Round-Optimal Correlation Extractors with Linear Production and Leakage Resilience

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

May 24, 2017

Abstract

Correlated private randomness, or correlation, in short, is a fundamental cryptographic resource that helps parties compute securely over their private data. An offline preprocessing step, which is independent of the eventual secure computation, generates correlated secret shares for parties and the parties use these shares during the final secure computation step. However, these secret shares are vulnerable to leakage attacks.

Inspired by the quintessential problem of privacy amplification, Ishai, Kushilevitz, Ostrovsky and Sahai (FOCS 2009) introduced the concept of correlation extractors. Correlation extractors are interactive protocols that take leaky correlations as input and produce secure independent copies of oblivious transfer (OT), the building blocks of secure computation protocols. This initial feasibility result has four rounds, which is not optimal. The sequence of works appearing in CRYPTO 2015 and CRYPTO 2017 only achieves sub-linear production, though they are round-optimal.

In this paper, we show the existence of a correlation that produces n-bit shares for the parties, and there exists a round-optimal correlation extractor that allows the extraction of αn secure OTs, despite βn bits of leakage on the secret shares, for appropriate positive constants α and β. Our construction has two primary components. The first component, the key technical contribution of this paper, uses suitable Algebraic Geometry Codes to provide new constructions for families of small-bias distributions that are also multiplication friendly secret sharing schemes. Using these distributions, we produce secure random oblivious linear function evaluations (ROLE) over a large (but constant-size) field. Next, we employ the "OT-embedding" technique introduced by Block et al. (CRYPTO 2017) to recover OTs from these ROLEs at a good rate.

The initial feasibility result by Ishai et al. is the only known correlation extractor that is resilient to a linear leakage and produces a linear number of "fresh" OTs. It employs an "OT reversal method" (a technique to amplify the "leakage resilience against one party" to achieve "leakage resilience against both parties simultaneously") that has a devastating effect on the fractional leakage resilience and production rates by reducing both these quantities quadratically. Our approach entirely circumvents this loss and, overall, achieves higher values of α and β.

[*]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.

1 Introduction

Correlated private randomness, or correlations, in short, are extremely fundamental cryptographic resources that help construct fast secure computation protocols with strong security guarantees. In a preprocessing step, a trusted dealer samples secret shares (r_A, r_B) from a joint distribution (R_A, R_B), namely the *correlated private randomness* or *correlation*. The dealer, then, provides r_A to Alice and r_B to Bob, their respective secret shares. Later, during the online step, Alice and Bob use their respective secret shares to perform their intended computation securely. Secure computation protocols offload most of their computational and cryptographic complexity to the preprocessing step and employ fast online protocols. There are suitable correlations that help preserve the privacy of an honest party's private input even when all other parties are adversarial, colluding, and have unbounded computational power. Besides, even computationally secure protocols or appropriate physical hardware can also implement the dealer, and the online phase can only be computationally secure. Due to these salient features, this versatile framework of protocol design has produced several success stories, for example, FairPlay [MNPS04, BDNP08], TinyOT [NNOB12] and SPDZ [DPSZ12] (pronounced Speedz).

Indeed, even secure computation protocols, not originally proposed in the preprocessing model, such as the influential GMW [GMW87] protocol, can easily be modified to work in the preprocessing model to utilize a fast online phase protocol. For the GMW protocol, the preprocessing step provides multiple samples of the *random oblivious transfer* correlation, represented by ROT. It samples three bits x_0, x_1, b independently and uniformly at random, and provides the secret shares (x_0, x_1) to Alice and (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}. Intuitively, ROT is an input-less functionality that implements a randomized version of the *oblivious transfer* functionality (represented as OT), where the sender sends (x_0, x_1) as input to the functionality and the receiver picks x_b out of the two input bits. Given m independent samples from the ROT distribution, parties can securely compute any functionality with circuit complexity (roughly) m. Using the random self-reducibility of oblivious transfer [WW06], we can reimagine the GMW protocol [GMW87], originally proposed in the OT hybrid, in this framework naturally.

However, there is a concern associated with generating secret shares in the preprocessing phase for future use in cryptographic protocols. For instance, adversarial parties can leak information about honest parties' secret shares. We emphasize that the leakage need not necessarily reveal individual bits of the other 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. To address this issue, Ishai, Kushilevitz, Ostrovsky, and Sahai (FOCS 2009) [IKOS09] introduced the concept of correlation extractors. A *correlation extractor* is an interactive protocol that takes leaky correlations as input and outputs fresh correlations that are information-theoretically secure. Parties can, first, use the correlation extractor on leaky correlations and, then, run the secure computation using the fresh correlations.

The reduction of the overheads of running a correlation extractor before the execution of a secure computation protocol will facilitate their adoption. We present, in the sequel, a few such representative prominent overheads.

- Round Complexity: Round complexity is a fundamental measure of efficiency for any interactive protocol. The latency of sending messages is often the dominating factor in the running time of cryptographic protocols and dictates the feasibility of actual usage of a protocol. The pure aesthetics of constructing round-optimal protocols is altogether an independent motivation. For correlation extractors, two rounds[1] are *necessary* [WW06].

[1] In a two-round protocol the first party sends the first message and then the second party sends the final message.

	Correlation Description	Round Complexity	Number of OTs Produced (m)	Number of Leakage bits (t)	Simulation Error (ε)
IKOS [IKOS09]	$\mathsf{ROT}^{n/2}$	4	$\alpha' n$	$\beta' n$	$2^{-\zeta' n}$
GIMS [GIMS15]	$\mathsf{ROT}^{n/2}$	2	$n/\operatorname{poly}\lg n$	$(1/4 - g)n$	$2^{-gn/m}$
	$\mathsf{IP}\left(\mathbb{GF}\left[2\right]^n\right)$	2	1	$(1/2 - g)n$	2^{-gn}
BMN [BMN17]	$\mathsf{IP}\left(\mathbb{F}^{n/\lg\lvert\mathbb{F}\rvert}\right)$	2	$n^{1-o(1)}$	$(1/2 - g)n$	2^{-gn}
Our Result	$\mathsf{ROLE}\left(\mathbb{F}\right)^{n/2\lg\lvert\mathbb{F}\rvert}$	2	αn	βn	$2^{-\zeta n}$

Figure 1: A qualitative summary of prior relevant works in correlation extractors and a comparison to our correlation extractor construction. All correlations have been normalized so that each party gets an n-bit secret share.

- Production (m): For the ease of presentation, we quantitatively measure the production of a correlation extractor based on the number of ROT samples it outputs. More concretely, if a correlation extractor outputs secret shares of the $\mathsf{ROT}^{m/2}$ correlation then the correlation extractor has production m, the length of the secret shares of each party output by the correlation extractor. This amount has direct consequences on the complexity of the cryptographic protocol that uses the output of the correlation extractor. For example, in the setting of secure computation, the production rate m (roughly) translates into an upper-bound on the circuit size that the parties can compute securely. We would like to maximize this quantity.

- Leakage Resilience (t): Given n-bit secret shares, leakage resilience is the maximum bits of leakage that a correlation extractor can tolerate before it becomes insecure. Ideally, we will like to maximize this parameter, but in certain scenarios, the parties might be willing to partially trade this off to gain better performance on other metrics.

- Insecurity Bound (ε): Just like any cryptographic protocol, there is a chance that the correlation extractor itself is not secure against adversarial attacks. We use standard simulation security, à la Canetti [Can00], to upper bound the insecurity induced by *any* adversarial attack. Ideally, we want this to be exponentially small so that even a small increase in the statistical security parameter prohibitively increases the computational cost of all adversarial attacks.

The list above is intended to represent a holistic set of optimization objectives instead of a prioritized list. Clearly, the priorities associated with these overheads are significantly dependent on the context, for example, the time elapsed since the preprocessing completion, and can guide the extractor choice. If parties established the secret shares only recently, then the parties could be willing to risk using a less resilient extractor. However, with the passage of time, they might prefer higher resilience.

The initial feasibility result of Ishai et al. [IKOS09] is a four round protocol and, hence, is not round optimal. The sequence of works of Gupta et al. [GIMS15] and Block et al. [BMN17] only achieves sub-linear production, though they are round-optimal. These results leave open the following natural and intriguing direction of inquiry.

"Can round-optimal correlation extractors have linear production and leakage resilience?"

We resolve this question in the affirmative. We construct the *first* correlation extractor that is round optimal and has linear production and leakage resilience (with exponentially low insecurity). 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 parameter for *all* the four objectives motivated above.

1.1 Model

This section presents the standard model of Ishai et al. [IKOS09] for correlation extractors, which subsequent works also use. 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 $(R_A, R_B)^{[t]}$.[2]

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.

1.2 Our Contribution

Our work presents the first round-optimal correlation extractor that has linear production and linear leakage resilience (along with exponentially low insecurity).

Theorem 1 (Round Optimal Asymptotically Good Correlation Extractor)**.** *There exists a correlation (R_A, R_B) that produces n-bit secret shares and there exists a round-optimal (n, m, t, ε)-correlation extractor for (R_A, R_B) such that m/n, t/n, and $-\frac{1}{n}\log\varepsilon$ are all positive constants.*

In the theorem above, we use a correlation (R_A, R_B) that performs multiple samples from a generalization of the ROT correlation. For any 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 $2\lg|\mathbb{F}|$. Therefore, the correlation used in Theorem 1 is $\mathsf{ROLE}(\mathbb{F})^{n/2\lg|\mathbb{F}|}$, i.e., each party receives $n/2\lg|\mathbb{F}|$ independent samples from the $\mathsf{ROLE}(\mathbb{F})$ correlation, for suitable constant-size fields $\mathbb{F}$. Figure 4 presents 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]. Section 1.4 summarizes the intuition underlying the entire construction.

The suitable multiplication friendly secret sharing scheme based on Algebraic Geometry Codes exist for all fields $\mathbb{F}$ such that $|\mathbb{F}|$ is an even power of a prime and $|\mathbb{F}| \geqslant 49$. Over $\mathbb{F} = \mathbb{GF}\left[2^6\right]$, the smallest such field with characteristic 2,[3] our construction achieves $\alpha = 1\%$ production rate, $\beta = 1\%$ fractional resilience, and $\zeta = -\frac{1}{n}\lg\varepsilon = 0.40\%$ insecurity (refer to Appendix G). Compared

[2] 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.

[3] The ROLE correlation over fields of characteristic 2 have a natural bit-representation for its secret shares.

to Ishai et al. [IKOS09], our result provides round optimality while, surprisingly, also provides comparatively higher production and resilience.[4] The primary rate loss in IKOS is attributable to the fact that they construct a one-sided correlation extractor, which is only secure against one party's leakage. Then, they sequentially compose this protocol twice (along with OT-reversal [WW06]) to protect against leakage of both parties. Our result sets forth the foundations for future work for round-optimal asymptotically good correlation extractor construction with observable parameters.

Similar to the construction of IKOS, our construction can also be used to construct a correlation extractor from *any* correlation and output samples of *any* correlation; albeit it is not round optimal anymore. However, our constructions achieve overall better production and resilience than the IKOS construction. Figure 2 outlines a comparison of these two correlation extractor construction for the general case.

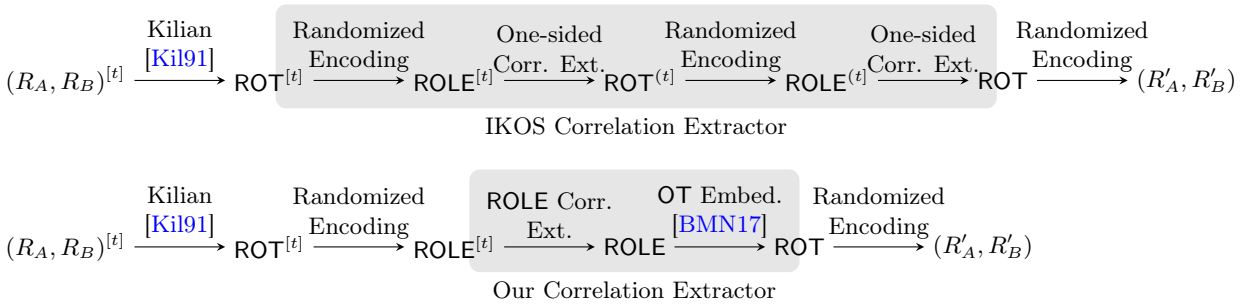

Figure 2: Correlation extractors in the general setting: Extracting arbitrary correlations from arbitrary correlations. Expanded IKOS [IKOS09] correlation extractor to enable efficiency comparison with our correlation extractor of Figure 4. In this figure, to reduce cumbersome notions, it is implicit 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.

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 leak individual bits of the other 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-round error-tolerant[5] combiners that produce fresh ROLEs over large fields[6] from ROLEs over the same field. Using multiplication friendly secret sharing schemes based on Algebraic Geometry Codes introduced by Chen and Cramer [CC06], a similar construction works over ROLEs over fields with appropriate constant size. We emphasize that this construction is *insecure* if an

[4] Even optimistic estimates of the parameters α and β for the IKOS construction are in the order of 10^{-6}.

[5] 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.

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

adversary can perform even 1-bit leakage on the whole secret of the other party. Section 1.4 provides further details on the limitations of this construction.

1.4 Technical Overview

This section briefly summarizes our construction and its underlying technical ideas.

Outline of the General Correlation Extractor Design Paradigm. Figure 3 introduces the correlation extractor design paradigm underlying the construction of this paper, which is also common to the protocols in [IMSW14, GIMS15, BMN17].

1. From an ensemble of pair of linear codes $\{(\mathcal{C}_k, \mathcal{D}_k)\colon k \text{ in the index set}\}$, Client A and B agree on a pair of linear codes $(\mathcal{C}, \mathcal{D})$
2. Let $\mathcal{E}$ be a linear code that contains all the coordinate-wise product of each codeword in $\mathcal{C}$ with each codeword in $\mathcal{D}$, represented by $\mathcal{E} \supseteq \mathcal{C} * \mathcal{D}$

---

3. Clients A and B have η samples from the $\mathsf{ROLE}(\mathbb{F})$ correlation from the preprocessing step

---

4. Client A picks a random codeword $(u_{-\gamma}, \ldots, u_{-1}, u_1, \ldots, u_\eta) \in \mathcal{C}$
5. Client B picks a random codeword $(r_{-\gamma}, \ldots, r_{-1}, r_1, \ldots, r_\eta) \in \mathcal{D}$
6. Client A picks a random codeword $(v_{-\gamma}, \ldots, v_{-1}, v_1, \ldots, v_\eta) \in \mathcal{E}$

---

7. For each $i \in \{1, \ldots, \eta\}$: Clients A and B use their respective i-th ROLE secret shares to help client B securely compute $z_i = u_i r_i + v_i$
8. Client B reconstructs $(z_{-\gamma}, \ldots, z_{-1}, z_1, \ldots, z_\eta) \in \mathcal{E}$ using erasure recovery algorithm for $\mathcal{E}$

---

9. Client A outputs (u_i, v_i) and Client B outputs (r_i, z_i), for each $i \in \{-\gamma, \ldots, -1\}$

Figure 3: Round-optimal correlation extractor design paradigm based on Massey secret sharing scheme.

Note that only steps (1) and (7) require interaction. Step (1), which is equivalent to secure coin tossing, can be performed by either party because the parties are semi-honest. Step (7) is a two-round protocol (cf. [WW06]). Hence, the overall protocol is a two-round protocol, if the client who sends the first message for step (7) also performs step (1). If $\mathcal{E}$ admits an efficient erasure recovery algorithm and $d(\mathcal{E}) > \gamma$, then client B can efficiently perform step (8). Note that, for every $i \in \{-\gamma, \ldots, -1\}$, the outputs (u_i, v_i) and (r_i, z_i) are correct $\mathsf{ROLE}(\mathbb{F})$ secret shares. The privacy of this protocol, which also subsumes the argument that the output $\mathsf{ROLE}(\mathbb{F})$ secret shares are independent, relies on the particulars of the leakage model and the choices of the ensemble of codes $\mathcal{C}$, $\mathcal{D}$, and $\mathcal{E}$.

Instantiation for [IMSW14, GIMS15, BMN17]. The recent works of [IMSW14, GIMS15, BMN17] on round-optimal correlation extractor construction create the ensemble of codes as follows. Let $\{\mathcal{C}_k\}$ be the set of all linear codes, and $\mathcal{D}_k$ is the dual code of $\mathcal{C}_k$. Consequently, for any pair of linear codes $(\mathcal{C}, \mathcal{D})$ in the ensemble, set $\mathcal{E}$ as the linear code such that the sum of every element in the codeword is 0, referred to as the *parity code*. Since the parity code has distance 2 and it can efficiently recover one erasure, we have $\gamma = 1$. We emphasize that [IMSW14, GIMS15] use $\mathbb{F} = \mathbb{GF}[2]$, while [BMN17] uses large fields with characteristic 2.

In each of these works, the security argument for the correlation extractor reduces to the observation that, given any particular non-trivial linear test, a random codeword from a random code fools

this linear test. Note that linear leakage is a special type of leakage, and surprisingly protecting only against all linear leakage suffices to protect against arbitrary leakage. Thus, protection against linear leakage is not only necessary but also sufficient.

More concretely, consider any non-zero $S = (S_{-\gamma}, \ldots, S_{-1}, S_1, \ldots, S_\eta) \in \mathbb{F}^{\gamma+\eta}$. The linear function $L_S \colon \mathbb{F}^{\gamma+\eta} \to \mathbb{F}$ is defined by $L_S(x_{-\gamma}, \ldots, x_{-1}, x_1, \ldots, x_\eta) = \sum_{i \in \{-\gamma,\ldots,-1,1,\ldots,\eta\}} S_i x_i$. If x is chosen uniformly at random from $\mathbb{F}^{\gamma+\eta}$ then the output of $L_S(x)$ is uniformly random over $\mathbb{F}$, for all non-zero S. However, if x is chosen uniformly at random from a vector subspace of $\mathbb{F}^{\gamma+\eta}$, then L_S is a constant function for every S in the dual of this subspace. So, sampling x from a *particular subspace* of $\mathbb{F}^{\gamma+\eta}$ is unable to fool every linear test. Sampling x from an *ensemble* of subspaces of $\mathbb{F}^{\gamma+\eta}$, on the other hand, can fool every non-trivial linear test, except with an exponentially low probability. Such ensembles are called a *family of small-bias distributions.* In these works, the privacy of client A and client B, respectively, reduces to demonstrating that the ensemble of the codes $\{\mathcal{C}_k\}$ and the ensemble of the codes $\{\mathcal{D}_k\}$, both, satisfy this property. We emphasize that if there exists S such that the linear test L_S is, say, not fooled by the ensemble of codes $\{\mathcal{C}_k\}$ then an adversarial client B can perform a 1-bit leakage to violate the privacy of client A. Moreover, intuitively, as the probability of fooling linear tests gets closer to 1, the protocol can have higher production (if permitted by the distance of $\mathcal{E}$) and tolerate more leakage.

The approach mentioned above only achieves $d(\mathcal{E}) = 2$ and, consequently, $\gamma = 1$. To achieve linear production, a potential approach is to ensure that $d(\mathcal{E})$ is linear. This approach reduces the goals of our work to the following.

Our Target Properties. Over constant size fields

1. Construct the ensemble $\{(\mathcal{C}_k, \mathcal{D}_k)\}$ such that the linear code $\mathcal{E} \supseteq \mathcal{C}_k * \mathcal{D}_k$ has linear distance, for each k, and
2. The ensembles of codes $\{\mathcal{C}_k\}$ and $\{\mathcal{D}_k\}$ are both families of small bias distributions.

Related work of [MPW07, PW08] using secret-sharing schemes of [CC06]. [7] Using Algebraic Geometry Codes, there are near-MDS codes with one of the properties mentioned above, namely, target property (1). There is an appropriate AG Code $\mathcal{C}^*$ such that, if $\mathcal{C} = \mathcal{D} = \mathcal{C}^*$ then the code $\mathcal{E}$ has linear distance. We have already discussed that any one code cannot fool all linear tests, so this idea clearly *does not* suffice for our goals. However, [MPW07, PW08] use this idea to achieve the partial goal of protection against the leakage of individual bits of the secret shares. In fact, the construction is robust to linear tests S with small support, and there are 1-bit linear leakages with a large support that render this construction insecure. To achieve our goals, we need to fool every linear test, including the ones with large support.

Related work of [IKOS09]. The approach of Ishai et al. [IKOS09], which also uses this AG Code $\mathcal{C}^*$, can be interpreted in the paradigm presented in Figure 3, albeit a minor modification. The ensemble of codes $\{\mathcal{C}_k\}$ is *non-linear* code,[8] that is a family of small biased distribution, while the code $\mathcal{D}$ is an appropriate fixed linear code. This approach, therefore, achieves security for client A against an adversarial client B. Recall that this is the primary reason that their construction is not round optimal. To achieve our goals, we need to construct $\{\mathcal{C}_k, \mathcal{D}_k\}$ that are both families of small bias distributions.

[7] We emphasize that the original constructions of [MPW07, PW08] used Reed-Solomon codes over large fields. We believe that near MDS AG codes over constant size fields can also be used in their protocols.

[8] Concatenation of an AG code with a binary representation of the field elements, a majority encoding of each bit, and a randomized encoding for a suitable constant-size functionality. The ensemble is constructed by enumerating all outcomes of the probabilistic encoding procedures.

Our Approach. Our starting point is the suitable AG code $\mathcal{C}^*$ mentioned above, and let G^* be the generator matrix of $\mathcal{C}^*$. Assume that its columns are indexed $\{-\gamma, \ldots, -1, 1, \ldots, \eta\}$. We explain our first step towards constructing the ensemble $\{(\mathcal{C}_k, \mathcal{D}_k)\}$. We pick a permutation $\pi\colon \{-\gamma, \ldots, -1, 1, \ldots, \eta\} \to \{-\gamma, \ldots, -1, 1, \ldots, \eta\}$ and permute the columns of G^* according to π. Let the resultant permuted code be $\mathcal{C}^*_\pi$. We consider the ensemble of codes $\{(\mathcal{C}^*_\pi, \mathcal{C}^*_\pi)\colon \pi \text{ is a permutation}\}$. Recall that the linear code $\mathcal{E}^* = \mathcal{C}^* * \mathcal{C}^*$. So, for every permutation π, we have $\mathcal{E}^*_\pi = \mathcal{C}^*_\pi * \mathcal{C}^*_\pi$, and the code $\mathcal{E}^*_\pi$ has identical distance as $\mathcal{E}^*$.

To illustrate the underlying intuition for this construction, we work over the binary field. We emphasize that the AG Codes mentioned above exist when the size of the field is at least 49 and is an even power of a prime. Making this simplifying assumption on the field size helps demonstrate the principle ideas and hurdles intuitively.

For simplicity, assume that $\mathbb{F} = \mathbb{GF}[2]$. Let L_S be an arbitrary linear test, and $\mathsf{wt}(S)$ represent the number of 1s in S. To assist the computation of the probability of fooling a particular linear test, observe that the following two quantities are identical.

1. The probability of fooling L_S when x is randomly sampled from $\mathcal{C}^*_\pi$, for random π, and
2. The probability of fooling L_T when x is randomly sampled from $\mathcal{C}^*$, for random T such that $\mathsf{wt}(T) = \mathsf{wt}(S)$.

Since the dual distance of $\mathcal{C}^*$ is linear, if a random $x \in \mathcal{C}^*$ does not fool L_{T_1} and L_{T_2}, then the Hamming distance between T_1 and T_2 is linear. Equivalently, a random $x \in \mathcal{C}^*$ fools linear tests in the neighborhood of L_{T_1}. We refer to this as the *empty neighborhood*.

Let $\mathsf{class}(S)$ be the set of all T such that $\mathsf{wt}(S) = \mathsf{wt}(T)$. If we can show that for every $T \in \mathsf{class}(S)$ that is not fooled by a random $x \in \mathcal{C}^*$ has a disjoint and exponentially large empty neighborhood in $\mathsf{class}(S)$, then we are done. Because, when T is randomly sampled from $\mathsf{class}(S)$ only one out of exponentially many linear tests will not be fooled for $x \in \mathcal{C}^*$.

We can show that this property holds only if S neither has low weight nor nearly full weight, i.e., the weight of S is *balanced*. Since $\mathcal{C}^*$ has linear dual distance, we know that S cannot have a low weight. So, the only concern is when S has nearly full weight. For the AG codes $\mathcal{C}^*$ that we are considering, there are indeed S with (nearly) full weight in the dual code. This hurdle motivates the second component of our technical contribution.

Given the generator matrix G^* for the code $\mathcal{C}^*$, we construct a new generator matrix defined by the following block matrix.

$$\widetilde{G} = \begin{bmatrix} I_{f\times f} & 0 \\ 0 & G^* \end{bmatrix}$$

Note that, if H^* is the generator matrix for the dual of $\mathcal{C}^*$, then the dual of the code generated by $\widetilde{G}$ has the generator matrix $\widetilde{H} = \begin{bmatrix} \overbrace{0\cdots 0}^{f\text{-times}} & H^* \end{bmatrix}$. By choosing large enough f, we ensure that the dual of the code generated by $\widetilde{G}$ does not have a high weight. However, the permutation π needs to be carefully chosen. We choose only those permutations π such that it maps $\{-\gamma, \ldots, -1\}$ only from the columns corresponding to G^* in $\widetilde{G}$; otherwise, erasure recovery will not be possible.

Using this technique, we construct ensembles of codes $\{(\mathcal{C}_\pi, \mathcal{C}_\pi)\colon \pi \text{ is a suitable permutation}\}$ such that their corresponding $\mathcal{E}_\pi$ has linear distance (so, we can set γ linear in η). Additionally, the ensembles $\{\mathcal{C}_\pi\}$ and $\{\mathcal{D}_\pi\}$ are families of small-bias distributions. Thus, we achieve round-optimal correlation extractor construction with linear production and resilience. Figure 4 provides the explicit protocol and Section 4.2 presents the security proof, which proceeds via an extraction lemma (Unpredictability Lemma, Lemma 4 in Section 3).

OT embedding [BMN17]. It suffices to construct a correlation extractor that outputs multiple samples of the $\mathsf{ROLE}(\mathbb{F})$ correlations. The recent work of [BMN17] provides a technique to obtain multiple ROT samples from every ROLE sample in two rounds with perfect security. For comparison, IKOS implement only one ROT from one $\mathsf{ROLE}(\mathbb{F})$. The construction of [BMN17] composes in parallel with the correlation extractor that outputs secret shares of the $\mathsf{ROLE}(\mathbb{F})$ correlation, thus preserving its round complexity.

2 Preliminaries

Symbolic Notations. We denote random variables by capital letters, for example X, and the values taken by small letters, for example $X = x$. We denote the set $\{1, \ldots, \eta\}$ by $[\eta]$. For any vector $x = (x_1, \ldots, x_\eta)$ and subset $T = (i_1, \ldots, i_{|T|})$, we use x_T to denote $(x_{i_1}, \ldots, x_{i_{|T|}})$. Let $\mathcal{S}_\eta$ be the set of all permutations $\pi : [\eta] \to [\eta]$. We consider the field $\mathbb{F} = \mathbb{GF}(q)$, where q is a power of prime p. For any $c = (c_1, \ldots, c_\eta) \in \mathbb{F}^\eta$, 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, $x * y = (x_1 y_1, x_2 y_2, \ldots, x_\eta y_\eta) \in \mathbb{F}^\eta$. For a set Y, U_Y denotes the uniform distribution on Y.

The statistical distance between two distributions X and Y, represented by $\mathsf{SD}(X, Y)$, over a sample space U is defined as: $\mathsf{SD}(X, Y) = \frac{1}{2} \sum_{u \in U} |\Pr[X = u] - \Pr[Y = u]|$

Entropy definitions. 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 1 ([DORS08]). *If $\mathbf{H}_\infty(X) \geqslant \eta$ and L be an arbitrary ℓ-bit leakage on X, then $\widetilde{\mathbf{H}}_\infty(X|L) \geqslant \eta - \ell$.*

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 $\mathsf{ROLE}(\mathbb{F})$. For completeness, we define these formally in Appendix A.

Let η be such that $2\eta \lg q = n$. In this work, we consider the setting when Alice and Bob start with η $\mathsf{ROLE}(\mathbb{F})$ 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 we 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. We define a correlation extractor in this hybrid as follows.

Definition 2 ((n,m,t,ε)-correlation extractor)**.** *Let (R_A, R_B) be correlated randomness such that the secret share of each party is n bits. An (n,m,t,ε)-correlation extractor 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 simulation error ε. Note that resulting share of each party is m bits.*

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., $\left\{s^{(i)}_{1-c^{(i)}}\right\}_{i\in[m/2]}$) 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.

Since our main protocol starts with $\mathsf{ROLE}(\mathbb{F})$ as initial correlations and produces secure $\mathsf{ROLE}(\mathbb{F})$, we define a $\mathsf{ROLE}(\mathbb{F})$-to-$\mathsf{ROLE}(\mathbb{F})$ extractor formally below.

Definition 3 ($(\eta,\gamma,t,\varepsilon)$-$\mathsf{ROLE}(\mathbb{F})$-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

Given a probability distribution M over the sample space $\mathbb{F}^\eta$, the function $f = M$ represents the function $f(x) = \Pr[M = x]$ for all $x \in \mathbb{F}^\eta$.

Definition 4 (Bias of a distribution)**.** *The bias of a distribution f with respect to $S \in \mathbb{F}^\eta$ is defined to be $\mathsf{Bias}_S(f) := |\mathbb{F}|^\eta \cdot |\widehat{f}(S)|$ where $\widehat{f}(S)$ is the Fourier coefficient of f w.r.t. S. For formal definition of fourier coefficients over $\mathbb{F}$, refer to Appendix B.*

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

Definition 5 (Small-bias distribution family)**.** *Let $\mathcal{F} = \{F_1, F_2, \cdots, F_k\}$ be a family of distributions over sample space $\mathbb{F}^\eta$ such that for every non-zero vector $S \in \mathbb{F}^\eta$ following holds*

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

Then the distribution family $\mathcal{F}$ is called a δ^2-biased family.

2.3 Distribution over Linear Codes

Let $\mathcal{C} = [\eta, \kappa, d, d^\perp]_{\mathbb{F}}$ be a linear code over $\mathbb{F}$ with generator matrix $G \in \mathbb{F}^{\kappa \times \eta}$. Let C be the uniform distribution over codewords generated by G. For any $\pi \in \mathcal{S}_\eta$, define G_π as the generator matrix obtained by permuting the columns of G under π. Also, define C_π as the uniform distribution of codewords generated by G_π.
The **dual code** of $\mathcal{C}$, represented by $\mathcal{C}^\perp$, is the set of all codewords that are orthogonal to every codeword in $\mathcal{C}$. That is, for any $c^\perp \in \mathcal{C}^\perp$, it holds that $\langle c, c^\perp \rangle = 0$ for all $c \in \mathcal{C}$. Let $H \in \mathbb{F}^{(\eta-\kappa)\times\eta}$ be a generator matrix of $\mathcal{C}^\perp$.
The **Schur product code** of $\mathcal{C}$, represented by $\mathcal{C}^{(2)}$, is the set of all codewords obtained as a Schur product of codewords in $\mathcal{C}$. That is, $C^{(2)} := \{c * c' \colon c, c' \in \mathcal{C}\} \subseteq \mathbb{F}^\eta$.

Lemma 2 (Small-bias distribution)**.** *Let $\mathcal{C} = [\eta, \kappa, d, d^\perp]_{\mathbb{F}}$ be a linear code generated by G such that $\mathsf{max}_{c\in\mathcal{C}^\perp}\mathsf{wt}(c) \leqslant \eta - f$. Then, for any $0^\eta \neq T \in \mathbb{F}^\eta$ following holds*

$$\mathop{\mathbb{E}}_{\pi \xleftarrow{\$} \mathcal{S}_\eta} \left[\mathsf{Bias}_T(C_\pi)^2\right] \leqslant \frac{1}{2^\delta}$$

where $\delta = \mathbf{h_2}(\sigma/\theta)\theta + \mathbf{h_2}(\sigma/(\eta-\theta))(\eta-\theta) - o(1), \sigma = \min(f, {d^\perp}/4)$, and $\theta = \min(f, d^\perp)$ or, equivalently, $\{C_\pi : \pi \in \mathcal{S}_\eta\}$ is a $\frac{1}{2^\delta}$-biased family of distributions.

We prove the above lemma in Appendix C. Note that to get a good bound on δ above, we need a good bound on parameter f. Looking ahead, to get good parameters for our correlation extractor, we would invoke this lemma for $f = d^\perp$. Below, we discuss extension of codes that would give us codes with such values for f.

2.3.1 Extension codes

We define a couple of code extensions and prove properties about the highest weight dual codewords of extended codes.

Definition 6 (Code Extension)**.** *Given a code $\mathcal{C}$ with generator matrix G, we define the two* code extension operations ext_0 *and* ext_1 *as follows.*

$$G' = \mathsf{ext}_0\,(G, \lambda) := [\overbrace{\mathbf{0}\cdots\mathbf{0}}^{\lambda} | G]$$
$$G'' = \mathsf{ext}_1\,(G, \lambda) := \begin{bmatrix} I_{\lambda\times\lambda} & 0 \\ 0 & G \end{bmatrix}, \text{ where } I_{\lambda\times\lambda} \in \mathbb{F}^{\lambda\times\lambda}.$$

*We say that $\mathcal{C}'$ is the $\lambda^{(0)}$-*extension code *generated by G', and $\mathcal{C}''$ is the $\lambda^{(1)}$-*extension code *generated by G''.*

Lemma 3. *Let $\mathcal{C}$ be a $[\eta, \kappa, d, d^\perp]_{\mathbb{F}}$ linear code generated by G such that $\max\limits_{c\in\mathcal{C}^\perp} \mathsf{wt}(c) = (\eta - f)$. Consider $\mathcal{C}'$ generated by $G' = \mathsf{ext}_1\,(G, \lambda)$. Then, $\mathcal{C}'$ is a $[\eta', \kappa', 1, d^\perp]_{\mathbb{F}}$ linear code such that $\eta' = (\eta + \lambda)$, $\kappa' = (\kappa + \lambda)$, and $\max\limits_{c\in\mathcal{C}'^\perp} \mathsf{wt}(c) = (\eta' - (f + \lambda))$.*

Proof. We first prove that distance of $\mathcal{C}'$ is 1. For this note that, if $c \in \mathcal{C}$, then $(a|c) \in \mathcal{C}'$ for all $a \in \mathbb{F}^\lambda$. Next, let H be the generator matrix of $\mathcal{C}^\perp$. Note that it can seen that the dual matrix of G' is $H' = \mathsf{ext}_0\,(H, \lambda)$. Hence, every codeword in $\mathcal{C}'^\perp$ is always in the form $(\mathbf{0}|e)$, where $\mathbf{0}$ is the zero row vector of length λ, and e is a codeword in $\mathcal{C}^\perp$. It follows that $\max\limits_{c\in\mathcal{C}'^\perp} \mathsf{wt}(c) = \max\limits_{c\in\mathcal{C}^\perp} \mathsf{wt}(c) = \eta - f = \eta' - (f + \lambda)$. □

3 Unpredictability Lemma

Notation. Consider a matrix $Y \in \mathbb{F}^{\kappa \times \eta}$ and set of indices $\mathcal{I} \subseteq [\eta]$ such that $|\mathcal{I}| = \gamma$. Then, we define the procedure $Z = \mathsf{Puncture}(Y, \mathcal{I})$ such that $Z = [Y_{\mathcal{I}} \| Y_{[\eta]-\mathcal{I}}]$, where $Y_{\mathcal{I}}$ denote the columns of Y corresponding to $\mathcal{I}$ and $Y_{[\eta]-\mathcal{I}}$ denotes the remaining columns. Alternatively, we would also write as $Z = [Z_{-\gamma}, \ldots, Z_{-1}, Z_1, \ldots, Z_{\eta-\gamma}] = [Z^{(0)}_{[-\gamma]} \| Z'_{[\eta-\gamma]}]$, where $Z^{(0)}$ has γ columns (indexed by $\mathcal{I}$ in Y) and Z' has remaining $\eta - \gamma$ columns.

Lemma 4 (Unpredictability Lemma)**.** *Let $\tilde{\mathcal{C}}$ be an a-priori fixed $[\tilde{\eta}, \tilde{\kappa}, \tilde{d}, \tilde{d}^{\perp}]_{\mathbb{F}}$ linear code generated by the (a-priori fixed) matrix $\tilde{G} \in \mathbb{F}^{\tilde{\kappa} \times \tilde{\eta}}$ such that $\mathsf{max}_{c \in \tilde{\mathcal{C}}^{\perp}} \mathsf{wt}(c) \leqslant \tilde{\eta} - f$. Let γ be fixed parameter. Define $\eta = \tilde{\eta} - \gamma$ and $\kappa = \tilde{\kappa}$. Consider the following game between an honest challenger and an adversary:*

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 $\pi \sim \mathcal{S}_{\tilde{\eta}}$ and sets $\hat{G} = \pi(\tilde{G}) \in \mathbb{F}^{\tilde{\kappa} \times \tilde{\eta}}$.*
5. *$\mathcal{H}$ picks an arbitrary index set $\mathcal{I} \subset [\tilde{\eta}]$ such that $|\mathcal{I}| = \gamma$.*

   $\mathcal{H}$ defines matrix $G = \mathsf{Puncture}(\hat{G}, \mathcal{I}) = [G^{(0)} \| G']$ where $G^{(0)}$ has γ columns (indexed by $\mathcal{I}$ in $\hat{G}$) and G' has η columns. $\mathcal{H}$ samples $x_{[\kappa]} \sim U_{\mathbb{F}^{\kappa}}$. $\mathcal{H}$ computes $y_{[\eta]} = x_{[\kappa]} \cdot G' + m_{[\eta]}$ and sends $(y_{[\eta]}, \pi, \mathcal{I})$ to $\mathcal{A}$.

   $\mathcal{H}$ computes $y_{[-\gamma]} = x_{[\kappa]} \cdot G^{(0)}$.

   $\mathcal{H}$ picks $b \xleftarrow{\$} \{0,1\}$. If $b = 0$, then $\mathcal{H}$ sends $\mathsf{chal} = y_{[-\gamma]}$ to $\mathcal{A}$; otherwise (if $b = 1$) $\mathcal{H}$ sends $\mathsf{chal} = u_{[\gamma]} \sim U_{\mathbb{F}^{\gamma}}$.

The adversary $\mathcal{A}$ wins the game if $b = \widetilde{b}$. For any $\mathcal{A}$, the advantage of the adversary is $\leqslant \frac{1}{2}\sqrt{\frac{|\mathbb{F}|\gamma 2^t}{2^{\delta}}}$, where $\delta = \mathbf{h_2}(\sigma/\theta)\theta + \mathbf{h_2}(\sigma/(\eta-\theta))(\eta-\theta) - o(1), \sigma = \min(f, \tilde{d}^{\perp}/4)$, and $\theta = \min(f, \tilde{d}^{\perp})$

We prove this lemma in Appendix D.

4 Oblivious Transfer Extractor

In this section, we shall prove Theorem 1. As already mentioned, the clients Alice and Bob start with leaky $\mathsf{ROLE}(\mathbb{F})$ hybrid, i.e., $((\mathsf{ROLE}(\mathbb{F}))^{\eta})^{[t]}$ and run a correlation extractor protocol to obtain secure $\mathsf{ROT}^{m/2}$ correlation. Our protocol has two main blocks. The first block is a round-optimal correlation extractor that produces secure $(\mathsf{ROLE}(\mathbb{F}))^{\gamma}$. The second block embeds multiple ROT in each $\mathsf{ROLE}(\mathbb{F})$ (for better production rate). Below, we describe the first block formally. We use the 2-round ROT embedding technique of [BMN17] as the second block (see Lemma 3, [BMN17]). Moreover, since we are in the semi-honest setting, we note that these protocol can be composed in parallel to maintain the round-optimality. Finally, we provide the concrete parameter setting for our scheme in Appendix G.

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

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.* Define $\tilde{G} = \mathsf{ext}_1(G^*, \lambda) \in \mathbb{F}^{\tilde{\kappa} \times \tilde{\eta}}$, where $\tilde{\kappa} = \kappa^* + \lambda$ and $\tilde{\eta} = \eta^* + \lambda$. Client B picks a permutation $\pi \in \mathcal{S}_{\tilde{\eta}}$ and generates $\hat{G} = \pi(\tilde{G})$. Next, define[a] $\mathcal{I} = \pi(\{\lambda+1, \ldots, \lambda+\gamma\})$. Client B generates matrix $G = \mathsf{Puncture}(\hat{G}, \mathcal{I}) = [G^{(0)} \| G']$ where $G^{(0)}$ has γ columns and G' has η columns, for $\eta = \eta^* + \lambda - \gamma$. Let $\mathcal{C}$ be the linear codespace generated by G.

2. *ROLE Extraction Protocol.*

   (a) Client B picks a random codeword $r = (r_{-\gamma}, \ldots, r_{-1}, r_1, \ldots, r_\eta) \in \mathcal{C}$ and computes $m_{[\eta]} = r_{[\eta]} + x_{[\eta]}$. Client B sends $(m_{[\eta]}, \pi, \mathcal{I})$ to client A.

   (b) Client A creates the same matrix G as client B using $\pi, \mathcal{I}$. Client A picks a random codeword $u = (u_{-\gamma}, \ldots, u_{-1}, u_1, \ldots, u_\eta) \in \mathcal{C}$ and a random codeword $v = (v_{-\gamma}, \ldots, v_{-1}, v_1, \ldots, v_\eta) \in \mathcal{C}^{(2)}$. 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 $t_{[\eta]} = (\alpha_{[\eta]} * r_{[\eta]}) + \beta_{[\eta]} - z_{[\eta]}$. Client B performs erasure recovery[b] on $t_{[\eta]}$ for $\mathcal{C}^{(2)}$ to obtain $t_{-\gamma}, \ldots, t_{-1}$.

   (d) Client A outputs $\{u_i, v_i\}_{i \in \{-\gamma, \ldots, -1\}}$ and Client B outputs $\{r_i, t_i\}_{i \in \{-\gamma, \ldots, -1\}}$.

[a] Note that the indices in $\mathcal{I}$ correspond to the first γ columns of code G^*.
[b] Erasure recovery only considers coordinates that belong to $C^{*(2)}$.

Figure 4: ROLE($\mathbb{F}$)-to-ROLE($\mathbb{F}$) Extractor Protocol

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

In this section, we describe our round-optimal protocol for $[\eta, \gamma, t, \varepsilon]$-ROLE($\mathbb{F}$)-to-ROLE($\mathbb{F}$) extractor. That is, the parties start with η 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.

Given a priori: a code $\mathcal{C}^* = [\eta^*, \kappa^*, d, d^\perp]_{\mathbb{F}}$ with generator matrix $G^* \in \mathbb{F}^{\kappa^* \times \eta^*}$. Let γ and λ be fixed natural numbers (to be determined later during parameter setting in Appendix G). Recall that for a code $\mathcal{C}$, we denote by $\mathcal{C}^{(2)}$ the Schur product code of $\mathcal{C}$ (see Section 2.3). Define $\eta = \eta^* + \lambda - \gamma$ and $\kappa = \kappa^* + \lambda$. We give the formal description of our round-optimal protocol in Figure 4.

Correctness. We first prove the correctness of the scheme presented in Figure 4. More precisely, we prove the following:

Lemma 5 (Correctness)**.** *Let $d^{*(2)}$ be the distance of the Schur product code of $C^{*(2)}$. Then, if $\gamma < d^{*(2)}$, for all $j \in \{-\gamma, \ldots, -1\}$, it holds that $t_j = u_j r_j + v_j$.*

Proof. First, we prove the following claim:

Claim 1. *For all $j \in [\eta]$, it holds that $t_j = u_j r_j + v_j$.*

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

For the rest of the proof, we transform the codewords in $\mathcal{C}$ back to codewords in $\mathcal{C}^*$ and use distance properties of $\mathcal{C}^{*(2)}$. Recall that $u = (u_{-\gamma}, \ldots, u_{-1}, u_1, \ldots, u_\eta) \in \mathcal{C}$. Define $\hat{u} = \mathsf{Puncture}^{-1}(u, \mathcal{I})$. (Note that $\mathsf{Puncture}$ is a reversible procedure.) Next, define $\tilde{u} = \pi^{-1}(\hat{u}) = \tilde{u}_1, \ldots, \tilde{u}_{\eta+\gamma}$. Finally, define $u^* = \tilde{u}_{\lambda+1}, \ldots, \tilde{u}_{\eta^*+\lambda} = u^*_1, \ldots, u^*_{\eta^*} \in \mathcal{C}^*$. Similarly, define $r^* \in \mathcal{C}^*$ using r and $v^* \in \mathcal{C}^{*(2)}$ using v. Finally, consider $t^* \in \mathbb{F}^{\eta^*}$ defined using t.

Now, note that above claim implies that $t^*_j = u^*_j r^*_j + v^*_j$ for all $j \in \{\gamma+1, \ldots, \eta^*\}$. This is because of the way we chose $\mathcal{I}$. Recall that $u^* * r^* + v^* \in \mathcal{C}^{*(2)}$. Hence, when $\gamma < d^{*(2)}$, the erasure recovery for $\{t^*_j\}_{j\in\{\gamma+1,\ldots,\eta^*\}}$ would result in $t^*_1, \ldots, t^*_\gamma$ such that $t^*_j = u^*_j r^*_j + v^*_j$ for all $j \in [\gamma]$. This proves the claim. □

4.2 Security

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 4) exactly. More formally, we show the following: Let $\tilde{\mathcal{C}}$ be the $[\tilde{\eta}, \tilde{\kappa}, \tilde{d}, \tilde{d}^\perp]$ codeword generated by $\tilde{G} = \mathsf{ext}_1(G^*, \lambda)$. Then, following holds:

Lemma 6. *The simulation error of our protocol is* $\varepsilon \leqslant \sqrt{\frac{|\mathbb{F}|\gamma 2^t}{2^\delta}}$, *where* $\delta = h_2(\sigma/\theta)\theta + h_2(\sigma/(\eta-\theta))(\eta-\theta) - o(1), \sigma = \min(\lambda, \tilde{d}^\perp/4)$, *and* $\theta = \min(\lambda, \tilde{d}^\perp)$.

We first claim that $\mathsf{max}_{c\in\tilde{\mathcal{C}}^\perp}\mathsf{wt}(c) \leqslant \tilde{\eta} - \lambda$. This follows from Lemma 3. Next, we will reduce the privacy of honest party to unpredictability lemma corresponding to $\tilde{G}$.

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 4) for the following variables: Let $\mathcal{I} = \pi(\{\lambda+1, \ldots, \lambda+\gamma\})$. 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. Moreover, note that in the protocol client B picks a random $r = (r_{-\gamma}, \ldots, r_{-1}, r_1, \ldots, r_\eta) \in \mathcal{C}$. Alternatively, B could pick $\mu \xleftarrow{\$} \mathbb{F}^\kappa$ and generate $r = \mu \cdot [G^{(0)} \| G']$ and $m_{[\eta]} = \mu \cdot G' + X$.

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.

We again reduce this to our unpredictability lemma (see Lemma 4). Let $A_{[\eta]}$ denote the random variable corresponding to the 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 4 in Figure 5. Given an adversary $\mathcal{A}$ who can distinguish between $(u_{-\gamma}, \ldots, u_{-1})$ and $U_{\mathbb{F}^\gamma}$, we construct an adversary $\mathcal{A}'$ against an honest challenger $\mathcal{H}$ of Lemma 4 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 permutation is picked by the honest challenger $\mathcal{H}$ instead of client B. This is identical because client B is a semi-honest adversary. Honest client A picks $u = (u_{-\gamma}, \ldots, u_{-1}, u_1, \ldots, u_\eta) \in \mathcal{C}$.

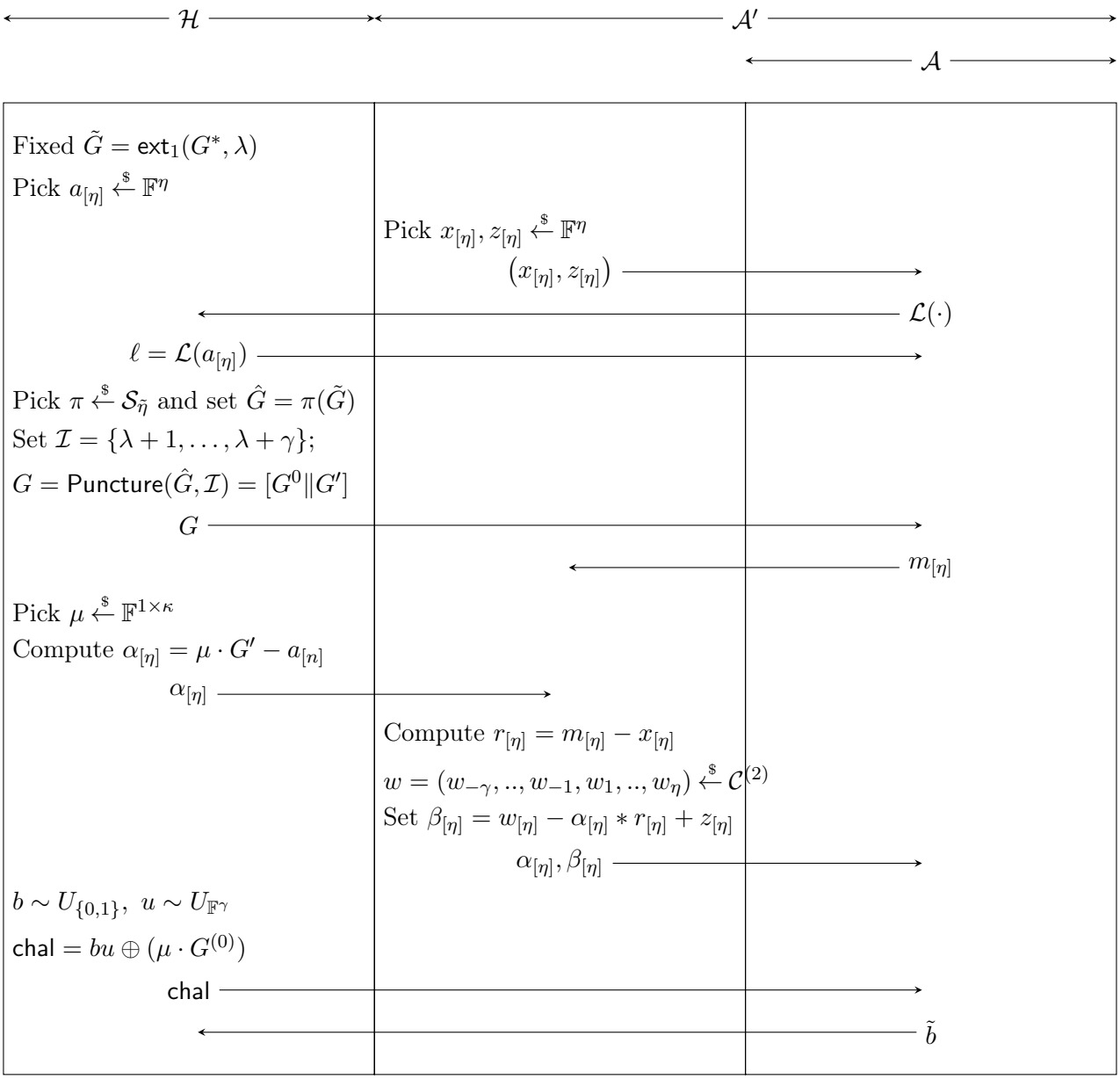

Figure 5: Simulator for Alice Privacy.

Alternatively, A could pick $\mu \xleftarrow{\$} \mathbb{F}^\kappa$ and generates $u = \mu \cdot [G^{(0)} \| G']$ and and $\alpha_{[\eta]} = \mu \cdot G' - A_{[\eta]}$ (as in simulation). 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 $\mathcal{C}^{(2)}$. This holds because in the real protocol $v_{[-\gamma,\eta]}$ is chosen as a random codeword in $\mathcal{C}^{(2)}$ and $u_{[-\gamma,\eta]} * r_{[-\gamma,\eta]} \in \mathcal{C}^{(2)}$. Here, we denote by $[-\gamma, \eta]$ the set $\{-\gamma, \ldots, -1, 1, \ldots, \eta\}$.

References

[BDNP08] Assaf Ben-David, Noam Nisan, and Benny Pinkas. FairplayMP: a system for secure multi-party computation. In Peng Ning, Paul F. Syverson, and Somesh Jha, editors, *ACM CCS 08*, pages 257–266. ACM Press, October 2008. 1

[BMN17] Alexander R. Block, Hemanta K. Maji, and Hai H. Nguyen. Secure computation based on leaky correlations: High resilience setting, 2017. 2, 3, 4, 5, 8, 11, 24

[Can00] Ran Canetti. Security and composition of multiparty cryptographic protocols. *Journal of Cryptology*, 13(1):143–202, 2000. 2

[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. 4, 6

[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. URL: http://dx.doi.org/10.1137/060651380, doi:10.1137/060651380. 8

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

[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. 9, 20, 21

[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. 23

[GIMS15] Divya Gupta, Yuval Ishai, Hemanta K. Maji, and Amit Sahai. Secure computation from leaky correlated randomness. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 701–720. Springer, Heidelberg, August 2015. doi:10.1007/978-3-662-48000-7_34. 2, 5

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

[Gop81] Valerii Denisovich Goppa. Codes on algebraic curves. In *Soviet Math. Dokl*, pages 170–172, 1981. 23

[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. 23

[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. 4

[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. 4

[IKOS09] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Extracting correlations. In *50th FOCS*, pages 261–270. IEEE Computer Society Press, October 2009. 1, 2, 3, 4, 6

[IMSW14] Yuval Ishai, Hemanta K. Maji, Amit Sahai, and Jürg Wullschleger. Single-use ot combiners with near-optimal resilience. In *2014 IEEE International Symposium on Information Theory, Honolulu, HI, USA, June 29 - July 4, 2014*, pages 1544–1548. IEEE, 2014. URL: http://dx.doi.org/10.1109/ISIT.2014.6875092, doi:10.1109/ISIT.2014.6875092. 4, 5

[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. 4

[Kil91] Joe Kilian. A general completeness theorem for two-party games. In *23rd ACM STOC*, pages 553–560. ACM Press, May 1991. 4

[MNPS04] Dahlia Malkhi, Noam Nisan, Benny Pinkas, and Yaron Sella. Fairplay - secure two-party computation system. In Matt Blaze, editor, *Proceedings of the 13th USENIX Security Symposium, August 9-13, 2004, San Diego, CA, USA*, pages 287–302. USENIX, 2004. URL: http://www.usenix.org/publications/library/proceedings/sec04/tech/malkhi.html. 1

[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. 4

[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. 4, 6

[NNOB12] Jesper Buus Nielsen, Peter Sebastian Nordholt, Claudio Orlandi, and Sai Sheshank Burra. A new approach to practical active-secure two-party computation. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 681–700. Springer, Heidelberg, August 2012. 1

[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. 23

[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. 4, 6

[WW06] Stefan Wolf and Jürg Wullschleger. Oblivious transfer is symmetric. In Serge Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 222–232. Springer, Heidelberg, May / June 2006. 1, 3, 4, 5

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

In this section, we give basic definitions for fourier analysis for general fields.

Definition 7 (Inner Product of Complex Functions)**.** *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.

Definition 8 (General Character Function)**.** *Let $|\mathbb{F}| = q$, where $q = p^a$ for prime p, and $\chi \colon \mathbb{F}^\eta \times \mathbb{F}^\eta \to \mathbb{C}^*$ such that*

$$\chi(S, x) := \chi_S(x) = \prod_{j=1}^{a} \exp\left(\frac{2\pi i (S_j \cdot x_j)}{p} \right),$$

where $S_j \cdot x_j$ is field multiplication over $\mathbb{F}$ and the quantity $(S_j \cdot x_j)$ is interpreted as an element of $\{0, 1, \ldots, p-1\}$ for all j. We say that $\chi_S(x)$ is a character function *of $\mathbb{F}^\eta$.*

Definition 9 (General Fourier Transformation)**.** *Let $f \colon \mathbb{F}^\eta \to \mathbb{C}$ and χ be a character function. For all $S \in \mathbb{F}^\eta$, define $\widehat{f} \colon \mathbb{F}^\eta \to \mathbb{C}$ as*

$$\widehat{f}(S) := \langle f, \chi_S \rangle .$$

We say that $\widehat{f}(S)$ *is a* Fourier coefficient *of* f *at* S *and* $\widehat{f}$ *is the* Fourier Transformation of f *with respect to character* χ_S.

Lemma 7 (Parseval's Identity)**.** *Let* $f\colon \mathbb{F}^\eta \to \mathbb{C}$. *The following always holds:*

$$\sum_{x\in\mathbb{F}^\eta} f(x)^2 = |\mathbb{F}|^\eta \sum_{S\in\mathbb{F}^\eta} \widehat{f}(S)^2$$

C Proof of Lemma 2

We begin by giving some notation and definitions. Assume $|\mathbb{F}| = q = p^a$ for prime p and some $a \in \mathbb{N}$. Recall that $\mathcal{C} = [\eta, \kappa, d, d^\perp]_\mathbb{F}$ be a linear code generated by G such that $\mathsf{max}_{c\in\mathcal{C}^\perp}\mathsf{wt}(c) \leqslant \eta - m$. Define $\sigma = \min(m, {}^{d^\perp}/_4)$, and $\theta = \min(m, d^\perp)$. Next, we define a functions $w_i : \mathbb{F}^\eta \to \mathbb{N}$ for all $i \in \mathbb{F}$ as follows:

Definition 10. *For any* $S \in \mathbb{F}^\eta$ *and* $i \in \mathbb{F}$, *we define* $w_i(S)$ *as the cardinality of the set* $\{j\colon S_j = i\}$.

Definition 11. *For any two vectors* $S, T \in \mathbb{F}^\eta$, *we say that* $S \sim T$ *if and only if for all* $i \in \mathbb{F}$, *we have* $w_i(S) = w_i(T)$. *We denote* $\widetilde{S}$ *as the equivalence class of* S *under the relation* $\sim$.

Recall that we need to prove that for any $0^\eta \neq T \in \mathbb{F}^\eta$ following holds

$$\mathop{\mathbb{E}}_{\pi\xleftarrow{\$}\mathcal{S}_\eta}\left[\mathsf{Bias}_T(C_\pi)^2\right] \leqslant \frac{1}{2^\delta}$$

where $\delta = h_2(\sigma/\theta)\theta + h_2(\sigma/(\eta-\theta))(\eta-\theta) - o(1)$.
Since, $\mathsf{Bias}_T(C_\pi) = |\mathbb{F}|^\eta \cdot |\widehat{C_\pi}(S)|$ (see Section 2.2), it suffices to show that

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

.
We prove the above relation using a sequence of claims.

Claim 2. *For all* $S \in \mathbb{F}^\eta$, $\widehat{C}(S) = \begin{cases} \frac{1}{|\mathbb{F}|^\eta} & \text{if } S \in \mathcal{C}^\perp \\ 0 & \text{otherwise} \end{cases}$

The proof of this claim follows from the basic fourier definitions. We give a formal proof in Appendix E.

Claim 3. $\mathop{\mathbb{E}}_{\pi}[\widehat{C_\pi}(S)^2] = \binom{\eta}{w_0(S), w_1(S), \cdots, w_{q-1}(S)}^{-1} \sum_{T\in\widetilde{S}} \widehat{C}(T)^2$

Proof. First note that $\widehat{C_\pi}(S) = \widehat{C}(\pi^{-1}(S))$ since a codeword $x \in C_\pi$ if and only if the codeword $\pi^{-1}(x) \in C$. Also note that for each $T \in \widetilde{S}$, there are exactly $w_0(S)! \cdot w_1(S)! \cdot \cdots \cdot w_{q-1}(S)!$ permutations π such that $\pi^{-1}(S) = T$. Thus,

$$\begin{aligned}
\mathop{\mathbb{E}}_{\pi}[\widehat{C_\pi}(S)^2] &= \mathop{\mathbb{E}}_{\pi}[\widehat{C}(\pi^{-1}(S))^2] \\
&= \frac{1}{\eta!}\sum_{\pi} \widehat{C}(\pi^{-1}(S))^2 \\
&= \frac{w_0(S)!\cdot w_1(S)!\cdot\cdots\cdot w_{q-1}(S)!}{\eta!}\sum_{T\in\widetilde{S}}\widehat{C}(T)^2 \\
&= \binom{\eta}{w_0(S), w_1(S), \ldots, w_{q-1}(S)}^{-1}\sum_{T\in\widetilde{S}}\widehat{C}(T)^2
\end{aligned}$$

□

Based on Claim 3 and Claim 2, an upper bound for the number of codewords which are both in $\mathcal{C}^\perp$ and in $\widetilde{S}$ will immediately give an upper bound for the expected bias. We achieve this via following claims.

In the next claim, for a $c \in \mathcal{C}^\perp$ we construct a ball of radius $\left\lfloor \frac{d^\perp}{2} \right\rfloor$ and count (lower-bound) the number of elements $c' \in \mathbb{F}^\eta$ that are equivalent to c, that is, $c \sim c'$. Note that since dual distance of $\mathcal{C}$ is $d^\perp$ and $c \in \mathcal{C}^\perp$, it implies that $c' \notin \mathcal{C}^\perp$.

Claim 4. *For any codeword $c \in \mathcal{C}^\perp$ such that $w_i(c) = w_i$ for all $i \in \mathbb{F}$, let $\mathcal{B}_c = \left\{ c' \in \mathbb{F}^\eta : c' \sim c, \text{and } \Delta(c, c') \leqslant \left\lfloor \frac{d^\perp}{2} \right\rfloor \right\}$. Then $|\mathcal{B}_c| \geqslant 2^{h_2(\sigma/\theta)\theta + h_2(\sigma/(\eta-\theta))(\eta-\theta) - o(1)}$.*

Proof. Intuitively, given a codeword $c \in \mathcal{C}^\perp$, changing a_i zero coordinates of c to i and also changing that many number of coordinates equal to i in c back to 0 gives a such c'. Recall that $\sigma = \min(f, {}^{d^\perp}/_4)$. Thus, the size of the ball $\mathcal{B}_c$ is at least

$$
\begin{aligned}
&\sum_{a_1+\cdots+a_{q-1} \leqslant \sigma} \binom{w_0}{a_0, a_1, \cdots, a_{q-1}} \binom{w_1}{a_1} \cdots \binom{w_{q-1}}{a_{q-1}} \\
&= \sum_{i=0}^{\sigma} \sum_{a_1+\cdots+a_{q-1}=i} \binom{w_0}{a_0, a_1, \cdots, a_{q-1}} \binom{w_1}{a_1} \cdots \binom{w_{q-1}}{a_{q-1}} \\
&\geqslant \sum_{i=0}^{\sigma} \sum_{a_1+\cdots+a_{q-1}=i} \binom{w_0}{a_0, a_1 + \cdots + a_{q-1}} \binom{w_1}{a_1} \cdots \binom{n_{q-1}}{a_{q-1}} \\
&= \sum_{i=0}^{\sigma} \binom{w_0}{i} \sum_{a_1+\cdots+a_{q-1}=i} \binom{w_1}{a_1} \cdots \binom{w_{q-1}}{a_{q-1}} \\
&= \sum_{i=0}^{\sigma} \binom{w_0}{i} \binom{\eta - w_0}{i} && \text{[by Vandermonde Identity]} \\
&\geqslant \binom{w_0}{\sigma} \binom{\eta - w_0}{\sigma} \\
&\geqslant \binom{\theta}{\sigma} \binom{\eta - \theta}{\sigma} && \text{[by } \textit{Claim 6}\text{]} \\
&\geqslant 2^{h_2(\sigma/\theta)\theta + h_2(\sigma/(\eta-\theta))(\eta-\theta) - o(1)} && \text{[by } \textit{Claim 5}\text{]} \\
&= 2^\delta
\end{aligned}
$$

As is implied my Claim 6, above bound holds when $d^\perp \leqslant \frac{\eta - 1}{2}, f \leqslant \frac{\eta - 1}{2}$. In our final parameter setting, these conditions would hold. □

We claim the following by using Stirling's Approximation, namely, $n! \approx \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$.

Claim 5. *For any integers n, m, we have*

$$\binom{n}{m} \approx \frac{2^{h_2(m/n)n}}{\sqrt{2(m/n)(1-m/n)\pi n}} = 2^{h_2(m/n)n - o(1)}$$

Claim 6. *Let $F(z) = \binom{z}{\sigma}\binom{\eta - z}{\sigma}$. Then, under the condition that $d^\perp \leqslant \frac{\eta - 1}{2}, f \leqslant \frac{\eta - 1}{2}$,*

$$\min_{f \leqslant z \leqslant \eta - d^\perp} F(z) = F(\min(d^\perp, f)) = F(\theta)$$

Proof. Note that

$$\frac{F(z+1)}{F(z)} = \frac{(z+1)}{(z+1)-\sigma} \cdot \frac{(\eta-z)-\sigma}{(\eta-z)} = \frac{(z+1)(\eta-z)-(z+1)\sigma}{(z+1)(\eta-z)-(\eta-z)\sigma}$$

Thus, $\frac{F(z+1)}{F(z)} \geqslant 1$ if $z \leqslant \frac{\eta-1}{2}$, and $\frac{F(z+1)}{F(z)} \leqslant 1$ if $z \geqslant \frac{\eta-1}{2}$. It means that the function F is increasing in $\left[\sigma, \frac{\eta-1}{2}\right]$ and decreasing in $\left[\frac{\eta-1}{2}, \eta - \sigma\right]$. Note also that $F(\eta-z) = F(z)$ for every z. Under the condition that $d^\perp \leqslant \frac{\eta-1}{2}, f \leqslant \frac{\eta-1}{2}$, we have the following:

$$\min_{f \leqslant z \leqslant \eta - d^\perp} F(z) = \min(F(f), F(\eta - d^\perp)) = \min(F(f), F(d^\perp)) = F(\min(d^\perp, f)) = F(\theta)$$

□

Concluding the proof of the lemma. Note that for any two codewords $e, e' \in \mathcal{C}^\perp$, we have $\mathcal{B}_e \cap \mathcal{B}_{e'} = \emptyset$ (using dual distance of $\mathcal{C}$) and the number of vectors in $\widetilde{S}$ is exactly

$$\binom{\eta}{w_0(S), w_1(S), \ldots, w_{q-1}(S)}.$$

This implies that the number of codewords in both $\mathcal{C}^\perp$ and $\widetilde{S}$ is at most

$$\binom{\eta}{w_0(S), w_1(S), \ldots, w_{q-1}(S)} \Big/ 2^\delta.$$

This is because if $c \in \mathcal{C}^\perp$, then for any $c' \in \mathcal{B}_c$ such that $c \neq c'$, it holds that $c' \notin \mathcal{C}^\perp$. Combining this and Claim 3, the proof is complete.

D Proof of Lemma 4

Recall that we are given $\tilde{\mathcal{C}}$ be an a-priori fixed $[\tilde{\eta}, \tilde{\kappa}, d, d^\perp]_{\mathbb{F}}$ linear code generated by the (a-priori fixed) matrix $\tilde{G} \in \mathbb{F}^{\tilde{\kappa} \times \tilde{\eta}}$ such that $\mathsf{max}_{c \in \tilde{\mathcal{C}}^\perp} \mathsf{wt}(c) \leqslant \eta - f$. Also, γ is a fixed parameter to be determined later. For other notation, see the Section 3. Let M, X, L be the random variables corresponding to $m_{[\eta]}, x_{[\kappa]}, \mathcal{L}(M)$, respectively. Also, for convenience, let Π denote the uniform random variable over $\mathcal{S}_{\tilde{\eta}}$. Then the following holds for any $\mathcal{I} \subseteq [\tilde{\eta}]$ of size γ:

$$2\mathrm{SD}\left(\left(XG^{(0)}, XG' + M, \Pi, \mathcal{I}, L\right), \left(U_{\mathbb{F}^\gamma}, U_{\mathbb{F}^\eta}, \Pi, \mathcal{I}, L\right) \right) \leqslant \sqrt{\frac{|\mathbb{F}|^\gamma 2^t}{2^\delta}},$$

Alternately, this can be viewed as follows: Define a new variable $\hat{M}$ over $\mathbb{F}^{\tilde{\eta}}$ such that $\hat{M}_i = M_i$ if $i \notin \mathcal{I}$, else $\hat{M}_i = 0_{\mathbb{F}}$. Then,

$$2\mathrm{SD}\left(\left(X\hat{G} + \hat{M}, \Pi, L\right), \left(U_{\mathbb{F}^{\tilde{\eta}}}, \Pi, L\right) \right) \leqslant \sqrt{\frac{|\mathbb{F}|^\gamma 2^t}{2^\delta}},$$

where $\hat{G} = \pi(\tilde{G})$ (see Section 3).

We note that the above statement is a generalization of result on min-entropy extraction via small-bias distributions of Dodis and Smith (Lemma 4, [DS05]) to arbitrary fields $\mathbb{F}$. Their lemma is stated over $\{0,1\}^\eta$ and is as follows:

Lemma 8 (Min-entropy Extraction [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:*

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

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

In our case, we know that $\{X\tilde{G}_\pi\}_\pi$ is a $\frac{1}{2^\delta}$-biased family of distributions (Lemma 2), where $\tilde{G}_\pi = \pi(\tilde{G})$. Also, $\widetilde{\mathbf{H}}_\infty(\hat{M}|L) \geqslant \eta \lg|\mathbb{F}| - t$ (Lemma 1). For completeness, we prove the above statement below.

Proof.

$$\begin{aligned}
&2\mathrm{SD}\left(\left(X\hat{G} + \hat{M}, \Pi, L\right) \ , \ (U_{\mathbb{F}^{\tilde{\eta}}}, \Pi, L) \right) \\
&= \mathop{\mathbb{E}}_{\pi\sim\Pi}\left[\mathop{\mathbb{E}}_{\ell\sim L}\left[2\mathrm{SD}\left(\left(X\hat{G} + \hat{M}|\pi,\ell\right) \ , \ (U_{\mathbb{F}^{\tilde{\eta}}}|\pi,\ell) \right)\right]\right] \\
&= \mathop{\mathbb{E}}_{\pi\sim\Pi}\left[\mathop{\mathbb{E}}_{\ell\sim L}\left[\sum_{y\in\mathbb{F}^{\tilde{\eta}}}\left|\left(X\hat{G} + \hat{M}|\pi,\ell\right)(y) - (U_{\mathbb{F}^{\tilde{\eta}}}|\pi,\ell)(y)\right|\right]\right] \\
&\leqslant \mathop{\mathbb{E}}_{\pi\sim\Pi}\left[\mathop{\mathbb{E}}_{\ell\sim L}\left[|\mathbb{F}|^{\tilde{\eta}/2}\sqrt{\sum_{y\in\mathbb{F}^{\tilde{\eta}}}\left[\left(X\hat{G} + \hat{M}|\pi,\ell\right)(y) - (U_{\mathbb{F}^{\tilde{\eta}}}|\pi,\ell)(y)\right]^2}\right]\right] && \text{[Cauchy-Schwartz]} \\
&= |\mathbb{F}|^{\tilde{\eta}} \mathop{\mathbb{E}}_{\pi\sim\Pi}\left[\mathop{\mathbb{E}}_{\ell\sim L}\left\|\left(X\hat{G} + \hat{M}|\pi,\ell\right) - (U_{\mathbb{F}^{\tilde{\eta}}}|\pi,\ell)\right\|_2\right] \\
&= |\mathbb{F}|^{\tilde{\eta}} \mathop{\mathbb{E}}_{\pi,\ell}\sqrt{\sum_{S\in\mathbb{F}^{\tilde{\eta}}}\left[\widehat{\left(X\hat{G} + \hat{M}|\pi,\ell\right)}(S) - \widehat{(U_{\mathbb{F}^{\tilde{\eta}}}|\pi,\ell)}(S)\right]^2} && \text{[Parseval's Identity]} \\
&\leqslant |\mathbb{F}|^{\tilde{\eta}} \sqrt{\mathop{\mathbb{E}}_{\pi,\ell}\sum_{S\in\mathbb{F}^{\tilde{\eta}}}\left[\widehat{\left(X\hat{G} + \hat{M}|\pi,\ell\right)}(S) - \widehat{(U_{\mathbb{F}^{\tilde{\eta}}}|\pi,\ell)}(S)\right]^2} && \text{[Jensen's Inequality]} \\
&= |\mathbb{F}|^{\tilde{\eta}} \sqrt{\mathop{\mathbb{E}}_{\pi,\ell}\sum_{S\neq\mathbf{0}}\widehat{\left(X\hat{G} + \hat{M}|\pi,\ell\right)}(S)^2} \\
&= |\mathbb{F}|^{2\tilde{\eta}} \sqrt{\mathop{\mathbb{E}}_{\pi,\ell}\sum_{S\neq\mathbf{0}}\widehat{\left(X\hat{G}|\pi,\ell\right)}(S)^2 \cdot \widehat{\left(\hat{M}|\pi,\ell\right)}(S)^2} && \text{[Convolution]} \\
&= |\mathbb{F}|^{2\tilde{\eta}} \sqrt{\sum_{S\neq\mathbf{0}}\mathop{\mathbb{E}}_{\pi}\widehat{\left(X\hat{G}|\pi\right)}(S)^2 \cdot \mathop{\mathbb{E}}_{\ell}\widehat{\left(\hat{M}|\ell\right)}(S)^2} \\
&\leqslant |\mathbb{F}|^{2\tilde{\eta}} \sqrt{\sum_{S\neq\mathbf{0}}\frac{1}{|\mathbb{F}|^{2\tilde{\eta}}\cdot 2^\delta}\cdot\mathop{\mathbb{E}}_{\ell}\widehat{\left(\hat{M}|\ell\right)}(S)^2} && \text{[Lemma 2]}
\end{aligned}$$

$$\leqslant \frac{|\mathbb{F}|^{\tilde{\eta}}}{2^{\delta/2}}\sqrt{\frac{2^t}{|\mathbb{F}|^{\tilde{\eta}}\cdot|\mathbb{F}|^{\eta}}} \qquad [*]$$

$$= \sqrt{\frac{|\mathbb{F}|^{\gamma}\cdot 2^t}{2^{\delta}}} \qquad [\tilde{\eta}=\eta+\gamma]$$

$[*]$ follows by using $\widetilde{\mathbf{H}}_{\infty}(\hat{M}|L) \geqslant \eta \lg|\mathbb{F}| - t$ (Lemma 1) and Parseval's identity. This completes the proof of the unpredictability lemma.

□

E Proof of Claim 2

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

$$\begin{aligned}
\widehat{C}(S) &= \frac{1}{|\mathbb{F}|^{\eta}}\sum_{x\in\mathbb{F}^{\eta}} C(x)\overline{\chi_S(x)} \\
&= \frac{1}{q^{\eta}}\sum_{x\in\mathcal{C}}\frac{1}{q^{\kappa}}\overline{\chi_S(x)} \\
&= \frac{1}{q^{\eta}}\cdot\frac{1}{q^{\kappa}}\sum_{x\in\mathcal{C}}\prod_{j=1}^{a}\overline{\exp\left(\frac{2\pi i(S_j\cdot x_j)}{p}\right)} \\
&= \frac{1}{q^{\eta}}\cdot\frac{1}{q^{\kappa}}\sum_{x\in\mathcal{C}}\prod_{j=1}^{a}\exp\left(\frac{-2\pi i(S_j\cdot x_j)}{p}\right) \\
&= \frac{1}{q^{\eta}}\cdot\frac{1}{q^{\kappa}}\sum_{x\in\mathcal{C}}\exp\left(\frac{-2\pi i\sum_{j=1}^{a}(S_j\cdot x_j)}{p}\right) \\
&= \frac{1}{q^{\eta}}\cdot\frac{1}{q^{\kappa}}\sum_{x\in\mathcal{C}}\exp\left(\frac{-2\pi i(S\cdot x)}{p}\right),
\end{aligned}$$

where $(S\cdot x)$ is the dot product over $\mathbb{F}^{\eta}$. By definition, if $S\in\mathcal{C}^{\perp}$, then for all $x\in\mathcal{C}$, $(S\cdot x)=0$, and we have

$$\begin{aligned}
\frac{1}{q^{\eta}}\cdot\frac{1}{q^{\kappa}}\sum_{x\in\mathcal{C}}\exp\left(\frac{-2\pi i(S\cdot x)}{p}\right) &= \frac{1}{q^{\eta}}\cdot\frac{1}{q^{\kappa}}\sum_{x\in\mathcal{C}}\exp(0) \\
&= \frac{q}{q^{\eta}}\cdot\frac{1}{q^{\kappa}}\sum_{x\in\mathcal{C}}1 \\
&= \frac{1}{q^{\eta}}.
\end{aligned}$$

To show the result for $S \notin \mathcal{C}^\perp$, we use Parseval's Identity; namely, $\sum_x f(x)^2 = |\mathbb{F}|^\eta \sum_S \widehat{f}(S)^2$.

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

F Algebraic Geometry Codes

Theorem 2 (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 3. *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. $d^\perp \geqslant \kappa + 1$.

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 2) 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. □

G Parameter Choices

Parameters of the AG Code in Appendix F.

1. $q = |\mathbb{F}| = 64 = 8^2$,
2. $\eta^* = 7 \cdot 8^u$, genus of the curve $g = 8^u$, for $u \in \mathbb{N}$,
3. Divisor D with degree $\mathsf{deg} D = (7/2 - \rho)8^u - 1$, for $\rho > 0$,
4. $\kappa^* = \deg D - g + 1 = (5/2 - \rho)8^u$,

5. $d = \eta^* - \deg D = (7/2 + \rho)8^u + 1$,
6. $d^\perp > \kappa^* = (5/2 - \rho)8^u$, and
7. $d^{(2)} = 2\rho \cdot 8^u + 2$.

Parameters of the Extension of the AG Code.

1. $q = |\mathbb{F}| = 8^2$,
2. $f = (5/2 - \rho)8^u$,
3. $\widetilde{\eta} = \eta^* + f = (19/2 - \rho)8^u$,
4. Weight of dual codewords are in the range $[(5/2 - \rho)8^u, 7 \cdot 8^u]$

Parameters of Puncturing.

1. $\gamma = d^{(2)} - 1 = 2\rho \cdot 8^u + 1$,
2. $\eta = \widetilde{\eta} - \gamma = (19/2 - 3\rho)8^u$,

Simulation Error Computation. We have secret share length $n = 2 \cdot \lg|\mathbb{F}| \cdot \eta = (114 - 36\rho)8^u$. For each $\mathsf{ROLE}\left(\mathbb{GF}\left[2^6\right]\right)$ we extractor 2 samples of ROT (using [BMN17]). Therefore, the number of ROT samples is $m/2 = 2 \cdot \gamma > 4\rho \cdot 8^u$. This implies that we have production rate $\alpha = m/n = \frac{\rho}{57/4 - 9/2\rho}$.

Define

$$Q_N := \lg|\mathbb{F}|\,(\alpha/2) + \beta = 3\alpha + \beta = \frac{\rho}{19/4 - 3/2\rho} + \beta$$

Then, we are interested in computing the small-bias.

1. $\theta = d^\perp = (5/2 - \rho)8^u$,
2. $\sigma = d^\perp/4 = (5/8 - 1/4\rho)8^u$,
3. $\sigma/\theta = 1/4$,
4. $\sigma/(\eta - \theta) = \frac{5/8 - 1/4\rho}{7 - 2\rho}$
5. $\lg\delta = h_2(\sigma/\theta)\theta + h_2(\sigma/(\eta-\theta))(\eta-\theta) = h_2(1/4)(5/2 - \rho)8^u + h_2\left(\frac{5/8 - 1/4\rho}{7-2\rho}\right)(7 - 2\rho)8^u$
6. $Q_D := \frac{\lg\delta}{n} = \frac{h_2(1/4)(5/2-\rho) + h_2\left(\frac{5/8 - 1/4\rho}{7-2\rho}\right)(7-2\rho)}{12(19/2 - 3\rho)}$

Now, $\zeta = -\frac{1}{n}\lg\varepsilon = Q_D - Q_N$.

One choice of parameters. Suppose we are interested in $\alpha = \beta = 1\%$. This implies that $Q_N = 4/100$.

From α, we can solve $\rho = 57/418$. This defines the AG code choice we need to make.

From the value of ρ, we can calculate $Q_D \approx 0.0440$. Therefore, $\zeta = 0.40\%$