \mathbb{F}^{\eta^*} \mid \mathsf{wt}(T) = \mathsf{wt}(S)\}.$$

It is easy to see that $|\mathcal{S}(S)| = \binom{\eta^*}{w_0}(q-1)^{\eta^*-w_0}$, where $w_0 = \eta^* - \mathsf{wt}(S)$; i.e., w_0 is the number of zeros in S. We prove the following claim.

Claim 1. *For any $S \in \mathbb{F}^{\eta^*}$, we have $\widehat{C_{\pi,\lambda}}(S) = \widehat{C}(\pi^{-1}(S) * \lambda)$.*

Proof. Notice that by definition for any $x \in C_{\pi,\lambda}$, we have $C_{\pi,\lambda}(x) = C(c)$ since $x = \pi(\lambda_1 c_1, \dots, \lambda_{\eta^*} c_{\eta^*})$ for $c \in C$. This is equivalently stated as $C_{\pi,\lambda}(\pi(c * \lambda)) = C(c)$. For $x = \pi(\lambda_1 y_1, \dots, \lambda_{\eta^*} y_{\eta^*}) \in \mathbb{F}^{\eta^*}$ and any $S \in \mathbb{F}^{\eta^*}$, we have

$$S \cdot x = \sum_{i=1}^{\eta^*} S_i x_i = \sum_{i=1}^{\eta^*} S_i(\lambda_{\pi(i)} y_{\pi(i)}) = \sum_{i=1}^{\eta^*} (S_{\pi^{-1}(i)})\lambda_i y_i = (\pi^{-1}(S) * \lambda) \cdot y.$$

where $S \cdot x$ is the vector dot product. By definition of $\chi_S(x)$, this implies $\chi_S(x) = \chi_y(\pi^{-1}(S) * \lambda)$. Using these two facts and working directly from the definition of Fourier Transform, we have

$$\begin{aligned}
\widehat{C_{\pi,\lambda}}(S) &= \frac{1}{|\mathbb{F}|^{\eta^*}} \sum_{x \in \mathbb{F}^{\eta^*}} C_{\pi,\lambda}(x)\overline{\chi_S(x)} \\
&= \frac{1}{|\mathbb{F}|^{\eta^*}} \sum_{c \in \mathbb{F}^{\eta^*}} C_{\pi,\lambda}(\pi(\lambda_1 c_1, \dots, \lambda_{\eta^*} c_{\eta^*}))\overline{\chi_S(\pi(\lambda_1 c_1, \dots, \lambda_{\eta^*} c_{\eta^*}))} \\
&= \frac{1}{|\mathbb{F}|^{\eta^*}} \sum_{c \in \mathbb{F}^{\eta^*}} C(c)\overline{\chi_c(\pi^{-1}(S) * \lambda)} = \widehat{C}(\pi^{-1}(S) * \lambda). \qquad \square
\end{aligned}$$

It is easy to see that $\mathsf{wt}(\pi^{-1}(S) * \lambda) = \mathsf{wt}(S)$, so $(\pi^{-1}(S) * \lambda) = T \in \mathcal{S}(S)$. From this fact and Claim 1, we prove the following claim.

Claim 2. *For any $S \in \mathbb{F}^n$, $\mathbb{E}_{\pi,\lambda}\left[\widehat{C_{\pi,\lambda}}(S)^2\right] = \mathbb{E}_{T \xleftarrow{\$} \mathcal{S}(S)}\left[\widehat{C}(T)^2\right]$.*

Proof. Suppose we have codeword $x \in C_{\pi,\lambda}$ such that $\pi(\lambda_1 c_1, \dots, \lambda_\eta^* c_\eta^*) = x$, for some codeword $c \in C$. Let $\{i_1, \dots, i_{w_0}\}$ be the set of indices of 0 in c; that is, $c_j = 0$ for all $j \in \{i_1, \dots, i_{w_0}\}$. Then for any permutation π, the set $\{\pi(i_0), \dots, \pi(i_{w_0})\}$ is the set of zero indices in x. Note also that for any index $j \notin \{\pi(i_0), \dots, \pi(i_{w_0})\}$, we have $x_j \neq 0$. If this was not the case, then we have $x_j = c_{\pi^{-1}(j)}\lambda_{\pi^{-1}(j)} = 0$. Since $j \notin \{\pi(i_0), \dots, \pi(i_{w_0})\}$, this implies $\pi^{-1}(j) \notin \{i_0, \dots, i_{w_0}\}$, which further implies that $c_{\pi^{-1}(j)} \neq 0$. This is a contradiction since $\lambda \in (\mathbb{F}^*)^{\eta^*}$. Thus any permutation π must map the zeros of S to the zeross of c, and there are $w_0!(\eta^* - w_0)!$ such permutations. Notice now that for any $c_k = 0$, λ_k can take any value in $\mathbb{F}^*$, so we have $(q-1)^{w_0}$ such choices. Furthermore, if $c_k \neq 0$ and $\lambda_k c_k = x_{\pi^{-1}(k)} \neq 0$, then there is exactly one $\lambda_k \in \mathbb{F}^*$ which satisfies this equation. Putting it all together, we have

$$\begin{aligned}
\mathop{\mathbb{E}}_{\pi,\lambda}\left[\widehat{C_{\pi,\lambda}}(S)^2\right] &= \frac{1}{\eta^*!(q-1)^{\eta^*}}\sum_{\pi,\lambda}\widehat{C_{\pi,\lambda}}(S)^2 \\
&= \frac{1}{\eta^*!(q-1)^{\eta^*}}\sum_{\pi,\lambda}\widehat{C}\left(\pi^{-1}(S)*\lambda\right)^2 && \text{[by Claim 1]} \\
&= \frac{(w_0!(\eta^*-w_0)!(q-1)^{w_0})}{\eta^*!(q-1)^{\eta^*}}\sum_{T\in\mathcal{S}(S)}\widehat{C}(T)^2 \\
&= \frac{w_0!(\eta^*-w_0)!}{\eta^*!(q-1)^{\eta^*-w_0}}\sum_{T\in\mathcal{S}(S)}\widehat{C}(T)^2 \\
&= \left(\binom{\eta^*}{w_0}(q-1)^{\eta^*-w_0}\right)^{-1}\sum_{T\in\mathcal{S}(S)}\widehat{C}(T)^2 \\
&= \mathop{\mathbb{E}}_{T\xleftarrow{\$}\mathcal{S}(S)}\left[\widehat{C}(T)^2\right]. && \square
\end{aligned}$$

With Claim 2, we now are interested in finding δ such that for $0^{\eta^*} \neq S \in \mathbb{F}^{\eta^*}$

$$\mathop{\mathbb{E}}_{T\xleftarrow{\$}\mathcal{S}(S)}\left[\widehat{C}(T)^2\right] \leqslant \frac{1}{|\mathbb{F}|^{2\eta^*}2^{\delta}}.$$

We first note that since C is a linear code, C has non-zero Fourier coefficients only at codewords in $C^\perp$. For completeness, we provide the proof in Appendix B.1.

Claim 3. *For all* $S \in \mathbb{F}^{\eta^*}$, $\widehat{C}(S) = \begin{cases} \frac{1}{|\mathbb{F}|^{\eta^*}} & S \in C^\perp \\ 0 & \textit{otherwise} \end{cases}$

Let $A_w = |C^\perp \cap \mathcal{S}(S)|$, where $w = \eta^* - w_0 = \mathsf{wt}(S)$. Intuitively, A_w is the number of codewords in $C^\perp$ with weight w. Then from Claim 3, we have

$$\mathop{\mathbb{E}}_{T\xleftarrow{\$}\mathcal{S}(S)}\left[\widehat{C}(T)^2\right] = \frac{|C^\perp \cap \mathcal{S}(S)|}{|\mathbb{F}|^{2\eta^*}\binom{\eta^*}{\eta^*-\mathsf{wt}(S)}(q-1)^{\mathsf{wt}(S)}} = \frac{A_w}{|\mathbb{F}|^{2\eta^*}\binom{\eta^*}{w}(q-1)^w}$$

Now, our goal is to upper bound A_w. Towards this goal, the weight enumerator for the code $C^\perp$ is defined as the following polynomial.

$$W_{C^\perp}(x) = \sum_{c\in C^\perp} x^{\eta^*-\mathsf{wt}(c)}$$

This polynomial can equivalently be written in the following manner.

$$W_{C^\perp}(x) = \sum_{w\in\{0,\ldots,\eta^*\}} A_w x^{\eta^*-w}$$

Define $a = \eta^* - d^\perp$.

Theorem 7 (Exercise 1.1.15 from [VNT07]). *We have the following relation*

$$W_{C^\perp}(x) = x^{\eta^*} + \sum_{i=0}^{a} B_i (x-1)^i,$$

where

$$B_i = \sum_{j=\eta^*-a}^{\eta^*-i} \binom{\eta^*-j}{i} A_j \geqslant 0 \qquad A_i = \sum_{j=\eta^*-i}^{a} (-1)^{\eta^*+i+j} \binom{j}{\eta^*-i} B_j$$

For weight $w \in \{d^\perp, \ldots, \eta^*\}$, we use the following expression to estimate A_w.

$$A_w = \binom{\eta^*-w}{\eta^*-w} B_{\eta^*-w} - \binom{\eta^*-w+1}{\eta^*-w} B_{\eta^*-w+1} + \cdots \pm \binom{\eta^*-d^\perp}{\eta^*-w} B_{\eta^*-d^\perp}$$

Since we are interested in the asymptotic behavior (and not the exact value) of A_w, we note that $\lg A_w \sim \lg \Gamma(w)$, where

$$\Gamma(w) = \max \left\{ \binom{\eta^*-w}{\eta^*-w} B_{\eta^*-w}, \binom{\eta^*-w+1}{\eta^*-w} B_{\eta^*-w+1}, \ldots, \binom{\eta^*-d^\perp}{\eta^*-w} B_{\eta^*-d^\perp} \right\}$$

Thus, it suffices to compute $\Gamma(w)$ for every w (see Appendix D, Lemma 20) and then the bias (see Appendix D.1). By Appendix D.1, we have the desired result.

$$\delta = \left(d^\perp + \frac{\eta^*}{\sqrt{q}-1} - 1 \right) \left(\lg(q-1) - \mathbf{h_2}\left(\frac{1}{q+1}\right) \right) - \frac{\eta^*}{\sqrt{q}-1} \lg q$$

which completes the proof. □

4 Unpredictability Lemma

In this section, we give our unpredictability lemma as a game between an honest challenger $\mathcal{H}$ and an adversary $\mathcal{A}$. This lemma crucially relies on a family of small-bias distributions. Later, we will prove the security of our $\mathsf{ROLE}(\mathbb{F})$ extractor protocol by reducing it to this unpredictability lemma.

Lemma 5 (Unpredictability Lemma). *Let $\mathcal{C} = \{C_j : j \in \mathcal{J}\}$ be a $\frac{1}{2^\delta}$-biased family of linear code distributions over $\mathbb{F}^{\eta^*}$, where $\eta^* = \gamma + \eta$. Consider the following game between an honest challenger $\mathcal{H}$ and an adversary $\mathcal{A}$:*

1. $\mathcal{H}$ *samples* $m_{[\eta]} \sim U_{\mathbb{F}^\eta}$.
2. $\mathcal{A}$ *sends a leakage function* $\mathcal{L}\colon \mathbb{F}^\eta \to \{0,1\}^t$.
3. $\mathcal{H}$ *sends* $\mathcal{L}(m_{[\eta]})$ *to* $\mathcal{A}$.
4. $\mathcal{H}$ *samples* $j \stackrel{\$}{\leftarrow} \mathcal{J}$. $\mathcal{H}$ *samples a uniform random* $(r_{-\gamma}, \ldots, r_{-1}, r_1, \ldots, r_\eta) \in C_j$. $\mathcal{H}$ *computes* $y_{[\eta]} = r_{[\eta]} + m_{[\eta]}$ *and sends* $(y_{[\eta]}, j)$ *to* $\mathcal{A}$.

   $\mathcal{H}$ *picks* $b \stackrel{\$}{\leftarrow} \{0,1\}$. *If* $b = 0$, *then* $\mathcal{H}$ *sends* $\mathsf{chal} = r_{[-\gamma]}$ *to* $\mathcal{A}$; *otherwise (if* $b = 1$*)* $\mathcal{H}$ *sends* $\mathsf{chal} = u_{[\gamma]} \sim U_{\mathbb{F}^\gamma}$.
5. $\mathcal{A}$ *sends* $\widetilde{b} \in \{0,1\}$.

The adversary $\mathcal{A}$ *wins the game if* $b = \widetilde{b}$. *For any* $\mathcal{A}$, *the advantage of the adversary is* $\leqslant \frac{1}{2}\sqrt{\frac{|\mathbb{F}|^\gamma 2^t}{2^\delta}}$.

Proof. Let $M_{[\eta]}$ be the distribution corresponding to $m_{[\eta]}$. Consider $M'_{[\eta+\gamma]} = (0^\gamma, M_{[\eta]})$. By Lemma 2, $\widetilde{\mathbf{H}}_\infty(M'|\mathcal{L}(M')) \geqslant \eta \log|\mathbb{F}| - t$. Recall that $\mathcal{C} = \{C_j : j \in \mathcal{J}\}$ is a $\frac{1}{2^\delta}$-bias family of distributions over $\mathbb{F}^{\eta+\gamma}$. Then, by Theorem 5, we have the following:

$$\mathrm{SD}\left(\, (C_\mathcal{J} \oplus M', \mathcal{L}(M'), \mathcal{J}) \, , \, (U_{\mathbb{F}^{\eta+\gamma}}, \mathcal{L}(M'), \mathcal{J}) \, \right) \leqslant \frac{1}{2}\left(\frac{|\mathbb{F}|^{\eta+\gamma}}{2^\delta \cdot |\mathbb{F}|^\eta \cdot 2^{-t}}\right)^{\frac{1}{2}} = \frac{1}{2}\sqrt{\frac{|\mathbb{F}|^\gamma 2^t}{2^\delta}}.$$

□

5 Construction of Correlation Extractor

In this section, we give our constructions of correlation extractors. In Section 5.1, we give our construction for Theorem 3. Later, in Section 5.4, we build on construction for Theorem 3 and give construction for Theorem 2.

5.1 Protocol for $\mathsf{ROLE}(\mathbb{F})$ correlation extractor

We give our construction proving Theorem 3. As already mentioned in Section 1.2, our main building block will be $(\eta, \gamma, t, \varepsilon)$-$\mathsf{ROLE}(\mathbb{F})$-to-$\mathsf{ROLE}(\mathbb{F})$ extractor (see Definition 2). That is, the parties start with η $\mathsf{ROLE}(\mathbb{F})$ correlations such that size of each party's share is $n = 2\eta \log|\mathbb{F}|$ bits. The adversarial party gets t bits of leakage. The protocol produces $(\mathsf{ROLE}(\mathbb{F}))^\gamma$ with simulation error ε. We give the formal description of the protocol, which is inspired by the Massey secret sharing scheme [Mas95], in Figure 5. Note that our protocol is round-optimal. The protocol uses a family of distributions $\mathcal{C} = \{C_j\}_{j\in\mathcal{J}}$ that satisfies Property 1 with parameters δ and γ.

Next, we use the ROT embedding technique from [BMN17] to embed σ ROTs in each fresh $\mathsf{ROLE}(\mathbb{F})$ obtained from above protocol. For example, we can embed two ROTs into one $\mathsf{ROLE}(\mathbb{GF}[2^6])$. Using this we get production $m = 2\sigma\gamma$, i.e., we get $m/2 = \sigma\gamma$ secure ROTs.

$(\eta, \gamma, t, \varepsilon)$-ROLE($\mathbb{F}$)-to-ROLE($\mathbb{F}$) **Extractor:**

Let $\mathcal{C} = \{C_j : j \in \mathcal{J}\}$ be a family of distributions over $\mathbb{F}^{\eta+\gamma}$ satisfying erasure recovery for appropriate values of δ and γ.

Hybrid (Random Correlations): Client A gets random $(a_{[\eta]}, b_{[\eta]}) \in \mathbb{F}^{2\eta}$ and Client B gets random $(x_{[\eta]}, z_{[\eta]}) \in \mathbb{F}^{2\eta}$ such that for all $i \in \{1, 2, \ldots, \eta\}$, $a_i x_i + b_i = z_i$.

1. *Code Generation.* Client B samples $j \xleftarrow{\$} \mathcal{J}$.
2. *ROLE Extraction Protocol.*
   (a) Client B picks random $r = (r_{-\gamma}, \ldots, r_{-1}, r_1, \ldots, r_\eta) \sim C_j$ and computes $m_{[\eta]} = r_{[\eta]} + x_{[\eta]}$. Client B sends $(m_{[\eta]}, j)$ to client A.
   (b) Client A picks the same distribution C_j as client B. Client A picks random $u = (u_{-\gamma}, \ldots, u_{-1}, u_1, \ldots, u_\eta) \sim C_j$ and random $v = (v_{-\gamma}, \ldots, v_{-1}, v_1, \ldots, v_\eta) \sim C_j^{(2)}$. Client A computes $\alpha_{[\eta]} = u_{[\eta]} - a_{[\eta]}$, and $\beta_{[\eta]} = a_{[\eta]} * m_{[\eta]} + b_{[\eta]} + v_{[\eta]}$ and sends $(\alpha_{[\eta]}, \beta_{[\eta]})$ to Client B.
   (c) Client B computes $t_{[\eta]} = (\alpha_{[\eta]} * r_{[\eta]}) + \beta_{[\eta]} - z_{[\eta]}$. Cleint B performs erasure recovery on $t_{[\eta]}$ for $C_j^{(2)}$ to obtain $t_{[-\gamma]}$.
   (d) Client A outputs $\{u_i, v_i\}_{i \in \{-1, \ldots, -\gamma\}}$ and Client B outputs $\{r_i, t_i\}_{i \in \{-1, \ldots, -\gamma\}}$

Figure 5: ROLE($\mathbb{F}$)-to-ROLE($\mathbb{F}$) Extractor Protocol.

We note that the protocol from [BMN17] is round-optimal, achieves perfect security and composes in parallel with our protocol in Figure 5. Hence, we maintain round-optimality. We give more details on this in Section 5.3.

Next, we prove the correctness of protocol in Figure 5 below. We prove the security in Section 5.2.

Correctness. We first prove the correctness of the scheme presented in Figure 5. More precisely, we prove the following:

Lemma 6 (Correctness). *If the family of distributions $\mathcal{C} = \{C_j\}_{j \in \mathcal{J}}$ satisfies Property 1, i.e., erasure recovery of first γ coordinates in Schur product, then for all $i \in \{-\gamma, \ldots, -1\}$, it holds that $t_i = u_i r_i + v_i$.*

Proof. First, we prove the following claim:

Claim 4. *For all $i \in [\eta]$, it holds that $t_i = u_i r_i + v_i$.*

$$
\begin{aligned}
t_i = \alpha_i r_i + \beta_i - z_i &= (u_i - a_i) r_i + (a_i m_i + b_i + v_i) - z_i \\
&= u_i r_i - a_i r_i + a_i (r_i + x_i) + b_i + v_i \\
&= u_i r_i + a_i x_i + b_i + v_i - z_i \\
&= u_i r_i + v_i
\end{aligned}
$$

From the above claim, we have that $t_{[\eta]} = u_{[\eta]} * r_{[\eta]} + v_{[\eta]}$. From the protocol, we have that $u, r \in C_j$ and $v \in C_j^{(2)}$. Consider $\tilde{t} = u * r + v \in C_j^{(2)}$. Note that $t_i = \tilde{t}_i$ for all $i \in [\eta]$. Hence, when client B performs erasure recovery on $t_{[\eta]}$ for a codeword in $C_j^{(2)}$, it would get $\tilde{t}_{[-\gamma]}$. This follows from erasure recovery guarantee for first γ coordinates by Property 1. □

5.2 Security of protocol in Figure 5

To argue the security of our protocol, we prove that the output of the protocol is secure $(\mathsf{ROLE}(\mathbb{F}))^\gamma$ against a semi-honest adversary that corrupts either the sender or the receiver and leaks at most t bits from the secret state of the honest party at the beginning of the protocol. At a high level, we prove the security of our protocol by reducing it to our unpredictability lemma (see Lemma 5) exactly. More formally, we prove the following security lemma.

Lemma 7. *The simulation error of our protocol is* $\varepsilon \leqslant \sqrt{\frac{|\mathbb{F}|^\gamma 2^t}{2^\delta}}$*, where* δ *is the parameter for family of distributions* $\mathcal{C}$ *provided by Property 1.*

We first prove Bob privacy followed by Alice privacy.

Bob Privacy. In order to prove privacy of client B against a semi-honest client A, it suffices to show that the adversary cannot distinguish between Bob's secret values $(r_{-\gamma}, \ldots, r_{-1})$ and $U_{\mathbb{F}^\gamma}$. We show that the statistical distance of $(r_{-\gamma}, \ldots, r_{-1})$ and $U_{\mathbb{F}^\gamma}$ given the view of the adversary is at most ε, where ε is defined above.

We observe that client B's privacy reduces directly to our unpredictability lemma (Lemma 5) for the following variables: Let $X_{[\eta]}$ be the random variable denoting the B's input in the initial correlations. Then, $X_{[\eta]}$ is uniform over $\mathbb{F}^\eta$. Note that the adversary gets $L = \mathcal{L}(X_{[\eta]})$ that is at most t bits of leakage. Next, the honest client B picks $j \xleftarrow{\$} \mathcal{J}$ and a random $r = (r_{-\gamma}, \ldots, r_{-1}, r_1, \ldots, r_\eta) \in C_j$. Client B sends $m_{[\eta]} = r_{[\eta]} + x_{[\eta]}$. This is exactly the game between the honest challenger and an semi-honest adversary in the unpredictability lemma (see Lemma 5). Hence, the adversary cannot distinguish between $r_{[-\gamma]}$ and $U_{\mathbb{F}^\gamma}$ with probability more than ε.

Alice Privacy. In order to prove privacy of client A against a semi-honest client B, it suffices to show that the adversary cannot distinguish between Alice's secret values $(u_{-\gamma}, \ldots, u_{-1})$ and $U_{\mathbb{F}^\gamma}$. We show that the statistical distance of $(u_{-\gamma}, \ldots, u_{-1})$ and $U_{\mathbb{F}^\gamma}$ given the view of the adversary is at most ε, where ε is defined above by reducing to our unpredictability lemma (see Lemma 5).

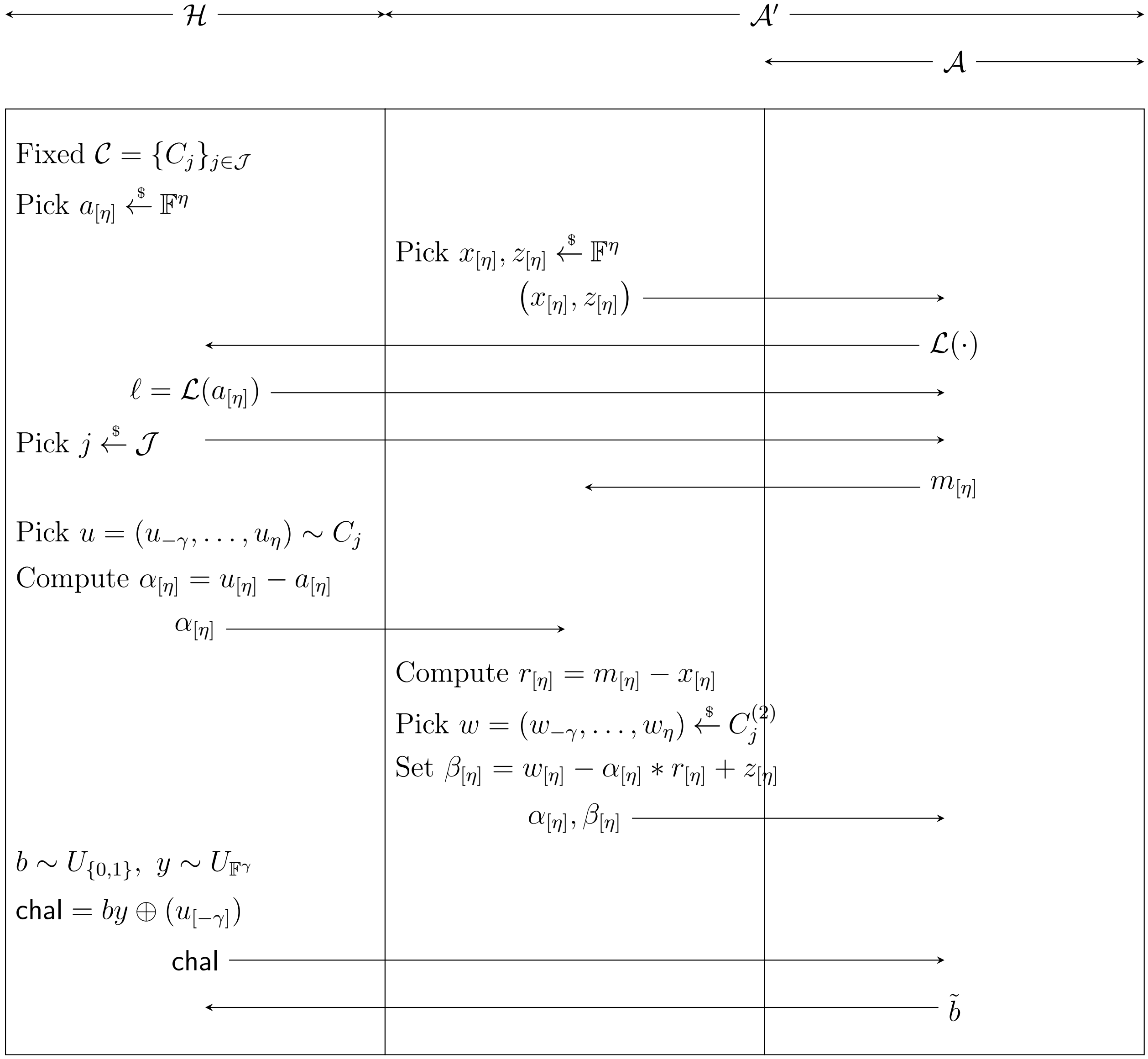

Figure 6: Simulator for Alice Privacy.

Let $A_{[\eta]}$ denote the random variable corresponding to the client A's input $a_{[\eta]}$ in the initial correlations. Then, without loss of generality, the adversary receives t bits of leakage $\mathcal{L}(A_{[\eta]})$. We show a formal reduction to Lemma 5 in Figure 6. Given an adversary $\mathcal{A}$ who can distinguish between $(u_{-\gamma}, \dots, u_{-1})$ and $U_{\mathbb{F}^\gamma}$, we construct an adversary $\mathcal{A}'$ against an honest challenger $\mathcal{H}$ of Lemma 5 with identical advantage. It is easy to see that this reduction is perfect. The only difference in the simulator from actual protocol are as follows: In the simulation, the index j of the distribution is picked by the honest challenger $\mathcal{H}$ instead of client B. This is identical because client B is a semi-honest adversary.

Also, the simulator $\mathcal{A}'$ generates $\beta_{[\eta]}$ slightly differently. We claim that the distribution of $\beta_{[\eta]}$ in simulation is identical to that of real protocol.

This holds by correctness of the protocol: $t_{[\eta]} = u_{[\eta]} * r_{[\eta]} + v_{[\eta]} = (\alpha_{[\eta]} * r_{[\eta]}) + \beta_{[\eta]} - z_{[\eta]}$.

Hence, $\beta_{[\eta]} = (u_{[\eta]} * r_{[\eta]} + v_{[\eta]}) - (\alpha_{[\eta]} * r_{[\eta]}) + z_{[\eta]} = w_{[\eta]} - (\alpha_{[\eta]} * r_{[\eta]}) + z_{[\eta]}$, where $w_{[-\gamma,\eta]}$ is chosen as a random codeword in $C_j^{(2)}$. This holds because in the real protocol $v_{[-\gamma,\eta]}$ is chosen as a random codeword in $C_j^{(2)}$ and $u_{[-\gamma,\eta]} * r_{[-\gamma,\eta]} \in C_j^{(2)}$. Here, we denote by $[-\gamma, \eta]$ the set $\{-\gamma, \ldots, -1, 1, \ldots, \eta\}$.

5.3 OT Embedding

The second conceptual block is the ROT embedding protocol from [BMN17], referred to as the BMN embedding protocol, that embeds a constant number of ROT samples into one sample of ROLE $(\mathbb{F})$, where $\mathbb{F}$ is a finite field of characteristic 2. The BMN embedding protocol is a two-message perfectly semi-honest secure protocol. For example, asymptotically, [BMN17] embeds $(s)^{1-o(1)}$ samples of ROT into one sample of the ROLE $(\mathbb{GF}[2^s])$ correlation. However, for reasonable values of s, say for $s \leqslant 2^{50}$, a recursive embedding embeds $s^{\log 10/\log 32}$ samples of ROT into one sample of the ROLE $(\mathbb{GF}[2^s])$ correlation, and this embedding is more efficient than the asymptotically good one. Below, we show that this protocol composes in parallel with our protocol in Figure 5 to give our overall round optimal protocol for (n, m, t, ε)-correlation extractor for ROLE$(\mathbb{F})$ correlation satisfying Theorem 3.

We note that the BMN embedding protocol satisfies the following additional properties. (1) The first message is sent by client B, and (2) this message depends only on the first share of client B in ROLE$(\mathbb{F})$ (this refers to r_i in Figure 5) and does not depend on the second share (this refers to t_i in Figure 5). With these properties, the BMN embedding protocol can be run in parallel with the protocol in Figure 5. Also, since protocol from BMN satisfies perfect correctness and perfect security, to prove overall security, it suffices to prove the correctness and security of our protocol in Figure 5. This holds because we are in the semi-honest information theoretic setting.

5.4 Protocol for ROT Extractor (Theorem 2)

In this section, we build on Theorem 3 to give a protocol to construct $(\mathsf{ROLE}(\mathbb{F})^\eta)^{[t]}$ using $(\mathsf{ROLE}^n)^{[t]}$, that is the starting point of our protocol in Section 5.1. This would prove Theorem 2. Recall that ROLE and ROT are equivalent.

One of the several fascinating applications of algebraic function fields pioneered by the seminal work of Chudnovsky and Chudnovsky [CC87], is the application to efficiently multiply over an extension field using multiplications over the base field. For example, 6 multiplications over $\mathbb{GF}[2]$ suffice to perform one multiplication over $\mathbb{GF}[2^3]$, or 15 multiplications over $\mathbb{GF}[2]$ suffice for one multiplication over $\mathbb{GF}[2^6]$ (cf., Table 1 in [CÖ10a]).

Our first step of the correlation extractor for $(\mathsf{ROLE}^n)^{[t]}$ uses these efficient multiplication algorithms to (perfectly and securely) implement $(\mathsf{ROLE}(\mathbb{F})^\eta)^{[t]}$, where $\mathbb{F} = \mathbb{GF}(2^\alpha)$ is a finite field with characteristic 2.

We start by describing a protocol for realizing one ROLE $(\mathbb{F})$ using ROLE^ℓ, i.e., ℓ independent samples of ROLE (in the absence of leakage) in Figure 7. Our protocol implements, for instance, one sample of ROLE $(\mathbb{GF}[2^3])$ correlation using 6 samples from the ROT correlation in two rounds. Our protocol uses a multiplication friendly code $\mathcal{D}$ over $\{0,1\}^\ell$ encoding $\mathbb{F}$.

That is, That is, $\mathcal{D} * \mathcal{D} = \mathcal{D}^{(2)} \subset \{0,1\}^\ell$ is also a code for $\mathbb{F}$. Later, we show how to extend this to the leakage setting.

Protocol for $\mathsf{ROLE}(\mathbb{F})$ in ROLE^ℓ hybrid:

Let $\mathcal{D} \subset \{0,1\}^\ell$ be a multiplication friendly code encoding $\mathbb{F} = \mathbb{GF}(2^\alpha)$. Let $(\mathsf{Enc}_\mathcal{D}, \mathsf{Dec}_\mathcal{D})$ (resp., $\mathsf{Enc}_{\mathcal{D}^{(2)}}, \mathsf{Dec}_{\mathcal{D}^{(2)}}$) be encoding and decoding procedures for $\mathcal{D}$ (resp., $\mathcal{D}^{(2)}$).
Hybrid ROT^ℓ: Client A and client B have access to a single call to ROLE^ℓ functionality. Client A will play as the sender and client B will play as the receiver.

Inputs: Client A has inputs $a_0, b_0 \in \mathbb{F}$ and client B has inputs $x_0 \in \mathbb{F}$.

1. Client A picks a random codeword $a_{[\ell]} \sim \mathsf{Enc}_\mathcal{D}(a_0)$ and $b_{[\ell]} \sim \mathsf{Enc}_{\mathcal{D}^{(2)}}(b_0)$ Client A sends $a_{[\ell]}, b_{[\ell]}$ as sender inputs to ROLE^ℓ functionality.
2. Client B picks a random codeword $x_{[\ell]} \sim \mathsf{Enc}_\mathcal{D}(x_0)$ and sends $x_{[\ell]}$ as receiver input to ROLE^ℓ. Client B gets $z_{[\ell]} \in \{0,1\}^\ell$ as output. Client B runs $\mathsf{Dec}_{\mathcal{D}^{(2)}}(z_{[\ell]})$ to obtain $z_0 \in \mathbb{F}$.
3. Client A outputs a_0, b_0 and Client B outputs x_0, z_0.

Figure 7: Perfectly secure protocol for $\mathsf{ROLE}(\mathbb{F})$ in ROLE^ℓ hybrid

Security Guarantee. It is easy to see that the protocol in Figure 7 is a perfectly secure realization of $\mathsf{ROLE}(\mathbb{F})$ in ROLE^ℓ hybrid against a semi-honest adversary. Moreover, [IKOS09] proved the following useful lemma to argue t-leaky realization of $\mathsf{ROLE}(\mathbb{F})$ if the perfect oracle call to ROLE^ℓ is replaced by a t-leaky oracle.

Lemma 8 ([IKOS09])**.** *Let π be a perfectly secure (resp., statistically ε secure) realization of f in the g-hybrid model, where π makes a single call to g. Then, π is also a perfectly secure (resp., statistically ε secure) realization of $f^{[t]}$ in the $g^{[t]}$-hybrid model.*

Using the above lemma, we get that the protocol in Figure 7 is a perfect realization of $(\mathsf{ROLE}(\mathbb{F}))^{[t]}$ in $(\mathsf{ROLE}^\ell)^{[t]}$ hybrid. Finally, by running the above protocol in parallel, we get a perfectly secure protocol for $(\mathsf{ROLE}(\mathbb{F})^\eta)^{[t]}$ in $(\mathsf{ROLE}^{\eta\ell})^{[t]}$ hybrid.
Round Optimality. Note that the first messages of protocols in Figure 7 and Figure 5 can be sent together. This is because the first message of client B in protocol of Figure 5 is independent of the second message in Figure 7. The security holds because we are in the semi-honest information theoretic setting. Hence, overall round complexity is still 2.

6 Parameter Comparison

6.1 Correlation Extractor from (X, Y)

In this section, we shall compare our correlation extractor for $\mathsf{ROLE}(\mathbb{F})$ correlation, where $\mathbb{F}$ is a constant size field with the BMN correlation extractor [BMN17].

Field $\mathbb{F}$	# of OTs Embedded Per $\mathsf{ROLE}(\mathbb{F})$ [BMN17]	Production ($\alpha = m/n$)
$\mathbb{GF}[2^6]$	2	4.83%
$\mathbb{GF}[2^8]$	3	11.39%
$\mathbb{GF}[2^{10}]$	4	15.59%
$\mathbb{GF}[2^{14}]$	5	16.32%
$\mathbb{GF}[2^{20}]$	6	14.31%

Figure 8: The production rate of our correlation extractor for $\mathsf{ROLE}(\mathbb{F})$, where $\beta = t/n = 1\%$ rate of leakage using different finite fields.

Production rate of BMN Correlation Extractor [BMN17]. The BMN correlation emphasizes high resilience while achieving multiple ROT as output. Roughly, they show the following. If parties start with the $\mathsf{IP}\left(\mathbb{GF}\left[2^{\Delta n}\right]^{1/\Delta}\right)$ correlation, then they (roughly) achieve $\frac{1}{2} - \Delta$ fractional resilience with production that depends on (Δn). Here, Δ has to be the inverse of an even natural number $\geqslant 4$.

In particular, the $\mathsf{IP}\left(\mathbb{GF}\left[2^{n/4}\right]^4\right)$ correlation achieves the highest production using the BMN correlation extractor. The resilience of this correlation is $(\frac{1}{4} - g)$, where $g \in (0, 1/4]$ is a positive constant. Then the BMN correlation extractor produces at most $(n/4)^{\log 10/\log 38} \approx (n/4)^{0.633}$ fresh samples from the ROT correlation as output when $n \leqslant 2^{50}$. This implies that the production is $m \approx 2 \cdot (n/4)^{0.633}$, because each ROT sample produces private shares that are two-bits long. For $n = 10^3$, for example, the production is $m \leqslant 66$, for $n = 10^6$ the production is $m \leqslant 5,223$, and for $n = 10^9$ the production is $m \leqslant 413,913$.

We emphasize that the BMN extractor *cannot* increase its production any further by sacrificing its leakage resilience by going below $1/4$.

Our Correlation Extractor for $\mathsf{ROLE}(\mathbb{F})$. We shall use $\mathbb{F}$ such that $q = |\mathbb{F}|$ is an even power of 2. For the suitable Algebraic Geometry codes [GS96] to exist, we need $q \geqslant 49$. Since, the last step of our construction uses the OT embedding technique introduced by BMN [BMN17], we need to consider only the smallest fields that allow a particular number of OT embeddings. Based on this observation, for fractional resilience $\beta = (t/n) = 1\%$, Figure 8 presents the achievable production rate $\alpha = (m/n)$. Note that the Algebraic Geometry codes become better with increasing q, but the BMN OT embedding gets worse. So, the optimum $\alpha = 16.32\%$ is achieved for $\mathbb{F} = \mathbb{GF}[2^{14}]$. For $n = 10^3$, for example, the production is $m = 163$, for $n = 10^6$ the production is $m = 163,200$, and for $n = 10^9$ the production is $m = 163,200,000$. The production rate is overwhelmingly higher than the BMN production rate.

Field $\mathbb{F} = \mathbb{GF}[2^s]$	Bilinear Comp. Mult. $\mu_2(s)$ [CÖ10b]	$n' = \frac{s}{\mu_2(s)} n$	$\beta' = \frac{\mu_2(s)}{s}\beta$	OT Embed. [BMN17]	α'	$\alpha = \frac{s}{\mu_2(s)}\alpha'$
$\mathbb{GF}[2^6]$	15	$\frac{6}{15}n$	2.50%	2	4.05%	1.62%
$\mathbb{GF}[2^8]$	24	$\frac{8}{24}n$	3.00%	3	10.07%	3.35%
$\mathbb{GF}[2^{10}]$	33	$\frac{10}{33}n$	3.30%	4	13.86%	4.20%
$\mathbb{GF}[2^{14}]$	51	$\frac{14}{51}n$	3.64%	5	14.46%	3.97%
$\mathbb{GF}[2^{20}]$	81	$\frac{20}{81}n$	4.05%	6	12.48%	3.08%

Figure 9: The production rate of our correlation extractor for ROT. We are given n-bit shares of the $\mathsf{ROT}^{n/2}$ correlation, and fix $\beta = t/n = 1\%$ fractional leakage. Each row corresponds to using our ROLE $(\mathbb{F})$-to-ROT correlation extractor as an intermediate step. The final column represents the production rate $\alpha = m/n$ of our ROT-to-ROT correlation extractor corresponding to the choice of the finite field $\mathbb{F}$.

6.2 Correlation Extraction from ROT

In this section we shall compare our construction with the GIMS [GIMS15] correlation extractor from ROT. The IKOS [IKOS09] is a feasibility result with minuscule fractional resilience and production rate.

GIMS Production. The GIMS correlation extractor for ROT [GIMS15] trades-off simulation error to achieve higher production by sub-sampling the precomputed ROTs. For $\beta = (t/n) = 1\%$ fractional leakage, the GIMS correlation extractor achieves (roughly) $m = n/4p$ production with $\varepsilon = m \cdot 2^{-p/4}$ simulation error. To achieve negligible simulation error, suppose $p = \log^2(n)$. For this setting, at $n = 10^3$, $n = 10^6$, and $n = 10^9$, the GIMS correlation extractor obtains $m = 3$, $m = 625$, $m = 277,777$, respectively. These numbers are significantly lower than what our construction achieves.

Our Production. We use a bilinear multiplication algorithm to realize one ROLE $(\mathbb{F})$ by performing several ROT. For example, we use $\mu_2(s) = 15$ ROTs to implement one ROLE $(\mathbb{GF}[2^s])$, where $s = 6$. Thus, our original n-bit share changes into n'-bit share, where $n' = (6/15)n$ while preserving the leakage $t = \beta n$. So, the fractional leakage now becomes $t = \beta' n'$, where $\beta' = (15/6)\beta$. Now, we can compute the production $m' = \alpha' n' = \alpha n$.

The highest rate is achieved for $s = 10$, i.e., constructing the correlation extractor for ROT via the correlation extractor for ROLE $(\mathbb{GF}[2^{10}])$. For this choice, our correlation extractor achieves production rate $\alpha = (m/n) = 4.20\%$, if the fractional leakage is $\beta = (t/n) = 1\%$. For $n = 10^3$, $n = 10^6$, and $n = 10^9$, our construction obtains $m = 42$, $m = 42,000$, and $m = 42,000,000$, respectively.

6.3 Close to Optimal Resilience

An interesting facet of our correlation extractor for ROLE $(\mathbb{F})$ is the following. As $q = |\mathbb{F}|$ increases, the maximum fractional resilience, i.e., the intercept of the feasibility curve on the

Y-axis, tends to $1/4$. Ishai et al. [IMSW14] showed that any correlation extractor cannot be resilient to fractional leakage $\beta = (t/n) = 25\%$. For every $g \in (0, 1/4)$, we show that, by choosing sufficiently large q, we can achieve positive production rate $\alpha = (m/n)$ for $\beta = (1/4 - g)$. Thus, our family of correlation extractors (for larger, albeit constant-size, finite fields) achieve near optimal fractional resilience. Figure 10 demonstrates this phenomenon for a few values of q. Appendix F provides a proof of this result, thus proving Theorem 4.

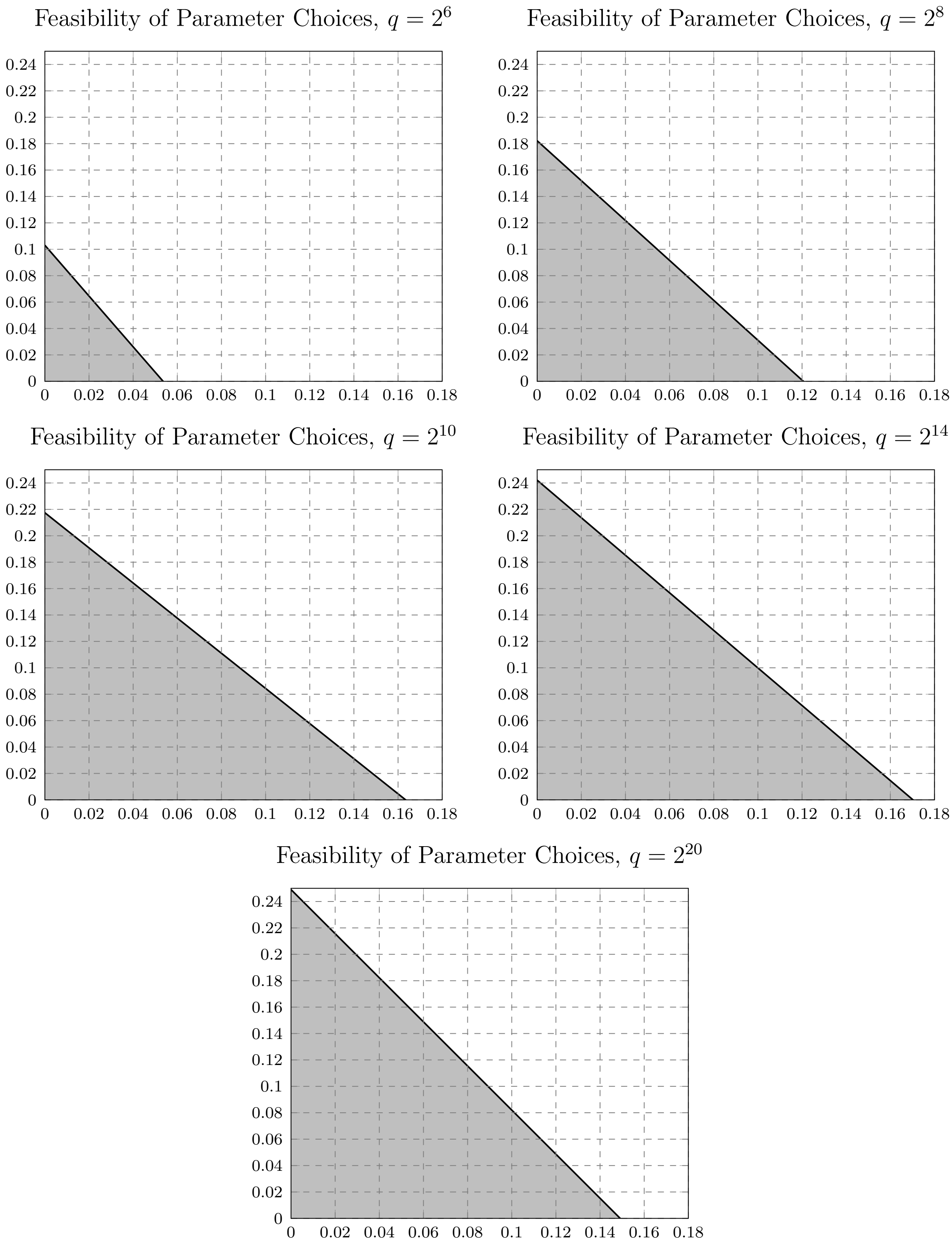

Figure 10: A comparison of the feasibility regions for our correlation extractors for $\mathsf{ROLE}\,(\mathbb{F})$ for various finite fields $\mathbb{F}$ of characteristic 2. For each plot, the X-axis represents the relative production rate $\alpha = m/n$ and the Y-axis represents the fractional leakage resilience $\beta = t/n$.

References

[AIK04] Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz. Cryptography in NC^0. In *45th FOCS*, pages 166–175. IEEE Computer Society Press, October 2004. 1

[App17] Benny Applebaum. Garbled circuits as randomized encodings of functions: a primer. Cryptology ePrint Archive, Report 2017/385, 2017. http://eprint.iacr.org/2017/385. 1

[AR94] Noga Alon and Yuval Roichman. Random cayley graphs and expanders. *Random Structures & Algorithms*, 5(2):271–284, 1994. 11

[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, 3, 4, 6, 18, 19, 22, 23, 24, 25, 45

[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. 4, 22

[CC06] Hao Chen and Ronald Cramer. Algebraic geometric secret sharing schemes and secure multi-party computations over small fields. In Cynthia Dwork, editor, *CRYPTO 2006*, volume 4117 of *LNCS*, pages 521–536. Springer, Heidelberg, August 2006. 5

[CDFR17] Ignacio Cascudo, Ivan Damgård, Oriol Farràs, and Samuel Ranellucci. Resource-efficient OT combiners with active security. In Yael Kalai and Leonid Reyzin, editors, *TCC 2017, Part II*, volume 10678 of *LNCS*, pages 461–486. Springer, Heidelberg, November 2017. 6

[CÖ10a] Murat Cenk and Ferruh Özbudak. On multiplication in finite fields. *Journal of Complexity*, 26(2):172–186, 2010. 4, 22

[CÖ10b] Murat Cenk and Ferruh Özbudak. On multiplication in finite fields. *Journal of Complexity*, 26(2):172–186, 2010. 25

[DORS08] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM J. Comput.*, 38(1):97–139, 2008. 11

[DS05] Yevgeniy Dodis and Adam Smith. Correcting errors without leaking partial information. In Harold N. Gabow and Ronald Fagin, editors, *37th ACM STOC*, pages 654–663. ACM Press, May 2005. 11

[FR93] Gui Liang Feng and Thammavarapu R. N. Rao. Decoding algebraic-geometric codes up to the designed minimum distance. *IEEE Transactions on Information Theory*, 39(1):37–45, 1993. 36

[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. 2, 4, 5, 25

[Gop81] Valerii Denisovich Goppa. Codes on algebraic curves. In *Soviet Math. Dokl*, pages 170–172, 1981. 36

[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. 7, 24, 36

[GW97] Oded Goldreich and Avi Wigderson. Tiny families of functions with random properties: A quality-size trade-off for hashing. *Random Struct. Algorithms*, 11(4):315–343, 1997. 11

[HIKN08] Danny Harnik, Yuval Ishai, Eyal Kushilevitz, and Jesper Buus Nielsen. OT-combiners via secure computation. In Ran Canetti, editor, *TCC 2008*, volume 4948 of *LNCS*, pages 393–411. Springer, Heidelberg, March 2008. 5

[HKN+05] Danny Harnik, Joe Kilian, Moni Naor, Omer Reingold, and Alon Rosen. On robust combiners for oblivious transfer and other primitives. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 96–113. Springer, Heidelberg, May 2005. 5

[IK02] Yuval Ishai and Eyal Kushilevitz. Perfect constant-round secure computation via perfect randomizing polynomials. In Peter Widmayer, Francisco Triguero Ruiz, Rafael Morales Bueno, Matthew Hennessy, Stephan Eidenbenz, and Ricardo Conejo, editors, *ICALP 2002*, volume 2380 of *LNCS*, pages 244–256. Springer, Heidelberg, July 2002. 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. 2, 4, 6, 23, 25

[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. 5, 26

[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. 5, 6

[Kil91] Joe Kilian. A general completeness theorem for two-party games. In *23rd ACM STOC*, pages 553–560. ACM Press, May 1991. 6

[Mas95] J. L. Massey. Some applications of coding theory in cryptography. In *Codes and Ciphers: Cryptography and Coding IV*, pages 33–47, 1995. 18

[MP06] Remo Meier and Bartosz Przydatek. On robust combiners for private information retrieval and other primitives. In Cynthia Dwork, editor, *CRYPTO 2006*, volume 4117 of *LNCS*, pages 555–569. Springer, Heidelberg, August 2006. 5

[MPW07] Remo Meier, Bartosz Przydatek, and Jürg Wullschleger. Robuster combiners for oblivious transfer. In Salil P. Vadhan, editor, *TCC 2007*, volume 4392 of *LNCS*, pages 404–418. Springer, Heidelberg, February 2007. 5

[NN90] Joseph Naor and Moni Naor. Small-bias probability spaces: Efficient constructions and applications. In *22nd ACM STOC*, pages 213–223. ACM Press, May 1990. 11

[O'S95] M. E. O'Sullivan. Decoding of codes defined by a single point on a curve. *IEEE Transactions on Information Theory*, 41(6):1709–1719, 1995. 36

[PW08] Bartosz Przydatek and Jürg Wullschleger. Error-tolerant combiners for oblivious primitives. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *ICALP 2008, Part II*, volume 5126 of *LNCS*, pages 461–472. Springer, Heidelberg, July 2008. 5

[Rao07] Anup Rao. An exposition of bourgain's 2-source extractor. *ECCCTR: Electronic Colloquium on Computational Complexity*, Technical Reports, 2007. 10

[VNT07] Serge Vladut, Dmitry Nogin, and Michael Tsfasman. *Algebraic Geometric Codes: Basic Notions*. American Mathematical Society, Boston, MA, USA, 2007. 17, 37

[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. 3

A Functionalities and Correlations

We define some useful functionalities and correlations below.

Oblivious Transfer. A *2-choose-1 bit Oblivious Transfer* (referred to as OT) is a two party functionality which takes input $(x_0, x_1) \in \{0,1\}^2$ from Alice and input $b \in \{0,1\}$ from Bob and outputs x_b to Bob.

Random Oblivious Transfer Correlation. A *Random* 2-choose-1-bit Oblivious Transfer (referred to as ROT) is an input-less two party correlation that samples bits x_0, x_1, b uniformly and independently at random. It outputs secret share $r_A = (x_0, x_1)$ to Alice and $r_B = (b, x_b)$ to Bob. The joint distribution of Alice and Bob shares is called a ROT-correlation.

Oblivious Linear-function Evalutation. Given a field $(\mathbb{F}, +, \cdot)$ an *Oblivious Linear-function Evaluation*, represented by $\mathsf{OLE}(\mathbb{F})$, is a two party functionality that takes input $(a, b) \in \mathbb{F}^2$ from Alice and input $x \in \mathbb{F}$ from Bob and outputs $ax + b$ to Bob. Moreover, we use OLE to denote $\mathsf{OLE}(\mathbb{GF}([2])$.

Random Oblivious Linear-function Evalutation. Given a field $(\mathbb{F}, +, \cdot)$ a em Random Oblivious Linear-function Evaluation, represented by $\mathsf{ROLE}(\mathbb{F})$, is a two party correlation that samples field elements $a, b, x \in \mathbb{F}$ uniformly and independently at random. It provides Alice the secret share $r_A = (a, b)$ and provides Bob the secret share $r_B = (x, ax + b)$. Moreover, we use ROLE to denote $\mathsf{ROLE}(\mathbb{GF}([2])$. Note that ROLE and ROT are functionally equivalent correlations.

B Fourier Analysis Basic Definitions

We show that χ as stated in Definition 4 is indeed a symmetric, non-degenerate, bilinear map.

Proof. The proof follows directly the definition of χ.

Bilinear map. The function χ is a bilinear map if and only if for every $x \in \mathbb{F}^\eta$, both $\chi(x, \cdot)$ and $\chi(\cdot, x)$ are homomorphisms. This follows immediately by the fact that ψ is a group homomorphism. Namely, for fixed $x \in \mathbb{F}^\eta$ and any $y, z \in \mathbb{F}^\eta$, we have

$$\chi_x(y+z) = \psi\left(x \cdot (y+z)\right) = \psi\left(\sum_i x_i (y+z)_i\right) = \psi\left(\sum_i x_i y_i + x_i z_i\right)$$
$$= \psi(x \cdot y + x \cdot z) = \psi(x \cdot y)\psi(x \cdot z) = \chi_x(y)\chi_x(z).$$

The function $\chi(\cdot, x)$ is a homomorphism by the same argument.

Non-degenerate. The function χ is non-degenerate if and only if for every $0^\eta \neq x \in \mathbb{F}^\eta$, both $\chi(x, \cdot)$ and $\chi(\cdot, x)$ are non-trivial. Taking the function ψ to be non-trivial ($\psi \neq 1$) immediately yields this property.

Symmetric. The function χ is symmetric if and only if for all $x, y \in \mathbb{F}^\eta$, we have $\chi_x(y) = \chi_y(x)$. This follows directly since the vector dot product is symmetric. $\square$

$\square$

We show properties of any character function χ_S.

Lemma 9 (Character Magnitude)**.** $|\chi_S| = 1$ *for any character* χ_S*.*

Proof. Since χ_S is a group homomorphism, we have $\chi_S(x+y) = \chi_S(x)\chi_S(y)$ for any $x, y \in \mathbb{F}^\eta$. Thus $\chi_S(0^\eta) = \chi_S(0^\eta)^2$, which implies that $\chi_S(0^\eta) = 1$ since $\psi(0) = 1$. Applying the homomorphism property repeatedly for $x = y$, we have

$$\chi_S(x)^{|\mathbb{F}^\eta|} = \chi_S(|\mathbb{F}^\eta|\, x) = \chi_S(0) = 1$$

Hence $|\chi_S(x)| = 1$ for all $x \in \mathbb{F}^\eta$. $\square$

Lemma 10 (Character Conjugate)**.** *For any character* χ_S *and any* $x \in \mathbb{F}^\eta$*, we have* $\overline{\chi_S(x)} = \chi_S(x)^{-1} = \chi_S(-x)$*.*

Proof. Note that $|\chi_S(x)| = 1$ for any $S, x \in \mathbb{F}^\eta$ by Lemma 9. Thus by definition of complex conjugate we have

$$\chi_S(x)\overline{\chi_S(x)} = |\chi_S(x)|^2 = 1.$$

This implies $\overline{\chi_S(x)} = \chi_S(x)^{-1}$ in $\mathbb{C}^*$. Furthermore, since χ is a bilinear map, for any $x \in \mathbb{F}^\eta$ we have

$$\chi_S(x)\chi_S(-x) = \chi_S(x - x) = \chi_S(0) = 1 = \chi_S(x)\overline{\chi_S(x)}$$

Therefore $\overline{\chi_S(x)} = \chi_S(-x)$. $\square$

Lemma 11. *For any non-trivial character* χ_S*, we have* $\sum_{x \in \mathbb{F}^\eta} \chi_S(x) = 0$*.*

Proof. Since χ_S is a non-trivial character, there exists a vector $v \in \mathbb{F}^\eta$ such that $\chi_S(v) \neq 1$. We have

$$\chi_S(v) \sum_{x \in \mathbb{F}^\eta} \chi_S(x) = \sum_{x \in \mathbb{F}^\eta} \chi_S(v)\chi_S(x) = \sum_{x \in \mathbb{F}^\eta} \chi_S(v + x) = \sum_{y \in \mathbb{F}^\eta} \chi_S(y) = \sum_{x \in \mathbb{F}^\eta} \chi_S(x)$$

Thus, we must have $\sum_{x \in \mathbb{F}^\eta} \chi_S(x) = 0$. $\square$

Lemma 12 (Orthogonality)**.** *For any two characters* χ_S *and* χ_T*, we have that*

$$\langle \chi_S, \chi_T \rangle = \begin{cases} 1 & \textit{if } S = T \\ 0 & \textit{otherwise} \end{cases}$$

Proof.

$$\langle \chi_S, \chi_T \rangle = \frac{1}{|\mathbb{F}|^\eta} \sum_{x \in \mathbb{F}^\eta} \chi_S(x)\overline{\chi_T(x)} = \frac{1}{|\mathbb{F}|^\eta} \sum_{x \in \mathbb{F}^\eta} \chi_x(S)\chi_x(-T) = \frac{1}{|\mathbb{F}|^\eta} \sum_{x \in \mathbb{F}^\eta} \chi_x(S - T)$$

If $S = T$, then $\langle \chi_S, \chi_T \rangle = \frac{1}{|\mathbb{F}|^\eta} \sum_{x \in \mathbb{F}^\eta} \chi_x(0) = 1$. Otherwise, by Lemma 11, we have $\langle \chi_S, \chi_T \rangle = 0$. □

The following corollary is a direct result of Lemma 9 and Lemma 12.

Corollary 8 (Orthonormal Basis). *The set $\{\chi_S\}_{S \in \mathbb{F}^\eta}$ is an orthonormal basis for the vector space $\{f \mid f \colon \mathbb{F}^\eta \to \mathbb{C}\}$.*

We show linearity of Definition 5.

Lemma 13 (Linearity of Fourier Transform). *For any two functions $f, g \colon \mathbb{F}^\eta \to \mathbb{C}$ and for any $a, b \in \mathbb{C}$ and $S \in \mathbb{F}^\eta$, we have*

$$(\widehat{af + bg})(S) = a\widehat{f}(S) + b\widehat{g}(S)$$

Proof. This follows from definition of Fourier transform and the linearity property of inner product.

$$\widehat{af + bg}(S) = \langle af + bg, \chi_S \rangle = \langle af, \chi_S \rangle + \langle bg, \chi_S \rangle = a\langle f, \chi_S \rangle + b\langle g, \chi_S \rangle = a\widehat{f}(S) + b\widehat{g}(S)$$

□

We note that Lemma 1 follows directly from Corollary 8 and Definition 5 since any $f \colon \mathbb{F}^\eta \to \mathbb{C}$ can be written as $f(x) = \sum_{S \in \mathbb{F}^\eta} \langle f, \chi_S \rangle \chi_S(x) = \sum_{S \in \mathbb{F}^\eta} \widehat{f}(S)\chi_S(x)$ by definition of orthonormal basis. Next we show how to express the inner product of two functions in terms of their Fourier coefficients.

Lemma 14. *For any two functions $f, g \colon \mathbb{F}^\eta \to \mathbb{C}$, we have $\langle f, g \rangle = \sum_{S \in \mathbb{F}^\eta} \widehat{f}(S)\overline{\widehat{g}(S)}$.*

Proof.

$$\begin{aligned}
\langle f, g \rangle &= \mathop{\mathbb{E}}_{x \xleftarrow{\$} \mathbb{F}^\eta} f(x)\overline{g(x)} \\
&= \frac{1}{|\mathbb{F}|^\eta} \sum_{x \in \mathbb{F}^\eta} \left(\sum_{S \in \mathbb{F}^\eta} \widehat{f}(S)\chi_S(x) \right) \left(\sum_{T \in \mathbb{F}^\eta} \overline{\widehat{g}(T)}\ \overline{\chi_T(x)} \right) && \text{[Lemma 1]} \\
&= \frac{1}{|\mathbb{F}|^\eta} \sum_{x,S,T \in \mathbb{F}^\eta} \widehat{f}(S)\chi_S(x)\overline{\widehat{g}(T)}\ \overline{\chi_T(x)} \\
&= \sum_{S,T \in \mathbb{F}^\eta} \widehat{f}(S)\overline{\widehat{g}(T)} \left(\frac{1}{|\mathbb{F}|^\eta} \sum_{x \in \mathbb{F}^\eta} \chi_S(x)\overline{\chi_T(x)} \right) \\
&= \sum_{S,T \in \mathbb{F}^\eta} \widehat{f}(S)\overline{\widehat{g}(T)}\langle \chi_S, \chi_T \rangle && \text{[Definition 3]} \\
&= \sum_{S \in \mathbb{F}^\eta} \widehat{f}(S)\overline{\widehat{g}(S)} && \text{[Lemma 12]}
\end{aligned}$$

□

When $f = g$, we have Parseval's identity as a corollary.

Corollary 9 (Parseval's Identity). *Let* $f\colon \mathbb{F}^\eta \to \mathbb{C}$. *Then* $\mathbb{E}_{x \xleftarrow{\$} \mathbb{F}^\eta} |f(x)|^2 = \sum_{S \in \mathbb{F}^\eta} |\widehat{f}(S)|^2$.

Next we prove Lemma 3.

Proof. By Corollary 9 and assumption $\mathbf{H}_\infty(X) \geqslant k$, we have

$$\begin{aligned}\sum_S |\widehat{X}(S)|^2 &= \frac{1}{|\mathbb{F}|^\eta} \sum_{x \in \mathbb{F}^\eta} |X(x)|^2 \leqslant \frac{1}{|\mathbb{F}|^\eta} \sum_{x \in \mathbb{F}^\eta} \frac{1}{2^k} |X(x)| \\ &= \frac{1}{|\mathbb{F}|^\eta} \frac{1}{2^k} \sum_{x \in \mathbb{F}^\eta} |X(x)| = \frac{1}{|\mathbb{F}|^\eta\, 2^k}\end{aligned}$$

□

We introduce the Convolution operator and prove related properties.

Definition 8 (Convolution). *For any two functions* $f, g : \mathbb{F}^\eta \to \mathbb{R}$, *the convolution of* f *and* g *is defined as*

$$(f * g)(x) := \mathbb{E}_{y \in \mathbb{F}^\eta} f(x-y) g(y)$$

Lemma 15 (Fourier Transform of Convolution). *For every vector* $S \in \mathbb{F}^\eta$, *we have* $\widehat{f * g}(S) = \widehat{f}(S)\widehat{g}(S)$

Proof.

$$\begin{aligned}\widehat{f * g}(S) &= \frac{1}{|\mathbb{F}|^\eta} \sum_{x \in \mathbb{F}^\eta} (f * g)(x) \overline{\chi_S(x)} = \frac{1}{|\mathbb{F}|^{2\eta}} \sum_{x, y \in \mathbb{F}^\eta} f(x-y) g(y) \overline{\chi_S(x)} \\ &= \frac{1}{|\mathbb{F}|^{2\eta}} \sum_{x, y \in \mathbb{F}^\eta} f(x-y) \overline{\chi_S(x-y)} g(y) \overline{\chi_S(y)} \\ &= \frac{1}{|\mathbb{F}|^{2\eta}} \sum_{y \in \mathbb{F}^\eta} g(y) \overline{\chi_S(y)} \sum_{x \in \mathbb{F}^\eta} f(x-y) \overline{\chi_S(x-y)} \\ &= \frac{1}{|\mathbb{F}|^\eta} \sum_{y \in \mathbb{F}^\eta} g(y) \overline{\chi_S(y)} \cdot \widehat{f}(S) = \frac{1}{|\mathbb{F}|^\eta} \widehat{f}(S) \sum_{y \in \mathbb{F}^\eta} g(y) \overline{\chi_S(y)} \\ &= \widehat{f}(S)\widehat{g}(S)\end{aligned}$$

□

We prove facts about distributions and their Fourier coefficients.

Lemma 16 (Masking Lemma). *Let* $X, Y\colon \mathbb{F}^\eta \to \mathbb{R}$ *be two independent random variables (functions, distributions). Then* $|\mathbb{F}^\eta| (X * Y)$ *is the distribution of the random variable* $Z = X \oplus Y$ *and* $\widehat{X \oplus Y}(S) = |\mathbb{F}|^\eta\, \widehat{(X * Y)}(S) = |\mathbb{F}|^\eta\, \widehat{X}(S)\widehat{Y}(S)$.

Proof.

$$\begin{aligned} Z(z) &= \Pr[Z = z] = \Pr[X + Y = z] = \Pr[X = z - Y] \\ &= \sum_{y \in \mathbb{F}^\eta} \Pr[X = z - y | Y = y] = \sum_{y \in \mathbb{F}^\eta} \Pr[X = z - y] \Pr[Y = y] \\ &= \sum_{y \in \mathbb{F}^\eta} X(z - y) Y(y) = |\mathbb{F}|^\eta (X * Y) \end{aligned}$$

□

Lemma 17 (Zeroth Fourier Coefficient of a Distribution)**.** *For any distribution* $f\colon \mathbb{F}^\eta \to \mathbb{R}$*, we have* $\widehat{f}(0) = \frac{1}{|\mathbb{F}|^\eta}$*.*

Proof.

$$\widehat{f}(0) = \frac{1}{|\mathbb{F}|^\eta} \sum_{x \in |\mathbb{F}|^\eta} f(x)\chi_0(x) = \frac{1}{|\mathbb{F}|^\eta} \sum_{x \in |\mathbb{F}|^\eta} f(x) \cdot 1 = \frac{1}{|\mathbb{F}|^\eta}$$

□

Lemma 18 (Fourier Coefficients of Uniform Distributions)**.** *Let* $U_{\mathbb{F}^\eta}$ *be the uniform distribution over* $\mathbb{F}^\eta$*. Then, for every nonzero* $S \in \mathbb{F}^\eta$*, we have* $\widehat{U}_{\mathbb{F}^\eta}(S) = 0$*.*

Proof.

$$\begin{aligned} \widehat{U}_{\mathbb{F}^\eta}(S) &= \frac{1}{|\mathbb{F}|^\eta} \sum_{x \in \mathbb{F}^\eta} U_{\mathbb{F}^\eta}(x)\overline{\chi_S(x)} = \frac{1}{|\mathbb{F}|^\eta} \sum_{x \in \mathbb{F}^\eta} \frac{1}{|\mathbb{F}|^\eta} \chi_S(-x) \\ &= \frac{1}{|\mathbb{F}|^{2\eta}} \sum_{S \in \mathbb{F}^\eta} \chi_S(-x) = 0 \qquad \text{[Lemma 11]} \end{aligned}$$

Note χ_S is non-trivial if $S \neq 0$. □

B.1 Proof of Claim 3

By definition of $\widehat{C}(S)$, we have

$$\begin{aligned} \widehat{C}(S) &= \frac{1}{|\mathbb{F}|^{\eta^*}} \sum_{x \in \mathbb{F}^{\eta^*}} C(x)\overline{\chi_S(x)} = \frac{1}{|\mathbb{F}|^{\eta^*}} \sum_{x \in C} \frac{1}{|\mathbb{F}|^\kappa} \chi_S(-x) \\ &= \frac{1}{|\mathbb{F}|^{\eta^* + \kappa}} \sum_{x \in C} \psi(-S \cdot x) \end{aligned}$$

where $(S \cdot x)$ is the vector dot product over $\mathbb{F}^{\eta^*}$. By definition if $S \in C^\perp$, then $(S \cdot x) = 0$ for all $x \in C$. Since $\psi(0) = 1$, this implies $\widehat{C}(S) = \frac{1}{|\mathbb{F}|^{\eta^* + \kappa}} \sum_{x \in C} \psi(-S \cdot x) = \frac{1}{|\mathbb{F}|^{\eta^*}}$ for all $S \in C^\perp$.

Next, for $S \notin C^\perp$, we use Parseval's identity (Corollary 9):

$$\begin{aligned}
\sum_{S \notin C^\perp} |\widehat{C}(S)|^2 &= \frac{1}{|\mathbb{F}|^{\eta^*}} \sum_{x \in \mathbb{F}^{\eta^*}} |C(x)|^2 - \sum_{S \in C^\perp} \widehat{C}(S)^2 \\
&= \frac{1}{|\mathbb{F}|^{\eta^*}} \sum_{x \in C} |C(x)|^2 - \sum_{S \in C^\perp} |\widehat{C}(S)|^2 \\
&= \frac{1}{|\mathbb{F}|^{\eta^*}} \sum_{x \in C} \frac{1}{|\mathbb{F}|^{2\kappa}} - \sum_{S \in C^\perp} \frac{1}{|\mathbb{F}|^{2\eta^*}} \\
&= \frac{1}{|\mathbb{F}|^{\eta^*}} \cdot \frac{|\mathbb{F}|^{\kappa}}{|\mathbb{F}|^{2\kappa}} - \frac{|\mathbb{F}|^{\eta^* - \kappa}}{|\mathbb{F}|^{2\eta^*}} = \frac{1}{|\mathbb{F}|^{\eta^* + \kappa}} - \frac{1}{|\mathbb{F}|^{\eta^* + \kappa}} = 0
\end{aligned}$$

C Algebraic Geometry Codes

Theorem 10 (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 points $\#C_u(\mathbb{F}_q) \geqslant q^{u/2}(\sqrt{q} - 1)$, and*
2. *The genus of the curve $g(C_u) \leqslant q^{u/2}$.*

Using the above theorem, we get the following corollary.

Corollary 11. *For every q that is an even power of a prime, there exists an $[\eta^*, \kappa, d, d^\perp]_q$ code $\mathcal{C}$ such that:*

1. $\eta^* = q^{u/2}(\sqrt{q} - 1)$,
2. $\kappa = \Delta - q^{u/2} + 1$,
3. $d = \eta^* - \Delta$, *and*
4. $d^\perp \geqslant \kappa - q^{u/2} + 1$.

Further, $d^{(2)} = d(\mathcal{C}^{(2)}) = \eta^* - 2\Delta$, and there exists an efficient decoding algorithm for $\mathcal{C}^{(2)}$ that can correct $\left\lfloor \frac{d^{(2)}-1}{2} \right\rfloor$ errors and $d^{(2)} - 1$ erasures.

Proof. By choosing the Garcia-Stichtenoth curves over $\mathbb{F}_q$ (see, Theorem 10) and a divisor D such that $\mathsf{deg} D = \Delta$, we can define a Goppa code [Gop81] with these parameters.

O'Sullivan [O'S95] proved that the unique decoding can be performed efficiently by the syndrome-based Berlekamp-Massey-Sakata algorithm with the Feng-Rao [FR93] majority voting. □

D Analysis of $\Gamma(w)$

In this section, we analyze the behavior of the function

$$\Gamma(w) = \max_{\eta^* - w \leqslant j \leqslant \eta^* - d^\perp} \left\{ \binom{j}{\eta^* - w} B_j \right\}$$

from Section 3. Let q be an even prime power and let

$$\begin{aligned} a &= \eta^* - d^\perp \\ a' &= a - \left(\frac{\eta^*}{\sqrt{q} - 1} \right) + 1 \\ a'' &= a - 2\left(\frac{\eta^*}{\sqrt{q} - 1} \right) + 1. \end{aligned}$$

We use the following results.

Theorem 12 (Theorem 1.1.18 and 1.1.28 from [VNT07])**.** *For $i \in \{0, 1, \ldots, a\}$, we have the following estimates of B_i.*

1. *For $0 \leqslant i \leqslant a''$*

$$B_i = \binom{\eta^*}{i} \left(\frac{q^{a'}}{q^i} - 1 \right)$$

2. *For $a'' < i \leqslant a'$*

$$\binom{\eta^*}{i} \left(q^{\frac{\eta^*}{(\sqrt{q}-1)}} - 1 \right) \geqslant B_i \geqslant \binom{\eta^*}{i} \left(\frac{q^{a'}}{q^i} - 1 \right)$$

3. *For $a' < i \leqslant a$*

$$\binom{\eta^*}{i} \left(\frac{q^{a+1}}{q^i} - 1 \right) \geqslant B_i \geqslant 0$$

Note that $\binom{i}{\eta^* - w}\binom{\eta^*}{i} = \binom{\eta^*}{w}\binom{w}{i - (\eta^* - w)}$. Thus the above theorem implies the following bounds.

1. For $0 \leqslant i \leqslant a''$

$$\binom{i}{\eta^* - w} B_i \leqslant \binom{\eta^*}{w} \binom{w}{i - (\eta^* - w)} q^{a' - i}$$

2. For $a'' < i \leqslant a'$

$$\binom{i}{\eta^* - w} B_i \leqslant \binom{\eta^*}{w} \binom{w}{i - (\eta^* - w)} q^{\frac{\eta^*}{(\sqrt{q}-1)}}$$

3. For $a' < i \leqslant a$

$$\binom{i}{\eta^* - w} B_i \leqslant \binom{\eta^*}{w} \binom{w}{i - (\eta^* - w)} q^{a + 1 - i}$$

Lemma 19. *Assume η^*, w are fixed. Let $f(i) = \binom{w}{i-(\eta^*-w)} q^{-i}$ for $\eta^* - w \leqslant i \leqslant \eta^*$. Let*

- $f_1(i) = \binom{\eta^*}{w} q^{a'} \cdot f(i)$ *for* $0 \leqslant i \leqslant a''$,
- $f_2(i) = \binom{\eta^*}{w} q^{\frac{\eta^*}{(\sqrt{q}-1)}+i} \cdot f(i)$ *for* $a'' < i \leqslant a'$,
- $f_3(i) = \binom{\eta^*}{w} q^{a+1} \cdot f(i)$, *for* $a' < i \leqslant a$

Then f, f_1, f_3 (asymptotically) have the same critical point at $i = \eta^* - w + w/(q+1)$. More concretely, they are asymptotically increasing in the range $[\eta^* - w, \eta^* - w + \frac{w}{q+1}]$ and asymptotically decreasing in the range $[\eta^* - w + \frac{w}{q+1}, \eta^*]$. In addition, the function f_2 is increasing in the range $[\eta^* - w, \eta^* - w/2]$,and decreasing in the range $[\eta^* - w/2, \eta^*]$.

Proof. The function f is asymptotically similar to a binomial distribution of bias p, where

$$\frac{p}{1-p} = \frac{1}{q} \iff p = \frac{1}{q+1}$$

The maximum of the binomial distribution shall be achieved at the critical point

$$i - (\eta^* - w) = p \cdot w = \frac{w}{q+1}$$

Thus, $f(i)$ is increasing in the range $[\eta^* - w, \eta^* - w + \frac{w}{q+1}]$ and is decreasing in the range $[\eta^* - w + \frac{w}{q+1}, w]$.
Since the three functions f_1, f_2, f_3 are just scalar multiplication of $f(i)$, they behave asymptotically same as f. □

Now, we state the result of upper-bounding $\Gamma(w)$ as following.

Lemma 20. *Let $p^* = \eta^* - w + \frac{w}{q+1}$. For $w \in \{d^\perp, \ldots, \eta^*\}$, we have $\Gamma(w)$ is less than or equal to*

1. $\binom{\eta^*}{w}\binom{w}{d^\perp} q$, *where* $w \in I_1 = [d^\perp, (\frac{q+1}{q})d^\perp]$
2. $\binom{\eta^*}{w}\binom{w}{\frac{w}{q+1}} q^{a+1-p^*}$, *where* $w \in I_2 = [(\frac{q+1}{q})d^\perp, \eta^* - a']$
3. $\binom{\eta^*}{w}\binom{w}{\frac{w}{q+1}} q^{\frac{\eta^*}{(\sqrt{q}-1)}}$, *where* $w \in I_3 = [\eta^* - a', (\frac{q+1}{q})(\eta^* - a')]$
4. $\binom{\eta^*}{w}\binom{w}{\eta^*-a'} q^{\frac{\eta^*}{\sqrt{q}-1}}$, *where* $w \in I_4 = [(\frac{q+1}{q})(\eta - a'), \eta^* - a'']$
5. $\binom{\eta^*}{w}\binom{w}{\eta^*-a'} q^{\frac{\eta^*}{(\sqrt{q}-1)}}$, *where* $w \in I_5 = [\eta^* - a'', \frac{q+1}{q}(\eta^* - a'')]$
6. $\binom{\eta^*}{w} \cdot \max\left\{ \binom{w}{\frac{w}{q+1}} q^{a'-p^*}, \binom{w}{\eta^*-a'} q^{\frac{\eta^*}{(\sqrt{q}-1)}} \right\}$, *if* $w \in I_6 = [\frac{q+1}{q}(\eta^* - a''), 2d^\perp + \frac{2\eta^*}{\sqrt{q}-1}]$ *or* $w \in I_8 = [2d^\perp + \frac{4\eta^*}{\sqrt{q}-1}, \eta^*]$.
   $\binom{\eta^*}{w} \cdot \max\left\{ \binom{w}{\frac{w}{q+1}} q^{a'-p^*}, \binom{w}{w/2} q^{\frac{\eta^*}{(\sqrt{q}-1)}} \right\}$, *if* $w \in I_7 = [2d^\perp + \frac{2\eta^*}{\sqrt{q}-1}, 2d^\perp + \frac{4\eta^*}{\sqrt{q}-1}]$.

Proof. We will use the facts stated in Lemma 19 frequently in our proof.

Case 1: $d^{\perp} \leqslant w \leqslant \left(\frac{q+1}{q}\right) d^{\perp}$**,** which implies $a \geqslant \eta - w \geqslant a'$ and $p^* > a$. In this case, the function f_3 is increasing. So $\Gamma(w)$ is maximized at a. Therefore

$$\Gamma(w) \leqslant \binom{\eta^*}{w}\binom{w}{a-\eta^*+w} q = \binom{\eta^*}{w}\binom{w}{w-d^{\perp}} q = \binom{\eta^*}{w}\binom{w}{d^{\perp}} q$$

Case 2: $\left(\frac{q+1}{q}\right) d^{\perp} \leqslant w \leqslant \eta^* - a'$**,** which implies $\eta^* - w \geqslant a'$ and $p^* \leqslant a$. In this case, the maximum is achieved at p^*. Thus

$$\Gamma(w) \leqslant \binom{\eta^*}{w}\binom{w}{\frac{w}{q+1}} q^{a+1-p^*}$$

Case 3: $\eta^* - a' \leqslant w \leqslant \left(\frac{q+1}{q}\right)(\eta^* - a')$**,** which implies $a'' < \eta - w \leqslant a'$, $p^* > a'$, and $\eta^* - w/2 > a'$. In this case, the function f_3 is maximized at p^*. Thus for $a' < i \leqslant a$,

$$\binom{i}{\eta^* - w} B_i \leqslant \binom{\eta^*}{w}\binom{w}{\frac{w}{q+1}} q^{a+1-p^*}$$

This also implies that $f_2(i)$ is increasing in the interval $[\eta^* - w, a']$, so the maximum within this interval is achieved at a', which yields

$$\binom{i}{\eta^* - w} B_i \leqslant \binom{\eta^*}{w}\binom{w}{a'-\eta^*+w} q^{\frac{\eta^*}{(\sqrt{q}-1)}} = \binom{\eta^*}{w}\binom{w}{\eta^*-a'} q^{\frac{\eta^*}{(\sqrt{q}-1)}}$$

Comparing the two expressions, we note that $\binom{w}{\frac{w}{q+1}} \geqslant \binom{w}{a'-\eta^*+w}$ since $w/2 > w/(q+1) \geqslant a' - \eta^* + w$, and similarly $q^{\frac{\eta^*}{(\sqrt{q}-1)}} \geqslant q^{a+1-p^*}$. So in this case, we can see that

$$\Gamma(w) \leqslant \binom{\eta^*}{w}\binom{w}{\frac{w}{q+1}} q^{\frac{\eta^*}{(\sqrt{q}-1)}}.$$

Case 4: $\left(\frac{q+1}{q}\right)(\eta^* - a') \leqslant w \leqslant \eta^* - a''$**,** which implies $a'' \leqslant \eta^* - w < a'$, $p^* \leqslant a'$, and $\eta^* - w/2 > a'$. In this case, the function f_2 is maximized at a'. This implies that for every $\eta^* - w \leqslant i \leqslant a'$

$$\binom{i}{\eta^* - w} B_i \leqslant \binom{\eta^*}{w}\binom{w}{a'-\eta^*+w} q^{\frac{\eta^*}{(\sqrt{q}-1)}}.$$

Further this implies that the function $f_3(i)$ is decreasing in the range $[a', a]$, and thus we have

$$\binom{i}{\eta^* - w} B_i \leqslant \binom{\eta^*}{w}\binom{w}{a'-\eta+w} q^{a+1-a'} = \binom{\eta^*}{w}\binom{w}{a'-\eta^*+w} q^{\frac{\eta^*}{\sqrt{q}-1}}$$

Thus we have

$$\Gamma(w) \leqslant \binom{\eta^*}{w}\binom{w}{a'-\eta+w} q^{\frac{\eta^*}{\sqrt{q}-1}} = \binom{\eta^*}{w}\binom{w}{\eta^*-a'} q^{\frac{\eta^*}{\sqrt{q}-1}}$$

Case 5: $\eta^* - a'' \leqslant w \leqslant \left(\frac{q+1}{q}\right)(\eta^* - a'')$**,** which implies $\eta^* - w \leqslant a''$, $p^* > a''$, and $\eta^* - w/2 > a'$ as long as $d^\perp \geqslant \frac{2\eta^*}{(q-1)(\sqrt{q}-1)}$. In this case, f_2 is maximized at a'. This implies that for every $a'' \leqslant i \leqslant a'$,

$$\binom{i}{\eta^* - w} B_i \leqslant \binom{\eta^*}{w}\binom{w}{a' - \eta^* + w} q^{\frac{\eta^*}{\sqrt{q}-1}}$$

Further this implies that the function f_1 is increasing. Thus we have for every $\eta^* - w \leqslant i \leqslant a''$,

$$\binom{i}{\eta^* - w} B_i \leqslant \binom{\eta^*}{w}\binom{w}{a'' - \eta^* + w} q^{\frac{\eta^*}{\sqrt{q}-1}}$$

It also implies that the function f_3 is decreasing. Thus we have for every $a' \leqslant i \leqslant a$,

$$\binom{i}{\eta^* - w} B_i \leqslant \binom{\eta^*}{w}\binom{w}{a' - \eta^* + w} q^{\frac{\eta^*}{(\sqrt{q}-1)}}$$

Note that $a' - \eta^* + w < \frac{w}{2}$ and $a'' < a'$. Hence, in this subcase

$$\Gamma(w) \leqslant \binom{\eta}{w}\binom{w}{a' - \eta^* + w} q^{\frac{\eta^*}{(\sqrt{q}-1)}} = \binom{\eta^*}{w}\binom{w}{\eta^* - a'} q^{\frac{\eta^*}{(\sqrt{q}-1)}}$$

.

Case 6: $\left(\frac{q+1}{q}\right)(\eta^* - a'') \leqslant w \leqslant \eta$**,** which implies $\eta^* - w \leqslant a''$ and $p^* \leqslant a''$. In this case, f_1 is maximized at p^*. Thus, for every $\eta^* - w \leqslant i \leqslant a''$,

$$\binom{i}{\eta^* - w} B_i \leqslant \binom{\eta^*}{w}\binom{w}{\frac{w}{q+1}} q^{a' - p^*}$$

Further this implies that the function f_3 is also decreasing in the range $[a', a]$, and thus we have

$$\binom{i}{\eta^* - w} B_i \leqslant \binom{\eta^*}{w}\binom{w}{a' - \eta^* + w} q^{\frac{\eta^*}{(\sqrt{q}-1)}} \text{ for every } a' \leqslant i \leqslant a$$

1. **Subcase 1:** $\left(\frac{q+1}{q}\right)(\eta^* - a'') \leqslant w \leqslant 2d^\perp + \frac{2\eta^*}{\sqrt{q}-1}$, which implies $\eta^* - w/2 \geqslant a'$. Thus, f_2 is maximized at a', which yields for every $a'' \leqslant i \leqslant a'$

$$\binom{i}{\eta^* - w} B_i \leqslant \binom{\eta^*}{w}\binom{w}{\eta^* - a'} q^{\frac{\eta^*}{\sqrt{q}-1}}$$

Hence,

$$\Gamma(w) \leqslant \max\left\{\binom{\eta^*}{w}\binom{w}{\frac{w}{q+1}} q^{a' - p^*}, \binom{\eta^*}{w}\binom{w}{\eta^* - a'} q^{\frac{\eta^*}{(\sqrt{q}-1)}}\right\}$$

2. **Subcase 2:** $2d^{\perp} + \frac{2\eta^*}{\sqrt{q}-1} \leqslant w \leqslant 2d^{\perp} + \frac{4\eta^*}{\sqrt{q}-1}$, which implies $a'' \leqslant \eta^* - w/2 \leqslant a'$. So f_2 is maximized at $\eta^* - w/2$, which yields for every $a'' \leqslant i \leqslant a'$

$$\binom{i}{\eta^* - w} B_i \leqslant \binom{\eta^*}{w}\binom{w}{w/2} q^{\frac{\eta^*}{\sqrt{q}-1}}$$

Hence,

$$\Gamma(w) \leqslant \max\left\{\binom{\eta^*}{w}\binom{w}{\frac{w}{q+1}} q^{a'-p^*}, \binom{\eta^*}{w}\binom{w}{w/2} q^{\frac{\eta^*}{(\sqrt{q}-1)}}\right\}$$

3. **Subcase 3:** $2d^{\perp} + \frac{4\eta^*}{\sqrt{q}-1} \leqslant w \leqslant \eta^*$, which implies $\eta^* - w/2 \leqslant a''$. So f_2 is maximized at a'', which yields for every $a'' \leqslant i \leqslant a'$

$$\binom{i}{\eta^* - w} B_i \leqslant \binom{\eta^*}{w}\binom{w}{\eta^* - a''} q^{\frac{\eta^*}{\sqrt{q}-1}}$$

By Lemma 21, we can show that $\binom{w}{\frac{w}{q+1}} q^{a'-p^*} \geqslant \binom{w}{\eta^* - a''} q^{\frac{\eta^*}{\sqrt{q}-1}}$. Hence,

$$\Gamma(w) \leqslant \max\left\{\binom{\eta^*}{w}\binom{w}{\frac{w}{q+1}} q^{a'-p^*}, \binom{\eta^*}{w}\binom{w}{\eta^* - a'} q^{\frac{\eta^*}{(\sqrt{q}-1)}}\right\}$$

This completes the proof. □

We prove the following lemma used to prove Lemma 20.

Lemma 21. *For every natural number Δ, we have the following inequality*

$$q^{\Delta} \cdot \binom{w}{w/(q+1)} \geqslant \binom{w}{w/(q+1) + \Delta}$$

Proof. Let $k = w/(q+1)$. then $w = k(q+1)$. It is easy to see that $\frac{w-k-i}{k+\Delta-i} \leqslant q$ for every $0 \leqslant i \leqslant \Delta - 1$. Therefore, we have

$$\frac{\binom{w}{k+\Delta}}{\binom{w}{k}} = \frac{k!(w-k)!}{(k+\Delta)!(w-k-\Delta)!} = \frac{(w-k)(w-k-1)\ldots(w-k-\Delta+1)}{(k+\Delta)(k+\Delta-1)\ldots(k+1)}$$
$$= \prod_{i=0}^{\Delta-1} \frac{w-k-i}{k+\Delta-i} \leqslant \prod_{i=0}^{\Delta-1} q$$
$$= q^{\Delta}$$

□

Lemma 22. *For every natural number Δ, we have the following inequality*

$$\binom{w}{w/(q+1)} \geqslant q^{\Delta}\binom{w}{w/(q+1) - \Delta}$$

Proof. Let $k = w/(q+1)$. then $w = k(q+1)$. It is easy to see that $\frac{w-k+\Delta-i}{k-i} \geqslant q$ for every $0 \leqslant i \leqslant \Delta - 1$. Therefore, we have

$$\begin{aligned}\frac{\binom{w}{k}}{\binom{w}{k-\Delta}} &= \frac{(k-\Delta)!(w-k+\Delta)!}{k!(w-k)!} = \frac{(w-k+\Delta)(w-k+\Delta-1)\dots(w-k+1)}{k(k-1)\dots(k-\Delta+1)} \\ &= \prod_{i=0}^{\Delta-1} \frac{w-k+\Delta-i}{k-i} \geqslant \prod_{i=0}^{\Delta-1} q \\ &= q^{\Delta}\end{aligned}$$

□

D.1 Bias Calculation

Note that in this section $\mathcal{S}(S)$ is the same as $\mathcal{S}(w)$, where $w = \mathsf{wt}(S)$. We are interested in finding the maximum possible bias. That is,

$$2^{-\delta} \leqslant \max_{d^{\perp} \leqslant w \leqslant \eta} \frac{\Gamma(w)}{|\mathcal{S}(w)|}.$$

which is equivalent to

$$\delta \geqslant \min_{d^{\perp} \leqslant w \leqslant \eta} \lg \frac{|\mathcal{S}(w)|}{\Gamma(w)}$$

Define $g(w) = \lg \frac{|\mathcal{S}(w)|}{\Gamma(w)}$.

Lemma 23. *We have the following.*

1. *Let* $g_1(w) = w \lg(q-1) - \mathbf{h_2}(\frac{d^{\perp}}{w})w - \lg q$ *for* $w \in I_1$, *then* g_1 *is decreasing.*
2. *Let* $g_2(w) = w \lg(q-1) - \mathbf{h_2}(\frac{1}{q+1})w - (\frac{wq}{q+1} - d^{\perp} + 1)(\lg q)$ *for* $w \in I_2$, *then* g_2 *is decreasing.*
3. *Let* $g_3(w) = w \lg(q-1) - \frac{\eta^*}{\sqrt{q}-1}(\lg q) - \mathbf{h_2}(\frac{1}{q+1})w$ *for* $w \in I_3$, *then* g_3 *is increasing.*
4. *Let* $g_4(w) = w \lg(q-1) - \mathbf{h_2}(\frac{\eta^*-a'}{w})w - (\frac{wq}{q+1} - d^{\perp} + 1)(\lg q)$ *for* $w \in I_4$, *then* g_4 *is decreasing.*
5. *Let* $g_5(w) = w \lg(q-1) - \mathbf{h_2}(\frac{\eta^*-a'}{w})w - \frac{\eta^*}{\sqrt{q}-1}(\lg q)$ *for* $w \in I_5$, *then* g_5 *is increasing.*
6. *Let* $g_6(w) = w \lg(q-1) - \frac{\eta^*}{\sqrt{q}-1}(\lg q) - \mathbf{h_2}\left(\frac{1}{2}\right) w$ *for* $w \in I_7$. *Then* g_6 *is increasing.*

We use the Lemma 23 to bound Lemma 20. We do case analysis on each case of $\Gamma(w)$. In the following proof, we will use the facts stated in Lemma 23 frequently. Recall that $g(w) = \lg \frac{|\mathcal{S}(w)|}{\Gamma(w)}$.

Case 1: $d^\perp \leqslant w \leqslant \left(\frac{q+1}{q}\right) d^\perp$**.** Let $w_1 = \left(\frac{q+1}{q}\right) d^\perp$, then we have

$$\begin{aligned} g(w) &\geqslant \lg (q-1)^w - \lg \left[q \binom{w}{d^\perp}\right] \approx w \lg(q-1) - \mathbf{h_2}\left(\frac{d^\perp}{w}\right) w - \lg q \\ &\geqslant g_1(w_1) \end{aligned}$$

Case 2: $\left(\frac{q+1}{q}\right) d^\perp \leqslant w \leqslant \eta^* - a'$**.** Let $w_2 = \eta^* - a'$, then

$$\begin{aligned} g(w) &\geqslant \lg(q-1)^w - \lg \left[\binom{w}{\frac{w}{q+1}} q^{a+1-p^*}\right] \\ &\approx w \lg(q-1) - \mathbf{h_2}\left(\frac{1}{q+1}\right) w - (a+1-p^*) \lg q \\ &= w \lg(q-1) - \mathbf{h_2}\left(\frac{1}{q+1}\right) w - \left(\frac{wq}{q+1} - d^\perp + 1\right) (\lg q) \\ &\geqslant g_2(w_2) \end{aligned}$$

Case 3: $\eta^* - a' \leqslant w \leqslant \frac{q+1}{q}(\eta^* - a')$**.** Let $w_3 = \eta^* - a'$, then

$$\begin{aligned} g(w) &\geqslant \lg(q-1)^w - \lg \left[\binom{w}{\frac{w}{q+1}} q^{\frac{\eta^*}{\sqrt{q}-1}}\right] \\ &= w \lg(q-1) - \frac{\eta^*}{\sqrt{q}-1} \lg q - \mathbf{h_2}\left(\frac{1}{q+1}\right) w \\ &\geqslant g_3(w_3) \end{aligned}$$

Case 4: $\frac{q+1}{q}(\eta^* - a') \leqslant w \leqslant \eta^* - a''$**.** Let $w_4 = \eta^* - a''$,

$$\begin{aligned} g(w) &\geqslant \lg(q-1)^w - \lg \left[\binom{w}{\eta^* - a'} q^{a+1-p^*}\right] \\ &\approx w \lg(q-1) - \mathbf{h_2}\left(\frac{\eta^* - a'}{w}\right) w - (a+1-p^*) \lg q \\ &= w \lg(q-1) - \mathbf{h_2}\left(\frac{\eta^* - a'}{w}\right) w - \left(\frac{wq}{q+1} - d^\perp + 1\right) (\lg q) \\ &\geqslant g_4(w_4) \end{aligned}$$

Case 5: $\eta^* - a'' \leqslant w \leqslant \frac{q+1}{q}(\eta^* - a'')$**.** Let $w_5 = \eta^* - a''$.

$$\begin{aligned} g(w) &\geqslant \lg(q-1)^w - \lg \left[\binom{w}{\eta^* - a'} q^{\frac{\eta^*}{\sqrt{q}-1}}\right] \\ &\approx w \lg(q-1) - \frac{\eta^*}{\sqrt{q}-1} (\lg q) - \mathbf{h_2}\left(\frac{\eta^* - a'}{w}\right) w \\ &\geqslant g_5(w_5) \end{aligned}$$

Case 6: $\frac{q+1}{q}(\eta^* - a'') \leqslant w \leqslant \eta^*$**.** Let $w_6 = \frac{q+1}{q}(\eta^* - a'')$, $w_7 = 2d^\perp + \frac{2\eta^*}{\sqrt{q}-1}$, and $w_8 = 2d^\perp + \frac{4\eta^*}{\sqrt{q}-1}$.

$$
\begin{aligned}
g(w) &\geqslant \lg(q-1)^w - \lg\binom{w}{\frac{w}{q+1}} - \lg q^{a'-p^*} \\
&\approx w\lg(q-1) - \mathbf{h_2}\left(\frac{1}{q+1}\right)w - (a'-p^*)\lg q \\
&= w\lg(q-1) - \mathbf{h_2}\left(\frac{1}{q+1}\right)w - \left(\frac{qw}{q+1} - d^\perp - \frac{\eta^*}{\sqrt{q}-1}\right)(\lg q)
\end{aligned}
$$

Let $g_7(w) = g_2(w) + \frac{\eta^*}{\sqrt{q}-1}(\lg q)$

1. **Subcase 1:** $\left(\frac{q+1}{q}\right)(\eta^* - a'') \leqslant w \leqslant 2d^\perp + \frac{2\eta^*}{\sqrt{q}-1}$, we have

$$g(w) \geqslant \min\left(g_7(w_7), g_5(w_6)\right)$$

2. **Subcase 2:** $2d^\perp + \frac{2\eta^*}{\sqrt{q}-1} \leqslant w \leqslant 2d^\perp + \frac{4\eta^*}{\sqrt{q}-1}$, we have

$$g(w) \geqslant \min\left(g_7(w_8), g_6(w_7)\right)$$

3. **Subcase 3:** $2d^\perp + \frac{4\eta^*}{\sqrt{q}-1} \leqslant w \leqslant \eta^*$, we have

$$g(w) \geqslant \min\left(g_7(\eta^*), g_5(w_8)\right)$$

Combining all cases together, we obtain

$$\delta \geqslant g_3(w_3) = (d^\perp + \frac{\eta^*}{\sqrt{q}-1} - 1)(\lg(q-1) - \mathbf{h_2}(\frac{1}{q+1})) - \frac{\eta^*}{\sqrt{q}-1}\lg q$$

Let $\mathbf{h_2}(x) = -x\lg x - (1-x)\lg(1-x)$. We claim the following result by applying Stirling's approximation.

Claim 5. *For every positive integers n, m, we have*

$$\lg\binom{n}{m} \approx \mathbf{h_2}(m/n)n$$

E Parameter Choices

We shall now instantiate the parameters of the code discussed in Appendix C. The code C has the following parameters.

- $|\mathbb{F}| = q = p^s$, for prime p and even integer s and $q \geqslant 49$.

- $\eta^* = (\sqrt{q}-1)\cdot(\sqrt{q})^u$, or equivalently $\eta^*/(\sqrt{q}-1) = (\sqrt{q})^u$, and genus $g = (\sqrt{q})^u$ for $u \in \mathbb{N}$
- Divisor D with $\deg D = (\frac{\sqrt{q}-1}{2} - \rho)g - 1$, for $\rho > 0$
- $\kappa = \deg\, D - g + 1 = (\frac{\sqrt{q}-1}{2} - \rho - 1)g$
- $d = \eta^* - \deg\, D = (\frac{\sqrt{q}-1}{2} + \rho)g + 1$

The code $C^{\perp}$ has the following parameters.

- Divisor $D^{\perp}$ with degree $\deg D^{\perp} = (\frac{\sqrt{q}-1}{2} + \rho + 2)g - 1$
- $\kappa^{\perp} = \deg\, D^{\perp} - g + 1 = (\frac{\sqrt{q}-1}{2} + \rho + 1)g$
- $d^{\perp} = \eta^* - \deg\, D^{\perp} = (\frac{\sqrt{q}-1}{2} - \rho - 2)g + 1$

The code $\mathcal{C}^{(2)}$ has the following parameters.

- Divisor $D^{(2)}$ with degree $\deg D^{(2)} = (\sqrt{q} - 1 - 2\rho)g - 2$
- $\kappa^{(2)} = \deg\, D^{(2)} - g + 1 = (\sqrt{q} - 2 - 2\rho)g - 1$
- $d^{(2)} = \eta^* - \deg\, D^{(2)} = 2\rho g + 2$
- Set $\gamma = d^{(2)} - 2 = 2\rho g$

Simulation Error Computation. We have secret share length $n = 2\cdot\eta\cdot\lg|\mathbb{F}| = 2(\eta^* - \gamma)\lg|\mathbb{F}|$, where $\eta = \eta^* - \gamma$. This implies $n = 2(\lg q)(\sqrt{q} - 1 - 2\rho)g$.

For each $\mathsf{ROLE}(\mathbb{GF}[2^s])$, let $f(s)$ be the number of samples of ROT we extract using [BMN17]. Therefore, the number of ROT samples is $m/2 = f(s)\gamma = f(s)2\rho g$, which implies that $m = f(s)4\rho g$.

We have production rate $\alpha = m/n = \frac{f(s)2\rho}{(\lg q)(\sqrt{q}-1-2\rho)}$. Given a fixed α, we can compute the value of ρ from this equation; namely, $\rho = \frac{(\lg q)(\sqrt{q}-1)\alpha}{2(f(s)+(\lg q)\alpha)}$.

Define

$$Q_N := (\gamma/n)\lg|\mathbb{F}| + (t/n) = [m/(2f(s)n)](\lg q) + \beta = [(\lg q)/(2f(s))]\alpha + \beta$$

Then we are interested in computing the small bias. By Theorem 6, we have that

$$\begin{aligned}\delta &= \left(d^{\perp} + \frac{\eta^*}{\sqrt{q}-1} - 1\right)\cdot\left(\lg(|\mathbb{F}|-1) - \mathbf{h_2}\left(\frac{1}{q+1}\right)\right) - \frac{\eta^*}{\sqrt{q}-1}\lg|\mathbb{F}| \\ &= \left[\left(\frac{\sqrt{q}-1}{2} - \rho - 1\right)g\right]\left[\lg(q-1) - \mathbf{h_2}\left(\frac{1}{q+1}\right)\right] - g(\lg q)\end{aligned}$$

Define $Q_D := \frac{\delta}{n}$. Then we have

$$Q_D = \frac{\left[\left(\frac{\sqrt{q}-1}{2} - \rho - 1\right) g\right]\left[\lg(q-1) - \mathbf{h_2}\left(\frac{1}{q+1}\right)\right] - g(\lg q)}{2(\lg q)(\sqrt{q} - 1 - 2\rho)g}$$
$$= \frac{\left(\frac{\sqrt{q}-1}{2} - \rho - 1\right)\left(\lg(q-1) - \mathbf{h_2}\left(\frac{1}{q+1}\right)\right) - \lg q}{2(\lg q)(\sqrt{q} - 1 - 2\rho)}$$

Now, $\zeta = -\frac{1}{n}\lg\varepsilon = Q_D - Q_N$. We need to ensure that $Q_D > Q_N$ so that $\zeta > 0$.

One Choice of parameters. Suppose for $q = 2^{14}$, we are interested in $\alpha = 16\%$ and $\beta = 1\%$. For these choices of α and β, we have $\zeta > 0$. Figure 10 shows the feasibility region for α and β for $q = 2^{14}$, as well as other values of q.

F Proof of Theorem 4

We will show that our correlation extractor can achieve $t = (1/4 - g)n$, $m = \Theta(n)$, and $\varepsilon = \exp(-\Theta(n))$. In this section we use the same parameters as in Appendix E for general field $\mathbb{F}$ of size q.

- production rate $\alpha = \frac{m}{n}$
- leakage resilience $\beta = \frac{t}{n} = \frac{1}{4} - g$, where $m = c'\gamma$ for some constant c'.
- $Q_D = \frac{\delta}{n}$, where δ is the small bias calculated in Appendix D.1
- $Q_N = (\gamma/n)\lg|\mathbb{F}| + (t/n) = c\alpha + \beta = c\alpha + 1/4 - g$ for some constant $c > 0$
- $\zeta = -\frac{1}{n}\lg\varepsilon = Q_D - Q_N = \delta/n - 1/4 - c\alpha + g$

Choose $\alpha = (g - \varepsilon')/c > 0$ for some constant $\varepsilon' \in (0, g)$. It is clear that α is a constant. Then we need to show that there exists a large enough field size q^* such that ζ is a positive constant. Recall that

- $\delta = (d^\perp + \frac{\eta^*}{\sqrt{q}-1} - 1)(\lg(q-1) - \mathbf{h_2}(\frac{1}{q+1})) - \frac{\eta^*}{\sqrt{q}-1}\lg q$
- $d^\perp = \left(\frac{\sqrt{q}-1}{2} - 2 - \rho\right)\frac{\eta^*}{\sqrt{q}-1}$
- $n = 2(\eta^* - \gamma)\lg q$
- $\gamma = \frac{2\rho\eta^*}{\sqrt{q}-1}$, where ρ is a constant

Thus, we have the following as $\eta^* \to \infty$

$$\begin{aligned}\frac{\delta}{n} &\approx \frac{(\frac{\sqrt{q}-1}{2} - 1 - \rho)\frac{\eta^*}{\sqrt{q}-1}(\lg(q-1) - \mathbf{h_2}(\frac{1}{q+1})) - \frac{\eta^*}{\sqrt{q}-1}\lg q}{2\eta^*(1-2\rho/(\sqrt{q}-1))\lg q} \\ &\approx \frac{\lg(q-1) - \mathbf{h_2}(\frac{1}{q+1})}{4(1-2\rho/(\sqrt{q}-1))\lg q} - \frac{(1+\rho)\left(\lg(q-1) - \mathbf{h_2}(\frac{1}{q+1})\right) - \lg q}{2(1-2\rho/(\sqrt{q}-1))(\sqrt{q}-1)\lg q} \\ &= f(q)\end{aligned}$$

Note that $f(q)$ is increasing and that $f(q) \to 1/4$ as $q \to \infty$, which implies that there exists a large enough constant q^* such that $f(q^*) \geqslant 1/4 - \varepsilon'/2$. Therefore

$$\zeta \geqslant (1/4 - \varepsilon'/2) - 1/4 - c \cdot \frac{g - \varepsilon'}{c} + g = \varepsilon'/2 > 0$$

which completes our proof.

G Proof of Theorem 5

For completeness, we restate and prove Theorem 5.

Let $\mathcal{F} = \{F_1, \ldots, F_\mu\}$ be a ρ^2-biased family of distributions over the sample space $\mathbb{F}^\eta$ for field $\mathbb{F}$ of size q. Let (M, L) be a joint distribution such that the marginal distribution M is over $\mathbb{F}^\eta$ and $\widetilde{\mathbf{H}}_\infty(M|L) \geqslant m$. Then, the following holds:

$$\mathrm{SD}\left(\ (F_J \oplus M, L, J)\ ,\ (U_{\mathbb{F}^\eta}, L, J)\ \right) \leqslant \frac{\rho}{2}\left(\frac{|\mathbb{F}|^\eta}{2^m}\right)^{1/2}$$

where J is a uniform distribution over $[\mu]$.

Proof.

$$\begin{aligned}&2\mathrm{SD}\left(\ (F_J \oplus M, L, J)\ ,\ (U_{\mathbb{F}^\eta}, L, J)\ \right) \\ &= \mathop{\mathbb{E}}_{\substack{\ell\sim L\\ j\sim J}} 2\mathrm{SD}\left(\ (F_j \oplus M \mid \ell, j)\ ,\ (U_{\mathbb{F}^\eta} \mid \ell, j)\ \right) \\ &= \mathop{\mathbb{E}}_{\substack{\ell\sim L\\ j\sim J}} \sum_{x\in\mathbb{F}^\eta} |(F_j \oplus M \mid \ell, j)(x) - (U_{\mathbb{F}^\eta} \mid \ell, j)(x)| \\ &\leqslant \mathop{\mathbb{E}}_{\substack{\ell\sim L\\ j\sim J}} \left(|\mathbb{F}|^\eta \sum_{x\in\mathbb{F}^\eta} |[(F_j \oplus M \mid \ell, j) - (U_{\mathbb{F}^\eta} \mid \ell, j)]\,(x)|^2\right)^{1/2} && [1] \\ &= |\mathbb{F}|^{\eta/2} \mathop{\mathbb{E}}_{\substack{\ell\sim L\\ j\sim J}} \left(|\mathbb{F}|^\eta \sum_{S\in\mathbb{F}^\eta} \left|\widehat{[(F_j \oplus M \mid \ell, j) - (U_{\mathbb{F}^\eta} \mid \ell, j)]}(S)\right|^2\right)^{1/2} && [2] \\ &= |\mathbb{F}|^\eta \mathop{\mathbb{E}}_{\substack{\ell\sim L\\ j\sim J}} \left(\sum_{S\in\mathbb{F}^\eta} \left|\widehat{(F_j \oplus M \mid \ell, j)}(S) - \widehat{(U_{\mathbb{F}^\eta} \mid \ell, j)}(S)\right|^2\right)^{1/2} && [3]\end{aligned}$$

$$= |\mathbb{F}|^\eta \mathop{\mathbb{E}}_{\substack{\ell\sim L\\ j\sim J}} \left(\sum_{S\in\mathbb{F}^\eta\setminus\{0\}} \left|\widehat{(F_j \oplus M \mid \ell, j)}(S)\right|^2 \right)^{1/2} \quad [4]$$

$$= |\mathbb{F}|^\eta \mathop{\mathbb{E}}_{\substack{\ell\sim L\\ j\sim J}} \left(\sum_{S\in\mathbb{F}^\eta\setminus\{0\}} |\mathbb{F}|^{2\eta} \left|\widehat{(F_j \mid \ell, j)}(S)\right|^2 \left|\widehat{(M \mid \ell, j)}(S)\right|^2 \right)^{1/2} \quad [5]$$

$$\leqslant |\mathbb{F}|^{2\eta} \left(\mathop{\mathbb{E}}_{\substack{\ell\sim L\\ j\sim J}} \sum_{S\in\mathbb{F}^\eta\setminus\{0\}} \left|\widehat{(F_j \mid \ell, j)}(S)\right|^2 \left|\widehat{(M \mid \ell, j)}(S)\right|^2 \right)^{1/2} \quad [6]$$

$$= |\mathbb{F}|^{2\eta} \left(\sum_{S\in\mathbb{F}^\eta\setminus\{0\}} \mathop{\mathbb{E}}_{\ell\sim L} \mathop{\mathbb{E}}_{j\sim J} \left|\widehat{(F_j \mid \ell, j)}(S)\right|^2 \left|\widehat{(M \mid \ell, j)}(S)\right|^2 \right)^{1/2} \quad [7]$$

$$= |\mathbb{F}|^{2\eta} \left(\sum_{S\in\mathbb{F}^\eta\setminus\{0\}} \mathop{\mathbb{E}}_{\ell\sim L} \left[\left|\widehat{(M \mid \ell)}(S)\right|^2 \mathop{\mathbb{E}}_{j\sim J} \left|\widehat{(F_j \mid \ell, j)}(S)\right|^2 \right] \right)^{1/2} \quad [8]$$

$$= |\mathbb{F}|^{2\eta} \left(\sum_{S\in\mathbb{F}^\eta\setminus\{0\}} \mathop{\mathbb{E}}_{\ell\sim L} \left[\left|\widehat{(M \mid \ell)}(S)\right|^2 \mathop{\mathbb{E}}_{j\sim J} \left|\widehat{(F_j \mid j)}(S)\right|^2 \right] \right)^{1/2} \quad [9]$$

$$\leqslant |\mathbb{F}|^{2\eta} \left(\sum_{S\in\mathbb{F}^\eta\setminus\{0\}} \mathop{\mathbb{E}}_{\ell\sim L} \left[\left|\widehat{(M \mid \ell)}(S)\right|^2 \cdot \frac{\rho^2}{|\mathbb{F}|^{2\eta}} \right] \right)^{1/2} \quad [10]$$

$$\leqslant \rho|\mathbb{F}|^\eta \left(\sum_{S\in\mathbb{F}^\eta} \mathop{\mathbb{E}}_{\ell\sim L} \left|\widehat{(M \mid \ell)}(S)\right|^2 \right)^{1/2}$$

$$= \rho|\mathbb{F}|^\eta \left(\mathop{\mathbb{E}}_{\ell\sim L} \sum_{S\in\mathbb{F}^\eta} \left|\widehat{(M \mid \ell)}(S)\right|^2 \right)^{1/2} \quad [11]$$

$$\leqslant \rho|\mathbb{F}|^\eta \left(\mathop{\mathbb{E}}_{\ell\sim L} 2^{-\mathbf{H}_\infty(M \mid \ell)} \right) \quad [12]$$

$$= \rho|\mathbb{F}|^\eta \left(2^{-\widetilde{\mathbf{H}}_\infty(M \mid L)} \right)^{1/2} \quad [13]$$

$$\leqslant \rho|\mathbb{F}|^\eta \left(\frac{1}{|\mathbb{F}|^\eta 2^m} \right)^{1/2} \quad [14]$$

$$= \rho \left(\frac{|\mathbb{F}|^\eta}{2^m} \right)^{1/2}$$

[1] Cauchy-Schwartz
[2] Corollary 9
[3] Linearity of Definition 5
[4] Lemma 17 and Lemma 18
[5] Lemma 16
[6] Jensen's Inequality
[7] Linearity of $\mathbb{E}$
[8] M is independent of j
[9] F_j is independent of ℓ for every j
[10] $\mathcal{F}$ is a ρ^2-biased family
[11] Linearity of $\mathbb{E}$
[12] Lemma 3
[13] Definition of $\widetilde{\mathbf{H}}_\infty$
[14] $\widetilde{\mathbf{H}}_\infty(M|L) \geqslant m$

$\square$