Limits of Polynomial Packings for $\mathbb{Z}_{p^k}$ and $\mathbb{F}_{p^k}$

Jung Hee Cheon[1,2] and Keewoo Lee[(✉)1]

[1] Seoul National University, Seoul, Republic of Korea
{jhcheon, activecondor}@snu.ac.kr
[2] Crypto Lab Inc., Seoul, Republic of Korea

Abstract. We formally define polynomial packing methods and initiate a unified study of related concepts in various contexts of cryptography. This includes homomorphic encryption (HE) packing and reverse multiplication-friendly embedding (RMFE) in information-theoretically secure multi-party computation (MPC). We prove several upper bounds and impossibility results on packing methods for $\mathbb{Z}_{p^k}$ or $\mathbb{F}_{p^k}$-messages into $\mathbb{Z}_{p^t}[x]/f(x)$ in terms of (i) packing density, (ii) level-consistency, and (iii) surjectivity. These results have implications on recent development of HE-based MPC over $\mathbb{Z}_{2^k}$ secure against actively corrupted majority and provide new proofs for upper bounds on RMFE.

Keywords: Packing method · Homomorphic encryption · Secure multi-party computation · Reverse multiplication-friendly embedding · $\mathbb{Z}_{p^k}$.

1 Introduction

HE Packing. Homomorphic encryption (HE), which allows computations on ciphertexts without decryption, is such a versatile tool that it is often referred as the holy grail of cryptography. After Gentry's breakthrough [23], HE has undergone extensive study and development. HE is now considered to be exploitable in real-life applications (e.g. privacy-preserving machine learning [28]) and regarded as a core building block in various cryptographic primitives (e.g. secure multi-party computation [21]).

One drawback of contemporary lattice-based HE schemes [4, 22] is that their plaintext space is of the form $\mathbb{Z}_q[x]/\Phi_M(x)$, as their security is based on Ring Learning with Errors (RLWE) [30]. That is, these schemes are homomorphic with regards to the addition and multiplication of polynomial ring $\mathbb{Z}_q[x]/\Phi_M(x)$. This raises a question of how to *homomorphically* encode messages into the plaintexts, as our data are usually binary bits, integers, fixed/floating point numbers, or at least $\mathbb{Z}_p$ and $\mathbb{F}_{p^k}$.

Among a number of works on how to encode data into HE plaintexts [11, 10, 8, 12], Smart-Vercauteren [33, 34] first introduced the idea of *packing* several $\mathbb{Z}_p$ (or $\mathbb{F}_{p^k}$) elements into the HE plaintext space $\mathbb{Z}_p[x]/\Phi_M(x)$ via CRT[3] ring isomorphism with *well-chosen* prime p. Their simple yet powerful technique enables SIMD[4]-like optimizations and enhances amortized performance. That is, with a

[3] Chinese Remainder Theorem
[4] Single Instruction, Multiple Data

polynomial packing method, we can securely compute on *multiple* $\mathbb{Z}_p$-messages simultaneously by homomorphically computing on a *single* packed HE plaintext in $\mathbb{Z}_p[x]/\Phi_M(x)$. In particular, through the packing, the complex multiplicative structure of $\mathbb{Z}_p[x]/\Phi_M(x)$ embeds the more handy coordinate-wise multiplication (a.k.a. Hadamard product) of $\mathbb{Z}_p^n$, where n denotes the number of packed messages. Packing has now become a standard technique in HE research, and it is not too much to say that the performance of HE applications are determined by how well packings are utilized.

However, this conventional packing method has a limitation: it cannot (efficiently) pack $\mathbb{Z}_{2^k}$-messages.[5] This limitation has recently attracted attention due to development of secure multi-party computation (MPC) over $\mathbb{Z}_{2^k}$ secure against actively corrupted majority by SPD$\mathbb{Z}_{2^k}$ [15]. SPD$\mathbb{Z}_{2^k}$ follows the framework of HE-based MPC protocol SPDZ [21], while targeting $\mathbb{Z}_{2^k}$-messages rather than prime field $\mathbb{Z}_p$-messages, with a motivation from the fact that $\mathbb{Z}_{2^k}$ arithmetic matches closely what happens on standard CPUs. In this context, Overdrive2k [31] and MHz2k [13], whose goal are efficient constructions of HE-based MPC over $\mathbb{Z}_{2^k}$, came up with new and more involved polynomial packing methods for $\mathbb{Z}_{2^k}$-messages (Section 4).

RMFE in Perfectly Secure MPC. Another context where polynomial packings appear is *information-theoretically secure MPC* (or perfectly secure MPC). A main tool in this area is Shamir's linear secret sharing scheme(LSSS). A cumbersome fact when using LSSS is that the number of shares is restricted by the field where computation takes place.[6] Thus, it is standard to *lift* the computation to a larger field which supports enough number of shares, but this causes substantial overheads. In their seminal work [5], Cascudo-Cramer-Xing-Yuan first defined and studied *reverse multiplication-friendly embedding (RMFE)* which is, roughly speaking, an embedding of several elements of small finite field into a larger finite field while providing *somewhat* homomorphism of degree-2. Note that an RMFE can be indeed viewed as a polynomial packing $\mathbb{F}_{p^k}^n \to \mathbb{F}_{p^d} \cong \mathbb{F}_p[x]/f(x)$, where p is a prime and $f(x) \in \mathbb{F}_p[x]$ is an irreducible polynomial of degree d. Surprisingly, [5] constructed *constant-rate* RMFEs, leveraging algebraic geometry, and applied them to remove logarithmic overhead in amortized communication complexity which appears to enable Shamir's secret sharing. Since [5], RMFE has become a standard tool in information-theoretically secure MPC, to achieve *linear* amortized communication cost while preserving optimal corruption tolerance: [3, 20, 7, 17, 18, 32].

In [16], the notion of RMFE was extended to *over Galois rings* for construction of efficient perfectly secure MPC over $\mathbb{Z}_{p^k}$. Again, RMFE over Galois rings for $\mathbb{Z}_{p^k}$-messages can be viewed as a polynomial packing $\mathbb{Z}_{p^k}^n \to GR(p^k, d) \cong$

[5] The original method of [33] does not consider packings for $\mathbb{Z}_{p^k}$. Gentry-Halevi-Smart [24] later generalized the method to support such packing. However, this method achieves only considerably low efficiency. See Section 4.1.

[6] Indeed, the number of evaluation points is bounded by the size of the field.

$\mathbb{Z}_{p^k}[x]/f(x)$, where p is a prime and $f(x) \in \mathbb{Z}_{p^k}[x]$ is a degree-d irreducible polynomial in $\mathbb{F}_p[x]$.

Other Contexts. Other than HE and perfectly secure MPC, there are still more areas where polynomial packings are used for amortization: correlation extraction for secure computation [2], zk-SNARK [6], etc. Moreover, we believe that polynomial packing will be even more prominent and universal tool for efficiency and practicality in the future: (i) RLWE-based cryptosystems are emerging, where plaintexts are $\mathbb{Z}_q[x]/\Phi_M(x)$; (ii) Secure computation is emerging, where some parts of protocols need to be large or of certain form due to security or mathematical properties required, whereas where we actually want to compute in is (extremely) small and typical such as $\mathbb{F}_2$ or $\mathbb{Z}_{2^{32}}$.

1.1 Our Contribution

Unified Definition and Survey. In this work, we formally define polynomial packing methods, which can be understood as (somewhat) homomorphic encoding for copies of a small ring, e.g. $\mathbb{Z}_p$ or $\mathbb{F}_{p^k}$, into a larger ring, e.g. $\mathbb{Z}_q[x]/f(x)$, (Section 3.1). The notion of polynomial packing unifies forementioned concepts in various contexts of cryptography, including HE packing and RMFE in perfectly secure MPC. Then, we gather existing packing methods in one place. This includes RMFE (Section 2.3 and 3.1), classic HE packing methods (Section 3.1), and recent development occurred in HE-based MPC over $\mathbb{Z}_{2^k}$ (Section 4). We also provide *decomposition* lemmas which suggest that it is enough to study packing methods for $\mathbb{Z}_{p^k}^n$ (or $\mathbb{F}_{p^k}^n$) into $\mathbb{Z}_{p^t}[x]/f(x)$ where $t \geq k$ and p is prime, instead of general case of $\mathbb{Z}_P^n$ (or $\mathbb{F}_P^n$) into $\mathbb{Z}_Q[x]/f(x)$ where $P, Q \in \mathbb{Z}^+$ (Section 3.2). The results also rule out the possibility of using composite modulus for better packing.

Upper Bounds and Impossibility. We prove several upper bounds and impossibility results on packing methods for $\mathbb{Z}_{p^k}$ or $\mathbb{F}_{p^k}$-messages into $\mathbb{Z}_{p^t}[x]/f(x)$.

- Upper Bounds on Packing Density (Section 5): We evaluate the efficiency of packing methods by packing density which measures how densely the messages are packed in (plaintext) polynomials (Def. 5).We prove that, when a packing method provides somewhat homomorphism upto degree-D polynomials, the packing density is roughly upper bounded by $1/D$ (Thm. 1 and 2). These results have several implications:
  - The packing method of MHz2k [13] achieves nearly optimal density in some sense when using their parameters (Example 6). Our results justify the *lifting* of MHz2k packing (See Section 4.3).
  - We provide the first upper bound on RMFE over Galois ring for $\mathbb{Z}_{p^k}$-messages (Example 7).

  - We provide a new proof for upper bound on RMFE, which can be extended to higher-degree settings unlike the previous proof (Example 10).

– Impossibility of Level-consistency (Section 6): The notion of level-consistency captures the property whether packings are decodable in an identical way at different multiplicative levels (Def. 6). The level-consistency is a desirable feature as it allows homomorphic computation between different packing levels. We prove sufficient and necessary conditions on parameters to allow a level-consistent packing method. These results have the following implications:
  - HELib packing [26] (a.k.a. GHS packing [24], See Section 4.1) is essentially the optimal method to use in *fully* homomorphic encryption(FHE) (Example 14).
  - It is impossible to construct efficient level-consistent packing methods in most cases. This justifies the use of *level-dependent* packings in SPDZ-like MPC protocols over $\mathbb{Z}_{2^k}$ [31, 13] and highlights the usefulness of the trick proposed by MHz2k [13], which closed the gap between the level-consistent and level-dependent packing methods in so-called *reshare* protocol. (See Section 6.1.)

– Impossibility of Surjectivity (Section 7): For a packing method into $\mathcal{R}$, the notion of surjectivity captures the condition whether every element of $\mathcal{R}$ is decodable (Def. 8). This distiction is essential when designing a cryptographic protocol with the packing method in a malicious setting, where an adversary might freely deviate from the protocol. If there is an element in $\mathcal{R}$ which fails to decode, a malicious adversary might make use of the element to illegitimately learn information of other parties, if such invalid packings are not properly handled. We prove sufficient and necessary conditions on parameters to allow a surjective packing method. Our results suggest that it is impossible to construct a meaningful surjective packing method in most cases. This justifies the use of *non*-surjective packings and the need of ZKPoMK[7], which ensures an HE ciphertext encrypts a validly packed plaintext, in SPDZ-like MPC protocols over $\mathbb{Z}_{2^k}$ [31, 13].

2 Preliminaries

2.1 Notations and Terminologies

In this paper, we only consider finite commutative rings with unity. Thus, we omit the long description and simply refer them as rings. Readers must understand the term *ring* as finite commutative rings with unity, even if not explicitly stated. In addition, we only consider monic polynomials when defining quotient rings. Thus, we omit description on *monic* property throughout the paper for readability. Readers must understand any polynomials defining quotient rings as monic polynomials, even if not explicitly stated.

[7] Zero-knowledge proof of message knowledge

This paper carefully distinguishes between the use of the terms *message* and *plaintext*. Messages are those we really want to compute with. On the other hand, plaintexts are defined by encryption scheme (particularly, HE schemes) we are using. In this paper, messages are in $\mathbb{Z}_{p^k}$ or $\mathbb{F}_{p^k}$ and plaintexts are in $\mathbb{Z}_q[x]/f(x)$.

For prime fields, we use both notations $\mathbb{F}_p$ and $\mathbb{Z}_p$, depending on whether we want to emphasize that it is a field or that it is the ring of integer modulo p. The multiplicative order of b modulo a is denoted as $\mathrm{ord}_a(b)$. We use $\mathrm{Inv}_a(b)$ to denote the smallest positive integer which is a multiplicative inverse of b modulo a. We use $\odot$ to denote the coordinate-wise multiplication (a.k.a. Hadamard product) in products of rings. In a product of rings R^n, the element $\boldsymbol{e}_i$ denotes a standard unit vector whose i-th coordinate is 1 and the other coordinates are 0. We denote the M-th cyclotomic polynomial as $\Phi_M(x)$ and the Euler's totient function as $\phi(\cdot)$. We use $GR(p^k, d)$ to denote the Galois ring, a degree-d extension of $\mathbb{Z}_{p^k}$. We use notations $[n] := \{1, 2, \cdots, n\}$ and $[0, n] := \{0, 1, \cdots, n\}$.

2.2 Polynomial Factorizations

Here, we briefly review some basic facts on polynomial factorizations in $\mathbb{Z}_{p^k}[x]$. First, recall Hensel lifting (or Hensel's lemma).

Lemma 1 (Hensel Lifting). *Let $f(x) \in \mathbb{Z}_{p^k}[x]$ be a monic polynomial which factors into $\prod_{i=1}^{r} g_i(x)^{\ell_i}$ in $\mathbb{F}_p[x]$, where $g_i(x)$ are distinct irreducible polynomials. Then there exist pairwise coprime monic polynomials $f_1(x), \cdots, f_r(x) \in \mathbb{Z}_{p^k}[x]$ such that $f(x) = \prod_{i=1}^{r} f_i(x)$ in $\mathbb{Z}_{p^k}[x]$ and $f_i(x) = g_i(x)^{\ell_i} \pmod{p}$, for all $i \in [r]$.*

When $\gcd(M, p) = 1$, $\Phi_M(x)$ factors into $\prod_{i=1}^{r} g_i(x)$ in $\mathbb{F}_p[x]$, where $g_i(x)$ are distinct irreducible polynomials of degree $d := \mathrm{ord}_M(p)$. Thus, $\phi(M) = r \cdot d$ holds. To see this, consider a primitive M-th root of unity in a sufficiently large extension field of $\mathbb{F}_p$. Then, it is easy to see that the number of its conjugates is d which coincides with the degree of its minimal polynomial. Applying Hensel's lemma, we have a factorization $\Phi_M(x) = \prod_{i=1}^{r} f_i(x)$ in $\mathbb{Z}_{p^k}[x]$, where $\deg(f_i) = d$ and $f_i(x) = g_i(x) \pmod{p}$. Accordingly, we have a CRT ring isomorphism $\mathbb{Z}_{p^k}[x]/\Phi_M(x) \cong \prod_{i=1}^{r} \mathbb{Z}_{p^k}[x]/f_i(x)$. Each $\mathbb{Z}_{p^k}[x]/f_i(x)$ is often referred to as a CRT *slot* of $\mathbb{Z}_{p^k}[x]/\Phi_M(x)$.

2.3 RMFE

Reverse multiplication-friendly embeddings (RMFE) were first defined and studied in-depth by [5].[8] At a high level, RMFEs are embeddings of several elements of small finite field into a larger finite field, while providing *somewhat* homomorphism of degree-2.

[8] Nonetheless, this object was also previously studied in [2] to amortize oblivious linear evaluations (OLE) into a larger extension field for correlation extraction problem in MPC. However, their construction achieved only sublinear density.

Definition 1 (RMFE). *A pair of maps (φ, ψ) is called an $(n, d)_{p^k}$-reverse multiplication-friendly embedding (RMFE) if it satisfies the following.*

- *The map $\varphi : \mathbb{F}_{p^k}^n \to \mathbb{F}_{p^{kd}}$ is $\mathbb{F}_{p^k}$-linear.*
- *The map $\psi : \mathbb{F}_{p^{kd}} \to \mathbb{F}_{p^k}^n$ is $\mathbb{F}_{p^k}$-linear.*
- *For all $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_{p^k}^n$, it holds $\psi(\varphi(\boldsymbol{a}) \cdot \varphi(\boldsymbol{b})) = \boldsymbol{a} \odot \boldsymbol{b}$*

Surprisingly, [5] constructed families of $(n, d)_{p^k}$-RMFE where the density n/d converges to some *constant*, for arbitrary prime power p^k, leveraging algebraic geometry. That is, [5] constructed *constant-rate* RMFEs. For instance, we have a family of $(n, d)_2$-RMFE with $n/d \to 0.203$ from [5]. Since this seminal work, RMFE has become a standard tool in information-theoretically secure MPC, to achieve *linear* amortized communication cost while preserving optimal corruption tolerance: [5, 3, 20, 7, 17, 18, 32]. RMFE was also leveraged in zk-SNARK context recently [6].

Recently in [16], RMFE *over Galois rings* was first defined and studied. It is a natural generalization of RMFE over fields to Galois rings.

Definition 2 (RMFE over Galois Ring). *A pair of maps (φ, ψ) is called an $(n, d)_{p^r}$-RMFE over modulus p^k if it satisfies the following.*

- *The map $\varphi : GR(p^k, r)^n \to GR(p^k, d)$ is $GR(p^k, r)$-linear.*
- *The map $\psi : GR(p^k, d) \to GR(p^k, r)^n$ is $GR(p^k, r)$-linear.*
- *For all $\boldsymbol{a}, \boldsymbol{b} \in GR(p^k, r)^n$, it holds $\psi(\varphi(\boldsymbol{a}) \cdot \varphi(\boldsymbol{b})) = \boldsymbol{a} \odot \boldsymbol{b}$*

The authors also showed that any $(n, d)_{p^r}$-RMFE over fields can be naturally lifted upto an $(n, d)_{p^r}$-RMFE over modulus p^k. That is, there are *asymptotically good* RMFE also in the Galois ring setting.

Their goal was to construct efficient $(n, d)_p$-RMFEs over modulus p^k for $\mathbb{Z}_{p^k}$-messages as a building block for more efficient information-theoretically secure MPC over $\mathbb{Z}_{p^k}$. More generally, it seems there are very limited applications where messages in Galois ring (except $\mathbb{Z}_{p^k}$ or $\mathbb{F}_{p^k}$) play important roles. Thus, in our work, we focus on $(n, d)_p$-RMFE over modulus p^k for $\mathbb{Z}_{p^k}$-messages. Note that this case can be interpreted as packing $\mathbb{Z}_{p^k}$-messages into $GR(p^k, d) \cong \mathbb{Z}_{p^k}[x]/f(x)$ for some degree-d $f(x) \in \mathbb{Z}_{p^k}[x]$ which is irreducible modulo p.

3 Packing: Definitions and Basic Facts

In this section, we formally define *packings* and related concepts which are our main interests in this work. Some basic examples of packing methods are introduced for illustrative purpose. We also present some propositions which allow us to modularize our study of packing methods. We begin with a formal definition of packing.

3.1 Definitions and Basic Examples

Definition 3 (Packing). *Let R and $\mathcal{R}$ be rings. We call a pair of algorithms* $(\mathsf{Pack}, \mathsf{Unpack})$ *a packing method for n R-messages into $\mathcal{R}$, if it satisfies the following.*

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

For simplicity, the definition is presented a bit generally. In this paper, we are mostly interested in the cases where R is $\mathbb{Z}_p$ with $p \in \mathbb{Z}^+$ (or a finite field $\mathbb{F}_{p^k}$) and $\mathcal{R}$ is a polynomial ring $\mathbb{Z}_q[x]/f(x)$ with $q \in \mathbb{Z}^+$ and monic $f(x)$.

Notice that in Def. 3 the ring structure is not considered. Packing methods are interesting only when algebraic structures of the rings come in, since otherwise a packing is nothing more than a vanilla data encoding. The following definition of *degree* captures quality of (somewhat) homomorphic correspondence between packed messages and a packing. In this work, we are interested in packings of at least degree-2.

Definition 4 (Degree-D Packing). *Let $\mathcal{P} = (\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^{D}$ be a collection of packing methods for R^n into $\mathcal{R}$. We call $\mathcal{P}$ a degree-D packing method, if it satisfies the following for all $1 \le i \le D$:*

- *If $a(x), b(x)$ satisfy $\mathsf{Unpack}_i(a(x)) = \boldsymbol{a}$, $\mathsf{Unpack}_i(b(x)) = \boldsymbol{b}$ for $\boldsymbol{a}, \boldsymbol{b} \in R^n$, then $\mathsf{Unpack}_i(a(x) \pm b(x)) = \boldsymbol{a} \pm \boldsymbol{b}$ holds;*
- *If $a(x), b(x)$ satisfy $\mathsf{Unpack}_s(a(x)) = \boldsymbol{a}$, $\mathsf{Unpack}_t(b(x)) = \boldsymbol{b}$ for $\boldsymbol{a}, \boldsymbol{b} \in R^n$ and $s, t \in \mathbb{Z}^+$ such that $s + t = i$, then $\mathsf{Unpack}_i(a(x) \cdot b(x)) = \boldsymbol{a} \odot \boldsymbol{b}$ holds.*

Notice that the definition is heavy on the use of Unpack rather than Pack. Some readers might find it unnatural to define a property of *packing* methods with their *unpacking* structures. However, this is how things are. For instance, given that a collection of unpacking algorithms $(\mathsf{Unpack}_i)_{i=1}^{D}$ allows a degree-D packing method, it is trivial to find an appropriate collection of packing algorithms $(\mathsf{Pack}_i)_{i=1}^{D}$: we can just define Pack_i as an algorithm which randomly outputs an preimage of the input regarding Unpack_i. On the other hand, if a collection of packing algorithms $(\mathsf{Pack}_i)_{i=1}^{D}$ is given, it requires non-trivial computations to find an appropriate collection of packing algorithms $(\mathsf{Unpack}_i)_{i=1}^{D}$ in this case. In this regard, definitions and proofs coming up are also aligned to Unpack rather than Pack.

Here are some direct but noteworthy consequences of the definition.

Remark 1. Note that the definition implies that $\mathsf{Unpack}_i(c \cdot a(x)) = c \cdot \boldsymbol{a}$ holds for all $c \in \mathbb{Z}$ with probability 1. In particular, $\mathsf{Unpack}_i(0) = \mathbf{0}$.

Remark 2. A packing method $\mathcal{P} = (\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^{D}$ is of degree-D, only if $\mathcal{P}' = (\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^{D'}$ is a degree-D' packing method for all $D' < D$.

The following are some basic examples of packing methods. More sophisticated examples are introduced in Section 4.

Example 1 (Coefficient Packing). Let $f(x)$ be a degree-d monic polynomial in $\mathbb{Z}_p[x]$. Define Pack as a bijection which maps $(a_0, \cdots, a_{d-1}) \in \mathbb{Z}_p^d$ to $\sum_{i=0}^{d-1} a_i \cdot x^i \in \mathbb{Z}_p[x]/f(x)$. Define Unpack as the inverse of Pack. Then, $(\mathsf{Pack}, \mathsf{Unpack})$ is a degree-1 packing method for $\mathbb{Z}_p^d$ into $\mathbb{Z}_p[x]/f(x)$. We often refer this method as *coefficient packing.* As coefficient packing is already too good, we do not further examine degree-1 packing methods in this paper. Note that this method also applies to $\mathbb{F}_{p^k}$-messages if degree-1 is sufficient, since $\mathbb{F}_{p^k}^n$ is isomorphic to $\mathbb{Z}_p^{kn}$ as $\mathbb{Z}_p$-modules.

Example 2 (Conventional HE Packing). When making use of lattice-based HE schemes, where the plaintext space is of the form $\mathbb{Z}_p[x]/\Phi_M(x)$, it is standard to choose prime p such that $p = 1 \pmod M$ (and M as a power-of-two to enable efficient implementations). Then, $\Phi_M(x)$ fully splits in $\mathbb{Z}_p[x]$, and $\mathbb{Z}_p[x]/\Phi_M(x) \cong \mathbb{Z}_p^{\phi(M)}$ holds. The isomorphism induces a natural packing method, which is of degree-∞, i.e. degree-D for any $D \in \mathbb{Z}^+$. This packing is more than good in several aspects, but has quite heavy restrictions on parameters. In particular, the method does not allow packing $\mathbb{Z}_{2^k}$-messages.

Example 3 (HE Packing for $\mathbb{F}_{p^d}$). If one want to pack $\mathbb{F}_{p^d}$-messages when making use of lattice-based HE schemes, we often choose M so that $\Phi_M(x)$ factorizes into r distinct degree-d irreducible polynomials in $\mathbb{Z}_p[x]$. Then, we have $\mathbb{Z}_p[x]/\Phi_M(x) \cong \mathbb{F}_{p^d}^r$. As Example 2, this isomorphism induces a natural packing method which is of degree-∞, but has even heavier restriction on parameters.

Example 4 (RMFE). Essentially, an RMFE is nothing more than a degree-2 packing method for copies of a finite field $\mathbb{F}_{p^k}$ into a larger finite field $\mathbb{F}_{p^d} \cong \mathbb{Z}_p[x]/f(x)$, where p is a prime and $f(x)$ is a monic degree-d irreducible polynomial in $\mathbb{Z}_p[x]$. The only additional requirement is that the packing algorithm at level-1 and unpacking algorithm at level-2 must be $\mathbb{Z}_p$-linear functions. However, any degree-2 packing method can be easily transformed to satisfy the requirement.

Example 5 (RMFE over Galois Ring). Essentially, an RMFE over Galois ring for $\mathbb{Z}_{p^k}$-messages is nothing more than a degree-2 packing method for copies of $\mathbb{Z}_{p^k}$ into a larger Galois ring $GR(p^k, d) \cong \mathbb{Z}_{p^k}[x]/f(x)$, where p is a prime and $f(x)$ is a degree-d irreducible polynomial in $\mathbb{Z}_p[x]$.

Lastly, we define *packing density* which measures efficiency of packing methods. It measures how dense messages are packed in a single packing.

Definition 5 (Packing Density). *For a packing method for R^n into $\mathcal{R}$, we define its* packing density *as* $\log(|R|^n)/\log(|\mathcal{R}|)$.

Example 1, 2, and 3 have perfect packing density of 1. However, we will see that these are very special cases. In most cases such perfect packing density is not achievable, and even moderate packing density is hard to achieve.

3.2 Decomposition Lemmas

In this subsection, we state and prove several necessary conditions on existence of certain packing methods. The following propositions allow us to modularize our study and focus on the case of packings into $\mathbb{Z}_{p^t}[x]/f(x)$.

Proposition 1. *Let R be a ring with characteristic p and $\mathcal{R}$ be a ring with characteristic q. There exists a degree-0 packing method $(\mathsf{Pack}, \mathsf{Unpack})$ for R^n into $\mathcal{R}$ only if p divides q.*

Proof. Let $a(x)$ be an output of $\mathsf{Pack}(\mathbf{1})$. Then, $\mathsf{Unpack}(q \cdot a(x)) = q \cdot \mathbf{1}$ by Remark 1. Meanwhile, $q \cdot a(x) = 0$ in $\mathcal{R}$. Thus, $q \cdot \mathbf{1} = \mathbf{0}$ in R^n, by Remark 1. ☐

Proposition 2. *Let R be a ring with characteristic p. Let $q = q_1 \cdot q_2$, where $p|q_1$ and $\gcd(q_1, q_2) = 1$. There exists a degree-D packing method $\mathcal{P}$ for R^n into $\mathbb{Z}_q[x]/f(x)$, if and only if there exists a degree-D packing method $\mathcal{P}'$ for R^n into $\mathbb{Z}_{q_1}[x]/f(x)$.*

Proof (Sketch). Suppose $(\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^D$ is a degree-D packing method $\mathcal{P}$ for R^n into $\mathbb{Z}_q[x]/f(x)$. Let $a(x)$ satisfy $\mathsf{Unpack}_i(a(x)) = \boldsymbol{a}$ for some $\boldsymbol{a} \in R^n$ and $1 \leq i \leq D$. We can identify $a(x)$ with $(a_1(x), a_2(x)) \in \mathbb{Z}_{q_1}[x]/f(x) \times \mathbb{Z}_{q_2}[x]/f(x)$ via CRT isomorphism. Now, consider multiplying a constant $\mathrm{Inv}_{q_1}(q_2) \cdot q_2$. Observe the following.

- $(\mathrm{Inv}_{q_1}(q_2) \cdot q_2) \cdot \boldsymbol{a} = (\mathrm{Inv}_p(q_2) \cdot q_2) \cdot \boldsymbol{a} = \boldsymbol{a} \in R^n$
- $(\mathrm{Inv}_{q_1}(q_2) \cdot q_2) \cdot a_1(x) = 1 \cdot a_1(x) = a_1(x) \in \mathbb{Z}_{q_1}[x]/f(x)$
- $(\mathrm{Inv}_{q_1}(q_2) \cdot q_2) \cdot a_2(x) = \mathrm{Inv}_{q_1}(q_2) \cdot 0 = 0 \in \mathbb{Z}_{q_2}[x]/f(x)$

Thus, if $\mathsf{Unpack}_i(a(x)) = \mathsf{Unpack}_i(a_1(x), a_2(x)) = \boldsymbol{a}$ then $\mathsf{Unpack}_i(a_1(x), 0) = \boldsymbol{a}$. Then, we can construct $\mathcal{P}'$ with appropriate projections and injections. The other direction is more direct. For the full proof, see the full version [14]. ☐

Proposition 3. *Let $p = p_1 \cdot p_2$ and $q = q_1 \cdot q_2$, satisfying $p_1|q_1$, $p_2|q_2$, and $\gcd(q_1, q_2) = 1$. There exists a degree-D packing method $\mathcal{P}$ for $\mathbb{Z}_p^n$ into $\mathcal{R} := \mathbb{Z}_q[x]/f(x)$, if and only if there exist degree-D packing methods $\mathcal{P}^{(j)}$ for $\mathbb{Z}_{p_j}^n$ into $\mathcal{R}_j := \mathbb{Z}_{q_j}[x]/f(x)$ for $j = 1, 2$.*

Proof (Sketch). Suppose $(\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^D$ is a degree-D packing method $\mathcal{P}$ for $\mathbb{Z}_p^n$ into $\mathcal{R}$. Let $a(x) \in \mathcal{R}$ satisfy $\mathsf{Unpack}_i(a(x)) = \boldsymbol{a}$ for some $\boldsymbol{a} \in \mathbb{Z}_p^n$ and $1 \leq i \leq D$. We can identify $a(x)$ with $(a_1(x), a_2(x)) \in \mathcal{R}_1 \times \mathcal{R}_2$ and $\boldsymbol{a}$ with $(\boldsymbol{a}_1, \boldsymbol{a}_2) \in \mathbb{Z}_{p_1}^n \times \mathbb{Z}_{p_2}^n$ via CRT isomorphisms. Now, consider multiplying a constant $\mathrm{Inv}_{q_1}(q_2) \cdot q_2$. Observe the following.

- $(\mathrm{Inv}_{q_1}(q_2) \cdot q_2) \cdot \boldsymbol{a}_1 = (\mathrm{Inv}_{p_1}(q_2) \cdot q_2) \cdot \boldsymbol{a}_1 = \boldsymbol{a}_1 \in \mathbb{Z}_{p_1}^n$

– $(\mathrm{Inv}_{q_1}(q_2) \cdot q_2) \cdot \boldsymbol{a}_2 = \mathrm{Inv}_{q_1}(q_2) \cdot \mathbf{0} = \mathbf{0} \in \mathbb{Z}_{p_2}^n$
– $(\mathrm{Inv}_{q_1}(q_2) \cdot q_2) \cdot a_1(x) = 1 \cdot a_1(x) = a_1(x) \in \mathcal{R}_1$
– $(\mathrm{Inv}_{q_1}(q_2) \cdot q_2) \cdot a_2(x) = \mathrm{Inv}_{q_1}(q_2) \cdot 0 = 0 \in \mathcal{R}_2$

That is, if $\mathsf{Unpack}_i(a_1(x), a_2(x)) = (\boldsymbol{a}_1, \boldsymbol{a}_2)$ then $\mathsf{Unpack}_i(a_1(x), 0) = (\boldsymbol{a}_1, \mathbf{0})$. The similar holds for $j = 2$. Then, we can construct $\mathcal{P}^{(1)}$ and $\mathcal{P}^{(2)}$ with appropriate projections and injections. The other direction is more direct. For the full proof, see the full version of this paper [14]. □

According to Prop. 1 and 2, to study degree-D packing methods for copies of a finite field $\mathbb{F}_{p^k}$ into $\mathbb{Z}_q[x]/f(x)$, it is enough to study degree-D packing methods into $\mathbb{Z}_{p^t}[x]/f(x)$ for some $t \geq 1$. The similar holds for packing methods for copies of $\mathbb{Z}_p$ according to Prop. 1, 2, and 3. That is, to study degree-D packing methods for copies of $\mathbb{Z}_p$ into $\mathbb{Z}_q[x]/f(x)$ where p is an arbitrary integer, it is enough to study degree-D packing methods for $\mathbb{Z}_{p^k}^n$ into $\mathbb{Z}_{p^t}[x]/f(x)$ for some $t \geq k$ where p is a prime.

Therefore, from now on, we focus on packing methods for $\mathbb{Z}_{p^k}^n$ or $\mathbb{F}_{p^k}^n$ into $\mathbb{Z}_{p^t}[x]/f(x)$ where p is a prime. (Afterwards, p is a fixed prime, even if it is not explicitly stated.) This is not only because they are the most interesting case containing $\mathbb{Z}_{2^k}$ and $\mathbb{F}_{2^k}$, but also because they play roles as building blocks when constructing general packing methods (Prop. 2, 3). We note that the properties of packing methods, which we examine in the following sections (level-consistency in Section 6 and surjectivity in Section 7), are preserved by the constructions in Prop. 2 and 3.

4 More Examples

In continuation of Section 3.1, we give more examples on packing methods. The following examples are degree-2 packing methods for $\mathbb{Z}_{2^k}$-messages, which are (or can be) used to construct HE-based MPC protocol over $\mathbb{Z}_{2^k}$ following the approach of SPDZ [21]. Most of definitions and statements in this paper are motivated from these examples.

4.1 HELib Packing

In Example 2, we introduced the conventional HE packing method for $\mathbb{Z}_q$-messages into $\mathbb{Z}_q[x]/\Phi_M(x)$, where M is a power-of-two and $q = 1 \pmod{M}$. However, it is not always applicable, e.g. if we consider $\mathbb{Z}_{2^k}$-messages. The problem here is that $\Phi_M(X)$ never fully splits in $\mathbb{Z}_{2^k}$. One way to detour this problem is the following. It was first proposed by Gentry-Halevi-Smart [24] and generalized by Halevi-Shoup [26] to optimize *bootstrapping* procedure for fully homomorphic encryption (particularly, for HELib [25]). In this paper, we will refer this method as HELib packing.

To construct a packing method for $\mathbb{Z}_{p^k}$-messages into $\mathbb{Z}_{p^k}[x]/\Phi_M(x)$, choose M to satisfy $\gcd(M, p) = 1$. Let $\Phi_M(x)$ factor into r distinct degree-d irreducible polynomials in $\mathbb{Z}_p[x]$, where $d := \mathrm{ord}_M(p)$. Then, we have the factorization $\Phi_M(x) = \prod_{i=1}^{r} f_i(x)$ in $\mathbb{Z}_{p^k}[x]$ via Hensel lifting and the CRT ring isomorphism $\mathbb{Z}_{p^k}[x]/\Phi_M(x) \cong \prod_{i=1}^{r} \mathbb{Z}_{p^k}[x]/f_i(x)$. The packing algorithm Pack puts i-th $\mathbb{Z}_{p^k}$-message at the constant term of $\mathbb{Z}_{2^k}[x]/f_i(x)$ and puts zeroes at the other coefficients. Define Unpack as the inverse of Pack. It is easy to see that $(\mathsf{Pack}, \mathsf{Unpack})$ defines a degree-∞ packing method. However, the HELib packing achieves very low packing density $1/d$.

4.2 Overdrive2k Packing

To design an efficient HE-based MPC protocol over $\mathbb{Z}_{2^k}$, Overdrive2k [31] constructed a degree-2 packing method for $\mathbb{Z}_{2^k}^n$ into $\mathbb{Z}_{2^k}[x]/\Phi_M(x)$, where M is odd (so yielding a CRT ring isomorphism $\mathbb{Z}_{2^k}[x]/\Phi_M(x) \cong \prod_{i=1}^{r} \mathbb{Z}_{2^k}[x]/f_i(x)$ with $\deg(f_i) = d$). For construction, they considered the following problem. Consider a subset A of $[0, d-1]$ with $A = \{a_1, \cdots, a_m\}$ so that $2a_i \neq a_j + a_k$ for all $(i, i) \neq (j, k)$ and $a_i + a_j < d$ for all i, j. The problem is to find the maximum value of $m = |A|$ with A for given d.[9] Given a solution m and A for given d, the packing algorithm of Overdrive2k at level-1 put i-th m messages in $\mathbb{Z}_{2^k}$ at the coefficients of x^{a_i} of an element in $\mathbb{Z}_{2^k}[x]/f_i(x)$ for $a_i \in A$ and put zeroes at the other coefficients. Then, via the ring homomorphism, we can pack $r \cdot m$ messages into a plaintext achieving the packing density of m/d. The authors Overdrive2k noted that the packing density of their method seems to follow the trend of approximately $d^{0.6}/d$.

Since the set A is carefully designed, if we multiply two packed plaintexts, the $(2 \cdot a_i)$-th coefficient of the result equals the multiplied value of a_i-th coefficients of the original plaintexts. That is, Overdrive2k packing is of degree-2. Note that Overdrive2k packing naturally extends to arbitrary degree-2 packing methods for $\mathbb{Z}_{p^k}^n$ into $\mathbb{Z}_{p^k}[x]/f(x)$.

4.3 MHz2k Packing

To further improve the packing density of Overdrive2k, MHz2k [13] construct a degree-2 packing method for $\mathbb{Z}_{2^k}$-messages into $\mathbb{Z}_{2^t}[x]/\Phi_M(x)$, where t is slightly larger than k. Their core idea is to pack messages at *evaluation points* via interpolation unlike Overdrive2k which rather pack at coefficients. The caveat here is, however, that the polynomial interpolation on $\mathbb{Z}_{2^k}$ is not always possible, e.g. there is no $f(x) \in \mathbb{Z}_{2^k}$ satisfying $f(0) = 1$ and $f(2) = 0$ simultaneously. In this context, they propose the *tweaked interpolation*, where they lift the target points of $\mathbb{Z}_{2^k}$ upto a larger ring $\mathbb{Z}_{2^{k+\delta}}$, multiplying an appropriate power-of-two to eliminate the effect of non-invertible elements.

Let $t = k + 2\delta$ and $\mathbb{Z}_{2^t}[x]/\Phi_M(x)$ factors into $\prod_{i=1}^{r} \mathbb{Z}_{2^t}[x]/f_i(x)$ via CRT, where $f_i(x)$ are all of degree-d. The packing algorithm at level-1 perform tweaked interpolation on i-th $\lfloor \frac{d+1}{2} \rfloor$ $\mathbb{Z}_{2^k}$-messages $\{\mu_{ij}\}$, so that we have $L_i(x) \in \mathbb{Z}_{2^t}[x]$

[9] Similar problems were also considered in other cryptography literature [29, 2, 18]. For more detailed discussions, see the full version [14].

which satisfies (i) $\deg(L_i) \leq \lfloor \frac{d-1}{2} \rfloor$ and (ii) $L_i(j) = \mu_{ij} \cdot 2^\delta$. Then, put $L_i(x)$ in the i-th CRT slot of $\mathbb{Z}_{2^t}[x]/\Phi_M(x)$, i.e. $\mathbb{Z}_{2^t}[x]/f_i(x)$. This gives us a packing density of roughly $k/(2k+2d)$. Since the degree condition on $L_i(x)$ and extra δ in the modulus are designed to avoid degree overflow and modulus overflow, when the product of two packings is given, we can decode the homomorphically multiplied messages without any loss of information. That is, we can unpack at level-2 by evaluating points on each CRT slot and observing the upper k bits of outputs.

Note that MHz2k packing can be naturally extended to a degree-D packing method for $\mathbb{Z}_{p^k}$-messages into $\mathbb{Z}_{p^t}[x]/\Phi_M(x)$ with $\gcd(M, p) = 1$ of density roughly

$$\frac{k}{D \cdot (k + \frac{d}{p-1})}.$$

4.4 Comparison

In this subsection, we compare some properties of the examples previously given in this section. These features are motivations of the definitions and results in later sections. This subsection is summarized in Table 1.

Table 1: Comparisons on degree-2 packing methods for $\mathbb{Z}_{2^k}$-messages

Method	HELib	Overdrive2k	MHz2k
Level-consistency	consistent	dependent	dependent
$t \stackrel{?}{=} k$	$t = k$	$t = k$	$t > k$
Density	$1/d$	$\approx d^{0.6}/d$	$\approx k/(2k+2d)$

Notice that, in HELib packing which is of degree-∞, packing algorithms and unpacking algorithms are identical for all level. We will later refer these kind of packings as *level-consistent* packings (Section 6). However, in Overdrive2k and MHz2k packing, the packing algorithm differs for each level. For example, in Overdrive2k packing, messages are coefficients of x^{a_i}'s at level-1, and coefficients of $x^{2 \cdot a_i}$'s at level-2. We will later refer these kind of packings as *level-dependent* packings (Section 6).

One big difference of MHz2k packing from the previous packings is that it uses larger modulus for polynomial ring than that of messages. The other packing methods are sort of coefficient packing, making it no use of increasing the modulus for polynomial ring. This difference will serve as one of the topics in Section 5 (e.g. Example 6).

Note that degree-2 MHz2k packing reaches density of nearly $1/2$ when k is sufficiently larger than d. This is true for typical parameters used in HE-based

MPC over $\mathbb{Z}_{2^k}$: $k = 64, 128, 196$ and $d \leq 20$. In Section 5, we will show that MHz2k packing achieves a certain form of near-optimality (Example 6).

We now examine common features of these methods. Note that there are *invalid* packings regarding to these packing methods. For example, in HELib packing, $a(x) \in \mathbb{Z}_{2^k}[x]/\Phi_M(x)$ is not a valid packing, i.e. $\mathsf{Unpack}(a(x)) = \perp$, if $a(x)$ modulo $f_i(x)$ is not a constant. We will later refer these kind of packings as non-*surjective* packings (Section 7).

Also notice that all these packings leverage CRT ring isomorphism, which is a natural and convenient way to achieve parallelism. They pack messages into each CRT slot in an identical and independent manner. We refer packing methods following this approach as *CRT packings*.

5 Bounds on Packing Density

In this section, we examine upper bounds on packing density of degree-D packing methods for $\mathbb{Z}_{p^k}$ and $\mathbb{F}_{p^k}$, where p is a prime (See Section 3.2).

5.1 Algebraic Background

We first remark some algebraic facts, which enable proofs in the following subsections.

Proposition 4. *When R is a principal ideal ring (PIR), every submodule of a free R-module of rank n can be finitely generated with n generators.*

Proof. See the full version of this paper [14]. □

Remark 3. Note that $\mathbb{Z}_{p^t}$ is a local PIR. Consider $\mathcal{R} := \mathbb{Z}_{p^t}[x]/f(x)$ as a free $\mathbb{Z}_{p^t}$-module with the rank $\deg(f)$. Then by Nakayama's lemma, the cardinality of minimal generating sets is a well-defined invariant for submodules of $\mathcal{R}$.

Let $\mathcal{A}$ be a linearly independent subset of $\mathcal{R}$. Then, since the span $\langle \mathcal{A} \rangle$ is a submodule of $\mathcal{R}$ with a minimal generating set $\mathcal{A}$, inequality $\deg(f) \geq |\mathcal{A}|$ holds by Prop. 4.

5.2 Packing Density of $\mathbb{Z}_{p^k}$-Message Packings

In this subsection, we examine upper bounds on packing density of degree-D $\mathbb{Z}_{p^k}$-message packings. We begin with an upper bound for degree-1 packing methods: we cannot pack copies of $\mathbb{Z}_{p^k}$ more than the degree of the quotient polynomial. Unlike the simple and plausible statement, the proof is quite involved. In particular, it depends on Remark 3. The following proposition says that we cannot reduce the degree of quotient polynomial significantly and tower the packings along a large modulus. Notice that there are no restriction on t and $f(x)$.

Proposition 5. *There exists a degree-*1 *packing method for $\mathbb{Z}_{p^k}^n$ into $\mathcal{R} := \mathbb{Z}_{p^t}[x]/f(x)$ with $k \leq t$, only if $n \leq \deg(f)$.*

Proof. Let $(\mathsf{Pack}_1, \mathsf{Unpack}_1)$ be a degree-1 packing method for $\mathbb{Z}_{p^k}^n$ into $\mathcal{R}$. For each $i \in [n]$, choose $a_i(x) \in \mathcal{R}$ such that $\mathsf{Unpack}_1(a_i(x)) = \boldsymbol{e}_i$. View $\mathcal{R}$ as a free $\mathbb{Z}_{p^t}$-module of rank $\deg(f)$, and consider the submodule $\langle a_1(x), \cdots, a_n(x)\rangle$. By linear homomorphic property (Remark 1), when $\sum_{i=1}^n c_i \cdot a_i(x) = 0$ for some $c_i \in \mathbb{Z}_{p^t}$, then $c_i = 0 \pmod{p^k}$ must hold. Thus, $\{a_1(x), \cdots, a_n(x)\}$ is a minimal generating set of $\langle a_1(x), \cdots, a_n(x)\rangle$, and therefore $n \leq \deg(f)$ holds (Remark 3). $\square$

In the rest of this subsection, we narrow our scope to packing methods for $\mathbb{Z}_{p^k}^n$ into $\mathbb{Z}_{p^k}[x]/f(x)$ with the same modulus. Indeed, this setting is less general. Nonetheless, our results still have interesting consequences (See Example 6 - 9). The following is a small remark on packings of non-zero elements modulo p in this setting.

Remark 4. Let $(\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^D$ be a degree-D packing method for $\mathbb{Z}_{p^k}^n$ into $\mathcal{R} := \mathbb{Z}_{p^k}[x]/f(x)$. For any $i \in [D]$, if $\mathsf{Unpack}_i(a(x)) = \boldsymbol{a}$ for some $\boldsymbol{a} \in \mathbb{Z}_{p^k}^n$ which is non-zero modulo p, then $a(x)$ is also non-zero modulo p. Otherwise, $\mathsf{Unpack}_i(p^{k-1} \cdot a(x)) = \mathsf{Unpack}_i(0) = \mathbf{0} \neq p^{k-1} \cdot \boldsymbol{a}$, contradicting the linear homomorphic property (Remark 1). In particular, when $f(x)$ is an irreducible polynomial in $\mathbb{Z}_p[x]$, such $a(x)$ is a unit in $\mathcal{R}$.

Roughly speaking, our main result is that we cannot pack more than d/D $\mathbb{Z}_{p^k}$-messages into $\mathbb{Z}_{p^k}[x]/f(x)$ while satisfying degree-D homomorphic property, where $d = \deg(f)$. Intuitively, the statement can be understood as that we must pack the inputs into lower d/D coefficients since reduction by the quotient polynomial act as randomization and will ruin the structure of packing. However, the proof is much more involved since we have to handle all possible packing methods. Notice that the following theorem subsumes Prop. 5 as the $D = 1$ case in the $t = k$ setting. The essence of the proof is a generic construction of a large set which is required to be linearly independent regardless of specific structures of packing methods.

Theorem 1. *There exists a degree-D packing method for $\mathbb{Z}_{p^k}^n$ into $\mathcal{R} := \mathbb{Z}_{p^k}[x]/f(x)$ where $f(x) \in \mathbb{Z}_{p^k}[x]$ is a degree-d irreducible polynomial modulo p, only if $d \geq D \cdot (n-1) + 1$.*

Proof. Let $(\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^D$ be a degree-D packing method for $\mathbb{Z}_{p^k}^n$ into $\mathcal{R}$. For each $i \in [n]$, choose $a_i(x) \in \mathcal{R}$ such that $\mathsf{Unpack}_1(a_i(x)) = \boldsymbol{e}_i$. Let us denote $\mathcal{A}^{(r,s)} := \{a_1(x)^r \cdot a_j(x)^s\}_{1<j\leq n}$. For example, $\mathcal{A}^{(0,D)} = \{a_2(x)^D, \cdots, a_n(x)^D\}$, $\mathcal{A}^{(D,0)} = \{a_1(x)^D\}$, and $\mathcal{A}^{(1,D-1)} = \{a_1(x)a_2(x)^{D-1}, \cdots, a_1(x)a_n(x)^{D-1}\}$.

Step 1: Consider the following set of level-t packings.

$$\mathcal{A}_t := \bigcup_{\substack{r+s=t \\ 0<s}} \mathcal{A}^{(r,s)}$$

We will show that $\mathcal{A}_t$ is linearly independent in $\mathcal{R}$ for all $t \leq D$ by induction on t. The case where $t = 1$ is true by the linear homomorphic property at level-1 (Remark 1): $\mathcal{A}_1 = \{a_2(x), \cdots, a_n(x)\}$ (See also Prop. 5).

Suppose $\mathcal{A}_t$ is linearly independent for some $t < D$. View $\mathcal{A}_{t+1}$ as $\mathcal{A}^{(0,t+1)} \cup a_1(x) \cdot \mathcal{A}_t$. Suppose $\sum_{a_\alpha(x) \in \mathcal{A}_{t+1}} (c_\alpha \cdot a_\alpha(x)) = 0$, for some $c_\alpha \in \mathbb{Z}_{p^k}$. Then, by linear homomorphic property at level-$(t+1)$, $c_\alpha = 0$ must hold for all $a_\alpha(x) \in \mathcal{A}^{(0,t+1)}$, since elements of $a_1(x) \cdot \mathcal{A}_t$ unpack to $\mathbf{0}$ and $\mathcal{A}^{(0,t+1)}$ unpacks to a linearly independent set by construction. Subsequently, we have again the following equality:

$$\sum_{a_\alpha(x) \in a_1(x) \cdot \mathcal{A}_t} (c_\alpha \cdot a_\alpha(x)) = 0.$$

Meanwhile, since $a_1(x)$ is a unit in $\mathcal{R}$ (Remark 4) and $\mathcal{A}_t$ is linearly independent by induction hypothesis, $c_\alpha = 0$ must also hold for all $a_\alpha(x) \in a_1(x) \cdot \mathcal{A}_t$. Thus, $\mathcal{A}_t$ is linearly independent in $\mathcal{R}$ for all $t \leq D$.

Step 2: Now consider the set $\mathcal{A} := \mathcal{A}_D \cup \{a_1(x)^D\}$, which coincides with $\{a_1(x)^D, \cdots, a_n(x)^D\} \cup a_1(x) \cdot \mathcal{A}_{D-1}$. Suppose $\sum_{a_p(x) \in \mathcal{A}} (c_\alpha \cdot a_\alpha(x)) = 0$, for some $c_\alpha \in \mathbb{Z}_{p^k}$. Then, by linear homomorphic property at level-D, $c_\alpha = 0$ must hold for all $a_\alpha(x) \in \{a_1(x)^D, \cdots, a_n(x)^D\}$, since elements of $a_1(x) \cdot \mathcal{A}_{D-1}$ unpack to $\mathbf{0}$ and $\{a_1(x)^D, \cdots, a_n(x)^D\}$ unpacks to a linearly independent set by construction. Subsequently, we have again the following equality:

$$\sum_{a_\alpha(x) \in a_1(x) \cdot \mathcal{A}_{D-1}} (c_\alpha \cdot a_\alpha(x)) = 0.$$

Meanwhile, since $a_1(x)$ is a unit in $\mathcal{R}$ and $\mathcal{A}_{D-1}$ is linearly independent by Step 1, $c_\alpha = 0$ must also hold for all $a_\alpha(x) \in a_1(x) \cdot \mathcal{A}_{D-1}$. Thus, $\mathcal{A}$ is linearly independent, and therefore $d \geq |\mathcal{A}| = D(n-1) + 1$ must hold (Remark 3). $\square$

The following are direct consequences of our theorem.

Example 6. Degree-D packing methods for $\mathbb{Z}_{p^k}$-messages into $\mathbb{Z}_{p^k}[x]/f(x)$, where $f(x)$ is a degree-d irreducible polynomial modulo p, have packing density of no larger than $\frac{1}{D} + \frac{1}{d} \cdot (1 - \frac{1}{D})$. Consequently, degree-$D$ *CRT* packing methods for $\mathbb{Z}_{p^k}$-messages into $\mathbb{Z}_{p^k}[x]/f(x)$, where $f(x)$ factors into r distinct irreducible factors modulo p, have packing density of no larger than $\frac{1}{D} + \frac{r}{\deg(f)} \cdot (1 - \frac{1}{D})$ (Section 4.4). In particular, degree-D CRT packing methods for $\mathbb{Z}_{2^k}$-messages into $\mathbb{Z}_{2^t}[x]/\Phi_M(x)$, where M is odd and $\Phi_M(x)$ factors into distinct degree-d irreducible factors modulo p, have packing density of no larger than $\frac{1}{D} + \frac{1}{d} \cdot (1 - \frac{1}{D})$.

That is, when parameters are carefully chosen, the MHz2k packing already nearly reach the optimal packing density for packing methods for $\mathbb{Z}_{p^k}$-messages into $\mathbb{Z}_{p^k}[x]/f(x)$ (Section 4.3). Thus, if one wants to construct a degree-D packing method for $\mathbb{Z}_{2^k}$-messages into $\mathbb{Z}_{2^t}[x]/\Phi_M(x)$ with substantially better density than the MHz2k packing, the only possibility is choosing $t > k$ or not employing the CRT approach.

Example 7 (RMFE over Galois Ring). Consider RMFE *over Galois rings* for copies of $\mathbb{Z}_{p^k}$ into a larger Galois ring isomorphic to $\mathbb{Z}_{p^k}[x]/f(x)$, which is exactly the setting of Thm. 1. The theorem states that such RMFE cannot have packing density larger than $\frac{1}{2} + \frac{1}{2\deg(f)}$. To the best of our knowledge, this is the first upper bound result on packing density of RMFE over Galois rings. Our theorem also yields upper bounds on packing density of degree-D generalization of RMFE over Galois rings.

Example 8. For $D > 1$, consider degree-D packing methods for $\mathbb{Z}_{p^k}$-messages into $\mathbb{Z}_{p^t}[x]/f(x)$, where $f(x)$ is irreducible modulo p. By Prop. 5, when $t > k$, we cannot achieve a perfect packing density 1. When $t = k$, we cannot achieve a perfect packing density 1 unless $\deg(f) = 1$, by Thm. 1. That is, there is no perfect degree-D packing method for $\mathbb{Z}_{p^k}$-messages into $\mathbb{Z}_{p^t}[x]/f(x)$, when $f(x)$ is irreducible modulo p and $\deg(f) > 1$.

Example 9. For $D > 1$, consider degree-D packing methods for $\mathbb{Z}_{p^k}$-messages into $\mathbb{Z}_{p^t}[x]/f(x)$, where $f(x)$ is square-free modulo p. By Example 8, there is no perfect degree-D CRT packing method for $\mathbb{Z}_{p^k}$-messages into $\mathbb{Z}_{p^t}[x]/f(x)$, unless $f(x)$ splits into distinct linear factors. In particular, there is no perfect degree-D CRT packing method for $\mathbb{Z}_{2^k}$-messages into $\mathbb{Z}_{2^t}[x]/\Phi_M(x)$ when M is odd.

5.3 Packing Density of $\mathbb{F}_{p^k}$-Message Packings

In this subsection, we examine upper bounds on packing density of degree-D $\mathbb{F}_{p^k}$-message packings. We begin with an upper bound for degree-1 packing methods, which is an analogue of Prop. 5. Unlike the simple and plausible statement, the proof is quite involved. In particular, it depends on Remark 3. The following proposition says that we cannot reduce the degree of quotient polynomial significantly and tower the packings along a large modulus. Notice that there are no restriction on t and $f(x)$.

Proposition 6. *There exists a degree-1 packing method for $\mathbb{F}_{p^k}^n$ into $\mathcal{R} := \mathbb{Z}_{p^t}[x]/f(x)$, only if $n \cdot k \leq \deg(f)$.*

Proof. Let $(\mathsf{Pack}_1, \mathsf{Unpack}_1)$ be a degree-1 packing method for $\mathbb{F}_{p^k}^n$ into $\mathcal{R}$. Fix a basis of $\mathbb{F}_{p^k}$ as $\{\beta_1, \cdots, \beta_k\}$. For each $i \in [n]$ and $j \in [k]$, choose $a_{ij}(x) \in \mathcal{R}$ such that $\mathsf{Unpack}_1(a_{ij}(x)) = \beta_j \cdot \boldsymbol{e}_i$. View $\mathcal{R}$ as a free $\mathbb{Z}_{p^t}$-module of rank $\deg(f)$, and consider the submodule $\langle a_{ij}(x)\rangle_{i\in[n],j\in[k]}$. By linear homomorphic property (Remark 1), when $\sum_{i=1}^n c_{ij} \cdot a_{ij}(x) = 0$ for $c_i \in \mathbb{Z}_{p^t}$, then $c_i = 0 \pmod p$ must hold. Thus, $\{a_{ij}(x)\}_{i\in[n],j\in[k]}$ is a minimal generating set of $\langle a_{ij}(x)\rangle_{i\in[n],j\in[k]}$, and therefore $n \cdot k \leq \deg(f)$ holds (Remark 3). $\square$

In the rest of this subsection, we narrow our scope to packing methods for $\mathbb{F}_{p^k}^n$ into $\mathbb{Z}_p[x]/f(x)$ with the prime modulus. Indeed, this setting is less general. Nonetheless, our results still have interesting consequences (See Example 10 - 13).

Our main result in this subsection is the following theorem, which is a finite field analogue of Thm. 1. However, it is much more involved since we must also handle the multiplicative structure inside $\mathbb{F}_{p^k}$. Notice that our theorem subsumes Prop. 6 as the $D = 1$ case in the $t = 1$ setting. The essence of the proof is again a generic construction of a large set which is required to be linearly independent regardless of specific structures of packing methods.

Theorem 2. *Let $\mathcal{B} := \{\beta_1, \cdots, \beta_k\}$ be a basis of $\mathbb{F}_{p^k}$ as a $\mathbb{F}_p$-vector space. There exists a degree-D packing method for $\mathbb{F}_{p^k}^n$ into $\mathcal{R} := \mathbb{Z}_p[x]/f(x)$ where $f(x) \in \mathbb{Z}_p[x]$ is a degree-d irreducible polynomial modulo p, only if the following inequality holds.*

$$d \geq \dim\langle \beta_1^D, \cdots, \beta_k^D \rangle + (n-1) \sum_{t=1}^{D} \dim\langle \beta_1^t, \cdots, \beta_k^t \rangle$$

Proof (Sketch). Similar to the proof of Thm. 1. See the full version [14]. □

To have a more concrete bound, we prove the following proposition. Let $\sigma_{p^k}^{(t)}$ denote the multiplicative order of p modulo $\frac{p^k-1}{\gcd(p^k-1,t)}$.

Proposition 7. *Let β be a primitive element of $\mathbb{F}_{p^k}$. Regarding the primitive element basis $\{1, \beta, \beta^2, \cdots, \beta^{k-1}\}$, the following equality holds.*

$$\dim\langle 1^t, \beta^t, \beta^{2t}, \cdots, \beta^{(k-1)t} \rangle = \sigma_{p^k}^{(t)}$$

Proof. Observe that $\dim\langle 1^t, \beta^t, \beta^{2t}, \cdots, \beta^{(k-1)t} \rangle$ is equal to the degree of the minimal polynomial of β^t in $\mathbb{F}_p[x]$. The degree of the minimal polynomial of β^t is again equal to the length of the orbit of β^t regarding Frobenius map $x \mapsto x^p$. Since β is a primitive element, we are finding the smallest $s \in \mathbb{Z}^+$ satisfying $t = t \cdot p^s \pmod{p^k - 1}$, which is $\sigma_{p^k}^{(t)}$ by definition. □

Corollary 1. *There exists a degree-D packing method for $\mathbb{F}_{p^k}^n$ into $\mathcal{R} := \mathbb{Z}_p[x]/f(x)$ where $f(x) \in \mathbb{Z}_p[x]$ is a degree-d irreducible polynomial modulo p, only if the following inequality holds.*

$$d \geq \sigma_{p^k}^{(D)} + (n-1) \sum_{t=1}^{D} \sigma_{p^k}^{(t)}$$

Proof. Choose a primitive element β of $\mathbb{F}_{p^k}$ and apply Thm. 2 on the basis $\{1, \beta, \beta^2, \cdots, \beta^{k-1}\}$ with the help of Prop. 7. □

The following are some consequences of our main result.

Example 10 (RMFE). Note that $\sigma_{p^k}^{(1)}$ and $\sigma_{p^k}^{(2)}$ are always k. Then, by Cor. 1, degree-2 packing methods for $\mathbb{F}_{p^k}$-messages into $\mathbb{Z}_p[x]/f(x)$, where $f(x)$ is a degree-d irreducible polynomial, have packing density of no larger than $\frac{1}{2} + \frac{k}{2d}$. That is, packing density of RMFE is upper bounded by $\frac{1}{2} + \frac{k}{2d}$. This is a known result (See [17]). However, previous proofs do not extend to higher-degree cases (See Example 12) or to the Galois ring case (See Example 7).

Example 11 (Degree-2 Packing). By Example 10, degree-2 *CRT* packing methods for $\mathbb{F}_{p^k}$-messages into $\mathbb{Z}_p[x]/f(x)$, where $f(x)$ factors into r distinct irreducible factors, have packing density of no larger than $\frac{1}{2}+\frac{r\cdot k}{2\deg(f)}$ (Section 4.4). In particular, degree-2 CRT packing methods for $\mathbb{F}_{2^k}$-messages into $\mathbb{Z}_2[x]/\Phi_M(x)$, where M is odd and $\Phi_M(x)$ factors into distinct degree-d irreducible factors modulo 2, have packing density of no larger than $\frac{1}{2}+\frac{k}{2d}$.

Suppose one wants to design a degree-2 packing method for $\mathbb{F}_{p^k}$-messages into $\mathbb{Z}_{p^t}[x]/f(x)$ which has a packing density substantially larger than 1/2. Note that choosing $t \geq 2$ already yields packing density no larger than 1/2 by Prop. 6. Thus, only possibility is not employing the CRT approach.

Example 12 (Degree-3 Packing). Note that $\sigma_{p^k}^{(3)}$ is always k, except the case of $p^k = 4$. Then, by Cor. 1, degree-3 packing methods for $\mathbb{F}_{p^k}$-messages into $\mathbb{Z}_p[x]/f(x)$, where $f(x)$ is a degree-d irreducible polynomial, have packing density of no larger than $\frac{1}{3}+\frac{2k}{3d}$, unless $p^k = 4$. Consequently, degree-3 *CRT* packing methods for $\mathbb{F}_{p^k}$-messages into $\mathbb{Z}_p[x]/f(x)$, where $f(x)$ factors into r distinct irreducible factors, have packing density of no larger than $\frac{1}{3}+\frac{2r\cdot k}{3\deg(f)}$. In particular, degree-3 CRT packing methods for $\mathbb{F}_{2^k}$-messages into $\mathbb{Z}_2[x]/\Phi_M(x)$, where M is odd and $\Phi_M(x)$ factors into distinct degree-d irreducible factors modulo 2, have packing density of no larger than $\frac{1}{3}+\frac{2k}{3d}$, given $k \neq 2$.

Suppose one wants to design a degree-3 packing method for $\mathbb{F}_{p^k}$-messages into $\mathbb{Z}_{p^t}[x]/f(x)$ which has a packing density substantially larger than 1/3. Note that choosing $t \geq 3$ already yields packing density no larger than 1/3 by Prop. 6. Thus, only possibility is choosing $t = 2$ or not employing the CRT approach.

Example 13. By the same arguments as in Example 8 and 9, we have the following: For $D > 1$, there is no perfect degree-D packing method for $\mathbb{F}_{p^k}$-messages into $\mathbb{Z}_{p^t}[x]/f(x)$, when $f(x)$ is irreducible modulo p and $\deg(f) > 1$. Thus, there is no perfect degree-D CRT packing method for $\mathbb{F}_{p^k}$-messages into $\mathbb{Z}_{p^t}[x]/f(x)$, unless $f(x)$ splits into distinct linear factors. In particular, there is no perfect degree-D CRT packing method for $\mathbb{F}_{2^k}$-messages into $\mathbb{Z}_{2^t}[x]/\Phi_M(x)$ when M is odd.

6 Level-consistency

In this section, we define and examine the concept of *level-consistency*, which is a favorable property for a packing method to have. Our main results are necessary and sufficient conditions for a polynomial ring to allow a level-consistent packing method for $\mathbb{Z}_{p^k}$ and $\mathbb{F}_{p^k}$, where p is a prime (See Section 3.2). They limit the achievable efficiency of level-consistent packing methods, yielding the impossiblity of designing an efficient packing methods while satisfying level-consistency.

6.1 Definition and Basic Facts

Definition 6. *For $D > 1$, a degree-D packing method* $(\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^{D}$ *is called* level-consistent *if* Unpack_i *is all identical for $1 \le i \le D$. Otherwise, we say a packing method is* level-dependent.

The notion of level-consistency captures the property whether packings are decodable in an identical way at different levels (Prop. 8). In an algebraic viewpoint, a level-consistent packing has a single Unpack for all levels, which is a *ring homomorphism* defined on where it does not abort. The level-consistency is a desirable feature, as it allows homomorphic computation between different packing levels. On the other hand, when working with level-dependent packing methods, we must be careful about whether the operands are packed in the same packing level as we perform homomorphic computation on packed messages.

For instance, Overdrive2k [31] and MHz2k [13] design and utilize $\mathbb{Z}_{2^k}$-message packing methods, which are *level-dependent*, to construct HE-based MPC protocols over $\mathbb{Z}_{2^k}$ following the approach of SPDZ [21]. Their level-dependency complicates the so-called *reshare* protocol which re-encrypts a *level-zero* HE ciphertext to a *fresh* ciphertext allowing two-level HE to be sufficient for their purpose. The problem here is that a masking HE ciphertext is used twice in the reshare protocol: once to mask the input ciphertext of level-zero and once to reconstruct the fresh ciphertext of level-one by subtracting it. While the difference of HE levels can be managed easily with modulus-switching, that of the packing levels seems to be problematic.

In order to remedy this issue caused by level-dependency, Overdrive2k and MHz2k had to come up with their own solutions. Overdrive2k provides two masking ciphertexts having the *same messages* but in *different packing*: one with level-zero packing and the other with level-one packing. However, this solution substantially degrades the efficiency of the protocol. MHz2k resolves this issue by a technical trick which does not cause any extra cost, closing the gap between the level-consistent and level-dependent packing methods in this case.

This issue does not arise in SPDZ-family [21, 19, 27, 1] over a finite field $\mathbb{Z}_p$, where the conventional packing method is already level-consistent (See Example 2). For detailed discussion, refer to [13]. In a later subsection, we prove the impossibility of designing an efficient $\mathbb{Z}_{2^k}$-message packings while satisfying level-consistency. This justifies the use of *level-dependent* packings in SPDZ-like MPC protocols over $\mathbb{Z}_{2^k}$ and highlights the usefulness of the trick proposed by MHz2k [13].

The following proposition says that a level-consistent packing method can be trivially extended to an arbitrary degree.

Proposition 8. *A level-consistent degree-D packing method $\mathcal{P}$ can be extended to a level-consistent degree-D' packing method $\mathcal{P}'$ for arbitrary $D' > D$.*

Proof. When $\mathcal{P}$ is $(\mathsf{Pack}_i, \mathsf{Unpack})_{i=1}^{D}$, just define $\mathcal{P}'$ as $(\mathsf{Pack}_1, \mathsf{Unpack})_{i=1}^{D'}$. □

A crucial tool when dealing with a level-consistent packing method is idempotents. We extensively leverage the concept of idempotents and their properties when proving our main results on level-consistency. Here, we list properties of idempotents which are used afterwards.

Proposition 9. *Let R be a finite ring. For all $a \in R$, there exists a positive integer s such that a^s is idempotent, i.e. $a^{2s} = a^s$.*

Proof. See the full version of this paper [14]. □

Proposition 10. *Let R and $\mathcal{R}$ be rings. Let $\mathcal{P}$ be a level-consistent packing method for R^n into $\mathcal{R}$ with identical unpacking algorithms* Unpack*. For any idempotent $\boldsymbol{a} \in R^n$, there exists an idempotent $a(x) \in \mathcal{R}$ such that $\mathsf{Unpack}(a(x)) = \boldsymbol{a}$.*

Proof. First, extend $\mathcal{P}$ to a degree-D packing method for a sufficiently large D (Prop. 8). Let $\boldsymbol{a} \in R^n$ be idempotent. Choose an element $\tilde{a}(x) \in \mathcal{R}$ such that $\mathsf{Unpack}(\tilde{a}(x)) = \boldsymbol{a}$. By Prop. 9, there exists $s \in \mathbb{Z}^+$ such that $a(x) := \tilde{a}(x)^s$ is idempotent in $\mathcal{R}$. Then, $\mathsf{Unpack}(a(x)) = \mathsf{Unpack}(\tilde{a}(x)^s) = \boldsymbol{a}^s = \boldsymbol{a}$ holds. □

Proposition 11. *For a prime p, let $\mathcal{R} := \mathbb{Z}_{p^t}[x]/f(x)$ and $f(x) = g(x)^\ell \pmod p$, where $g(x)$ is an irreducible polynomial in $\mathbb{F}_p[x]$. Then, an idempotent element of $\mathcal{R}$ is either 0 or 1.*

Proof. See the full version of this paper [14]. □

Another tool which is useful when dealing with level-consistent packing methods is nilpotents. The following proposition says any nilpotent must unpack to a nilpotent, given it is a valid packing regarding to a level-consistent method.

Proposition 12. *Let R and $\mathcal{R}$ be rings, and let $\mathcal{P}$ be a level-consistent packing method for R^n into $\mathcal{R}$ with identical unpacking algorithms* Unpack*. For any nilpotent $a(x) \in \mathcal{R}$, $\mathsf{Unpack}(a(x))$ outputs a nilpotent $\boldsymbol{a} \in R^n$ or a failure $\perp$.*

Proof. Suppose $\mathsf{Unpack}(a(x))$ outputs $\boldsymbol{a} \in R^n$. Let s be a positive integer such that $a(x)^s = 0$ in $\mathcal{R}$. Extend $\mathcal{P}$ to a degree-s packing method (Prop. 8). Then, $\boldsymbol{a}^s = \mathsf{Unpack}(a(x)^s) = \mathsf{Unpack}(0) = \mathbf{0}$ holds. □

Lastly, we introduce the notion of *one-to-one* packing which plays an important role in the proof of our main result.

Definition 7 (One-to-one Packing). *Let R and $\mathcal{R}$ be rings. We say a packing method $(\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^D$ for R^n into $\mathcal{R}$ is* one-to-one*, if there is unique $a(x) \in \mathcal{R}$ such that $\mathsf{Unpack}_i(a(x)) = \boldsymbol{a}$ for all $\boldsymbol{a} \in R^n$ and $i \in [D]$.*

6.2 Level-consistency in $\mathbb{Z}_{p^k}$-Message Packings

Our main result on level-consistency in $\mathbb{Z}_{p^k}$-message packings is the following theorem. Our theorem illustrates a necessary condition for a surjective packing method for $\mathbb{Z}_{p^k}$-messages to exist. As mentioned, the proof regards the notion of idempotents (Prop. 10, 11).

Theorem 3. *For a prime p, let $f(x) \in \mathbb{Z}_{p^t}[x]$ have exactly r distinct irreducible factors in $\mathbb{Z}_p[x]$. There exists a level-consistent packing method for $\mathbb{Z}_{p^k}^n$ into $\mathbb{Z}_{p^t}[x]/f(x)$ only if $n \le r$.*

Proof. Let $f(x)$ be factorized into $\prod_{i=1}^r \bar{f}_i(x)$ in $\mathbb{Z}_p[x]$, where each $\bar{f}_i(x)$ is a power of a distinct irreducible polynomial in $\mathbb{Z}_p[x]$. The factorization can be lifted upto $\mathbb{Z}_{p^t}[x]$ via Hensel lifting. Let $f(x) = \prod_{i=1}^r f_i(x)$, where $f_i(x) \in \mathbb{Z}_{p^t}[x]$ is the Hensel lift of $\bar{f}_i(x)$ satisfying $\bar{f}_i(x) = f_i(x) \pmod p$. By Prop. 11, there are 2^r idempotents in $\mathbb{Z}_{p^t}[x]/f(x) \approx \prod_{i=1}^r \mathbb{Z}_{p^t}[x]/f_i(x)$, namely $\{0,1\}^r$. Also note that there are 2^n idempotents in $\mathbb{Z}_{p^k}^n$, namely $\{0,1\}^n$.

By Prop. 10, for each idempotent $\boldsymbol{a}$ of $\mathbb{Z}_{p^k}^n$, there is a distinct idempotent $a(x)$ of $\mathbb{Z}_{p^t}[x]/f(x)$ such that $\mathsf{Unpack}(a(x)) = \boldsymbol{a}$. Thus, the number of idempotents in $\mathbb{Z}_{p^k}^n$ cannot be larger than that of $\mathbb{Z}_{p^t}[x]/f(x)$, and $n \le r$ holds. $\square$

The following are some consequences of Thm. 3. We begin with an optimality result for HELib packing (Section 4.1).

Example 14. Essentially, Thm. 3 asserts that HELib packing offers the optimal packing density if level-consistency is required. As level-consistency is more than a favorable feature for *fully* homomorphic encryption(FHE), our result reassures that HELib packing is an excellent packing method to use for FHE, and it strongly justifies long line of researches based on such packing method [24, 26, 9].

The following examples illustrate the hardness of designing an efficient HE packing method for $\mathbb{Z}_{2^k}$-messages while satisfying level-consistency. We have similar results for $\mathbb{Z}_{p^k}$-messages with $p \neq 2$.

Example 15. When $M = 2^m$, since $\Phi_M(x) = (x+1)^{2^{m-1}}$ in $\mathbb{F}_2[x]$, we can pack at most one copy of $\mathbb{Z}_{2^k}$ into $\mathbb{Z}_{2^t}[x]/\Phi_M(x)$ while satisfying level-consistency.

Example 16. When M is an odd, $\Phi_M(x)$ factors into a product of distinct irreducible polynomials of degree $d = \mathrm{ord}_M(2)$ in $\mathbb{F}_2[x]$. Let $\phi(M) = r \cdot d$. Then, we can pack at most r copies of $\mathbb{Z}_{2^k}$ into $\mathbb{Z}_{2^t}[x]/\Phi_M(x)$ while satisfying level-consistency. Note that, since $d > \log M$ by definition, $r < \phi(M)/\log M$.

Example 17. When $M = 2^s \cdot M'$, where M' is an odd, $\Phi_M(x) = \Phi_{M'}(-x^{2^{s-1}}) = \Phi_{M'}(x)^{2^{s-1}}$ in $\mathbb{F}_2[x]$. Thus, we cannot pack more copies of $\mathbb{Z}_{2^k}$ into $\mathbb{Z}_{2^t}[x]/\Phi_M(x)$ than $\mathbb{Z}_{2^t}[x]/\Phi_{M'}(x)$ while satisfying level-consistency.

Thm. 3 also yields the impossibility of level-consistent RMFEs over Galois ring for $\mathbb{Z}_{p^k}$-messages.

Example 18. In $GR(p^t, d) \cong \mathbb{Z}_{p^t}[x]/f(x)$ with a degree-d $f(x)$ which is irreducible modulo p, we can pack at most one copy of $\mathbb{Z}_{p^k}$ while satisfying level-consistency. That is, there is no meaningful level-consistent RMFE over Galois ring for $\mathbb{Z}_{p^k}$-messages.

On the other side, we have the following theorem with a constructive proof, which asserts that the necessary condition in Thm. 3 is also a sufficient one.

Theorem 4. *If there are r distinct irreducible factors of $f(x) \in \mathbb{Z}_{p^t}[x]$ in $\mathbb{F}_p[x]$, then there is a level-consistent packing method for $\mathbb{Z}_{p^k}^r$ into $\mathbb{Z}_{p^t}[x]/f(x)$.*

Proof. Let $f(x)$ be factorized into $\prod_{i=1}^{s} g_i(x)^{\ell_i}$ in $\mathbb{F}_p[x]$, where $s \geq r$ and each $g_i(x)$ is distinct irreducible polynomial in $\mathbb{F}_p[x]$. The factorization can be lifted upto $\mathbb{Z}_{p^k}[x]$ via Hensel lifting. Let $f(x) = \prod_{i=1}^{s} f_i(x)$, where $f_i(x) \in \mathbb{Z}_{p^k}[x]$ is the Hensel lift of $g_i(x)^{\ell_i}$ satisfying $f_i(x) = g_i(x)^{\ell_i} \pmod p$. Then, we can identify $\mathbb{Z}_{p^k}[x]/f(x)$ with $\prod_{i=1}^{s} \mathbb{Z}_{p^k}[x]/f_i(x)$ via the CRT ring isomorphism.

There is a trivial ring monomorphism $\psi : \mathbb{Z}_{p^k}^r \to \mathbb{Z}_{p^k}[x]/f(x)$ defined as the following.

$$\psi(a_1, \cdots, a_r) = (a_1, \cdots, a_r, 0, \cdots, 0) \in \prod_{i=1}^{s} \mathbb{Z}_{p^k}[x]/f_i(x)$$

Define the function $\psi^{-1} : \mathbb{Z}_{p^k}[x]/f(x) \to \mathbb{Z}_{p^k}^r \cup \{\perp\}$ as the following.

$$\psi^{-1}(a(x)) = \begin{cases} \boldsymbol{a}, & \text{if there is } \boldsymbol{a} \in \mathbb{Z}_{p^k}^r \text{ such that } \psi(\boldsymbol{a}) = a(x) \\ \perp, & \text{otherwise} \end{cases}$$

Let π_k and ι_k denote the projection and injection between $\mathbb{Z}_{p^t}[x]/f(x)$ and $\mathbb{Z}_{p^k}[x]/f(x)$ respectively. Define $\mathsf{Pack} := \iota_k \circ \psi$ and $\mathsf{Unpack} := \psi^{-1} \circ \pi_k$ (Fig. 1). Then, it is straightforward that $(\mathsf{Pack}, \mathsf{Unpack})$ is a level-consistent packing method. $\square$

$$\begin{tikzcd} \mathbb{Z}_{p^k}^r \arrow[rr, "\mathsf{Pack}"] \arrow[drr, "\psi"'] & & \mathbb{Z}_{p^t}[x]/f(x) \\ & & \mathbb{Z}_{p^k}[x]/f(x) \arrow[u, "\iota_k"'] \end{tikzcd}$$

(a) Pack

$$\begin{tikzcd} \mathbb{Z}_{p^k}^r & & \mathbb{Z}_{p^t}[x]/f(x) \arrow[ll, "\mathsf{Unpack}"'] \arrow[d, "\pi_k"] \\ & & \mathbb{Z}_{p^k}[x]/f(x) \arrow[ull, "\psi^{-1}"] \end{tikzcd}$$

(b) Unpack

Fig. 1: Definitions of Pack and Unpack in Thm. 4

6.3 Level-consistency in $\mathbb{F}_{p^k}$-Message Packings

Our main result on level-consistency in $\mathbb{F}_{p^k}$-message packings is the following theorem. It is a finite field analogue of Thm. 3 which is on $\mathbb{Z}_{p^k}$-message packings. Our theorem illustrates a necessary condition for a level-consistent packing method for $\mathbb{F}_{p^k}$-messages to exist.

Theorem 5. *Let r be the number of distinct irreducible factors of $f(x) \in \mathbb{Z}_{p^t}[x]$ in $\mathbb{F}_p[x]$ whose degrees are multiples of k. There exists a level-consistent packing method $\mathbb{F}_{p^k}^n$ into $\mathbb{Z}_{p^t}[x]/f(x)$ only if $n \leq r$.*

Proof (Sketch). Then, using Prop. 12 with the fact that $\mathbf{0}$ is the only nilpotent element in $\mathbb{F}_{p^k}^n$, we can modify given $(\mathsf{Pack}, \mathsf{Unpack})$ to a level-consistent packing method $(\mathsf{Pack}', \mathsf{Unpack}')$ for $\mathbb{F}_{p^k}^n$ into $\mathbb{F}_p[x]/\hat{g}(x)$, where $\hat{g}(x)$ is the largest square-free factor of $f(x)$.

Moreover, we can find $g(x)$, a divisor of $\hat{g}(x)$, such that for any $a(x) \in \mathbb{F}_p[x]/\hat{g}(x)$ satisfying $\mathsf{Unpack}'(a(x)) = \mathbf{0}$, it holds that $a(x) = 0 \pmod{g(x)}$. That is, we can again modify $(\mathsf{Pack}', \mathsf{Unpack}')$ into a level-consistent *one-to-one* packing method $(\mathsf{Pack}'', \mathsf{Unpack}'')$ for $\mathbb{F}_{p^k}^n$ into $\mathbb{F}_p[x]/g(x)$. Then, by arguments on multiplicative orders with help of Prop. 10 and 11, we can eventually prove that $g(x)$ must have n distinct irreducible factors in $\mathbb{F}_p[x]$ whose degrees are multiples of k, in order to such $(\mathsf{Pack}'', \mathsf{Unpack}'')$ to exist. For the full proof, see the full version of this paper [14]. $\square$

The following are some consequences of Thm. 5. They illustrate the hardness of designing an efficient HE packing method for $\mathbb{F}_{2^k}$-messages while satisfying level-consistency. We have similar results for $\mathbb{F}_{p^k}$-messages with $p \neq 2$.

Example 19. When $M = 2^m$, since $\Phi_M(x) = (x+1)^{2^{m-1}}$ in $\mathbb{F}_2[x]$, we can only pack copies of $\mathbb{F}_2$ into $\mathbb{Z}_{2^t}[x]/\Phi_M(x)$ while satisfying level-consistency. Even in that case, we can pack at most one copy of $\mathbb{F}_2$.

Example 20. When M is an odd, $\Phi_M(x)$ factors into a product of distinct irreducible polynomials of degree $d = \mathrm{ord}_M(2)$ in $\mathbb{F}_2[x]$. Let $\phi(M) = r \cdot d$. Then, we can only pack copies of $\mathbb{F}_{2^k}$ such that $k|d$ into $\mathbb{Z}_{2^t}[x]/\Phi_M(x)$ while satisfying level-consistency. In that case, we can pack at most r copies of $\mathbb{F}_{2^k}$. Note that, since $d > \log M$ by definition, $r < \phi(M)/\log M$. For instance, if one wants to pack $\mathbb{F}_{2^8}$ into $\mathbb{Z}_{2^t}[x]/\Phi_M(x)$ with an odd M while satisfying level-consistency, then one must choose M such that $\mathrm{ord}_M(2)$ is a multiple of 8.

Example 21. When $M = 2^s \cdot M'$, where M' is an odd, $\Phi_M(x) = \Phi_{M'}(-x^{2^{s-1}}) = \Phi_{M'}(x)^{2^{s-1}}$ in $\mathbb{F}_2[x]$. Thus, we cannot pack more copies of $\mathbb{F}_{2^k}$ into $\mathbb{Z}_{2^t}[x]/\Phi_M(x)$ than $\mathbb{Z}_{2^t}[x]/\Phi_{M'}(x)$ while satisfying level-consistency.

Thm. 5 also yields the impossibility of level-consistent RMFEs.

Example 22. In $\mathbb{F}_{p^d} \cong \mathbb{Z}_p[x]/f(x)$ with a degree-d irreducible $f(x)$, we can pack at most one copy of $\mathbb{F}_{p^k}$ while satisfying level-consistency. Furthermore, if $k \nmid d$, we cannot pack even a single copy of $\mathbb{F}_{p^k}$ into $\mathbb{F}_{p^d}$ while satisfying level-consistency. That is, there is no meaningful level-consistent RMFE.

On the other side, we have the following theorem with a constructive proof, which asserts that the necessary condition in Thm. 5 is also a sufficient one.

Theorem 6. *Suppose there are r distinct irreducible factors of $f(x) \in \mathbb{Z}_{p^t}[x]$ in $\mathbb{F}_p[x]$ whose degrees are multiples of k. Then, there exists a level-consistent packing method $\mathbb{F}_{p^k}^r$ into $\mathbb{Z}_{p^t}[x]/f(x)$.*

Proof (Sketch). Similar to the proof of Thm. 4. See the full version [14]. $\square$

7 Surjectivity

In this section, we define and examine the concept of *surjectivity*, which is a favorable property for a packing method to have. Our main results are necessary and sufficient conditions for a polynomial ring to allow a surjective packing method for $\mathbb{Z}_{p^k}$ and $\mathbb{F}_{p^k}$, where p is a prime (See Section 3.2). They limit the achievable efficiency of surjective packing methods, yielding the impossiblity of designing an efficient packing methods while satisfying surjectivity.

7.1 Definition and Basic Facts

Definition 8 (Surjective Packing). *Let $\mathcal{R}$ be a ring. We say a degree-D packing method* $(\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^{D}$ *into $\mathcal{R}$ is* surjective[10] *if there is no $a(x) \in \mathcal{R}$ such that* $\mathsf{Unpack}_1(a(x)) = \perp$.

For a packing method for R^n into $\mathcal{R}$, the notion of surjectivity captures the condition whether every element of $\mathcal{R}$ is decodable. This distiction is essential when designing a cryptographic protocol with the packing method in a malicious setting, where an adversary might freely deviate from the protocol. If there is $a(x) \in \mathcal{R}$ such that $\mathsf{Unpack}_1(a(x)) = \perp$, a malicious adversary might make use of $a(x)$, when one is supposed to use a valid packing according to the protocol. The deviation may not only harm the correctness of the protocol, but also may leak information of honest parties, if such invalid packings are not properly handled.

For instance, Overdrive2k [31] and MHz2k [13] design and utilize $\mathbb{Z}_{2^k}$-message packings which are *not* surjective to construct HE-based MPC protocols over $\mathbb{Z}_{2^k}$ following the approach of SPDZ [21]. In order to mitigate the *invalid* packings, they perform ZKPoMK (Zero-Knowledge Proof of Message Knowledge) to ensure an HE ciphertext encrypts a validly packed plaintext.[11] ZKPoMK do not appear in SPDZ-family [21, 19, 27, 1] over a finite field $\mathbb{Z}_p$, where the conventional packing method is already surjective with perfect packing density (See Example 2). In a later subsection, we prove the impossibility of designing an efficient $\mathbb{Z}_{2^k}$-message packings while satisfying surjectivity. This justifies the use of *non*-surjective packings and the need of ZKPoMK in SPDZ-like MPC protocols over $\mathbb{Z}_{2^k}$.

The following proposition says that the definition of surjectivity trivially extends to all levels. The fact is used throughout this section.

Proposition 13. *Suppose* $(\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^{D}$ *is a degree-D surjective packing method for R^n into $\mathcal{R}$. Then, there is no $a(x) \in \mathcal{R}$ such that* $\mathsf{Unpack}_i(a(x)) = \perp$, *for all $i \in [D]$.*

Proof. By surjectivity and multiplicative homomorphic property, it holds that $\mathsf{Unpack}_2(a(x)) = \mathsf{Unpack}_1(1) \odot \mathsf{Unpack}_1(a(x)) \in R^n$, for all $a(x) \in \mathcal{R}$. Likewise, we can proceed inductively upto $\mathsf{Unpack}_D(\cdot)$. □

[10] In a sense that any element of $\mathcal{R}$ *could* be an image of $\mathsf{Pack}_1(\cdot)$.

[11] ZKPoMK was first conceptualized in MHZ2k [13], but it is also performed in Overdrive2k [31] implicitly. For detailed discussion, refer to [13].

A crucial fact when dealing with a surjective packing method is the following proposition on zero-sets. We extensively use the proposition when proving our main results on surjectivity.

Proposition 14 (Zero-set Ideal). *Let R and $\mathcal{R}$ be rings. For $D > 1$, let $(\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^{D}$ be a degree-D surjective packing method for R^n into $\mathcal{R}$. Let Z_i be the set consisting of elements $a(x) \in \mathcal{R}$ such that $\mathsf{Unpack}_i(a(x)) = \mathbf{0}$. Then, $Z = Z_1 = \cdots = Z_D$ for some ideal Z of $\mathcal{R}$. Moreover, $|Z| = |\mathcal{R}|/|R|^n$.*

Proof. By Prop. 13 and multiplicative homomorphic property, $\mathcal{R} \cdot Z_i \subset Z_{i+1}$ holds for $i < D$. Since $1 \in \mathcal{R}$, $Z_i \subset \mathcal{R} \cdot Z_i$ holds, and therefore $Z_i \subset \mathcal{R} \cdot Z_i \subset Z_{i+1}$. By Prop. 13 and additive homomorphic property, Z_i's have the same size, namely $|Z_i| = |\mathcal{R}|/|R|^n$. Thus, $Z_i = \mathcal{R} \cdot Z_i = Z_{i+1}$ holds. We can now put $Z := Z_1 = \cdots = Z_D$. Moreover, since $\mathcal{R} \cdot Z = Z$ holds, Z is an ideal of $\mathcal{R}$. $\square$

7.2 Surjectivity in $\mathbb{Z}_{p^k}$-Message Packings

Our main result on surjectivity in $\mathbb{Z}_{p^k}$-message packings is the following theorem. Our theorem illustrates a necessary condition for a surjective packing method for $\mathbb{Z}_{p^k}$-messages to exist.

Theorem 7. *Let $\check{r}$ be the number of linear factors of $f(x) \in \mathbb{Z}_{p^t}[x]$ in $\mathbb{Z}_{p^k}[x]$ which are mutually distinct modulo p. For $D > 1$, there exists a degree-D surjective packing method $\mathbb{Z}_{p^k}^n$ into $\mathbb{Z}_{p^t}[x]/f(x)$ only if $n \le \check{r}$.*

Proof (Sketch). Let $(\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^{D}$ be a degree-D surjective packing method for $\mathbb{Z}_{p^k}^n$ into $\mathbb{Z}_{p^t}[x]/f(x)$. For all $b(x) \in \mathbb{Z}_{p^t}[x]/f(x)$, since $\mathsf{Unpack}_i(b(x)) = \boldsymbol{b}$ for some $\boldsymbol{b} \in \mathbb{Z}_{p^k}^n$ by surjectivity(Prop. 13), $\mathsf{Unpack}_i(p^k \cdot b(x)) = \mathbf{0}$ holds. Thus, we can construct a degree-D surjective packing method $(\mathsf{Pack}'_i, \mathsf{Unpack}'_i)_{i=1}^{D}$ for $\mathbb{Z}_{p^k}^n$ into $\mathbb{Z}_{p^k}[x]/f(x)$ with appropriate projections and injections. Then, we repeatedly apply Prop. 14 to show that, for each unit vector $\boldsymbol{e}_i \in \mathbb{Z}_{p^k}^n$, there exists $a_i(x) \in \mathbb{Z}_{p^k}[x]/f(x)$ such that (i) $\mathsf{Unpack}'_1(a_i(x)) = \boldsymbol{e}_i$ (ii) $a_i(x)$ is non-zero at exactly one CRT slot. Eventually, again with Prop. 14, we can couple each $a_i(x)$ with distinct linear factors of $f(x) \in \mathbb{Z}_{p^k}[x]$. For a full proof, see the full version of this paper [14]. $\square$

Before we proceed, we state a simple fact on irreducibility of $\Phi_{2^m}(x)$ over a power-of-two modulus.

Proposition 15 (Irreducibility of $\Phi_{2^m}(x)$). *For $M = 2^m$, cyclotomic polynomial $\Phi_M(x)$ is irreducible modulo 4, i.e. there are no $f(x), g(x) \in \mathbb{Z}_4[x]$ such that $f(x) \cdot g(x) = \Phi_M(x) \pmod 4$ and $\deg(f), \deg(g) \ge 1$.*

Proof. See the full version of this paper [14]. $\square$

The following are some consequences of Thm. 7. They illustrate the impossibility of designing a surjective HE packing method for $\mathbb{Z}_{2^k}$-messages with cyclotomic polynomials. We have similar results for $\mathbb{Z}_{p^k}$-messages with $p \neq 2$.

Example 23. When $M = 2^m$, by Prop. 15, we cannot pack any copies of $\mathbb{Z}_{2^k}$ into $\mathbb{Z}_{2^t}[x]/\Phi_M(x)$ while satisfying surjectivity and degree-2 homomorphism.

Example 24. When M is an odd, $\Phi_M(x)$ factors into a product of distinct irreducible polynomials of degree $d = \mathrm{ord}_M(2)$ in $\mathbb{F}_2[x]$. Thus, we cannot pack any copies of $\mathbb{Z}_{2^k}$ into $\mathbb{Z}_{2^t}[x]/\Phi_M(x)$ while satisfying surjectivity and degree-2 homomorphism.

Example 25. When $M = 2^s \cdot M'$, where M' is an odd, $\Phi_M(x) = \Phi_{M'}(-x^{2^{s-1}})$ in $\mathbb{Z}[x]$. Thus, by Example 24, we cannot pack any copies of $\mathbb{Z}_{2^k}$ into $\mathbb{Z}_{2^t}[x]/\Phi_M(x)$ while satisfying surjectivity and degree-2 homomorphism.

Thm. 7 also yields the impossibility of surjective RMFEs over Galois ring for $\mathbb{Z}_{p^k}$-messages.

Example 26. In $GR(p^t, d) \cong \mathbb{Z}_{p^t}[x]/f(x)$ with a degree-d $f(x)$ which is irreducible modulo p, we cannot pack any copy of $\mathbb{Z}_{p^k}$ while satisfying surjectivity, unless $d = 1$. That is, there is no meaningful surjective RMFE over Galois ring for $\mathbb{Z}_{p^k}$-messages.

On the other side, we have the following theorem with a constructive proof, which asserts that the necessary condition in Thm. 7 is also a sufficient one.

Theorem 8. *Suppose there are r linear factors of $f(x) \in \mathbb{Z}_{p^t}[x]$ in $\mathbb{Z}_{p^k}[x]$ which are mutually distinct modulo p. Then, there exists a surjective packing method $\mathbb{Z}_{p^k}^r$ into $\mathbb{Z}_{p^t}[x]/f(x)$.*

Proof. Let $g(x) \in \mathbb{Z}_{p^k}[x]$ be the product of such r linear factors of $f(x)$ in $\mathbb{Z}_{p^k}[x]$. Then, there is a CRT ring isomophism $\psi : \mathbb{Z}_{p^k}^r \xrightarrow{\cong} \mathbb{Z}_{p^k}[x]/g(x)$. Let π_k and ι_k denote the projection and injection between $\mathbb{Z}_{p^t}[x]/f(x)$ and $\mathbb{Z}_{p^k}[x]/f(x)$, and let π_g and ι_g denote those of $\mathbb{Z}_{p^k}[x]/f(x)$ and $\mathbb{Z}_{p^k}[x]/g(x)$ respectively.

Define $\mathsf{Pack} := \iota_k \circ \iota_g \circ \psi$ and $\mathsf{Unpack} := \psi^{-1} \circ \pi_h \circ \pi_k$ (Fig. 2). Then, it is straightforward that $(\mathsf{Pack}, \mathsf{Unpack})$ is a surjective packing method. $\square$

$$\begin{tikzcd}
\mathbb{Z}_{p^k}^r \arrow[r, "\mathsf{Pack}"] \arrow[ddr, "\psi"'] & \mathbb{Z}_{p^t}[x]/f(x) \\
& \mathbb{Z}_{p^k}[x]/f(x) \arrow[u, "\iota_k"'] \\
& \mathbb{Z}_{p^k}[x]/g(x) \arrow[u, "\iota_g"']
\end{tikzcd}$$

(a) Pack

$$\begin{tikzcd}
\mathbb{Z}_{p^k}^r & \mathbb{Z}_{p^t}[x]/f(x) \arrow[l, "\mathsf{Unpack}"'] \arrow[d, "\pi_k"] \\
& \mathbb{Z}_{p^k}[x]/f(x) \arrow[d, "\pi_g"] \\
& \mathbb{Z}_{p^k}[x]/g(x) \arrow[uul, "\psi^{-1}"]
\end{tikzcd}$$

(b) Unpack

Fig. 2: Definitions of Pack and Unpack in Thm. 8

7.3 Surjectivity in $\mathbb{F}_{p^k}$-Message Packings

Our main result on surjectivity in $\mathbb{F}_{p^k}$-message packings is the following theorem. It is a finite field analogue of Thm. 7 which is on $\mathbb{Z}_{p^k}$-message packings. Our theorem illustrates a necessary condition for a surjective packing method for $\mathbb{F}_{p^k}$-messages to exist.

Theorem 9. *Let r be the number of distinct degree-k irreducible factors of $f(x) \in \mathbb{Z}_{p^t}[x]$ in $\mathbb{F}_p[x]$. For $D > 1$, there exists a degree-D surjective packing method $\mathbb{F}_{p^k}^n$ into $\mathbb{Z}_{p^t}[x]/f(x)$ only if $n \leq r$.*

Proof (Sketch). Let $(\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^D$ be a degree-D surjective packing method for $\mathbb{F}_{p^k}^n$ into $\mathbb{Z}_{p^t}[x]/f(x)$. For all $b(x) \in \mathbb{Z}_{p^t}[x]/f(x)$, since $\mathsf{Unpack}_i(b(x)) = \boldsymbol{b}$ for some $\boldsymbol{b} \in \mathbb{F}_{p^k}^n$ by surjectivity(Prop. 13), $\mathsf{Unpack}_i(p \cdot b(x)) = \mathbf{0}$ holds. Thus, we can construct a degree-D surjective packing method $(\mathsf{Pack}'_i, \mathsf{Unpack}'_i)_{i=1}^D$ for $\mathbb{F}_{p^k}^n$ into $\mathbb{F}_p[x]/f(x)$ with appropriate projections and injections.

By Prop. 14 and the fact that $\mathcal{R} := \mathbb{F}_p[x]/f(x)$ is a principal ideal ring, the zero-set ideal can be set as $Z = \breve{g}(x) \cdot \mathcal{R}$ for some $\breve{g}(x) \in \mathbb{F}_p[x]$ which divides $f(x)$. Let $g(x) := f(x)/\breve{g}(x)$. Then, using $\mathcal{R}/Z \cong \mathbb{F}_p[x]/g(x)$, we can construct a degree-D surjective packing method $(\mathsf{Pack}''_i, \mathsf{Unpack}''_i)_{i=1}^D$ for $\mathbb{F}_{p^k}^n$ into $\mathbb{F}_p[x]/g(x)$ with appropriate projections and injections. Note that $\deg(g) = k \cdot n$ since $|\mathcal{R}/Z| = p^{kn}$ by Prop. 14. Then by a counting argument on zero-divisors, we can show that $g(x)$ must factor into n distinct degree-k irreducible polynomials to allow such packing. For the full proof, see the full version [14]. $\square$

The following are some consequences of Thm. 9. They illustrate the hardness of designing an efficient HE packing method for $\mathbb{F}_{2^k}$-messages while satisfying surjectivity. We have similar results for $\mathbb{F}_{p^k}$-messages with $p \neq 2$.

Example 27. When $M = 2^m$, since $\Phi_M(x) = (x+1)^{2^{m-1}}$ in $\mathbb{F}_2[x]$, we can only pack copies of $\mathbb{F}_2$ into $\mathbb{Z}_{2^t}[x]/\Phi_M(x)$ while satisfying surjectivity and degree-2 homomorphism. Even in that case, we can pack at most one copy of $\mathbb{F}_2$.

Example 28. When M is an odd, $\Phi_M(x)$ factors into a product of distinct irreducible polynomials of degree $d = \mathrm{ord}_M(2)$ in $\mathbb{F}_2[x]$. Let $\phi(M) = r \cdot d$. Then, we can only pack copies of $\mathbb{F}_{2^d}$ into $\mathbb{Z}_{2^t}[x]/\Phi_M(x)$ while satisfying surjectivity and degree-2 homomorphism. In that case, we can pack at most r copies of $\mathbb{F}_{2^d}$. Note that, since $d > \log M$ by definition, $r < \phi(M)/\log M$.

For instance, if one wants to pack $\mathbb{F}_{2^8}$ into $\mathbb{Z}_{2^t}[x]/\Phi_M(x)$ with an odd M while satisfying the conditions, then one must choose M such that $\mathrm{ord}_M(2) = 8$. However, such M cannot be larger than $(2^8 - 1)$ and might be too small for a secure parameter of HE.

Example 29. When $M = 2^s \cdot M'$, where M' is an odd, $\Phi_M(x) = \Phi_{M'}(-x^{2^{s-1}}) = \Phi_{M'}(x)^{2^{s-1}}$ in $\mathbb{F}_2[x]$. Thus, we cannot pack more copies of $\mathbb{F}_{2^k}$ into $\mathbb{Z}_{2^t}[x]/\Phi_M(x)$ than $\mathbb{Z}_{2^t}[x]/\Phi_{M'}(x)$ while satisfying surjectivity and degree-2 homomorphism.

Meanwhile, using such M can be useful when packing copies of a small field: it enables to meet certain level of HE security by enlarging the degree of the ring. See Example 28.

Thm. 9 also yields the impossibility of surjective RMFEs.

Example 30. In $\mathbb{F}_{p^d} \cong \mathbb{Z}_p[x]/f(x)$ with a degree-d irreducible $f(x)$, we cannot pack even a single copy of $\mathbb{F}_{p^k}$ while satisfying surjectivity and degree-2 homomorphism, if $k \neq d$. That is, there is no meaningful surjective RMFE.

On the other side, we have the following theorem with a constructive proof, which asserts that the necessary condition in Thm. 9 is also a sufficient one.

Theorem 10. *If there are r distinct degree-k irreducible factors of $f(x) \in \mathbb{Z}_{p^t}[x]$ in $\mathbb{F}_p[x]$, then there exists a surjective packing method $\mathbb{F}_{p^k}^r$ into $\mathbb{Z}_{p^t}[x]/f(x)$.*

Proof (Sketch). Similar to the proof of Thm. 8. See the full version [14]. □

Acknowledgement

The authors thank Dongwoo Kim for insightful discussions on packing methods, Donggeon Yhee for discussions on Prop. 7, and Minki Hhan for constructive comments on an earlier version of this work. The authors also thank the reviewers of Eurocrypt 2022 who provided thoughtful suggestions to improve the earlier version of this paper. This work was supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No.2020-0-00840, Development and Library Implementation of Fully Homomorphic Machine Learning Algorithms supporting Neural Network Learning over Encrypted Data)

References

1. Baum, C., Cozzo, D., Smart, N.P.: Using topgear in overdrive: a more efficient zkpok for spdz. In: International Conference on Selected Areas in Cryptography. pp. 274–302. Springer (2019)
2. Block, A.R., Maji, H.K., Nguyen, H.H.: Secure computation based on leaky correlations: high resilience setting. In: Annual International Cryptology Conference. pp. 3–32. Springer (2017)
3. Block, A.R., Maji, H.K., Nguyen, H.H.: Secure computation with constant communication overhead using multiplication embeddings. In: International Conference on Cryptology in India. pp. 375–398. Springer (2018)
4. Brakerski, Z., Gentry, C., Vaikuntanathan, V.: (leveled) fully homomorphic encryption without bootstrapping. In: Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. pp. 309–325 (2012)
5. Cascudo, I., Cramer, R., Xing, C., Yuan, C.: Amortized complexity of information-theoretically secure mpc revisited. In: Annual International Cryptology Conference. pp. 395–426. Springer (2018)
6. Cascudo, I., Giunta, E.: On interactive oracle proofs for boolean r1cs statements. Cryptology ePrint Archive, Report 2021/694 (2021)
7. Cascudo, I., Gundersen, J.S.: A secret-sharing based mpc protocol for boolean circuits with good amortized complexity. In: Theory of Cryptography Conference. pp. 652–682. Springer (2020)

8. Castryck, W., Iliashenko, I., Vercauteren, F.: Homomorphic sim^{2}d operations: Single instruction much more data. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 338–359. Springer (2018)
9. Chen, H., Han, K.: Homomorphic lower digits removal and improved fhe bootstrapping. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 315–337. Springer (2018)
10. Chen, H., Laine, K., Player, R., Xia, Y.: High-precision arithmetic in homomorphic encryption. In: Cryptographers' Track at the RSA Conference. pp. 116–136. Springer (2018)
11. Cheon, J.H., Jeong, J., Lee, J., Lee, K.: Privacy-preserving computations of predictive medical models with minimax approximation and non-adjacent form. In: International Conference on Financial Cryptography and Data Security. pp. 53–74. Springer (2017)
12. Cheon, J.H., Kim, A., Kim, M., Song, Y.: Homomorphic encryption for arithmetic of approximate numbers. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 409–437. Springer (2017)
13. Cheon, J.H., Kim, D., Lee, K.: Mhz2k: Mpc from he over $\mathbb{Z}_{2^k}$ with new packing, simpler reshare, and better zkp. In: Annual International Cryptology Conference. pp. 426–456. Springer (2021)
14. Cheon, J.H., Lee, K.: Limits of polynomial packings for $\mathbb{Z}_{p^k}$ and $\mathbb{F}_{p^k}$. Cryptology ePrint Archive, Report 2021/1033 (2021)
15. Cramer, R., Damgård, I., Escudero, D., Scholl, P., Xing, C.: Spd$\mathbb{Z}_{2^k}$: Efficient mpc mod 2^k for dishonest majority. In: Annual International Cryptology Conference. pp. 769–798. Springer (2018)
16. Cramer, R., Rambaud, M., Xing, C.: Asymptotically-good arithmetic secret sharing over $\mathbb{Z}/(p^\ell\mathbb{Z})$ with strong multiplication and its applications to efficient mpc. In: Annual International Cryptology Conference. pp. 656–686. Springer (2021)
17. Cramer, R., Xing, C., Yuan, C.: On the complexity of arithmetic secret sharing. In: Theory of Cryptography Conference. pp. 444–469. Springer (2020)
18. Dalskov, A., Lee, E., Soria-Vazquez, E.: Circuit amortization friendly encodings and their application to statistically secure multiparty computation. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 213–243. Springer (2020)
19. Damgård, I., Keller, M., Larraia, E., Pastro, V., Scholl, P., Smart, N.P.: Practical covertly secure mpc for dishonest majority–or: breaking the spdz limits. In: European Symposium on Research in Computer Security. pp. 1–18. Springer (2013)
20. Damgård, I., Larsen, K.G., Nielsen, J.B.: Communication lower bounds for statistically secure mpc, with or without preprocessing. In: Annual International Cryptology Conference. pp. 61–84. Springer (2019)
21. Damgård, I., Pastro, V., Smart, N., Zakarias, S.: Multiparty computation from somewhat homomorphic encryption. In: Annual Cryptology Conference. pp. 643–662. Springer (2012)
22. Fan, J., Vercauteren, F.: Somewhat practical fully homomorphic encryption. Cryptology ePrint Archive, Report 2012/144 (2012)
23. Gentry, C.: Fully homomorphic encryption using ideal lattices. In: Proceedings of the forty-first annual ACM symposium on Theory of computing. pp. 169–178 (2009)
24. Gentry, C., Halevi, S., Smart, N.P.: Better bootstrapping in fully homomorphic encryption. In: International Workshop on Public Key Cryptography. pp. 1–16. Springer (2012)

25. Halevi, S., Shoup, V.: Helib. Retrieved from HELib: `https://github.com.homenc/HElib` (2014)
26. Halevi, S., Shoup, V.: Bootstrapping for helib. In: Annual International conference on the theory and applications of cryptographic techniques. pp. 641–670. Springer (2015)
27. Keller, M., Pastro, V., Rotaru, D.: Overdrive: Making spdz great again. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 158–189. Springer (2018)
28. Kim, A., Song, Y., Kim, M., Lee, K., Cheon, J.H.: Logistic regression model training based on the approximate homomorphic encryption. BMC medical genomics **11**(4), 23–31 (2018)
29. Lipmaa, H.: Progression-free sets and sublinear pairing-based non-interactive zero-knowledge arguments. In: Theory of Cryptography Conference. pp. 169–189. Springer (2012)
30. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: Annual international conference on the theory and applications of cryptographic techniques. pp. 1–23. Springer (2010)
31. Orsini, E., Smart, N.P., Vercauteren, F.: Overdrive2k: Efficient secure mpc over $\mathbb{Z}_{2^k}$ from somewhat homomorphic encryption. In: Cryptographers' Track at the RSA Conference. pp. 254–283. Springer (2020)
32. Polychroniadou, A., Song, Y.: Constant-overhead unconditionally secure multiparty computation over binary fields. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 812–841. Springer (2021)
33. Smart, N.P., Vercauteren, F.: Fully homomorphic encryption with relatively small key and ciphertext sizes. In: International Workshop on Public Key Cryptography. pp. 420–443. Springer (2010)
34. Smart, N.P., Vercauteren, F.: Fully homomorphic simd operations. Designs, codes and cryptography **71**(1), 57–81 (2014)