Degree-D Reverse Multiplication-Friendly Embeddings: Constructions and Applications

Daniel Escudero,[1] Cheng Hong,[2] Hongqing Liu,[3] Chaoping Xing[3] and Chen Yuan[3]

[1] J.P. Morgan AI Research & J.P. Morgan AlgoCRYPT CoE, New York, U.S.A.
[2] Ant Group, China
[3] Shanghai Jiao Tong University, Shanghai, China

Abstract. In the recent work of (Cheon & Lee, Eurocrypt'22), the concept of a *degree-D packing method* was formally introduced, which captures the idea of embedding multiple elements of a smaller ring into a larger ring, so that element-wise multiplication in the former is somewhat "compatible" with the product in the latter. Then, several optimal bounds and results are presented, and furthermore, the concept is generalized from one multiplication to degrees larger than two. These packing methods encompass several constructions seen in the literature in contexts like secure multiparty computation and fully homomorphic encryption.

One such construction is the concept of reverse multiplication-friendly embeddings (RMFEs), which are essentially degree-2 packing methods. In this work we generalize the notion of RMFEs to *degree-D RMFEs* which, in spite of being "more algebraic" than packing methods, turn out to be essentially equivalent. Then, we present a general construction of degree-D RMFEs by generalizing the ideas on algebraic geometry used to construct traditional degree-2 RMFEs which, by the aforementioned equivalence, leads to explicit constructions of packing methods. Furthermore, our theory is given in a unified manner for general Galois rings, which include both rings of the form $\mathbb{Z}_{p^k}$ and fields like $\mathbb{F}_{p^k}$, which have been treated separately in prior works. We present multiple concrete sets of parameters for degree-D RMFEs (including $D = 2$), which can be useful for future works.

Finally, we discuss interesting applications of our RMFEs, focusing in particular on the case of non-interactively generating high degree correlations for secure multiparty computation protocols. This requires the use of Shamir secret sharing for a large number of parties, which requires large-degree Galois ring extensions. Our RMFE enables the generation of such preprocessing data over small rings, without paying for the multiplicative overhead incurred by using Galois ring extensions of large degree. For our application we also construct along the way, as a side contribution of potential independent interest, a pseudo-random secret-sharing solution for non-interactive generation of packed Shamir-sharings over Galois rings with structured secrets, inspired by the PRSS solutions from (Benhamouda *et al*, TCC 2021).

1 Introduction

Several cryptographic constructions are designed to work over finite discrete structures. For example, encryption schemes, digital signatures, or message authentication codes, all widely used in day-to-day digital systems, are designed to manipulate bit strings of certain length. The same holds for cryptographic hash functions, or key exchange protocols. However, there is a large body of cryptographic constructions that, on top of working over a finite discrete structure, require certain minimal algebraic properties, either for the definition of the primitive itself or for their construction. For example, Diffie-Hellman key exchange [18] makes use of a finite group where the discrete logarithm problem is hard. Similarly, encryption schemes such as Paillier [28] or RSA [30] make use of group of invertible integers modulo N^2 and N respectively, where N is the product of two large primes.

On the other hand, other cryptographic primitives not only make use of algebraic structures underneath, but their security definition is actually tied to some algebraic structure. For example, in fully homomorphic encryption two messages over some finite ring can be encrypted, and the two corresponding ciphertexts can be added/multiplied together to obtain encryptions of the sum/product of the two underlying plaintexts. Also, functional encryption for dot products (*cf.* [1]) is a primitive that enables the encryption of a message under some public key so that, having certain special secret key, only the dot product between the plaintext and the secret key can be recovered. Again, such definition is tied to a specific algebraic structure in order for the notion of a "dot product" to be well defined. Finally, another good example is secure multiparty computation, where different parties compute a given function securely without leaking their inputs. Such function is typically defined as an arithmetic circuit over some finite algebraic structure.

Typically, the most general algebraic structure that underpins many cryptographic primitives, including the ones exemplified above, is that of a *finite ring*. This is a finite set where a product and addition operation are defined, and these satisfy certain basic properties such as commutativity of addition, associativity, or distributivity. Unfortunately, not all cryptographic primitives can be instantiated under any arbitrary finite ring. For example, most homomorphic encryption techniques work over rings of the form $\mathbb{Z}_N$ for very specific integers N, lattice-based construction typically makes use of polynomial rings extensions of a very structured form [27], and most secure multiparty computation protocols are designed to work over finite fields, which are a subset of finite rings where every non-zero element has a multiplicative inverse, and in some cases this finite field cannot be small. Only recently the case of MPC over rings of the form $\mathbb{Z}_N$ for more general N was considered (*cf.* [13]), and in [20] the case of MPC over a (possibly non-commutative) arbitrary finite ring was studied. In addition, zero-knowledge proofs are typically designed for arithmetic circuits over finite fields, with the case of more general rings only being explored recently [33].

The use of ring extensions. As we mentioned above, ring extensions—which are rings of polynomials reduced modulo some fixed polynomials—appear naturally in the context of lattice-based cryptography. However, that is not the only context where this type of extension rings are used. An interesting and relevant algebraic structure is the ring of integers $\mathbb{Z}_{p^k}$ modulo a prime power p^k. The relevance of this structure is two-fold. On the one hand, it contains as a particular case the integers modulo powers of two, like 2^{64} or 2^{128}, which are good for many applications since they are closer to hardware implementations and they are more "compatible" with binary circuits [16]. On the other hand, having constructions that work over $\mathbb{Z}_{p^k}$ for any arbitrary prime power p^k typically lead, with the help of the Chinese remainder theorem, to constructions that work over $\mathbb{Z}_N$ for *any* positive integer N. It has been identified in many different works (*e.g.* [20]) that the main property required by the underlying ring $\mathbb{Z}_{p^k}$ in order for certain cryptographic primitive (*e.g.* MPC or ZKP) to be instantiable over $\mathbb{Z}_{p^k}$ is that the *Lenstra constant* of the ring, which is the size of the largest subset where every non-zero pairwise difference is invertible, has to be large enough. Since the Lenstra constant of $\mathbb{Z}_{p^k}$ is p, this means that p cannot be very small, which rules out important cases such as $\mathbb{Z}_{2^k}$.

To address the complication above, multiple works such as [7,8,5,2,21] have made use of ring extensions of $\mathbb{Z}_{p^k}$ to ensure the Lenstra constant of the resulting ring is large enough, hence enabling the construction of the specific cryptographic primitive at hand. Such ring extensions are known as *Galois rings*, and they have the form $\mathbb{Z}_{p^k}[\mathtt{X}]/(f(\mathtt{X}))$, where $f(\mathtt{X})$ is some polynomial of degree d over $\mathbb{Z}_{p^k}$ that is irreducible when taken modulo p. This ring is denoted by $\mathsf{GR}(p^k, d)$, and it is known to have a Lenstra constant of p^d, which increases exponentially as the extension degree d grows. Because of this, works in the context of secure multiparty computation (*cf.* [2]) and more recently zero-knowledge proofs [26,10] have made use of such extensions in order to instantiate these cryptographic primitives over $\mathbb{Z}_{p^k}$.

Packing methods. As we have mentioned above, ring extensions are required in contexts such as fully homomorphic encryption, which is typically based on lattices, or secure multiparty computation and zero-knowledge proofs over rings of the form $\mathbb{Z}_{p^k}$. However, most applications do not make use of these ring extensions directly, but rather they are better suited for the underlying base ring. In the context of lattice-based FHE, this has been addressed by making use of ring extensions that are ring-isomorphic to multiple copies of the underlying base ring via CRT. These extensions require the quotient polynomial to split completely into linear factors, and in particular it cannot be invertible.

For MPC and ZKPs, the quotient polynomial has to be irreducible in order to guarantee a large-enough Lenstra constant, so in particular packing elements using CRT-based techniques is not possible. To address this complication, a tool named *reverse multiplication-friendly embeddings*, or RMFEs for short, was introduced in [9]. At a high level, an RMFE is a pair of additive homomorphisms from/to a Galois ring to/from $\mathbb{Z}_{p^k}^r$ that map polynomial product in the Galois

ring to element-wise product in $\mathbb{Z}_{p^k}^r$. More precisely, an RMFE is a pair of $\mathbb{Z}_{p^k}$-linear homomorphisms $(\phi : \mathbb{Z}_{p^k}^r \to \mathsf{GR}(p^k, d), \psi : \mathsf{GR}(p^k, d) \to \mathbb{Z}_{p^k}^r)$ such that $\psi(\phi(\boldsymbol{x}) \cdot \phi(\boldsymbol{y})) = \boldsymbol{x} \star \boldsymbol{y}$ for every $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}_{p^k}^r$, where $\cdot$ denotes product in $\mathsf{GR}(p^k, d)$ and $\star$ denotes component-wise product in $\mathbb{Z}_{p^k}^r$. This is less ideal than the CRT-based packing techniques used in lattice-based cryptography since it does not hold that the product of *any* two ring extension elements $x \cdot y$ somehow "encodes" multiple products over $\mathbb{Z}_{p^k}$, but rather, if $x = \phi(\boldsymbol{x})$ and $y = \phi(\boldsymbol{y})$, then $x \cdot y$ can be "decoded" to the products $\boldsymbol{x} \star \boldsymbol{y}$ by mapping this value with ψ. Furthermore, very importantly, unlike CRT-based techniques it is not possible to multiply more than two values before "decoding" with ψ, since it is not necessarily the case that $\psi(\phi(\boldsymbol{x}) \cdot \phi(\boldsymbol{y}) \cdot \phi(\boldsymbol{z})) = \boldsymbol{x} \star \boldsymbol{y} \star \boldsymbol{z}$. As a result, for multiple products all existing cryptographic constructions making use of RMFEs must follow a pattern that somewhat resembles "encode $\to$ multiply $\to$ decode $\to$ repeat". In contrast, CRT-based packing can follow the pattern "encode $\to$ multiply $\to \cdots \to$ multiply $\to$ decode".

RMFEs have played a major role in enabling multiple recent results in the literature. In the work where they were introduced [9], they were used in order to achieve honest majority MPC without the $\log n$ overhead stemming from the use of field extensions. This only works for SIMD circuits, a restriction that was later removed in [29] again by using RMFEs. The work of [11] uses RMFEs to improve the state-of-the-art in dishonest majority MPC over $\mathbb{Z}_2$, and [21] uses again RMFEs, this time over more general Galois rings—which are constructed in [15]—to improve the communication of SPD$\mathbb{Z}_{2^k}$ [13], the state-of-the-art protocol for dishonest majority MPC over $\mathbb{Z}_{2^k}$. RMFEs have also found applications in the zero-knowledge domain: [10] improves the Aurora and Ligero proof systems by using RMFEs; and in [26] a *concretely efficient* post-quantum signature scheme based on MPC-in-the-Head is proposed, Helium, which makes use of RMFEs in order to increase the field size, which improves the soundness of the proof and hence reduces signature size), while reducing the penalty of using a larger field.

Finally, in the recent work of [12], the concept of a *packing method* was introduced, with the aim of unifying and generalizing the notion of RMFEs and CRT-based packings, already used in the literature. A packing method is similar to an RMFE in that it is comprised of packing ("encoding", ϕ) and unpacking ("decoding", ψ) methods, but: (1) their additive homomorphism property is more relaxed, (2) they can be randomized, (3) unpacking/decoding can lead to an error and, crucially, (4) they allow for more than one multiplication to be carried out before decoding (and in fact there could be different packing/unpacking methods depending on the degree of the multiplication being decoded). In [12], the authors show how packing methods generalize existing approaches in the literature, and they show lower and upper bounds on the parameters of these constructions. We discuss in much more detail the work of [12] in Section 1.2.

1.1 Our Contribution

The packing methods defined in [12] allow for several multiplications to be carried out before decoding, while as we discussed above, RMFEs only allow for one single multiplication. On the other hand, RMFEs have better properties than packing methods in that they are $\mathbb{Z}_{p^k}$-homomorphisms that do not output errors and are not randomized. This is important for their applications to MPC and ZKPs. This is the motivation of our work, which includes the following contributions.

Degree-D RMFEs. In this work, we extend the important notion of RMFEs by introducing the concept of *Degree-D Reverse Multiplication-Friendly Embeddings*, which is a generalization of RMFEs that enable $D-1$ multiplications to be carried out before "decoding". In more detail, a degree-D RMFE is a pair of $\mathbb{Z}_{p^k}$-linear homomorphisms $(\phi : \mathbb{Z}_{p^k}^r \to \mathsf{GR}(p^k, d), \psi : \mathsf{GR}(p^k, d) \to \mathbb{Z}_{p^k}^r)$ such that $\psi(\phi(\boldsymbol{x}_1) \cdot \phi(\boldsymbol{x}_2) \cdots \phi(\boldsymbol{x}_D)) = \boldsymbol{x}_1 \star \boldsymbol{x}_2 \star \cdots \star \boldsymbol{x}_D$ for every $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_D \in \mathbb{Z}_{p^k}^r$.[4] We call $\frac{r}{d}$ the ratio of RMFE. Fix p to be a constant, we call a RMFE asymptotically good if this ratio is a constant for growing r and d. In our work we put forward the study of these objects and make substantial progress in this direction by presenting a construction of an asymptotically good degree-D RMFE for Galois rings over $\mathbb{Z}_{p^k}$ for any r, D, p and k, where the rate is roughly $\frac{3}{D(2D+1)}$, which is *constant* in the length r.

To illustrate how such objects may be constructed, let us first present a simple example of degree-D RMFE which is *not* asymptotically good. Given a vector $\boldsymbol{x} = (x_1, \ldots, x_r) \in \mathbb{Z}_{p^k}^r$ with $p > r$, we define the map ϕ as $\phi(\boldsymbol{x}) = f(x) \in \mathsf{GR}(p^k, (r-1)D+1) \cong \mathbb{Z}_{p^k}/(g(x))$ with $f(i) = x_i$ and degree-$((r-1)D+1)$ irreducible polynomial $g(x)$ over $\mathbb{Z}_{p^k}$. The map ψ is defined as $\psi(f(x)) = (f(1), \ldots, f(r))$. The multiplication relation holds as the product of any D degree-$(r-1)$ polynomials is a polynomial of degree at most $D(r-1)$. Since the degree of this polynomial is less than $\deg(g(x)) = D(r-1)+1$, we can recover r evaluations of this polynomial. The construction of this degree-D RMFE is simple and effective, and its ratio is $\frac{r}{(r-1)D+1}$, which is optimal. However, the length r of the vector $\boldsymbol{x}$ is upper bounded by p, while instead, we would like a single RMFE construction that works for *any* choice of r.[5] Inspired by the approach taken in the original work on (degree-2) RMFEs [9], in order to obtain an asymptotically good degree-D RMFEs we resort to the theory of *function fields*. By applying certain "concatenation" method to the asymptotically good RMFEs derived from these mathematical objects, we are then able to obtain our asymptotically good degree-D RMFEs over $\mathbb{Z}_{2^k}$.

Our results on degree-D RMFEs generalize these in [9] from $D = 2$ to $D > 2$, showing that the techniques in that work are a particular case of a more general

[4] In our actual definition, as in the definition of traditional (degree-2) RMFEs, the domain of ϕ/codomain of ψ can be a Galois ring as well instead of $\mathbb{Z}_{p^k}$.

[5] It is possible to improve this basic construction via certain concatenation techniques. However, any construction based on this polynomial evaluation cannot achieve constant ratio, which can be seen as an analogue of the concatenation of Reed-Solomon codes in the classic coding theory.

framework. This improves our understanding on these important tools, and furthermore, we believe our work opens an interesting direction of study in terms of constructing even better degree-D RMFEs, and expanding the set of applications that can benefit from them.

Relations to the packing methods from [12]. We show that degree-D RMFEs are particular cases of packing methods, but in the general case the converse direction does not hold, that is, not every degree-D packing method is a degree-D RMFE. In fact, we are able to prove that packing methods that satisfy certain *additional* linearity properties can be turned into degree-D RMFEs. Crucially, degree-D RMFEs satisfy the following highly relevant properties not held by packing methods:

- Degree-D RMFEs are actual $\mathbb{Z}_{p^k}$-homomorphisms, so unlike the packing methods from [12], they are not randomized, they are fully linear and they do not output errors.
- A degree-D packing method consists of different packing/unpacking methods, one for every "level" $\ell \in \{1, \ldots, D\}$. In contrast, degree-$D$ RMFEs consist of only *one* "packing/unpacking" pair (ϕ, ψ), which works for all levels.

The relations between packing methods and our degree-D RMFEs are explored in detail in Section 3. We show that a degree-D RMFE is actually a degree-D packing method. This means the lower bound on the ratio in [12] can be applied to degree-D RMFE. We provide several constructions of degree-D RMFE which can be directly transformed to degree-D packing method. Unlike the construction in [12], our packing methods obtained from RMFEs are $\mathbb{Z}_{p^k}$-homomorphism. Our construction of RMFE implies that there exists degree-D packing method of density roughly $\frac{3}{D(1+2D)}$ over $\mathbb{Z}_{2^\ell}$ for any D and ℓ, which is *constant* in the length. On the other hand, if we add an extra requirement on the packing method that the packing algorithm in the packing method is deterministic and linear, then a degree-D packing method is a degree-D RMFE as well.

Applications of degree-D RMFEs. As discussed previously, RMFEs have found multiple theoretical and practical applications across different domains such as MPC and zero-knowledge proofs. From this, our degree-D RMFEs can be used as a drop-in replacement in settings that currently use traditional (degree-2) RMFEs, but require large degree evaluation. For example, it can be used to amortize the communication of securely computing the product of, say, three secrets, or proving in zero-knowledge the correctness of a, say, product of three witnesses. Unfortunately, some of these applications do not benefit directly from products of more than two terms, essentially because of the fact that single multiplication is "complete" to represent a more general computation, and aspects such as interaction enable weaker notions such as traditional degree-2 RMFEs to be sufficient. In Section 5 we add a thorough discussion on potential applications of this type, where existing RMFE-based solutions are "enhanced" by enabling larger degree.

In this work we identify a concrete application that benefits extensively by the use of degree-D RMFEs for $D > 2$. This corresponds to delegating the generation of preprocessing material for certain secure computation (*e.g.* authenticated multiplication triples) to a large committee, which is in charge of generating said correlations in order to later re-share them for the target MPC execution. Since the larger the committee the better the ratio of honest parties, it is good if such a protocol for correlation generation scales well as the number of parties grows. We model this by requiring *no interaction* among the parties in the large committee, which can be enabled by means of pseudo-random Shamir secret-sharing techniques and local multiplications with low-enough threshold. However, when the target ring structure has a small Lenstra constant, such techniques do not work, and hence require a large ring extension.

This is precisely where our degree-D RMFEs prove themselves useful: they enable the use of ring extensions while non-interactively multiplying several secrets in order to generate the desired correlations, but without paying the "penalty" of using said large degree extensions. As a result, we obtain efficient delegation of correlations of degree ≥ 2, while avoiding communication among the generating committee (which enables larger and hence more trustworthy quorums). This application, however, is not a simple "plug-and-play" of our degree-D RMFEs, and we introduce several techniques of potential independent interest to tackle this. The main challenge lies in ensuring that pseudo-random secret-sharing techniques can be adapted to generate the concrete type of sharings we need in our context, given that the underlying secrets will have to belong to a particular submodule. In Section 5, where we describe this application in detail, we show how such PRSS constructions can be instantiated, drawing inspiration from the techniques in [3] in order to improve the storage complexity by exploiting a small corruption threshold.

We fully prove the security of our PRSS construction, and then we use it in conjunction with our degree-D RMFEs to efficiently instantiate the application above. We refer to the full version[19] for a more detailed overview on this application.

1.2 Related Work

The first constructions of (degree-2) RMFEs appeared in [9], although some ideas were already present in [4]. After these works, there is a large body of research that has applied RMFEs for different settings such as secure multiparty computation or zero-knowledge proofs, with a non-exhaustive list including [21,2,26,10].

Given the traction achieved by the concept of RMFEs, and also given the use of other forms of packing in domains such as lattice-based homomorphic encryption [32], the work of [12] aimed at presenting a unified framework that captures these different packing notions. The resulting concept, *packing methods*, constitutes a generalization of both (degree-2) RMFEs and the CRT-based packing used in lattice-based cryptography. The authors then present a survey of existing techniques that fit their framework, and present bounds and impossibility result on the existence and the efficiency of their packing methods. Our degree-D

RMFEs constitute a generalization of degree-2 RMFEs, and, as we show in Section 3, they turn out to be particular instances of the packing methods from [12]. Furthermore, with a minor extra condition, packing methods turn out to be equivalent to our degree-D RMFEs. The relation between these two notions is explored in detail in Section 3.

Regarding delegation of correlation generation for MPC, the work of [24], which introduces an MPC protocol based on packed secret-sharing that is particularly suitable for parallel computation, presents an application where this protocol is used by a committee $\mathcal{P}$ to generate multiplication triples to another committee $\mathcal{Q}$. We note that their protocol requires communication among the parties in committee $\mathcal{P}$, whereas our solution is fully non-interactive. Even more—and very importantly for our application of degree-D RMFEs—our techniques are used to generate arbitrary degree-D correlations, while in [24] only multiplication triples, a particular case of degree-2 correlations, is considered. However, the non-interactivity aspect of our solution is achieved at the expense of using pseudo-random secret-sharing (which requires exponential storage for some parameter choices), and the high degree aspect requires tolerating a smaller threshold. Furthermore, the techniques in [24] support an active adversary, while our solution in Section 5 is only passively secure.

Finally, in terms of pseudo-random secret-sharing, earlier techniques [14,23] required an exponential amount of seeds to be held by each party, and they were only suitable for Shamir secret-sharing over fields where the underlying secret is uniformly random in the field. In the recent work of [3] this was generalized by making use of covering designs, and instantiations of PRSS solutions for sharings of higher-degree with more structured underlying secrets were proposed. These techniques serve as the basis for our PRSS from Section 5.2, but we cannot use it directly since (1) they are designed for use over finite fields while in our case we have a Galois ring, and most importantly, (2) the type of correlations we need to generate are not included in the ones proposed in [3]. The first issue is easily addressed by making use of the fact that Galois rings have a large enough Lenstra constant. On the other hand, the second complication requires us to propose from scratch a new PRSS solution for our correlations at hand, based on the covering design approach from [3].

2 Preliminaries

Notation. We let p be a prime, and d, k, m, n be positive integers. Generally, p^k will be the characteristic of the rings we consider, d, m will be the degree of certain ring extensions, and n will be the dimension of the vectors that will be packed. Vectors are denoted with bold characters, and, following the notation in [12], element-wise multiplication of vectors is denoted by $\boldsymbol{a} \star \boldsymbol{b}$.

Galois Rings. Let $\mathsf{Irr}(\mathtt{X})$ be a polynomial over $\mathbb{Z}_{p^k}$ of degree d, such that reducing its coefficients modulo p leads to an irreducible polynomial over the field $\mathbb{Z}_p$. Consider the quotient ring $\mathbb{Z}_{p^k}[\mathtt{X}]/(\mathsf{Irr}(\mathtt{X}))$. This is a *Galois ring* of degree d and

characteristic p^k, and we denote it by $\mathsf{GR}(p^k, d)$. As particular cases, we have that $\mathsf{GR}(p^k, 1)$ equals $\mathbb{Z}_{p^k}$, the ring of integers modulo p^k, and $\mathsf{GR}(p, d)$ equals $\mathbb{F}_{p^d}$, the finite field with p^d elements.

A crucial fact of Galois rings is that their non-invertible elements are exactly the elements that are multiples of p. From this, it can be proven that one can do polynomial interpolation over Galois rings in essentially the same way similarly as in the finite field case, as the following proposition shows.

Proposition 1 ([35,2]). *Assume that $p^d \geq n$. There exists n elements $\alpha_1, \ldots, \alpha_n$ in $\mathsf{GR}(p^k, d)$ such that given any $x_1, \ldots, x_n \in \mathsf{GR}(p^k, d)$, there is a unique polynomial of degree $n-1$, $f(\mathtt{X}) \in \mathsf{GR}(p^k, d)[\mathtt{X}]$, with $f(\alpha_i) = x_i$. We call such $\{\alpha_1, \ldots, \alpha_n\}$ an exceptional set.*

Using Proposition 1, all of the results from finite fields regarding interpolation and polynomial evaluation carry over to the Galois ring setting. For example, Schwartz-Zippel lemma holds, and also Shamir secret-sharing can be constructed.

Function Fields. Let us briefly recall some background on algebraic function fields, which will play a crucial role in our constructions. The reader may refer to [34] for the details.

A function field F over $\mathbb{F}_q$ is a field extension over $\mathbb{F}_q$ in which there exists an element z of F that is transcendental over $\mathbb{F}_q$ such that $F/\mathbb{F}_q(z)$ is a finite extension. $\mathbb{F}_q$ is called the full constant field of F if the algebraic closure of $\mathbb{F}_q$ in F is $\mathbb{F}_q$ itself. In this paper, we always assume that $\mathbb{F}_q$ is the full constant field of F, denoted by $F/\mathbb{F}_q$.

Each discrete valuation ν from F to $\mathbb{Z} \cup \{\infty\}$ defines a local ring $O = \{f \in F : \nu(f) \geq 0\}$. The maximal ideal P of O is called a *place*. We denote the valuation ν and the local ring O corresponding to P by ν_P and O_P, respectively. The residue class field O_P/P, denoted by F_P, is a finite extension of $\mathbb{F}_q$. The extension degree $[F_P : \mathbb{F}_q]$ is called *degree* of P, denoted by $\deg(P)$. For a place P and a function $f \in O_P$, we denote by $f(P)$ the evaluation of f at place P if $f \in O_P$. We note that $f(P) \in F_p$.

A divisor G is a formal sum of places, $G = \sum c_P P$, such that $c_P \in \mathbb{Z}$ and $c_P = 0$ except for a finite number of P.[6] We call this set of places where $c_P \neq 0$ the support of G, denoted by $\mathrm{supp}(G)$. The degree of G is $\deg G := \sum c_P \deg P \in \mathbb{Z}$. The Riemann-Roch space $\mathcal{L}(G)$ is the set of all functions in F with certain prescribed poles and zeros depending on G (together with the zero function). More precisely if $G = \sum c_P P$, every function $f \in \mathcal{L}(G)$ must have a zero of order at least $|c_P|$ in the places P with $c_P < 0$, and f can have a pole of order at most c_P in the places with $c_P > 0$. The space $\mathcal{L}(G)$ is a vector space over $\mathbb{F}_q$. Its dimension is governed by certain laws (given by the so-called Riemann-Roch theorem). A weaker version of that theorem called Riemann's theorem states that if $\deg G \geq$

[6] c_P is only used for expressing divisor G explicitly so as to present the basic property of the function field. The explicit construction of G is not the focus of this paper. Thus, c_p will not appear in our construction.

$2\mathfrak{g}-1$ then $\dim \mathcal{L}(G) = \deg(G) - \mathfrak{g} + 1$. On the other hand, if $\deg G < 0$, then $\dim \mathcal{L}(G) = 0$. Let $P_1, \ldots, P_n$ be $n > \deg(G)$ rational places of F that is disjoint from the support of divisor G. Then, $(f(P_1), \ldots, f(P_n))$ has at most $\deg(G)$'s 0 components as $f \in \mathcal{L}(G - \sum_{f(P_i)=0} P_i)$ implying $\dim \mathcal{L}(G - \sum_{f(P_i)=0} P_i) > 0$. Moreover, if $f, g \in \mathcal{L}(G)$, then $fg \in \mathcal{L}(2G)$ as fg has the pole of order at most $2c_P$ in the place P with $G = \sum c_P P$. This property can be seen as the generalization of the polynomials in the function field.

Packing Methods. Now we present the notion of packing methods, as introduced in [12, Definition 3.1], together with some results given in that work. The definition in [12], however, considers arbitrary rings, while we adapt it here to focus only on Galois rings. This is not restrictive: as we have mentioned, important rings such as $\mathbb{Z}_{p^k}$ or $\mathbb{F}_{p^d}$ are particular cases, and these are the only types of structures considered in [12] ultimately.

Definition 1 (Packing methods). *Consider two Galois rings* $\mathsf{GR}(p^k, d)$ *and* $\mathsf{GR}(p^k, m)$*. We call a pair of algorithms* $(\mathsf{Pack}, \mathsf{Unpack})$ *a packing method for* n $\mathsf{GR}(p^k, d)$*-messages into* $\mathsf{GR}(p^k, m)$*, if it satisfies the following.*

- Pack *is an algorithm (possibly probabilistic) which, given* $\boldsymbol{a} \in \mathsf{GR}(p^k, d)^n$ *as an input, outputs an element of* $\mathsf{GR}(p^k, m)$*.*
- Unpack *is a deterministic algorithm which, given* $a \in \mathsf{GR}(p^k, m)$ *as an input, outputs an element of* $\mathsf{GR}(p^k, d)^n$ *or* $\perp$ *denoting a failure.*
- $\mathsf{Unpack}(\mathsf{Pack}(\boldsymbol{a})) = \boldsymbol{a}$ *holds for all* $\boldsymbol{a} \in \mathsf{GR}(p^k, d)^n$ *with probability* 1*.*

The notion of a packing method does not capture how the packing and unpacking algorithms should behave with respect to the operations of the two involved rings. This is captured by the concept of a degree-D packing, which in essence, requires that these methods must be additively homomorphic, and they must be compatible with "up to D multiplications".

Definition 2 (Degree-D packing, definition 3.1 in [12]). *Let* $(\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^{D}$ *be a collection of packing methods of* $\mathsf{GR}(p^k, d)^n$ *into* $\mathsf{GR}(p^k, m)$*. We call this collection a degree-*D packing method*, if it satisfies the following: for any* $1 \leq i \leq D$*, then*

- $\mathsf{Unpack}_i(a \pm b) = \boldsymbol{a} \pm \boldsymbol{b}$*, if* $a, b \in \mathsf{GR}(p^k, m)$ *satisfy* $\mathsf{Unpack}_i(a) = \boldsymbol{a} \neq \perp$ *and* $\mathsf{Unpack}_i(b) = \boldsymbol{b} \neq \perp$*;*
- *If* $s, t \in \mathbb{Z}^+$ *are such that* $s + t = i \leq D$*, then* $\mathsf{Unpack}_i(a \cdot b) = \boldsymbol{a} \star \boldsymbol{b}$ *holds, where* $a, b \in \mathsf{GR}(p^k, m)$ *satisfy* $\mathsf{Unpack}_s(a) = \boldsymbol{a} \neq \perp$ *and* $\mathsf{Unpack}_t(b) = \boldsymbol{b} \neq \perp$*.*

These definitions imply that $\mathsf{Unpack}_i(c \cdot a) = c \cdot \mathsf{Unpack}_i(a)$ for any $c \in \mathbb{Z}_{p^k}$, and in particular $\mathsf{Unpack}_i(0) = \mathbf{0}$.

We define the *packing density* of a packing method to be the ratio $n \cdot d/m$. Notice that, even though the Pack algorithm of a packing method can be probabilistic, we can make this algorithm deterministic by fixing the random coins. This will not affect Definition 2, and the packing density does not decrease. In what follows, we focus on the deterministic packing algorithms.

3 Degree-D RMFEs and Relations to Packing Methods

We now introduce the novel concept of a degree-D reverse multiplication-friendly embedding, or RMFE, for short. For $D = 2$, the notion of an RMFE was introduced in [9], where explicit constructions based on techniques from algebraic geomtry were given. Here we consider a natural generalization for $D \geq 2$.

Definition 3 (Degree-D Reverse Multiplication-Friendly Embedding). *Consider two Galois rings* $\mathsf{GR}(p^k, d)$ *and* $\mathsf{GR}(p^k, rd)$*. Let* $\phi : \mathsf{GR}(p^k, d)^n \to \mathsf{GR}(p^k, rd)$ *and* $\psi : \mathsf{GR}(p^k, rd) \to \mathsf{GR}(p^k, d)^n$ *be two group homomorphisms (*i.e. *they are additively homomorphic). The pair* (ϕ, ψ) *is a* degree-D reverse multiplication-friendly embedding*, or degree-D RMFE for short, if, for any* $\boldsymbol{a}_1 \ldots, \boldsymbol{a}_D \in \mathsf{GR}(p^k, d)^n$*, it holds that* $\psi(\phi(\boldsymbol{a}_1) \cdot \phi(\boldsymbol{a}_2) \cdots \phi(\boldsymbol{a}_D)) = \boldsymbol{a}_1 \star \boldsymbol{a}_2 \star \cdots \star \boldsymbol{a}_D$*. We call such RMFE a* $(n, r; D)$*-RMFE over* $\mathsf{GR}(p^k, d)$*.*

Some important direct consequences of this definition are presented in the following propositions.

Proposition 2. *Let* (ϕ, ψ) *be a degree-D RMFE. Then* ϕ *is injective and* ψ *is surjective.*

Proof. To see that ϕ is injective it suffices to show that $\phi(\boldsymbol{a}) = 0$ implies that $\boldsymbol{a} = \boldsymbol{0}$. Indeed, if $\phi(\boldsymbol{a}) = 0$ then $\boldsymbol{0} = \psi(0) = \psi(\phi(\boldsymbol{a}) \star \phi(\boldsymbol{1}) \cdots \phi(\boldsymbol{1})) = \boldsymbol{a} \star \boldsymbol{1} \star \cdots \star \boldsymbol{1} = \boldsymbol{a}$. Similarly, given $\boldsymbol{a} \in \mathsf{GR}(p^k, d)^n$, it can be verified that a preimage of $\boldsymbol{a}$ under ψ is given by $\phi(\boldsymbol{a}) \cdot \phi(\boldsymbol{1}) \cdots \phi(\boldsymbol{1})$, which shows that ψ is surjective. □

Lemma 1. *Both* ϕ *and* ψ *are* $\mathbb{Z}_{p^k}$*-linear maps.*

Proof. The proof is quite straightforward. Due to the fact that ϕ is group homomorphism, we have $\phi(h\boldsymbol{a}) = \phi(\sum_{i=1}^{h} \boldsymbol{a}) = \sum_{i=1}^{h} \phi(\boldsymbol{a}) = h\phi(\boldsymbol{a})$ for any $h \in \mathbb{Z}_{p^k}$ and $\boldsymbol{a} \in \mathsf{GR}(p^k, d)^n$. The same argument can be applied to ψ as well. □

Lemma 2. *Let* $(\phi : \mathsf{GR}(p^k, d)^n \to \mathsf{GR}(p^k, m),\ \psi : \mathsf{GR}(p^k, m) \to \mathsf{GR}(p^k, d)^n)$ *be a degree-D RMFE. Then there exists a degree-D RMFE* $(\phi' : \mathsf{GR}(p^k, d)^n \to \mathsf{GR}(p^k, m),\ \psi' : \mathsf{GR}(p^k, m) \to \mathsf{GR}(p^k, d)^n)$ *with* $\phi'(\boldsymbol{1}) = 1$*.*

Proof. We begin by claiming that $\phi(\boldsymbol{1}) \in \mathsf{GR}(p^k, m)$ is invertible. Assume not, and thus $p \mid \phi(\boldsymbol{1})$. As ϕ is a $\mathbb{Z}_{p^k}$-linear map, we have $\phi(p^{k-1}\boldsymbol{1}) = p^{k-1}\phi(\boldsymbol{1}) = 0$ which contradicts to Proposition 2. Now, we define $\phi' : \mathsf{GR}(p^k, d)^n \to \mathsf{GR}(p^k, m)$ and $\psi' : \mathsf{GR}(p^k, m) \to \mathsf{GR}(p^k, d)^n$ as follows: $\phi'(\boldsymbol{a}) = \phi(\boldsymbol{a}) \cdot \phi(\boldsymbol{1})^{-1}$ for $\boldsymbol{a} \in \mathsf{GR}(p^k, d)^n$, and $\psi'(a) = \psi(\boldsymbol{a} \cdot \phi(\boldsymbol{1})^D)$ for $a \in \mathsf{GR}(p^k, m)$. It is easy to verify that these functions are additively homomorphic. We can also see that $\phi'(\boldsymbol{1}) = \phi(\boldsymbol{1}) \cdot \phi(\boldsymbol{1})^{-1} = 1$, as required. It is only left to check then that (ϕ', ψ') is indeed a degree-D RMFE. To see this, consider $\boldsymbol{a}_1 \ldots, \boldsymbol{a}_D \in \mathsf{GR}(p^k, d)^n$, then $\psi'(\phi'(\boldsymbol{a}_1) \cdot \phi'(\boldsymbol{a}_2) \cdots \phi'(\boldsymbol{a}_D)) = \psi'(\phi(\boldsymbol{a}_1) \cdots \phi(\boldsymbol{a}_D) \cdot \phi(\boldsymbol{1})^{-D}) = \psi(\phi(\boldsymbol{a}_1) \cdots \phi(\boldsymbol{a}_D) \cdot \phi(\boldsymbol{1})^{-D} \cdot \phi(\boldsymbol{1})^D) = \psi(\phi(\boldsymbol{a}_1) \cdots \phi(\boldsymbol{a}_D)) = \boldsymbol{a}_1 \star \boldsymbol{a}_2 \star \cdots \star \boldsymbol{a}_D$. □

A degree-D RMFE (ϕ, ψ) that satisfies $\phi(\mathbf{1}) = 1$ has several interesting properties, and due to the previous lemma, we assume this to be the case from now on. First, the composition $\psi \circ \phi$ is the identity function $\mathsf{GR}(p^k, d)^n \to \mathsf{GR}(p^k, d)^n$, which follows from $\psi(\phi(\boldsymbol{a})) = \psi(\phi(\boldsymbol{a}) \cdot 1 \cdots 1) = \psi(\phi(\boldsymbol{a}) \cdot \phi(\mathbf{1}) \cdots \phi(\mathbf{1})) = \boldsymbol{a} \star \mathbf{1} \star \cdots \star \mathbf{1} = \boldsymbol{a}$.

In addition, such a degree-D RMFE is also a degree-D' RMFE for any $D' \leq D$ (a property that does not necessarily hold for a more general RMFE). Indeed, given $\boldsymbol{a}_1 \ldots, \boldsymbol{a}_{D'} \in \mathsf{GR}(p^k, d)^n$, we have that $\psi(\phi(\boldsymbol{a}_1) \cdots \phi(\boldsymbol{a}_{D'})) = \psi(\phi(\boldsymbol{a}_1) \cdots \phi(\boldsymbol{a}_{D'}) \cdot 1 \cdots 1) = \psi(\phi(\boldsymbol{a}_1) \cdots \phi(\boldsymbol{a}_{D'}) \cdot \phi(\mathbf{1}) \cdots \phi(\mathbf{1})) = \boldsymbol{a}_1 \star \cdots \star \boldsymbol{a}_{D'} \star \mathbf{1} \star \cdots \star \mathbf{1} = \boldsymbol{a}_1 \star \cdots \star \boldsymbol{a}_{D'}$.

These properties will be used later. In what follows, we discuss the equivalence between the degree-D RMFEs introduced here, and the packing methods from [12], discussed in Section 2.

3.1 From Degree-D RMFEs to Packing Methods

In this section, we show that every degree-D RMFE is a packing method of degree-D. Let $(\phi : \mathsf{GR}(p^k, d)^n \to \mathsf{GR}(p^k, m),\ \psi : \mathsf{GR}(p^k, m) \to \mathsf{GR}(p^k, d)^n)$ be a degree-D RMFE. From Proposition 2, we can assume without loss of generality that $\phi(\mathbf{1}) = 1$.

Theorem 1 (from RMFEs to packing methods). *Let* $(\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^D$ *be defined as follows:*

- $\mathsf{Pack}_i = \phi$ *for* $i = 1, \ldots, D$.
- *For each* $i = 1, \ldots, D$, $\mathsf{Unpack}_i(a) = \psi(a)$ *if* $a \in \mathsf{span}_{\mathbb{Z}_{p^k}}(M_i)$ *and* $\mathsf{Unpack}_i(a) = \perp$ *otherwise, where* $\mathsf{span}_{\mathbb{Z}_{p^k}}(M_i)$ *is the* $\mathbb{Z}_{p^k}$*-module generated by* $M_i = \{\prod_{j=1}^i \phi(\boldsymbol{x}_j) : \boldsymbol{x}_j \in \mathsf{GR}(p^k, d)^n\}$.

Then, this constitutes a degree-D packing method.

Proof. It is easy to check that $\mathsf{Unpack}_i(a \pm b) = \boldsymbol{a} \pm \boldsymbol{b}$ whenever $a, b \in \mathsf{GR}(p^k, m)$ satisfy $\mathsf{Unpack}_i(a) = \boldsymbol{a} \neq \perp$ and $\mathsf{Unpack}_i(b) = \boldsymbol{b} \neq \perp$, which follows from the fact that ψ is additively homomorphic and from the linearity of the $\mathbb{Z}_{p^k}$-module M_i.

It remains to be checked that, if $s, t \in \mathbb{Z}^+$ are such that $s + t = i$, then $\mathsf{Unpack}_i(a \cdot b) = \boldsymbol{a} \star \boldsymbol{b}$ holds, where $\mathsf{Unpack}_s(a) = \boldsymbol{a} \neq \perp$ and $\mathsf{Unpack}_t(b) = \boldsymbol{b} \neq \perp$. To see this, first we notice that, since $\boldsymbol{a} \neq \perp$ and $\boldsymbol{b} \neq \perp$, it must be that $a \in \mathsf{span}_{\mathbb{Z}_{p^k}}(M_s)$ and $b \in \mathsf{span}_{\mathbb{Z}_{p^k}}(M_t)$, so we can write a and b in the form $a = \sum_{j=1}^{\ell_a} \alpha_j m_j^{(a)}$ and $b = \sum_{j=1}^{\ell_b} \beta_j m_j^{(b)}$, where each $m_j^{(a)}$ is in M_s, each $m_j^{(b)}$ is in M_t, and each α_j, β_j is in $\mathbb{Z}_{p^k}$. Furthermore, we write $m_j^{(a)} = \prod_{q=1}^s \phi(\boldsymbol{x}_q^{(j)})$, and $m_j^{(b)} = \prod_{q=1}^t \phi(\boldsymbol{y}_q^{(j)})$. Now, we prove some claims that will be useful.

Claim. It holds that $\mathsf{Unpack}_s(a) = \sum_{j=1}^{\ell_a} \alpha_j \prod_{q=1}^s \boldsymbol{x}_q^{(j)}$, and similarly $\mathsf{Unpack}_i(b) = \sum_{j=1}^{\ell_b} \beta_j \prod_{q=1}^s \boldsymbol{y}_q^{(j)}$.

Proof (of claim). We prove this for a only, as the proof of b is similar. First, notice that $\psi(m_j^{(a)}) = \psi(\prod_{q=1}^{s} \boldsymbol{\phi}(\boldsymbol{x}_q^{(j)})) = \prod_{q=1}^{s} \boldsymbol{x}_q^{(j)}$, which follows from the fact that (ϕ, ψ) is not only a degree-D RMFE, but also a degree-s RMFE. The claim then holds because of the linearity of ψ.

Claim. For each j it holds that $\psi((\prod_{q=1}^{s} \phi(\boldsymbol{x}_q^{(j)}))\cdot(\prod_{q=1}^{t} \phi(\boldsymbol{y}_q^{(j)}))) = (\prod_{q=1}^{s} \boldsymbol{x}_q^{(j)})\star (\prod_{q=1}^{t} \boldsymbol{y}_q^{(j)})$.

Proof (of claim). This follows directly from the fact that (ϕ, ψ) is a degree-D' RMFE for any $D' \leq D$, and the fact that $s + t = i \leq D$.

It is easy to see that $a \cdot b \in \mathsf{span}_{\mathbb{Z}_{p^k}}(M_i)$. With this, and the two claims above at hand, we can compute the following:

$$
\begin{aligned}
\mathsf{Unpack}_i(a \cdot b) &= \psi(a \cdot b) \\
&= \psi((\sum_{j=1}^{\ell_a} \alpha_j m_j^{(a)}) \cdot (\sum_{h=1}^{\ell_b} \beta_h m_h^{(b)})) \\
&= \psi(\sum_{j,h} \alpha_j \beta_h \cdot m_j^{(a)} m_h^{(b)}) \\
&= \sum_{j,h} \alpha_j \beta_h \cdot \psi(m_j^{(a)} m_h^{(b)}) && \text{linearity of } \psi \\
&= \sum_{j,h} \alpha_j \beta_h \cdot ((\prod_{q=1}^{s} \boldsymbol{x}_q^{(j)}) \star (\prod_{q=1}^{t} \boldsymbol{y}_q^{(j)})) && \text{second claim} \\
&= (\sum_{j=1}^{\ell_a} \alpha_j \prod_{q=1}^{s} \boldsymbol{x}_q^{(j)}) \star (\sum_{h=1}^{\ell_b} \beta_h \prod_{q=1}^{t} \boldsymbol{y}_q^{(j)}) \\
&= \mathsf{Unpack}_s(a) \star \mathsf{Unpack}_t(b). && \text{first claim}
\end{aligned}
$$

This concludes the proof of the theorem. □

3.2 From Degree-D Packing to Degree-D RMFEs

In general, not every degree-D packing is a degree-D RMFE. First, a degree-D packing is a *family* of pairs $(\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^{D}$, while a degree-$D$ RMFE is only made of one pair of functions. In addition, packing methods do not need to be deterministic or linear, which are properties satisfied by RMFEs. Finally, the Unpack algorithm of a packing method can result in $\perp$ while RMFEs, being homomorphisms, do not. In this direction, consider the following example.

Example 1. Consider a packing method for n $\mathsf{GR}(p^k, d)$-messages into a $\mathsf{GR}(p^k, 2 \cdot n \cdot d)$ message for $p^d \geq n$. From proposition 1, we can find n distinct elements $\alpha_1, \ldots, \alpha_n \in \mathsf{GR}(p^k, d)$ to do interpolation on. The packing algorithm is defined

as follows: given $(x_1, \ldots, x_n) \in \mathsf{GR}(p^k, d)^n$, we randomly select a polynomial $f(x)$ of degree n over $\mathsf{GR}(p^k, d)$ such that $f(\alpha_i) = x_i$. Note that this $f(x)$ is not unique as we only interpolate f at n points. Then, the pack algorithm is defined as $\mathsf{Pack}((x_1, \ldots, x_n)) = f(x) \in \mathsf{GR}(p^k, 2nd)$ as $\mathsf{GR}(p^k, 2nd) \cong \mathsf{GR}(p^k, d)/(g(x))$ with a degree-$2n$ irreducible polynomial $g(x)$ over $\mathsf{GR}(p^k, d)$. The unpack algorithm is also clear as we define $\mathsf{Unpack}(f(x)) = (f(\alpha_1), \ldots, f(\alpha_n))$. One can also easily show that this packing method is a degree-2 packing. However, it is not a degree-2 RMFE as the packing method is not deterministic.

In this section, we show that being deterministic and linear is not only necessary for a degree-D packing to be a degree-D RMFE, but they are in fact *sufficient*. In other words, we show that a degree-D RMFE can be derived from any degree-D packing $(\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^D$, as long as each Pack_i is $\mathbb{Z}_{p^k}$-linear and deterministic. This is proven in Theorem 2 below. However, we first present Proposition 3 and Lemma 3, which are useful tools for proving the claimed result.

Proposition 3. *Let $(\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^D$ be a degree-D packing method. Then, for any $\boldsymbol{a}_1 \ldots, \boldsymbol{a}_D \in \mathsf{GR}(p^k, d)^n$, we have that $\mathsf{Unpack}_D(\mathsf{Pack}_1(\boldsymbol{a}_1) \cdots \mathsf{Pack}_1(\boldsymbol{a}_D)) = \boldsymbol{a}_1 \star \cdots \star \boldsymbol{a}_D$.*

Proof. We prove it by induction. For $D = 2$, it is clear that $\mathsf{Unpack}_D(\mathsf{Pack}_1(\boldsymbol{a}_1) \cdot \mathsf{Pack}_1(\boldsymbol{a}_2)) = \boldsymbol{a}_1 \star \boldsymbol{a}_2$ as we let $i = 2, s = t = 1$ in Definition 2. We proceed to the case D. Let $a = \mathsf{Pack}_1(\boldsymbol{a}_1) \cdots \mathsf{Pack}_1(\boldsymbol{a}_{D-1})$ and $b = \mathsf{Pack}_1(\boldsymbol{a}_D)$ in Definition 2, we have $\mathsf{Unpack}_D(a \cdot b) = \mathsf{Unpack}_{D-1}(a) \star \mathsf{Unpack}_1(b) = \mathsf{Unpack}_{D-1}(a) \star \boldsymbol{a}_D$. The proof is completed by applying the induction $\mathsf{Unpack}_{D-1}(\mathsf{Pack}_1(\boldsymbol{a}_1) \cdots \mathsf{Pack}_1(\boldsymbol{a}_{D-1})) = \boldsymbol{a}_1 \star \cdots \star \boldsymbol{a}_{D-1}$. □

From the proposition above, the following observation holds. Let $a \in M_D = \{\prod_{j=1}^D \mathsf{Pack}_1(\boldsymbol{x}_j) : \boldsymbol{x}_j \in \mathsf{GR}(p^k, d)^n\}$, then $\mathsf{Unpack}_D(a) = \prod_{j=1}^D \boldsymbol{x}_j$, and in particular, $\mathsf{Unpack}_D(a) \neq \perp$. Furthermore, this also extends naturally to the case in which $a \in \mathsf{span}_{\mathbb{Z}_{p^k}}(M_D)$ by using the linearity of Unpack_1. In particular, Unpack_1 restricted to $\mathsf{span}_{\mathbb{Z}_{p^k}}(M_D)$ is a $\mathbb{Z}_{p^k}$-linear homomorphism, and therefore, the following lemma can be applied to it.

Lemma 3. *Let $f : M \to \mathsf{GR}(p^k, d)^n$ be a $\mathbb{Z}_{p^k}$-linear function, where M is a $\mathbb{Z}_{p^k}$-submodule of $\mathsf{GR}(p^k, m)$. Then, f can be extended to a $\mathbb{Z}_{p^k}$-linear function $g : \mathsf{GR}(p^k, m) \to \mathsf{GR}(p^k, d)^n$.*

Proof. As M is $\mathbb{Z}_{p^k}$-submodule of $\mathsf{GR}(p^k, m)$, by the fundamental decomposition theorem, we write $M = \sum_{i=1}^a S_i \beta_i$ with $S_1 \subseteq \cdots \subseteq S_a$ are the ideal of $\mathbb{Z}_{p^k}$ and $\beta_i \in \mathsf{GR}(p^k, m)$. To extend f, it suffices to decide the value of $g(\beta_i)$. Assume $S_i = p^{\alpha_i}\mathbb{Z}_{p^k}$. As $g(x)$ is $\mathbb{Z}_{p^k}$-linear, we have $f(p^{\alpha_i}\beta_i) = g(p^{\alpha_i}\beta_i) = p^{\alpha_i} g(\beta_i)$. This implies that $g(\beta_i) = p^{-\alpha_i} f(p^{\alpha_i}\beta_i)$. Thus, we extend the domain of f from M to a free module $M' := \bigoplus_{i=1}^a \mathbb{Z}_{p^k}\beta_i$. As we can write $\mathsf{GR}(p^k, m) = M' \oplus N$ where $N = \bigoplus_{i=1}^{m-a} \mathbb{Z}_{p^k}\gamma_i$, define the value $g(\gamma_i) \in \mathsf{GR}(p^k, d)^n$ in an arbitrary manner and the proof is completed. □

With this lemma at hand we can finally construct our degree-D RMFE from the degree-D packing method $(\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^D$.

Theorem 2 (from packing methods to RMFEs). *Consider the following functions $\phi : \mathsf{GR}(p^k, d)^n \to \mathsf{GR}(p^k, m)$ and $\psi : \mathsf{GR}(p^k, m) \to \mathsf{GR}(p^k, d)^n$:*

- *$\phi(\boldsymbol{a}) = \mathsf{Pack}_1(\boldsymbol{a})$ for $\boldsymbol{a} \in \mathsf{GR}(p^k, d)^n$;*
- *ψ is defined by applying Lemma 3 to $f = \mathsf{Unpack}_D$ and $M = \mathsf{span}_{\mathbb{Z}_{p^k}}(M_D)$. In a bit more detail, $\psi(a) = \mathsf{Unpack}_D(a)$ for $a \in \mathsf{span}_{\mathbb{Z}_{p^k}}(M_D)$, and for $a \notin \mathsf{span}_{\mathbb{Z}_{p^k}}(M_D)$ $\psi(a)$ is defined as to preserve linearity.*

Then, (ϕ, ψ) is a degree-D RMFE.

Proof. First, from Lemma 3, we know that ψ is a $\mathbb{Z}_{p^k}$-linear map. The linearity of ϕ is followed by the fact that Pack_1 is $\mathbb{Z}_{p^k}$-linear. Since both Pack_1 and Unpack_D are deterministic, ϕ and ψ are well defined.

Finally, we prove the required multiplicative relation. Let $\boldsymbol{a}_1 \ldots, \boldsymbol{a}_D \in \mathsf{GR}(p^k, d)^n$, then, from Proposition 3, we have that

$$\begin{aligned}\psi(\phi(\boldsymbol{a}_1) \cdots \phi(\boldsymbol{a}_D)) &= \mathsf{Unpack}_D(\mathsf{Pack}_1(\boldsymbol{a}_1) \cdots \mathsf{Pack}_1(\boldsymbol{a}_D)) \\ &= \boldsymbol{a}_1 \star \cdots \star \boldsymbol{a}_D,\end{aligned}$$

as required. This completes the proof. □

4 Constructing Degree-D RMFEs

This section is devoted to the explicit construction of degree-D RMFEs over Galois rings. The organization of this section is the following. First, in Section 4.1 we provide a series of results that will be useful in our general construction. Then, in Section 4.2 we begin with the particular case of $D = 2$, presenting explicit constructions of degree-2 RMFEs over Galois rings. This serves two purposes. First, even though the results of [15] show that degree-2 RMFEs over Galois rings can be obtained by *lifting* existing RMFE constructions over fields (like, for example, the constructions from [9]), no explicit constructions or explicit parameters were provided. Second, we generalize the ideas in our degree-2 constructions in Section 4.3 to obtain our main result: degree-D RMFE constructions for $D \geq 2$.

4.1 Lemmata

We first provide a composition lemma that shows that composing two degree-D RMFEs results in a degree-D RMFE. Such lemma can be seen as an analogue of concatenation in classical coding theory. The composition lemma of RMFEs over fields in [9] can reduce the task of designing an RMFE over a general field extension to the case of a prime field. Here we present a version of this lemma over Galois rings. Generally speaking, given one RMFE of large dimension over

a big Galois ring and another RMFE of small dimension over a small Galois ring, the composition of these two RMFEs gives rise to an RMFE of large dimension over the small Galois ring.

Lemma 4 (Composition Lemma). *Assume that (ϕ_1, ψ_1) is an $(n_1, k_1; D)$-RMFE over $\mathsf{GR}(p^\ell, k_2 r)$ and (ϕ_2, ψ_2) is an $(n_2, k_2; D)$-RMFE over $\mathsf{GR}(p^\ell, r)$. Then $\phi: \mathsf{GR}(p^\ell, r)^{n_1 n_2} \to \mathsf{GR}(p^\ell, r k_1 k_2)$ given by*

$$(\mathbf{x}_1, \ldots, \mathbf{x}_{n_1}) \mapsto (\phi_2(\mathbf{x}_1), \ldots, \phi_2(\mathbf{x}_{n_1})) \in \mathsf{GR}(p^\ell, r k_2)^{n_1} \mapsto \phi_1(\phi_2(\mathbf{x}_1), \ldots, \phi_2(\mathbf{x}_{n_1}))$$

and $\psi: \mathsf{GR}(p^\ell, r k_1 k_2) \to \mathsf{GR}(p^\ell, r)^{n_1 n_2}$ given by

$$\alpha \mapsto \psi_1(\alpha) = (\mathbf{u}_1, \ldots, \mathbf{u}_{n_1}) \in \mathsf{GR}(p^\ell, r k_2)^{n_1} \mapsto (\psi_2(\mathbf{u}_1), \ldots, \psi_2(\mathbf{u}_{n_1}))$$

define an $(n_1 n_2, k_1 k_2; D)$-RMFE over $\mathsf{GR}(p^\ell, r)$.

Proof. It is clear that both ϕ and ψ are $\mathsf{GR}(p^\ell, r)$-linear. For any $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \cdots, \mathbf{x}^{(D)} \in \mathsf{GR}(p^\ell, r)^{n_1 n_2}$, we have

$$\begin{aligned}
\psi(\prod_{i=1}^{D} \phi(\mathbf{x}^{(i)})) &= \psi_2 \circ \psi_1(\phi_1(\prod_{i=1}^{D}(\phi_2(\mathbf{x}_1^{(i)}), \ldots, \phi_2(\mathbf{x}_{n_1}^{(i)})))) \\
&= \psi_2((\phi_2(\mathbf{x}_1^{(1)}), \ldots, \phi_2(\mathbf{x}_{n_1}^{(1)})) * \cdots * (\phi_2(\mathbf{x}_1^{(D)}), \ldots, \phi_2(\mathbf{x}_{n_1}^{(D)}))) \\
&= (\psi_2(\phi_2(\mathbf{x}_1^{(1)}) * \cdots * \phi_2(\mathbf{x}_1^{(D)})), \ldots, \psi_2(\phi_2(\mathbf{x}_{n_1}^{(1)}) * \cdots * \phi_2(\mathbf{x}_{n_1}^{(D)}))) \\
&= (\mathbf{x}_1^{(1)} * \cdots * \mathbf{x}_1^{(D)}, \ldots, \mathbf{x}_{n_1}^{(1)} * \cdots * \mathbf{x}_{n_1}^{(D)}) \\
&= \mathbf{x}^{(1)} * \cdots * \mathbf{x}^{(D)}.
\end{aligned}$$

This completes the proof. □

It will be important for our constructions to establish a relation between RMFEs and function fields. This is achieved by the following lemma.

Lemma 5. *Let q be a power of a prime. Let $F/\mathbb{F}_q$ be a function field of genus $\mathfrak{g}$ with n distinct rational places $P_1, P_2, \ldots, P_n$. Let G be a divisor of F such that $\mathrm{supp}(G) \cap \{P_1, \ldots, P_n\} = \emptyset$ and $\dim_{\mathbb{F}_q} \mathcal{L}(G) - \dim_{\mathbb{F}_q} \mathcal{L}(G - \sum_{i=1}^{n} P_i) = n$. If there is a place R of degree k with $k > D \deg(G)$, then there exists an $(n, k; D)$-RMFE over $\mathbb{F}_q$.*

Proof. Consider the map $\pi: \mathcal{L}(G) \to \mathbb{F}_q^n; \quad f \mapsto (f(P_1), \ldots, f(P_n))$. Then the kernel of π is $\mathcal{L}(G - \sum_{i=1}^{n} P_i)$. Since $\dim_{\mathbb{F}_q} \mathsf{Im}(\pi) = \dim_{\mathbb{F}_q} \mathcal{L}(G) - \dim_{\mathbb{F}_q} \mathcal{L}(G - \sum_{i=1}^{n} P_i) = n$, π is surjective. Choose a subspace V of $\mathcal{L}(G)$ of dimension n such that π induces an isomorphism between V and $\mathbb{F}_q^n$.

We identify $\mathbb{F}_{q^k}$ with the residue field F_R of R. We write by $\mathbf{c}_f$ (and f_R, respectively) the vector $(f(P_1), \ldots, f(P_n))$ (and the residue class of f in F_R, respectively) for a function $f \in \mathcal{L}(D \cdot G)$. Define the linear map $\phi: \pi(V) = \mathbb{F}_q^n \to F_R = \mathbb{F}_{q^k}; \mathbf{c}_f \mapsto f_R \in \mathbb{F}_{q^k}$. Note that the above $f \in V$ is uniquely determined by $\mathbf{c}_f$. It is clear that ϕ is $\mathbb{F}_q$-linear and injective since $\deg(R) > \deg(G)$.

Define $\tau: \mathcal{L}(D \cdot G) \to F_R = \mathbb{F}_{q^k}; f \mapsto f_R \in \mathbb{F}_{q^k}$. Then τ is $\mathbb{F}_q$-linear and injective since $\deg(R) > D \deg(G) = \deg(D \cdot G)$.

Define the map $\psi: \mathsf{Im}(\tau) \subseteq F_R \to \mathbb{F}_q^n; f_R \mapsto (f(P_1), \ldots, f(P_n)) \in \mathbb{F}_q^n$. Note that the above $f \in \mathcal{L}(D \cdot G)$ is uniquely determined by f_R. ψ is $\mathbb{F}_q$-linear and surjective (but not injective). We extend ψ from $\mathsf{Im}(\tau)$ to F_R linearly. We obtain the pair (ϕ, ψ).

For any $\mathbf{c}_{f^{(1)}}, \ldots, \mathbf{c}_{f^{(D)}} \in \mathbb{F}_q^n$ with uniquely determined $f^{(1)}, \ldots, f^{(D)} \in V$, we have

$$\psi(\prod_{i=1}^{D} \phi(\mathbf{c}_{f^{(i)}})) = \psi(\prod_{i=1}^{D} f_R^{(i)}) = \psi((\prod_{i=1}^{D} f^{(i)})_R) = \mathbf{c}_{\prod_{i=1}^{D} f^{(i)}} = \mathbf{c}_{f^{(1)}} * \cdots * \mathbf{c}_{f^{(D)}}.$$

Note that $(\prod_{i=1}^{D} f^{(i)})_R$ belongs to $\mathsf{Im}(\tau)$ since $\prod_{i=1}^{D} f^{(i)} \in \mathcal{L}(DG)$. We conclude that (ϕ, ψ) defined above is an $(n, k; D)$-RMFE over $\mathbb{F}_q$. □

Note that Galois rings are a generalization of finite fields. In [15], the authors manage to show that one can explicitly construct RMFEs over the Galois ring $\mathsf{GR}(p^\ell, k)$ if there exists a explicit construction of RMFEs over the finite field $\mathbb{F}_{p^k}$. This is captured by the lifting result in Theorem 18 of [15], adapted below to our setting.

Lemma 6. *Let $q = p^r$ for a prime p. Then the $(n, k; D)$-RMFE over $\mathbb{F}_q$ constructed in Lemma 5 can be lifted to an $(n, k; D)$-RMFE over $\mathsf{GR}(p^\ell, r)$ for any $\ell \geq 1$.*

Note that although Theorem 18 of [15] only proves the above lemma for the case where $D = 2$, it can be easily generalized to arbitrary D. Let us explain this briefly. The map ϕ in the proof of Lemma 5 is injective, thus by Lemma 9 of [15] it can be lifted to a map ϕ' from $\mathsf{GR}(p^\ell, r)^n$ to $F_R = \mathsf{GR}(p^\ell, kr)$ for any $\ell \geq 1$ and ϕ' is also injecive. As the map τ in the proof of Lemma 5 is also injective, we can apply Lemma 9 of [15] again to get a map τ' from $\mathcal{L}(D \cdot D)$ to $F_R = \mathsf{GR}(p^\ell, kr)$. Finally, the map ψ' can be defined by sending $f_R \in F_R = \mathsf{GR}(p^\ell, kr)$ to $(f(P_1), \ldots, f(P_n)) \in \mathsf{GR}(p^\ell, r)^n$. Thus, the pair (ϕ', ψ') is the desired RMFE.

Corollary 1. *If $p \geq n$, then there exists an $(n, k = D(n-1)+1; D)$-RMFE over $\mathsf{GR}(p^\ell, r)$ for any $\ell \geq 1$.*

Proof. We take the rational function field $\mathbb{F}_p(x)$ and a divisor G of degree $n-1$, a place of degree $D \deg(G)+1 = D(n-1)+1$, we obtain an $(n, k = D(n-1)+1; D)$-RMFE over $\mathbb{F}_p$ by Lemma 5. The desired result follows from Lemma 6. □

4.2 Construction of Degree-2 RMFEs

In this subsection, we provide some explicit constructions of degree-2 RMFEs. We begin with an RMFE of bounded length. This RMFE is derived from rational function fields, or function fields of small genus. Then, we provide the asymptotic

construction of degree-2 RMFE based on function field towers. This will be useful to settle ideas that will be generalized in Section 4 when we construct degree-D RMFEs. Furthermore, we observe that even though degree-2 RMFEs over Galois rings were first proposed in [15], in that work the authors only presented asymptotic constructions of degree-2 RMFEs. These objects have found many applications in recent cryptographic constructions (*cf.* [7,8,5,2,21]), which motivates the task of finding explicit constructions with clear and well determined parameters. We achieve this in this section by providing explicit degree-2 RMFE constructions over Galois rings, with a wide variety of parameters. We remark that these constructions have not appeared in the literature before.

Example 2 (concrete degree-2 RMFEs of bounded dimension). Consider the rational function field over $\mathbb{F}_2$. Take $n = 2$. Choose a divisor G of degree 1 and a place of degree 2, we obtain a $(2, 3; 2)$-RMFE over $\mathbb{F}_2$ by Lemma 5. Hence, by Lemma 6, there is a $(2, 3; 2)$-RMFE over $\mathbb{Z}_{2^\ell}$ for all $\ell \geq 1$. With a divisor G of degree 2 and a place of degree 5, we obtain a $(3, 5; 2)$-RMFE over $\mathbb{F}_2$ by Lemma 5. Hence, by Lemma 6, there is a $(3, 5; 2)$-RMFE over $\mathbb{Z}_{2^\ell}$ for all $\ell \geq 1$.

Now, consider a function field over $\mathbb{F}_8$ with n rational places and genus $\mathfrak{g}$. Then for any $m \leq n$, we choose m distinct points and a divisor of degree $m + 2\mathfrak{g} - 1$. Let $k = 2(m+2\mathfrak{g}-1)+1 = 2m+4\mathfrak{g}-1$. Then we have an $(m, k = 2m+4\mathfrak{g}-1; 2)$-RMFE over $\mathbb{F}_8$. Hence, we obtain a $(2m, 6m + 12\mathfrak{g} - 3; 2)$-RMFE over $\mathsf{GR}(2^\ell, 3)$. Hence, by Lemma 5, there is a $(2m, 6m+12\mathfrak{g}-3; 2)$-RMFE over $\mathbb{Z}_{2^\ell}$ for all $\ell \geq 1$. As particular cases:

- Taking $(\mathfrak{g}, m) = (0, 9)$, we get a $(2m, 6m-3; 2)$-RMFE over $\mathbb{Z}_{2^\ell}$ for any $m \leq 9$. For instance, we have a $(8, 21; 2)$-RMFE, $(10, 27; 2)$-RMFE, $(18, 51; 2)$-RMFE over $\mathbb{Z}_{2^\ell}$ for all $\ell \geq 1$.
- Taking $(\mathfrak{g}, m) = (1, 14)$, we get a $(2m, 6m + 9; 2)$-RMFE over $\mathbb{Z}_{2^\ell}$ for any $m \leq 14$. For instance, we have a $(28, 93; 2)$-RMFE over $\mathbb{Z}_{2^\ell}$ for all $\ell \geq 1$.
- Taking $(\mathfrak{g}, m) = (2, 18)$, we get a $(2m, 6m + 21; 2)$-RMFE over $\mathbb{Z}_{2^\ell}$ for any $m \leq 18$. For instance, we have a $(36, 129; 2)$-RMFE over $\mathbb{Z}_{2^\ell}$ for all $\ell \geq 1$.

Finally, consider a function field over $\mathbb{F}_{32}$ with n rational places and genus $\mathfrak{g}$. Then for any $m \leq n$, we choose m distinct points and a divisor of degree $m+2\mathfrak{g}-1$. Let $k = 2(m+2\mathfrak{g}-1)+1 = 2m+4\mathfrak{g}-1$. Then we have an $(m, k = 2m+4\mathfrak{g}-1; 2)$-RMFE over $\mathbb{F}_{32}$. Hence, we obtain a $(3m, 10m+20\mathfrak{g}-5; 2)$-RMFE over $\mathsf{GR}(2^\ell, 5)$. Hence, by Lemma 6, there is a $(3m, 10m + 20\mathfrak{g} - 5; 2)$-RMFE over $\mathbb{Z}_{2^\ell}$ for all $\ell \geq 1$.

- Taking $(\mathfrak{g}, m) = (0, 33)$, we get a $(3m, 10m - 5; 2)$-RMFE over $\mathbb{Z}_{2^\ell}$ for any $m \leq 33$. For instance, we have a $(99, 325; 2)$-RMFE over $\mathbb{Z}_{2^\ell}$ for all $\ell \geq 1$.
- Taking $(\mathfrak{g}, m) = (1, 44)$, we get a $(3m, 10m + 15; 2)$-RMFE over $\mathbb{Z}_{2^\ell}$ for any $m \leq 44$. For instance, we have a $(132, 455; 2)$-RMFE over $\mathbb{Z}_{2^\ell}$ for all $\ell \geq 1$.
- Taking $(\mathfrak{g}, m) = (2, 53)$, we get a $(3m, 10m + 35; 2)$-RMFE over $\mathbb{Z}_{2^\ell}$ for any $m \leq 53$. For instance, we have a $(159, 565; 2)$-RMFE over $\mathbb{Z}_{2^\ell}$ for all $\ell \geq 1$.
- Taking $(\mathfrak{g}, m) = (3, 64)$, we get a $(3m, 10m + 55; 2)$-RMFE over $\mathbb{Z}_{2^\ell}$ for any $m \leq 64$. For instance, we have a $(192, 695; 2)$-RMFE over $\mathbb{Z}_{2^\ell}$ for all $\ell \geq 1$.

Asymptotic Construction of Degree-2 RMFEs. Now we consider the task of constructing degree-2 RMFEs of unbounded dimension. We begin by considering two function field towers. The first tower was introduced in [22]. Let $q = r^2$, where r is a prime power. For $t \geq 1$, let $F_t = \mathbb{F}_q(x_1, x_2, \ldots, x_t)$ with

$$x_{i+1}^r + x_{i+1} = \frac{x_i^r}{x_i^{r-1} + 1} \tag{1}$$

for $i = 1, 2, \ldots, t-1$. Then the genus $\mathfrak{g}(F_t)$ of F_t is at most r^t and the number $N(F_t)$ of rational places is at least $1 + r^t(r-1)$.

We proceed to the second tower. Let $q = p^{2m+1}$, where p is a prime and $m \geq 1$ is an integer. For $t \geq 1$, let $F_t = \mathbb{F}_q(x_1, x_2, \ldots, x_t)$ with

$$\mathrm{Tr}_m\left(\frac{x_{i+1}}{x_i^{q^{m+1}}}\right) + \mathrm{Tr}_{m+1}\left(\frac{x_{i+1}^{q^m}}{x_i}\right) = 1 \tag{2}$$

for $i = 1, 2, \ldots, t-1$, where $\mathrm{Tr}_a(T) = T + T^q + \cdots + T^{q^{a-1}}$. Then $\lim_{t\to\infty} \mathfrak{g}(F_t) = \infty$. Furthermore, for all $t \geq 1$, we have $\frac{N(F_t)}{\mathfrak{g}(F_t)-1} \geq \frac{2(p^{m+1}-1)}{p+1+\epsilon}$ with $\epsilon = \frac{p-1}{p^m-1}$, where $\mathfrak{g}(F_t)$ and $N(F_t)$ stands for the genus and the number rational places of F_t, respectively. Coupling these observations with our previous results, we obtain Corollary 2, which shows the existence of degree-D RMFEs over Galois rings for any dimension and any characteristic q. Then, in Corollary 3 we apply this to the relevant case of Galois rings over $\mathbb{Z}_{2^k}$.

Corollary 2. *Let $F/\mathbb{F}_q$ be a function field of genus $\mathfrak{g}$ with n distinct rational places and a place of degree $k \geq 2n + 4\mathfrak{g} - 1$. Then there exists an $(n, k; 2)$-RMFE over $\mathbb{F}_q$. In particular,*

(i) *if q is a square, there is a constructive family of $(n, k; 2)$-RMFE over $\mathbb{F}_q$ with $n \to \infty$ and $\frac{k}{n} \to 2 + \frac{4}{\sqrt{q}-1}$;*

(ii) *if $q = p^{2m+1}$ for a prime p, there is a constructive family of $(n, k; 2)$-RMFE over $\mathbb{F}_q$ with $n \to \infty$ and $\frac{k}{n} \to 2 + \frac{2(p+1+\epsilon)}{p^{m+1}-1}$, where $\epsilon = \frac{p-1}{p^m-1}$.*

Proof. One can take a divisor of degree $n + 2\mathfrak{g} - 1$. Then by the Riemann-Roch Theorem, we have $\dim_{\mathbb{F}_q} \mathcal{L}(G) - \dim_{\mathbb{F}_q} \mathcal{L}(G - \sum_{i=1}^n) = \deg(G) - \mathfrak{g} + 1 - (\deg(G) - \mathfrak{g} + 1 - n) = n$. Take $k = 1 + 2\deg(G) = 1 + 2(n + 2\mathfrak{g} - 1) = 2n + 4\mathfrak{g} - 1$. Then $k > 2\deg(G)$. Thus, by Lemma 5, we have an $(n, k; 2)$-RMFE over $\mathbb{F}_q$.

(i) Applying to the first tower with n being the number $N(F_t)$, we have $\frac{k}{n} = \frac{2n+4\mathfrak{g}-1}{n} = 2 + \frac{4\mathfrak{g}}{n} - \frac{1}{n} \to 2 + \frac{4}{\sqrt{q}-1}$.

(ii) Applying to the second tower with n being the number $N(F_t)$, we have $\frac{k}{n} = \frac{2n+4\mathfrak{g}-1}{n} = 2 + \frac{4\mathfrak{g}}{n} - \frac{1}{n} =\to 2 + \frac{2(p+1+\epsilon)}{p^{m+1}-1}$. □

Corollary 3. *There exists a constructive family of $(n, k; 2)$-RMFE over $\mathbb{Z}_{2^\ell}$ for all $\ell \geq 1$ with $n \to \infty$ and $\frac{k}{n} \to 4.92$.*

Proof. Consider the rational function field over $\mathbb{F}_2$. Choose a divisor G of degree 2 and a place of degree 5, we obtain a $(3,5;2)$-RMFE over $\mathbb{F}_2$. Hence, by Lemma 6, there is a $(3,5;2)$-RMFE over $\mathbb{Z}_{2^\ell}$ for all $\ell \geq 1$.

By Corollary 2(ii), there is a constructive family of $(N,K;2)$-RMFE over $\mathbb{F}_{32}$ with $\frac{K}{N} \to 2 + \frac{20}{21} = \frac{62}{21}$. Thus, we obtain $(N,K;2)$-RMFE over $\mathsf{GR}(2^\ell,5)$ with $\frac{K}{N} \to 2 + \frac{20}{21} = \frac{62}{21}$.

By Lemma 4, we obtain a constructive family of $(n = 3N, k = 5K; 2)$-RMFE over $\mathbb{Z}_{2^\ell}$ with $n \to \infty$ and $\frac{k}{n} \to \frac{62}{21} \times \frac{5}{3} \approx 4.92$. □

4.3 Construction of Degree-D RMFEs

Finally, in this section we provide some explicit constructions of degree-D RMFEs for $D \geq 2$. As before, we begin by considering RMFEs of bounded dimension, which are obtained from function fields with small genus. Then, we provide degree-D RMFEs with unbounded dimension, which are obtained by making use of certain function field towers. We remark that these constructions are entirely new, considering that the notion of degree-D RMFEs is introduced in our work.

Example 3 (concrete degree-D RMFEs of bounded dimension). Consider the rational function field over $\mathbb{F}_2$. Choose a divisor G of degree 2 and a place of degree $1+2t$ for all $t \geq 2$, we obtain a $(3, 1+2t; t)$-RMFE over $\mathbb{F}_2$ by Lemma 5. Hence, by Lemma 6, there is a $(3, 1+2t; t)$-RMFE over $\mathbb{Z}_{2^\ell}$ for all $\ell \geq 1$.

Consider a function field over $\mathbb{F}_{2^{2t+1}}$ with n rational places and genus $\mathfrak{g}$. Then for any $m \leq n$, we choose m distinct points and a divisor of degree $m + 2\mathfrak{g} - 1$. Let $k = t(m + 2\mathfrak{g} - 1) + 1 = tm + 2t\mathfrak{g} - t + 1$. Then we have an $(m, k = tm + 2t\mathfrak{g} - t + 1; t)$-RMFE over $\mathbb{F}_{2^{2t+1}}$. Hence, by Lemma 4, we obtain a $(3m, (1+2t)(tm + 2t\mathfrak{g} - t + 1); t)$-RMFE over $\mathbb{F}_2$ by composing the $(3, 1+2t; t)$-RMFE above and $(m, tm + 2t\mathfrak{g} - t + 1; t)$-RMFE. Hence, by Lemma 6, there is a $(3m, (1+2t)(tm + 2t\mathfrak{g} - t + 1); t)$-RMFE over $\mathbb{Z}_{2^\ell}$ for all $\ell \geq 1$.

- Taking $(\mathfrak{g}, m) = (0, 1 + 2^{2t+1})$, we get a $(3m, (1+2t)(tm - t + 1); t)$-RMFE over $\mathbb{Z}_{2^\ell}$ for any $m \leq 1 + 2^{2t+1}$. For instance, we have a $(3(1+2^{2t+1}), (1+2t)(t(1+2^{2t+1}) - t + 1); t)$-RMFE over $\mathbb{Z}_{2^\ell}$ for all $\ell \geq 1$.
- Taking $(t, \mathfrak{g}, m) = (3, 1, 150)$, we get a $(3m, 7(3m+4); 3)$-RMFE over $\mathbb{Z}_{2^\ell}$ for any $m \leq 150$. For instance, we have a $(450, 3178; 3)$-RMFE over $\mathbb{Z}_{2^\ell}$ for all $\ell \geq 1$.
- Taking $(t, \mathfrak{g}, m) = (3, 2, 172)$, we get a $(3m, 7(3m+10); 3)$-RMFE over $\mathbb{Z}_{2^\ell}$ for any $m \leq 172$. For instance, we have a $(516, 3682; 3)$-RMFE over $\mathbb{Z}_{2^\ell}$ for all $\ell \geq 1$.

Asymptotic Construction of Degree-D RMFEs. We now proceed to the asymptotic construction of degree-D RMFEs of unbounded dimension. The construction makes use of the same function field tower we use in the asymptotic construction of degree-2 RMFE. Our results are presented in the following two corollaries. As with the degree-2 case, Corollary 4 shows the existence of degree-D RMFEs over Galois rings for any dimension and any characteristic q, while Corollary 5 is a particular case for the relevant setting of Galois rings over $\mathbb{Z}_{2^k}$.

Corollary 4. *Let $F/\mathbb{F}_q$ be a function field of genus $\mathfrak{g}$ with n distinct rational places and a place of degree k. Then there exists an $(n, k; D)$-RMFE over $\mathbb{F}_q$ as follows.*

(i) *if q is a square, there is a constructive family of $(n, k; D)$-RMFE over $\mathbb{F}_q$ with $n \to \infty$ and $\frac{k}{n} \to D + \frac{2D}{\sqrt{q}-1}$;*
(ii) *if $q = p^{2m+1}$ for a prime p, there is a constructive family of $(n, k; D)$-RMFE over $\mathbb{F}_q$ with $n \to \infty$ and $\frac{k}{n} \to D + \frac{D(p+1+\epsilon)}{p^{m+1}-1}$, where $\epsilon = \frac{p-1}{p^m-1}$.*

Proof. One can take a divisor of degree $n + 2\mathfrak{g} - 1$. Then by the Riemann-Roch Theorem, we have $\dim_{\mathbb{F}_q} \mathcal{L}(G) - \dim_{\mathbb{F}_q} \mathcal{L}(G - \sum_{i=1}^{n}) = \deg(G) - \mathfrak{g} + 1 - (\deg(G) - \mathfrak{g} + 1 - n) = n$. Take $k = 1 + D\deg(G) = 1 + D(n + 2\mathfrak{g} - 1)$. Then $k > D\deg(G)$. Thus, by Lemma 5, we have an $(n, k; D)$-RMFE over $\mathbb{F}_q$.

(i) Applying to the first tower in (1) with n being the number $N(F_D)$, we have $\frac{k}{n} = \frac{tn+2D\mathfrak{g}-D}{n} = D + \frac{2D\mathfrak{g}}{n} - \frac{D}{n} \to D + \frac{2D}{\sqrt{q}-1}$.

(ii) Applying to the second tower in (2) with n being the number $N(F_D)$, we have $\frac{k}{n} = \frac{Dn+2D\mathfrak{g}-D}{n} = D + \frac{2D\mathfrak{g}}{n} - \frac{D}{n} \to D + \frac{D(p+1+\epsilon)}{p^{m+1}-1}$. □

Corollary 5. *There exists a constructive family of $(n, k; D)$-RMFE over $\mathbb{Z}_{2^\ell}$ for all $\ell \geq 1$ with $n \to \infty$ and $\frac{k}{n} \to \frac{1+2D}{3} \times \left(D + \frac{D(3+1/(2^D-1))}{2^{D+1}-1}\right)$.*

Proof. Consider the rational function field over $\mathbb{F}_2$. Choose a divisor G of degree 2 and a place of degree $1 + 2D$, we obtain a $(3, 1 + 2D; D)$-RMFE over $\mathbb{F}_2$. Hence, by Lemma 6, there is a $(3, 1 + 2D; D)$-RMFE over $\mathbb{Z}_{2^\ell}$ for all $\ell \geq 1$.

By Corollary 4(ii), there is a constructive family of $(N, K; D)$-RMFE over $\mathbb{F}_{2^{1+2D}}$ with $\frac{K}{N} \to D + \frac{D(3+1/(2^D-1))}{2^{D+1}-1}$. Thus, we obtain $(N, K; D)$-RMFE over $R_\ell(2, 1 + 2D)$ with $\frac{K}{N} \to D + \frac{D(3+1/(2^D-1))}{2^{D+1}-1}$.

By Lemma 4, we obtain a constructive family of $(n = 3N, k = (1 + 2D)K)$-RMFE over $\mathbb{Z}_{2^\ell}$ with $n \to \infty$ and $\frac{k}{n} \to \left(D + \frac{D(3+1/(2^D-1))}{2^{D+1}-1}\right) \times \frac{1+2D}{3}$. □

Remark 1. The degree-D RMFE over $\mathbb{Z}_{2^\ell}$ presented in Corollary 5 achieves the ratio $\frac{k}{n} \approx \frac{D(1+2D)}{3}$. By Theorem 1, this also means there exists degree-D packing method of density roughly $\frac{3}{D(1+2D)}$ over $\mathbb{Z}_{2^\ell}$.

5 Applications of Degree-D RMFEs

Having established the relations between our novel degree-D RMFEs and the degree-D packing methods from [12] in Section 3, and after showing explicit constructions of degree-D RMFEs in Section 4, we now proceed to discuss settings in which degree-D RMFEs can prove useful. At a high level, degree-D RMFEs find applications in settings where (1) the goal is to operate over a Galois ring $\mathsf{GR}(p^k, d)$ of small degree d, but the underlying machinery requires a Galois ring extension $\mathsf{GR}(p^k, m)$ of a large degree m; and (2) degree-D computation is needed.

Examples of scenarios that meet these conditions include somewhat homomorphic encryption (SHE), secure multiparty computation (MPC), and even zero knowledge proofs (ZKPs). However, finding *direct* applications of our novel degree-D RMFEs for $D > 2$ to these settings is not trivial since, as we discuss in the full version[19], degree-2 computation seems to be enough for many use-cases. Fortunately, there are certain "less direct" scenarios that benefit from computation of higher degree, and after our initial discussion below we will focus this section on one of these applications, which have to do with generating correlated randomness *non-interactively* for use in secure multiparty computation protocols.

We refer to the full version[19] for a detailed discussion of *potential* applications to SHE and MPC, but here we focus on the following.

Our main application: non-interactive correlation generation. Here, we consider an application to MPC where high degree computation is required, but interaction is less desired. Instead of aiming at directly improving the efficiency of MPC protocols, we consider the different but closely related problem of generating preprocessing material used for secure computation. To provide context, we observe that it is a common practice to divide the execution of an MPC protocol into two phases: an *offline phase* (also known as *preprocessing phase*) that is independent of the inputs and hence can be executed by the parties before the inputs are known, and an *online phase*, which depends on the inputs and tends to be much lighter and more efficient than the offline phase, on top of using in some cases less computational assumptions and simpler tools. The motivation behind such separation is to push most of the complexities and inefficiencies to the offline phase which, being independent of the inputs, can be in principle executed by the parties before the inputs are known (say, overnight before a computation that will happen next day). This way, the latency from input provision to output computation, which is dictated by the efficiency of the online phase, can be minimized.

The role of the offline phase is to establish certain *correlated randomness* among the parties (which is, again, independent of the inputs for the computation), which is then "consumed" in the online phase by the parties in order to securely compute the given function. An alternative to letting the parties run the offline phase to generate this correlated randomness themselves, which could be expensive or prohibitive in some settings where no "overnight" computation is available, is to let the parties receive this correlated randomness from some external source. For example, a trusted dealer could be in charge of distributing such randomness [25], using trusted hardware [17], or using PCGs [6].

Another approach to generating the required correlated randomness consists of replacing the trusted dealer with a different set of parties who run an MPC protocol among themselves to generate the required correlations. This way, there is no single point of failure such as a trusted dealer. This approach can be regarded as some form of "correlations-as-a-service", which is a model that has been considered before in the literature [31,24]. In our application, we require

minimal interaction among the set of parties in charge of generating the correlated randomness for other committees.

5.1 Degree-D Correlations

We denote by $\mathcal{P} = \{P_1, \ldots, P_n\}$ the parties in the *preprocessing committee*, *i.e.* the parties that will generate the required correlations, and we denote by $\mathcal{Q} = \{Q_1, \ldots, Q_N\}$ the parties in the *online committee*, *i.e.* the parties who will "consume" these correlations to securely compute the desired functionality on their private inputs. We consider an adversary that *passively* corrupts t out of the n parties in $\mathcal{P}$. For simplicity we consider correlations over $\mathbb{Z}_{p^k}$, although this can be easily generalized to Galois rings of arbitrary degree. In its more general form, a correlation is a distribution over vectors of the form $(\boldsymbol{y}^{(1)}, \ldots, \boldsymbol{y}^{(N)}) \in (\mathbb{Z}_{p^k})^N$, where, in the MPC context, each party Q_i is intended to receive $\boldsymbol{y}^{(i)}$. However, in this work we focus on a particular case of high relevance, which is the case in which the parties obtain *sharings* of m values $(y_1, \ldots, y_m) \in \mathbb{Z}_{p^k}$ following certain distribution computable from degree-D polynomials. The sharings are done using some target linear secret-sharing scheme over $\mathbb{Z}_{p^k}$, which we denote by $\langle \cdot \rangle$. That is, the correlation consists of the parties in $\mathcal{Q}$ receiving sharings $(\langle y_1 \rangle, \ldots, \langle y_m \rangle)$.

Definition 4 (Degree-D correlations). *Consider a degree-D function $F : (\mathbb{Z}_{p^k})^\ell \to (\mathbb{Z}_{p^k})^m$, meaning that, if $(y_1, \ldots, y_m) = F(x_1, \ldots, x_\ell)$, then each y_i is the evaluation of a multivariate polynomial $F_i(x_1, \ldots, x_\ell)$ of degree at most D. A* degree-D correlation *is a list of sharings of the form $(\langle y_1 \rangle, \ldots, \langle y_m \rangle)$, where $(y_1, \ldots, y_m) = F(\boldsymbol{x})$ for some uniformly random $\boldsymbol{x} \in \mathbb{Z}_{p^k}^\ell$.*

We present several examples of useful degree-D correlations in the full version[19], which include multiplication triples, authenticated triples, and generalizations.

Overview of our correlation generation techniques. From now onwards, let $F : (\mathbb{Z}_{p^k})^\ell \to (\mathbb{Z}_{p^k})^m$ be a degree-D function given by $\boldsymbol{y} = F(\boldsymbol{x})$, with $y_i = F_i(\boldsymbol{x})$ for $i \in \{1, \ldots, m\}$. At a high level, our approach for the parties in $\mathcal{P}$ to generate the degree-D correlations derived from F towards committee $\mathcal{Q}$ consist of the following steps.

1. Parties in $\mathcal{P}$ generate Shamir sharings $(\llbracket x_1 \rrbracket, \ldots, \llbracket x_\ell \rrbracket)$, where each $x_i \in \mathbb{Z}_{p^k}$ is uniformly random.
2. Parties in $\mathcal{P}$ securely compute $(\llbracket y_1 \rrbracket, \ldots, \llbracket y_m \rrbracket)$, where $y_i = F_i(\boldsymbol{x})$ for $i \in \{1, \ldots, m\}$.
3. Parties in $\mathcal{P}$ reshare $(\llbracket y_1 \rrbracket, \ldots, \llbracket y_m \rrbracket)$ towards $\mathcal{Q}$, which enable the latter committee to obtain $(\langle y_1 \rangle, \ldots, \langle y_m \rangle)$.

Recall that our main goal is to achieve the above while maintaining *no interaction* among the parties in $\mathcal{P}$. The rest of this section is devoted to describing these ideas in detail, and overcoming the following challenges:

- The parties in $\mathcal{P}$ must generate $(\llbracket x_1 \rrbracket, \ldots, \llbracket x_\ell \rrbracket)$ non-interactively. This is done with the help of pseudo-random secret-sharing (PRSS), as described in Section 5.2. We build on top of the techniques from [3], adapting to the case of Galois rings, and considering certain extensions we will need for our concrete use-case.
- The parties in $\mathcal{P}$ must compute $(\llbracket y_1 \rrbracket, \ldots, \llbracket y_m \rrbracket)$ non-interactively. This is achieved by requiring the initial threshold in Shamir secret-sharing to be low enough, so that D sequential multiplications can be carried out locally without losing the ability to reconstruct the underlying secrets.
- In our case where the ring is $\mathbb{Z}_{p^k}$, Shamir secret-sharing does not work directly, and instead a Galois ring extension $\mathsf{GR}(p^k, \delta)$ of large enough degree $\delta = \Theta(\log(n))$ must be used. This is exactly where our degree-D RMFEs come into the picture: we make use of our RMFEs to remove asymptotically the overhead caused by this extension, achieving zero overhead and enabling efficient correlation generation. The use of RMFEs and the use of Galois rings introduce some changes with respect to the PRSS from [3]. This is discussed below.

5.2 Pseudo-Random Secret-Sharing

Let $R = \mathsf{GR}(p^k, \delta)$. Committee $\mathcal{P}$ generates the Shamir sharings $(\llbracket x_1 \rrbracket, \ldots, \llbracket x_\ell \rrbracket)$ where $x_i \in_R R$ for $i \in \{1, \ldots, \ell\}$ using pseudo-random secret sharing, or PRSS for short, which is a technique that enables the parties in $\mathcal{P}$ to generate Shamir shares of random values without interaction, assuming only a setup phase where the parties receive certain "seeds" that are used to feed pseudo-random functions that will determine the corresponding shares. Recall that t is the number of corrupted parties in $\mathcal{P}$, and D is the degree of the correlation. We assume that $t \cdot D < n$, and we let $d = \left\lfloor \frac{n-1}{D} \right\rfloor \geq t$, which is the largest integer such that $d \cdot D < n$. The Shamir sharings that we generate will have degree d, which is in principle larger than the corruption threshold t.

We use $\llbracket \boldsymbol{x} \rrbracket_d = (z_1, \ldots, z_n)$ to denote packed secret-sharing of a vector $\boldsymbol{x} \in R^\kappa$, meaning that there exists a polynomial $f(\mathtt{X})$ over R of degree at most d such that $z_i = f(\alpha_i)$ for $i \in \{1, \ldots, n\}$ and $x_j = f(\beta_j)$ for $j \in \{1, \ldots, \kappa\}$, where $\{\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_\kappa\}$ is an exceptional set over R. It is well known that the secret $\boldsymbol{x}$ is determined by any $d+1$ shares, but given any t of these shares, the secret vector $\boldsymbol{x}$ is kept private. For our construction we will actually need $\{\beta_0\} \cup \{\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_\kappa\}$ to be an exceptional set, which requires $1+n+\kappa \leq p^\delta$.

Recall that $R = \mathsf{GR}(p^k, \delta)$. From now on we fix a degree-D RMFE $(\phi : \mathbb{Z}_{p^k}^r \to R, \psi : R \to \mathbb{Z}_{p^k}^r)$. In our work, we make use of PRSS to non-interactively generate sharings of the form $\llbracket \boldsymbol{x} \rrbracket_d$, where $\boldsymbol{x} = (x_1, \ldots, x_\kappa)$ with $x_i \in \mathsf{Im}(\phi)$ for $i \in \{1, \ldots, \kappa\}$. Inspired by the approach in [3], we construct a PRSS solution suited for our algebraic structure R, which is in general not a field, and also ensuring the underlying secrets are uniformly random in the $\mathbb{Z}_{p^k}$-submodule $(\mathsf{Im}(\phi))^\kappa$, rather than just being uniformly random in R^κ.

Covering designs. The main insight in [3] is that any PRSS solution is closely tied to the notion of a covering design, and that the latter become more efficient as the gap between the adversarial threshold t and the desired degree d increases. We begin by reusing the definition of a covering design from [3].

Definition 5 (Covering design, Definition 3.2 in [3]). *Fix integers $0 < t \leq m \leq n$, and let $\mathcal{C} = (S_1, \ldots, S_\ell)$ be a collection of ℓ different subsets $S_j \subseteq \{1, \ldots, n\}$, all of size $|S_j| = m$. $\mathcal{C}$ is said to be an (n, m, t)-*cover *if for every size-t subset $T \subseteq \{1, \ldots, n\}$, $|T| = t$, there is a set $S_j \in \mathcal{C}$ that covers it,* i.e. *$T \subseteq S_j$.*

The goal of pseudo-random secret-sharing (PRSS) as we use it in our work is to enable n parties $\mathcal{P} = \{P_1, \ldots, P_n\}$ to generate a large amount of sharings $[\![\boldsymbol{r}]\!]_d$, where $\boldsymbol{r}$ is uniformly random in the $\mathbb{Z}_{p^k}$-module $(\mathsf{Im}(\phi))^\kappa$. This was first considered in [14] for the case $d = t$ (*i.e.* the degree d equals the desired threshold t, and $\kappa = 1$ so only one secret can be stored), and the secret lies in R with $k = 1$ (*i.e.* the algebraic structure is a finite field and the secret is uniform in the field itself, not in a subset of it). These traditional solutions require the parties to hold an exponential amount of different seeds, or more precisely, each party must hold $\binom{n}{t}$ seeds, which is exponential in n for parameter ranges of interest. In the recent work of [3], a generalization of the techniques in [14] was presented, where the authors considered the case in which $t < d$, or in other words, the case where there is a gap between the threshold and the degree, which enables for packing more than one secret using packed secret-sharing. In [3], the authors show that such gap can be used to drastically reduce the amount of seeds required to achieve PRSS. We draw inspiration from their construction to design our PRSS solution.

PRSS construction. Now we are ready to describe our PRSS solution. Recall that the goal is to let the parties obtain a large amount of sharings $[\![\boldsymbol{x}]\!]_d$ where each x_i is uniformly random in $\mathsf{Im}(\phi)$. Also, recall that the packing parameter is $1 \leq \kappa \leq (d - t) + 1$. Let $\mathcal{C}' = \{S'_1, \ldots, S'_{\ell'}\}$ be a $(n, d - \kappa + 1, t)$-cover. Consider the collection $\overline{\mathcal{C}} = \{S' \setminus \{j\} : S' \in \mathcal{C}', j \in S'\} = \{\overline{S}_1, \ldots, \overline{S}_\ell\}$, which contains $\ell \leq \ell'(d - \kappa + 1)$ different subsets, each of size $d - \kappa$. Let us denote $S_i = \{1, \ldots, n\} \setminus \overline{S}_i$, for each $i \in \{1, \ldots, \ell\}$. Notice that $|S_i| = n - (d - \kappa)$.

PRSS Construction

Setup: The parties start with the following setup.

1. For each S_i as defined above, sample a uniformly random key $k_i \in \{0,1\}^\kappa$ for a PRF, which we denote by $\mathsf{PRF}_{k_i}(\cdot)$.
2. Each party P_j for $j \in \{1, \ldots, n\}$ receives the seeds k_i for every $i \in \{1, \ldots, \ell\}$ such that $P_j \in S_i$.

Share generation: In order to *non-interactively* generate shares $[\![\boldsymbol{r}]\!]_d$ where $\boldsymbol{r}$ is uniformly random in the $\mathbb{Z}_{p^k}$-module $(\mathsf{Im}(\phi))^\kappa \subseteq R^\kappa$, the parties proceed as follows.

1. For each $\overline{S}_i = \{1, \ldots, n\} \setminus S_i$, consider the polynomial $P_{\overline{S}_i}(\mathtt{X})$ obtained by interpolating the following conditions: $P_{\overline{S}_i}(X)$ equals 0 if $X = \alpha_h$ with $h \in \overline{S}_i$, it equals r_{ij} if $X = \beta_j \in \{\beta_1, \ldots, \beta_\kappa\}$, and it equals s_i if $X = \beta_0$, where $(r_{i1}, \ldots, r_{i\kappa} \| s_i) = \mathsf{PRF}_{k_i}(\mathtt{id}, j) \in (\mathsf{Im}(\phi))^\kappa \oplus R$, where $\mathtt{id}$ is some common identifier corresponding to the current PRSS run (*e.g.* a counter). Note that:
   - This polynomial has degree at most d since there are $(d - \kappa) + \kappa + 1 = d + 1$ conditions above given that $|\overline{S}_i| = d - \kappa$.
   - Each party $P_j \in S_i$ can compute the polynomial $P_{\overline{S}_i}(\mathtt{X})$ (and in particular $P_{\overline{S}_i}(\alpha_j)$).
   - Each party $P_j \notin S_i$ can trivially compute $P_{\overline{S}_i}(\alpha_j)$, since this value is equal to zero.
2. Define the polynomial $Q(\mathtt{X}) := \sum_{i=1}^{\ell} P_{\overline{S}_i}(\mathtt{X})$, which has degree at most d. From the observations above, each party P_j can compute $Q(\alpha_j)$.
3. The parties output the shares $[\![\boldsymbol{r}]\!]_d = (Q(\alpha_1), \ldots, Q(\alpha_n))$, where $\boldsymbol{r} = (Q(\beta_1), \ldots, Q(\beta_\kappa))$.

Theorem 3. *Fix integers $0 < t \leq d \leq n$ and $1 \leq \kappa \leq (d - t) + 1$. Given a size-$\ell'$ $(n, d - \kappa + 1, t)$-cover, the construction above is a PRSS solution for t-secure distribution of sharings $[\![\boldsymbol{r}]\!]_d$ where $\boldsymbol{r} \in_R (\mathsf{Im}(\phi))^\kappa$, with the following complexity measures:*

- *The total number of different PRSS seeds is $\ell \leq \ell'(d - \kappa + 1)$, and*
- *Each key is received by $|S_i| = n - (d - \kappa)$ parties.*
- *In average, each party in $\mathcal{P}$ stores $\frac{\sum_{i=1}^{\ell} |S_i|}{n} \leq \frac{\ell'(d-\kappa+1)(n-(d-\kappa))}{n}$.*

Proof. The claimed complexities can be verified by inspection. For the purpose of the proof we assume that the values $(r_{i1}, \ldots, r_{i\kappa} \| s_i)$ are *uniformly random* (instead of pseudo-random) in $(\mathsf{Im}(\phi))^\kappa \oplus R$. The general case is achieved by a standard reduction to the security of the PRF.

Let $T \subseteq \{1, \ldots, n\}$ be any set with $|T| = t$. Such set determines t shares $Q(\alpha_j)$ for $j \in T$. To see that the PRSS construction is secure we need to show that, even with the knowledge of the seeds of parties P_i for $i \in T$, the output polynomial $Q(\mathtt{X})$ is uniformly random subject to its shares for indices $j \in T$ being equal to $Q(\alpha_j)$, and its secrets being uniformly random in $\mathsf{Im}(\phi)$. Clearly, $Q(\mathtt{X})$ has degree $\leq d$. From this, it suffices to show that, even with knowledge of $(r_{i1}, \ldots, r_{i\kappa} \| s_i)$ for i such that $S_i \cap T \neq \emptyset$ (*i.e.* knowledge of k_i), $Q(\mathtt{X})$ satisfies the following:

1. $Q(\alpha_j) = \sum_{S_i \cap T \neq \emptyset} P_{\overline{S}_i}(\alpha_j)$ for $j \in T$ (these are the shares corresponding to the indices in T, which are computable from $(r_{i1}, \ldots, r_{i\kappa} \| s_i)$ for S_i with $S_i \cap T \neq \emptyset$).
2. $(Q(\beta_1), \ldots, Q(\beta_\kappa)) \in_R (\mathsf{Im}(\phi))^\kappa$.
3. $Q(\mathtt{X})$ evaluated at *any other* $\lambda := d + 1 - \kappa - t \geq 0$ points is uniformly random in R^λ.

Now, observe that, since $\mathcal{C}' = \{S'_1, \ldots, S'_{\ell'}\}$ is a $(n, d-\kappa+1, t)$-cover, we have that there exists $S' \in \mathcal{C}'$ such that $T \subseteq S'$. Notice that $|S' \setminus T| = (d-\kappa+1)-t = \lambda$. Let us write $S' \setminus T = \{\mu_1, \ldots, \mu_\lambda\}$. By definition of $\overline{\mathcal{C}}$, for each $j \in \{1, \ldots, \lambda\}$ there exists $i_j \in \{1, \ldots, \ell\}$ such that $\overline{S}_{i_j} = S' \setminus \{\mu_j\}$. Notice that $T \subseteq \bigcap_{j=1}^{\lambda} \overline{S}_{i_j}$.

Let us write $Q(\mathtt{X}) = Q'(\mathtt{X}) + Q''(\mathtt{X})$, where $Q'(\mathtt{X}) = \sum_{i \in \{i_1, \ldots, i_\lambda\}} P_{\overline{S}_i}(\mathtt{X})$ and $Q''(\mathtt{X}) = \sum_{i \in \{1, \ldots, \ell\} \setminus \{i_1, \ldots, i_\lambda\}} P_{\overline{S}_i}(\mathtt{X})$. Property (1) above follows directly from the definition of $Q(\mathtt{X})$. Notice that the polynomials Q' and Q'' follow independent distributions, so to prove properties (2) and (3) it suffices to show they hold for the polynomial $Q'(\mathtt{X})$. Also, importantly, notice that for every $j \in \{1, \ldots, \lambda\}$, it holds that $S_{i_j} \cap T = \emptyset$ and therefore $(r_{i_j 1}, \ldots, r_{i_j \kappa} \| s_{i_j})$ are uniformly random in $(\mathsf{Im}(\phi))^\kappa \oplus R$. Due to this, $(P_{\overline{S}_{i_j}}(\beta_1), \ldots, P_{\overline{S}_{i_j}}(\beta_\kappa)) = (r_{i_j 1}, \ldots, r_{i_j \kappa}) \in_R (\mathsf{Im}(\phi))^\kappa$, which proves property (2).

For property (3), we claim that $(Q'(\mu_1), \ldots, Q'(\mu_\lambda))$ is uniformly random in R^λ. It is useful to observe that we can write each $P_{\overline{S}_{i_j}}(\mathtt{X})$ as $P_{\overline{S}_{i_j}}(\mathtt{X}) = s_{i_j} \cdot H_{i_j}(\mathtt{X}) + \sum_{a=1}^{\kappa} r_{i_j a} \cdot G_{\overline{S}_{i_j}, a}(\mathtt{X})$. where all $G_{\overline{S}_{i_j}, a}(\alpha_h) = H_{i_j}(\alpha_h) = 0$ for $h \in \overline{S}_i$, but also $H_{i_j}(\beta_h) = 0$ for $h \in \{1, \ldots, \kappa\}$, and equals 1 if $h = 0$; and finally $G_{\overline{S}_{i_j}, \ell}(\beta_h) = 0$ for $h \in \{0, 1, \ldots, \kappa\} \setminus \{j\}$, and $G_{\overline{S}_{i_j}, a}(\beta_j) = 1$. Notice that $\deg(G_{\overline{S}_{i_j}, a}), \deg(H_{i_j}) \leq d+1$ as we only interpolate $G_{\overline{S}_{i_j}, a}(\mathtt{X})$ and $H_{i_j}(\mathtt{X})$ at $d - \kappa + 1 + \kappa + 1 = d + 2$ points.

In addition to the above, we observe that for every $j, j' \in \{1, \ldots, \lambda\}$ it holds that $\mu_{j'} \in \overline{S}_{i_j}$ if $j \neq j'$ and, otherwise $\mu_{j'} \in S_{i_j}$. Therefore, $P_{\overline{S}_{i_j}}(\alpha_{\mu_{j'}}) = 0$ if $j \neq j'$. Otherwise, if $j = j'$, we have that $P_{\overline{S}_{i_j}}(\alpha_{\mu_j}) = s_{i_j} \cdot H_{i_j}(\alpha_{\mu_j}) + z_j$, where $z_j = \sum_{h=1}^{\kappa} r_{i_j h} \cdot G_{\overline{S}_{i_j}, h}(\alpha_{\mu_j})$.

Importantly, since z_j is independent of s_{i_j}, and s_{i_j} is uniformly random, for Property (3) it suffices to show that $H_{i_j}(\alpha_{\mu_j})$ is invertible in R. By the definition of $H_{i_j}(\mathtt{X})$, we have $H_{i_j}(\mathtt{X}) = c_{i_j} \cdot \prod_{h \in \overline{S}_{i_j}} (x - \alpha_h) \cdot \prod_{h=1}^{\kappa} (x - \beta_h)$ with $H_{i_j}(\beta_0) = c_{i_j} \cdot \prod_{h \in \overline{S}_{i_j}} (\beta_0 - \alpha_h) \cdot \prod_{h=1}^{\kappa} (\beta_0 - \beta_h) = 1$. This implies that c_{i_j} is invertible in R. Combining with the fact that $\{\alpha_1, \ldots, \alpha_n, \beta_0, \beta_1, \ldots, \beta_\kappa\}$ is an exceptional set over R and $\mu_j \notin \overline{S}_{i_j}$ implies that

$$H_{i_j}(\alpha_{\mu_j}) = c_{i_j} \prod_{h \in \overline{S}_{i_j}} (\alpha_{\mu_j} - \alpha_h) \prod_{h=1}^{\kappa} (\alpha_{\mu_j} - \beta_h)$$

is invertible in R. This leads to the claim that $P_{\overline{S}_{i_j}}(\alpha_{\mu_j})$ distributes uniformly at random over R.

Putting the pieces together, we see then that $(Q(\alpha_{\mu_1}), \ldots, Q(\alpha_{\mu_\lambda}))$ is equal to $(s_{i_j} \cdot H_{i_j}(\alpha_{\mu_j}) + z_j)_{j=1}^{\lambda}$, which is in a 1-1 correspondence with $(s_{i_1}, \ldots, s_{i_\lambda})$, which is uniformly random in R^λ. This concludes the proof. □

On the amount of seeds. An important metric for the efficiency of a PRSS solution is the amount of seeds that every party should hold. In our case, this

corresponds to $(\ell'(d-\kappa+1)(n-d+\kappa))/n$, where ℓ' is the size of the smallest $(n, d-\kappa+1, t)$-cover. As noted in [3], there is not a closed expression for ℓ', but concrete lower and upper bounds are known in several cases. First, recall that $1 \leq \kappa \leq d-t+1$. In the case in which $\kappa = d-t+1$, we have that $d-\kappa+1 = t$, and in this case the smallest (n,t,t)-cover is comprised of all possible subsets of size t, so $\ell' = \binom{n}{t}$.

For the case in which $\kappa < d-t+1$, smaller covering designs can be obtained. For example, if $n = 72$, $t = 6$ and $d = 23$ (as we will see in Section 5.3, taking $d = 23 < 72/3 = n/3$ enables us to handle degree-3 correlations) and $d-\kappa+1 = 18$ (so $\kappa = 6$), the best known size of a $(72, 18, 6)$-cover is $\ell' = 10092$.[7] Assuming 128-bit seeds, the average seed size per party becomes only ≈ 2.2Mb.

5.3 Non-Interactive Correlation Generation

With the building blocks presented previously, we are ready to present our end-to-end protocol for the committee $\mathcal{P}$ to generate a sample from the degree-D correlation towards committee $\mathcal{Q}$. Recall that $R = \mathsf{GR}(p^k, \delta)$, and that $(\phi : \mathbb{Z}_{p^k}^r \to R, \psi : R \to \mathbb{Z}_{p^k}^r)$ is a degree-D RMFE. The correlation we aim at generating is $(\langle y_1 \rangle, \ldots, \langle y_m \rangle)$, where $y_i = F_i(\boldsymbol{x}) \in \mathbb{Z}_{p^k}$ for some degree-D polynomial F_i over $\mathbb{Z}_{p^k}$, and $\boldsymbol{x} \in \mathbb{Z}_{p^k}^\ell$ is uniformly random. Jumping ahead, due to the use of RMFEs and packed secret-sharing, our method not only produces one single sample from such distribution, but it actually generates multiple samples $(\langle y_{1jl} \rangle, \ldots, \langle y_{mjl} \rangle)$ for $j \in \{1, \ldots, \kappa\}$ and $l \in \{1, \ldots, r\}$.

We first introduce some preliminaries. Recall that $t < n/D$ is the number of corrupted parties in $\mathcal{P}$, and $d = \lfloor \frac{n-1}{D} \rfloor$, so $t \leq d < n$. Also recall that $1 \leq \kappa \leq (d-t)+1$ is the amount of secrets packed. We denote by $\pi : R \to (\mathbb{Z}_{p^k})^\delta$ the natural bijection between R and δ-dimensional vectors over $\mathbb{Z}_{p^k}$. As before, we use $[\![\boldsymbol{x}]\!]_d = (z_1, \ldots, z_n)$ to denote Shamir secret-sharing of degree d of a secret $\boldsymbol{x} = (x_1, \ldots, x_\kappa) \in R^\kappa$, meaning there is a polynomial $f(\mathtt{X})$ over R of degree at most d such that $z_i = f(\alpha_i)$ for $i \in \{1, \ldots, n\}$ and $x_j = f(\beta_j)$ for $j \in \{1, \ldots, \kappa\}$, where $\{\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_\kappa\}$ is an exceptional set over R. A simple but important property of packed secret-sharing we will make use of is that, if $[\![\boldsymbol{x}]\!]_{d_1} = (z_1, \ldots, z_n)$ and $[\![\boldsymbol{y}]\!]_{d_2} = (w_1, \ldots, w_n)$, then $[\![\boldsymbol{x} \star \boldsymbol{y}]\!]_{d_1+d_2} = (z_1 \cdot w_1, \ldots, z_n \cdot w_n)$, where $\star$ denotes component-wise product. This implies that, when the parties in $\mathcal{P}$ hold packed sharings, they can *locally* compute their product of their shares to obtain shares of the product of the underlying secrets, albeit with a larger degree.

For $j \in \{1, \ldots, \kappa\}$ and $h \in \{1, \ldots, q+1\}$ for some q, we let $\lambda_{q,j,h} \in R$ be the coefficient such that, for every polynomial $f(\mathtt{X})$ over R of degree at most q, it holds that $f(\beta_j) = \sum_{h=1}^{d+1} \lambda_{q,j,h} f(\alpha_h)$. These correspond to standard Lagrange coefficients used in polynomial interpolation. Given $c \in R$, we denote by $M_c \in \mathbb{Z}_{p^k}^{\delta \times \delta}$ the matrix that represents multiplication by c over $\mathbb{Z}_{p^k}^\delta$, that is, for every $x \in R$ it holds that $\pi(c \cdot x) = M_c \cdot \pi(x)$. Finally, we use $M_\phi \in \mathbb{Z}_{p^k}^{\delta \times r}$

[7] Such covering design sizes can be found in `https://www.dmgordon.org/cover/`.

and $M_\psi \in \mathbb{Z}_{p^k}^{r\times\delta}$ to denote the matrices representing the linear transformations $\pi \circ \phi : \mathbb{Z}_{p^k}^r \to \mathbb{Z}_{p^k}^\delta$ and $\psi \circ \pi^{-1} : \mathbb{Z}_{p^k}^\delta \to \mathbb{Z}_{p^k}^r$, respectively. In other words, $M_\phi \cdot \boldsymbol{x} = \pi(\phi(\boldsymbol{x}))$ for every $\boldsymbol{x} \in \mathbb{Z}_{p^k}^r$ and $M_\psi \cdot \boldsymbol{y} = \psi(\pi^{-1}(\boldsymbol{y}))$ for every $\boldsymbol{y} \in \mathbb{Z}_{p^k}^\delta$.

With this notation at hand, we are ready to introduce our protocol to generate the desired correlation.

Degree-D correlation generation

The following protocol enables the parties in $\mathcal{Q}$ to receive $\kappa \cdot r$ degree-D correlations $(\langle y_{1jl}\rangle, \ldots, \langle y_{mjl}\rangle)$ for $j \in \{1,\ldots,\kappa\}$ and $l \in \{1,\ldots,r\}$, generated non-interactively by the parties in $\mathcal{P}$. Assume $t \le d$. Let $d = \left\lfloor \frac{n-1}{D} \right\rfloor$, and $\kappa = (d-t)+1$. Let $F_i : \mathbb{Z}_{p^k}^\ell \to \mathbb{Z}_{p^k}$ be a polynomial over $\mathbb{Z}_{p^k}$ of degree $D_i \le D$.

Setup: The parties in $\mathcal{P}$ have the PRSS seeds from Thm 3.
Protocol: The parties proceed as follows:

1. The parties in $\mathcal{P}$ use PRSS to obtain non-interactively $(\llbracket \boldsymbol{u}_1 \rrbracket_d, \ldots, \llbracket \boldsymbol{u}_\ell \rrbracket_d)$, where each $\boldsymbol{u}_i$ is equal to $(u_{i1},\ldots,u_{i\kappa}) \in R^\kappa$, with $u_{ij} = \phi(\boldsymbol{x}_{ij}) \in R$, where $\boldsymbol{x}_{ij} = (x_{ij1},\ldots,x_{ijr}) \in (\mathbb{Z}_{p^k})^r$.
2. The parties in $\mathcal{P}$ locally compute $(\llbracket \boldsymbol{v}_1 \rrbracket_{d\cdot D_1}, \ldots, \llbracket \boldsymbol{v}_m \rrbracket_{d\cdot D_m})$, where $v_{ij} = F_i(u_{1j},\ldots,u_{\ell j}) \in R$ for every $i \in \{1,\ldots,m\}$ and $j \in \{1,\ldots,\kappa\}$. Notice that here, F_i is treated as a polynomial over R. We denote $d_i = d \cdot D_i$ and $\llbracket \boldsymbol{v}_i \rrbracket_{d_i} = (v_i^{(1)},\ldots,v_i^{(n)})$.
3. For each $i \in \{1,\ldots,m\}$, each $P_h \in \mathcal{P}$ with $h \in \{1,\ldots,d_i+1\}$ computes $\boldsymbol{w}_i^{(h)} = \pi(v_i^{(h)}) \in (\mathbb{Z}_{p^k})^\delta$. Then P_h distributes shares $(\langle w_{i1}^{(h)}\rangle, \ldots, \langle w_{i\delta}^{(h)}\rangle)$ to the parties in $\mathcal{Q}$.
4. For each $i \in \{1,\ldots,m\}$, and for each $j \in \{1,\ldots,\kappa\}$, the parties in $\mathcal{Q}$ compute locally $(\langle z_{ij1}\rangle,\ldots,\langle z_{ij\delta}\rangle)^\intercal = \sum_{h=1}^{d_i+1} M_{\lambda_{d_i,j,h}} \cdot (\langle w_{i1}^{(h)}\rangle,\ldots,\langle w_{i\delta}^{(h)}\rangle)^\intercal$.
5. The parties in $\mathcal{Q}$ compute locally $(\langle y_{ij1}\rangle,\ldots,\langle y_{ijr}\rangle)^\intercal = M_\psi \cdot (\langle z_{ij1}\rangle,\ldots,\langle z_{ij\delta}\rangle)^\intercal$. Finally, the parties in $\mathcal{Q}$ output the $r\cdot\kappa$ correlations $(\langle y_{1jl}\rangle,\ldots,\langle y_{mjl}\rangle)$ for $j \in \{1,\ldots,\kappa\}$ and $l \in \{1,\ldots,r\}$.

Theorem 4. *At the end of the protocol above, the $r\cdot\kappa$ correlations $\{(\langle y_{1jl}\rangle,\ldots,\langle y_{mjl}\rangle)\}_{j=1,l=1}^{\kappa,r}$ that the parties in $\mathcal{Q}$ obtain follow the desired correlation distribution. Moreover, a passive adversary corrupting at most t parties in $\mathcal{Q}$ does not learn anything about the underlying secrets.*

Proof. Privacy follows straightforwardly from the properties of the PRSS construction, discussed in Section 5.2. Therefore, it only remains to be seen that the sharings output by the parties in $\mathcal{Q}$ follow the correct distribution.

We begin by observing that $(w_{i1}^{(h)},\ldots,w_{i\delta}^{(h)}) = \pi(v_i^{(h)})$ by definition. Then, for each $i \in \{1,\ldots,m\}$ and $j \in \{1,\ldots,\kappa\}$, the definition of the matrix $M_{\lambda_{d_i,j,h}}$

implies that

$$\begin{aligned}
(z_{ij1},\ldots,z_{ij\delta})^{\intercal} &= \sum_{h=1}^{d_i+1} M_{\lambda_{d_i,j,h}} \cdot (w_{i1}^{(h)},\ldots,w_{i\delta}^{(h)})^{\intercal} && \text{(by definition)}\\
&= \sum_{h=1}^{d_i+1} M_{\lambda_{d_i,j,h}} \cdot \pi(v_i^{(h)}) && \text{(observation above)}\\
&= \sum_{h=1}^{d_i+1} \pi(\lambda_{d_i,j,h} \cdot v_i^{(h)}) && \text{(definition of } M_{\lambda_{d_i,j,h}})\\
&= \pi\left(\sum_{h=1}^{d_i+1} \lambda_{d_i,j,h} \cdot v_i^{(h)}\right) && \text{(linearity of } \pi)\\
&= \pi\left(v_{ij}\right) && \text{(definition of } \{\lambda_{d_i,j,h}\}).
\end{aligned}$$

Now, notice that since $(y_{ij1},\ldots,y_{ijr})^{\intercal} = M_\psi \cdot (z_{ij1},\ldots,z_{ij\delta})^{\intercal}$ and $(z_{ij1},\ldots,z_{ij\delta}) = \pi(v_{ij})$ from the analysis above, the definition of M_ψ implies that $(y_{ij1},\ldots,y_{ijr}) = \psi(v_{ij})$. Furthermore, each $v_{ij} \in R$ for $i \in \{1,\ldots,m\}$ and $j \in \{1,\ldots,\kappa\}$ satisfies $v_{ij} = F_i(u_{1j},\ldots,u_{\ell j}) = F_i(\phi(\boldsymbol{x}_{1j}),\ldots,\phi(\boldsymbol{x}_{\ell j}))$. Since F_i has degree $D_i \le D$, the properties of the degree-D RMFE (ϕ,ψ) imply that, for each $l \in \{1,\ldots,r\}$, it holds that

$$\underbrace{(\psi(v_{ij}))_l}_{l\text{-th coordinate of } \psi(v_{ij}) \in \mathbb{Z}_{p^k}^r} = (\psi(F_i(\phi(\boldsymbol{x}_{1j}),\ldots,\phi(\boldsymbol{x}_{\ell j}))))_l = F_i(x_{1jl},\ldots,x_{\ell jl}).$$

However, recall that $(y_{ij1},\ldots,y_{ijr}) = \psi(v_{ij})$. This implies that $(\psi(v_{ij}))_l$ is precisely equal to y_{ijl}, so $y_{ijl} = F_i(x_{1jl},\ldots,x_{\ell jl})$.

The above leads us to conclude that the outputs $(\langle y_{1jl}\rangle,\ldots,\langle y_{mjl}\rangle)$ for $j \in \{1,\ldots,\kappa\}$ and $l \in \{1,\ldots,r\}$ follow the correct correlation. This is because, for every j,l, each y_{ijl} is equal to $F_i(\boldsymbol{r})$, where $\boldsymbol{r} = (x_{1jl},\ldots,x_{\ell jl}) \in \mathbb{Z}_{p^k}^\ell$, and by the properties of the PRSS, the distribution of this $\boldsymbol{r}$ is uniformly random over $\mathbb{Z}_{p^k}^\ell$, as required by the correlation. □

Communication complexity. In step 3 of our correlation generation protocol, for every $i \in \{1,\ldots,m\}$, each party $P_h \in \mathcal{P}$ with $h \in \{1,\ldots,D_i \cdot n + 1\}$ must distribute a total of δ shares to each of the N parties in $\mathcal{Q}$. Denoting by s the size in bits of each $\langle\cdot\rangle$-sharing corresponding to each party in $\mathcal{Q}$, this communication sums up to $\delta \cdot N \cdot s \cdot \sum_{i=1}^m (D_i \cdot d + 1)$. Since $\kappa \cdot r$ correlation samples are produced in total, and taking into account that $D_i \le D$ and $\kappa = (d-t)+1$ with $d = \left\lfloor \frac{n-1}{D} \right\rfloor$, the amortized total cost per correlation is

$$Ns \cdot \left(\frac{\delta \sum_{i=1}^m (D_i \cdot d + 1)}{\kappa r}\right) = O\left(Ns\left(\frac{\delta}{r}\right)\left(\frac{d}{\kappa}\right)(mD)\right) = O\left(Ns\left(\frac{\delta}{r}\right)\left(\frac{n}{\kappa}\right)m\right).$$

Notice now that we use the construction of degree-D RMFE (ϕ,ψ) in Corollary 5. This map yields $\frac{\delta}{r} \approx \frac{(1+2D)D}{3}$, which crucially, is *constant* in the number of

parties n. In contrast, if we did not use our degree-D RMFEs, there would be an overhead that is logarithmic in n. For the factor n/κ, recall that κ is a term such that $1 \leq \kappa \leq \lfloor \frac{n-1}{D} \rfloor - t + 1$. In the extreme case in which $\kappa = 1$, the factor n/κ equals n, so we get a communication complexity that is *quadratic* in n, but we get the smallest possible covers. We can achieve *linear* communication complexity by taking $\kappa = \Omega(n)$, although this would increase the cover sizes. We refer the reader to the discussion in [3] for more details on known cover sizes.

Acknowledgments

The work of Hongqing Liu was supported in part by the National Key Research and Development Program under the grant 2022YFA1004900. The work of Chaoping Xing was supported in part by the National Key Research and Development Project under the Grant 2021YFE0109900 and by the National Natural Science Foundation of China (NSFC) under the Grant 12031011. The work of Chen Yuan was supported in part by the National Natural Science Foundation of China under Grant 12101403.

This paper was prepared in part for information purposes by the Artificial Intelligence Research group of JPMorgan Chase & Co and its affiliates ("JP Morgan"), and is not a product of the Research Department of JP Morgan. JP Morgan makes no representation and warranty whatsoever and disclaims all liability, for the completeness, accuracy or reliability of the information contained herein. This document is not intended as investment research or investment advice, or a recommendation, offer or solicitation for the purchase or sale of any security, financial instrument, financial product or service, or to be used in any way for evaluating the merits of participating in any transaction, and shall not constitute a solicitation under any jurisdiction or to any person, if such solicitation under such jurisdiction or to such person would be unlawful.

References

1. M. Abdalla, F. Bourse, A. D. Caro, and D. Pointcheval. Simple functional encryption schemes for inner products. In *IACR International Workshop on Public Key Cryptography*, pages 733–751. Springer, 2015.
2. M. Abspoel, R. Cramer, I. Damgård, D. Escudero, and C. Yuan. Efficient information-theoretic secure multiparty computation over zpk via galois rings. In *Theory of Cryptography Conference*, pages 471–501. Springer, 2019.
3. F. Benhamouda, E. Boyle, N. Gilboa, S. Halevi, Y. Ishai, and A. Nof. Generalized pseudorandom secret sharing and efficient straggler-resilient secure computation. In *Theory of Cryptography Conference*, pages 129–161. Springer, 2021.
4. A. R. Block, H. K. Maji, and H. H. Nguyen. Secure computation based on leaky correlations: high resilience setting. In *Annual International Cryptology Conference*, pages 3–32. Springer, 2017.
5. D. Boneh, E. Boyle, H. Corrigan-Gibbs, N. Gilboa, and Y. Ishai. Zero-knowledge proofs on secret-shared data via fully linear pcps. In *Annual International Cryptology Conference*, pages 67–97. Springer, 2019.

6. E. Boyle, G. Couteau, N. Gilboa, Y. Ishai, L. Kohl, and P. Scholl. Efficient pseudorandom correlation generators: Silent ot extension and more. In *Annual International Cryptology Conference*, pages 489–518. Springer, 2019.
7. E. Boyle, N. Gilboa, Y. Ishai, and A. Nof. Practical fully secure three-party computation via sublinear distributed zero-knowledge proofs. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 869–886, 2019.
8. E. Boyle, N. Gilboa, Y. Ishai, and A. Nof. Efficient fully secure computation via distributed zero-knowledge proofs. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 244–276. Springer, 2020.
9. I. Cascudo, R. Cramer, C. Xing, and C. Yuan. Amortized complexity of information-theoretically secure mpc revisited. In *Annual International Cryptology Conference*, pages 395–426. Springer, 2018.
10. I. Cascudo and E. Giunta. On interactive oracle proofs for boolean r1cs statements. *Cryptology ePrint Archive*, 2021.
11. I. Cascudo and J. S. Gundersen. A secret-sharing based mpc protocol for boolean circuits with good amortized complexity. In *TCC*, pages 652–682. Springer, 2020.
12. J. H. Cheon and K. Lee. Limits of polynomial packings for $\mathbb{Z}_{p^k}$ and $\mathbb{F}_{p^k}$. *Eurocrypt'22*, 2022.
13. R. Cramer, I. Damgård, D. Escudero, P. Scholl, and C. Xing. SPDZ2k: Efficient MPC mod 2^k for dishonest majority. In *Annual International Cryptology Conference*, pages 769–798. Springer, 2018.
14. R. Cramer, I. Damgård, and Y. Ishai. Share conversion, pseudorandom secret-sharing and applications to secure computation. In *Theory of Cryptography Conference*, pages 342–362. Springer, 2005.
15. R. Cramer, M. Rambaud, and C. Xing. Asymptotically-good arithmetic secret sharing over $\mathbb{Z}/p^\ell\mathbb{Z}$ with strong multiplication and its applications to efficient MPC. In *CRYPTO*. Springer, 2021.
16. I. Damgård, D. Escudero, T. Frederiksen, M. Keller, P. Scholl, and N. Volgushev. New primitives for actively-secure mpc over rings with applications to private machine learning. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 1102–1120. IEEE, 2019.
17. D. Demmler, T. Schneider, and M. Zohner. {Ad-Hoc} secure {Two-Party} computation on mobile devices using hardware tokens. In *23rd USENIX Security Symposium (USENIX Security 14)*, pages 893–908, 2014.
18. W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), 1976.
19. D. Escudero, H. Liu, C. Xing, and C. Yuan. Degree-d reverse multiplication-friendly embeddings: Constructions and applications. Cryptology ePrint Archive, Paper 2023/173, 2023. `https://eprint.iacr.org/2023/173`.
20. D. Escudero and E. Soria-Vazquez. Efficient information-theoretic multi-party computation over non-commutative rings. In *Annual International Cryptology Conference*, pages 335–364. Springer, 2021.
21. D. Escudero, C. Xing, and C. Yuan. More efficient dishonest majority secure computation over zpk via galois rings. *CRYPTO*, 2022.
22. A. Garcia and H. Stichtenoth. A tower of artin-schreier extensions of function fields attaining the drinfeld-vladut bound. *Inventiones mathematicae*, 121:211–222, 1995.
23. N. Gilboa and Y. Ishai. Compressing cryptographic resources. In *Annual International Cryptology Conference*, pages 591–608. Springer, 1999.

24. S. D. Gordon, D. Starin, and A. Yerukhimovich. The more the merrier: reducing the cost of large scale mpc. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 694–723. Springer, 2021.
25. Y. Huang. Practical secure two-party computation. 2012.
26. D. Kales and G. Zaverucha. Efficient lifting for shorter zero-knowledge proofs and post-quantum signatures. *IACR Cryptol. ePrint Arch.*, page 588, 2022.
27. V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 1–23. Springer, 2010.
28. P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *International conference on the theory and applications of cryptographic techniques*, pages 223–238. Springer, 1999.
29. A. Polychroniadou and Y. Song. Constant-overhead unconditionally secure multiparty computation over binary fields. In *Advances in Cryptology–EUROCRYPT 2021: 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17–21, 2021, Proceedings, Part II*, pages 812–841. Springer, 2021.
30. R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.
31. N. P. Smart and T. Tanguy. Taas: Commodity mpc via triples-as-a-service. In *Proceedings of the 2019 ACM SIGSAC Conference on Cloud Computing Security Workshop*, pages 105–116, 2019.
32. N. P. Smart and F. Vercauteren. Fully homomorphic encryption with relatively small key and ciphertext sizes. In *International Workshop on Public Key Cryptography*, pages 420–443. Springer, 2010.
33. E. Soria-Vazquez. Doubly efficient interactive proofs over infinite and non-commutative rings. *Cryptology ePrint Archive*, 2022.
34. H. Stichtenoth. *Algebraic function fields and codes*. Universitext. Springer, 1993.
35. Z.-X. Wan. *Lectures on finite fields and Galois rings*. World Scientific Publishing Company, 2003.