이학박사 학위논문

A Study on Homomorphic Packing:
Definitions, Constructions, and Limitations
(동형팩킹에 관한 연구)

2023년 8월

서울대학교 대학원

수리과학부

이 기 우

A Study on Homomorphic Packing:
Definitions, Constructions, and Limitations

(동형팩킹에 관한 연구)

지도교수 천정희

이 논문을 이학박사 학위논문으로 제출함

2023년 4월

서울대학교 대학원

수리과학부

이 기 우

이기우의 이학박사 학위논문을 인준함

2023년 6월

위 원 장	현 동 훈	(인)
부 위 원 장	천 정 희	(인)
위 원	이 주 영	(인)
위 원	서 재 홍	(인)
위 원	송 용 수	(인)

A Study on Homomorphic Packing:
Definitions, Constructions, and Limitations

A dissertation submitted in partial fulfillment
of the requirements for the degree
Doctor of Philosophy in Mathematical Science

by

Keewoo Lee

Doctoral Advisor : Professor Jung Hee Cheon

Department of Mathematical Sciences
Seoul National University

August 2023

Abstract

In cryptography, using large or complex mathematical structures is often required for security or other functionality. On the other hand, small or moderate-sized messages with a familiar algebraic structure are used in real-life computations. Regarding this discrepancy, similar concepts of embedding multiple messages into a large structure while preserving their algebra have been independently studied in various contexts of secure computation. This includes the packing technique in homomorphic encryption (HE) and the reverse multiplication-friendly embedding (RMFE) in information-theoretically secure multi-party computation (MPC).

In this thesis, we formally define homomorphic packing and initiate a unified study of related concepts in various contexts of cryptography. We review existing packing methods through our systematic framework and prove several mathematical limitations on the performance of homomorphic packing.

As an application, we devise a new packing method and utilize it to design an HE-based MPC protocol for $\mathbb{Z}_{2^k}$-messages. Our results on the limitations of homomorphic packing justify our approaches and design choices for the packing method and the MPC protocol.

Keywords: Cryptography, Homomorphic packing, Homomorphic encryption, Secure multi-party computation, Reverse multiplication-friendly embedding, $\mathbb{Z}_{2^k}$
Student Number: 2017-28540

Contents

CONTENTS

Chapter 1

Introduction

In cryptography, using large or complex mathematical structures is often required for security or other functionality. On the other hand, small or moderate-sized messages with a familiar algebraic structure are used in real-life computations. Regarding this discrepancy, similar concepts of embedding multiple messages into a large structure while preserving their algebra have been independently studied in various contexts of secure computation:

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 [Gen09], HE has undergone extensive study and development. HE is now considered to be exploitable in real-life applications (e.g. privacy-preserving machine learning [KSK+18]) and regarded as a core building block in various cryptographic primitives (e.g. secure multi-party computation [DPSZ12]).

One drawback of contemporary lattice-based HE schemes [BGV12, FV12] 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) [LPR10]. That is, these schemes are homomorphic with regards to the addition and multiplication of polyno-

mial 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 line of works on how to encode data into HE plaintexts [CJLL17, CLPX18, CIV18, CKKS17], Smart-Vercauteren [SV10, SV14] 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[1] ring isomorphism with *well-chosen* prime p. Their simple yet powerful technique enables SIMD[2]-like optimizations and enhances amortized performance. That is, with a 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.[3] 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$\mathbb{Z}_{2^k}$ [CDE+18]. SPD$\mathbb{Z}_{2^k}$ follows the framework of HE-based MPC protocol SPDZ [DPSZ12], 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 [OSV20], whose goal is an effi-

[1] Chinese Remainder Theorem

[2] Single Instruction, Multiple Data

[3] The original method of [SV10] does not consider packings for $\mathbb{Z}_{p^k}$. Gentry-Halevi-Smart [GHS12] later generalized the method to support such packing. However, this method achieves only considerably low efficiency. See Section 4.1.1.

cient construction of HE-based MPC over $\mathbb{Z}_{2^k}$, came up with a new and more involved polynomial packing method for $\mathbb{Z}_{2^k}$-messages (Section 4.1).

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.[4] 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 [CCXY18], 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, [CCXY18] 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 [CCXY18], RMFE has become a standard tool in information-theoretically secure MPC, to achieve *linear* amortized communication cost while preserving optimal corruption tolerance: [BMN18, DLN19, CG20, CXY20, DLSV20, PS21].

In [CRX21], 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 $\mathbb{Z}_{p^k}^n \to GR(p^k, d) \cong \mathbb{Z}_{p^k}[x]/f(x)$, where p is a prime and $f(x) \in \mathbb{Z}_{p^k}[x]$ is a degree-d irreducible polynomial in $\mathbb{F}_p[x]$.

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

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 [BMN17], zk-SNARK [CG22], 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 Contributions and Results

Unified Definition and Survey. In this work, we formally define homomorphic 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 4.1). We also define several properties of homomorphic packing (Section 3.2) and analyze existing homomorphic packing methods regarding these properties (Section 4.3).

We then 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 3.3). The results also rule out the possibility of using composite modulus for better packing.

New Construction and Application to MPC over $\mathbb{Z}_{2^k}$. We propose a new efficient homomorphic packing method for $\mathbb{Z}_{2^k}$-messages (Section 4.2) and apply it to secure multi-party computation (MPC) protocol over $\mathbb{Z}_{2^k}$ (Chapter 5). Our protocol is secure against actively corrupted majority and based on non-trivial adaptations of techniques used in the finite field case to the $\mathbb{Z}_{2^k}$ case. Our techniques improve the efficiency of MPC over $\mathbb{Z}_{2^k}$ considerably.

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.

- Upper Bounds on Packing Density (Section 6.1): We evaluate the efficiency of packing methods by packing density which measures how densely the messages are packed in a plaintext (Def. 3.2.1).[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. 6.1.5 and 6.1.14). These results have several implications:
  - Our new homomorphic packing method 4.2 achieves nearly optimal density in certain parameter regimes (Example 6.1.6). Our results justify the *lifting* of our packing (See Section 4.2).
  - We provide the first upper bound on RMFE over Galois ring for $\mathbb{Z}_{p^k}$-messages (Example 6.1.7).
  - We provide a new proof for upper bound on RMFE, which can be extended to higher-degree settings unlike the previous proof (Example 6.1.18).

[5] We note that packing density differs from *ciphertext rate* which is the main interest of recent developments in compressible or optimal-rate FHE [BDGM19, GH19]. Ciphertext rate measures the ratio of *plaintext* size to *ciphertext* size, whereas packing density measures the ratio of *message* size to *plaintext* size. On the distinction of message and plaintext, please refer to Section 2.1.

- Impossibility of Level-consistency (Section 6.2): The notion of level-consistency captures the property whether packings are decodable in an identical way at different multiplicative levels (Def. 3.2.2). 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 [HS15] (a.k.a. GHS packing [GHS12], Section 4.1.1) is essentially the optimal method to use in *fully* homomorphic encryption(FHE) (Example 6.2.6).
  - 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 $\mathbb{Z}_{2^k}$ [OSV20, CKL21] and highlights the usefulness of the trick proposed in Chapter 5.4, which closed the gap between the level-consistent and level-dependent packing methods in so-called *reshare* protocol. (See Section 6.2.)
- Impossibility of Surjectivity (Section 6.3): For a packing method into $\mathcal{R}$, the notion of surjectivity captures the condition whether every element of $\mathcal{R}$ is decodable (Def. 3.2.5). 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[6], which ensures an HE ciphertext encrypts a validly packed plaintext, in SPDZ-like MPC protocols over $\mathbb{Z}_{2^k}$ [OSV20, CKL21].

1.2 Included Publications

This thesis contains the results of the following papers.

- [CKL21] Jung Hee Cheon, Dongwoo Kim, and Keewoo Lee. MHz2k: MPC from HE over $\mathbb{Z}_{2^k}$ with New Packing, Simpler Reshare, and Better ZKP. In *Advances in Cryptology – CRYPTO 2021*.
- [CL22] Jung Hee Cheon and Keewoo Lee. Limits of Polynomial Packings for $\mathbb{Z}_{p^k}$ and $\mathbb{F}_{p^k}$. In *Advances in Cryptology – EUROCRYPT 2022*.

[6] Zero-knowledge proof of message knowledge

Chapter 2

Preliminaries

2.1 Notations and Terminologies

- In this work, 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 this work, we only consider monic polynomials when defining quotient rings. Thus, we omit description on *monic* property throughout the thesis for readability. Readers must understand any polynomials defining quotient rings as monic polynomials, even if not explicitly stated.
- This work 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 work, 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 Factorization of Cyclotomic Polynomials

2.2.1 Factorization of $\Phi_M(x)$ in $\mathbb{Z}_{p^k}[x]$

We first recall Hensel's lifting lemma. For proof and detailed discussions, refer to [Wan03] or other textbooks.

Lemma 2.2.1 (Hensel Lifting)**.** *Let p be a prime and $f(x) \in \mathbb{Z}[x]$ be a monic polynomial which factorizes into $\prod_{i=1}^{r} g_i(x)^{\ell_i} \pmod p$, where $g_i(x)$'s are distinct irreducible polynomials in $\mathbb{F}_p[x]$. 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, $\varphi(M) = r \cdot d$ 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 $f_i(x) = g_i(x) \pmod p$. Such factorization induces the following CRT ring isomorphism.

$$\mathbb{Z}_{p^k}[x]/\Phi_M(x) \cong \prod_{i=1}^{r} \mathbb{Z}_{p^k}[x]/f_i(x) \tag{2.1}$$

Each $\mathbb{Z}_{p^k}[x]/f_i(x)$ is often referred to as a CRT *slot* of $\mathbb{Z}_{p^k}[x]/\Phi_M(x)$. In this thesis, we frequently refer to the isomorphism Eq. 2.1 and the notation $\varphi(M) = N = r \cdot d$.

2.2.2 Irreducibility of $\Phi_{2^m}(x)$ in $\mathbb{Z}_{2^k}[x]$

We note that the above factorizations (Sec. 2.2.1) hold only when $\gcd(M, p) = 1$. In particular, we have the following irreducibility result.

Proposition 2.2.2 (Irreducibility of $\Phi_{2^m}(x)$ in $\mathbb{Z}_{2^k}[x]$)**.** *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 $\deg(f), \deg(g) \geq 1$.*

Proof. Suppose such $f(x)$ and $g(x)$ exist. Let $f(x) := \sum_{i=0}^{d_f} f_i \cdot X^i$ and similarly for $g(x)$, with $d_f + d_g = \varphi(M) = 2^{m-1}$. Since $\Phi_M(x)$ factorizes into $(X+1)^{2^{m-1}}$ in $\mathbb{F}_2[x]$, $f(x)$ and $g(x)$ must be $X^{d_f} + 1 = (X+1)^{d_f}$ and $X^{d_g} + 1 = (X+1)^{d_g}$ in $\mathbb{F}_2[x]$, respectively. Thus, $f_i = 0 \pmod 2$ for $0 < i < d_f$, and $g_i = 0 \pmod 2$ for $0 < i < d_g$. Meanwhile, we can assume $f_{d_f} = g_{d_g} = 1 \pmod 4$ without loss of generality. Also note that, since $f_0 \cdot g_0 = 1 \pmod 4$, either $f_0 = g_0 = 1$ or $f_0 = g_0 = 3$ must hold modulo 4.

Suppose $d_f \neq d_g$, and without loss of generality assume $d_f > d_g$. Consider the d_g-th coefficient of $\Phi_M(x)$. It is 0 mudulo 2 as $\Phi_M(x) = X^{2^{m-1}} + 1$. However, expressing it as $\sum_{i=0}^{d_g} f_i \cdot g_{d_g - i} = f_0 \cdot g_{d_g} \pmod 2$, it is 1 modulo 2 and leads to a contradiction. Thus, $d_f = d_g$ must hold.

Again, consider the d_g-th coefficient of $\Phi_M(x)$. It is 0 mudulo 4 as $\Phi_M(x) = X^{2^{m-1}} + 1$. However, expressing it as $\sum_{i=0}^{d_g} f_i \cdot g_{d_g - i} = f_0 \cdot g_{d_g} + f_{d_f} \cdot g_0 \pmod 4$,

it is 2 modulo 4 and leads to a contradiction. Thus, such $f(x)$ and $g(x)$ do not exist. □

2.3 RMFE

Reverse multiplication-friendly embeddings (RMFE) were first defined and studied in-depth by [CCXY18].[1] 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.

Definition 2.3.1 (RMFE)**.** A pair of maps (φ, ψ) is called a $(n, d)_{p^k}$-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, [CCXY18] 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, [CCXY18] constructed *constant-rate* RMFEs. For instance, we have a family of $(n, d)_2$-RMFE with $n/d \to 0.203$ from [CCXY18].[2] 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: [CCXY18, BMN18, DLN19, CG20, CXY20, DLSV20, PS21]. RMFE was also leveraged in zk-SNARK context recently [CG22].

[1] Nonetheless, this object was also previously studied in [BMN17] to amortize oblivious linear evaluations (OLE) into a larger extension field for correlation extraction problem in MPC. However, their construction achieved only sublinear density (See Section 4.1.3).

[2] We have found out that we can slightly improve this rate by the hybrid approach with *3-free sets* (Section 4.1.3), but we omit here for simplicity.

Recently in [CRX21], RMFE *over Galois rings* was first defined and studied. It is a natural generalization of RMFE over fields to Galois rings.

Definition 2.3.2 (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.

Chapter 3

Definitions and Basic Concepts

In this chapter, we formally define *homomorphic packing* 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 homomorphic packing.

3.1 Homomorphic Packing

We begin with a formal definition of packing.

Definition 3.1.1 (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 thesis, 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. 3.1.1 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 3.1.2 (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 $1 \leq i \leq D$:

- 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 3.1.3. 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 3.1.4. 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 4.1.

Example 3.1.5 (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 thesis. 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 3.1.6 (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 3.1.7 (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 3.1.6, this isomorphism induces a natural packing method which is of degree-∞, but has even heavier restriction on parameters.

Example 3.1.8 (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 3.1.9 (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 $\mathbb{Z}_p[x]$. The only additional requirement is that the packing algorithm at level-1 and unpacking algorithm at level-2 must be $\mathbb{Z}_{p^k}$-linear functions. However, any degree-2 packing method can be easily transformed to satisfy the requirement.

3.2 Properties of Homomorphic Packing

In this section, we define several properties of homomorphic packing.

3.2.1 Packing Density

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

Definition 3.2.1 (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 3.1.5, 3.1.6, and 3.1.7 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.

3.2.2 Level-Consistency

We define and examine the concept of *level-consistency*, which is a favorable property for a packing method to have.

Definition 3.2.2. 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 $1 \leq i \leq D$. 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. 3.2.3). 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.

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

Proposition 3.2.3. *A level-consistent degree-D packing method $\mathcal{P}$ can be extended to a level-consistent degree-D' packing $\mathcal{P}'$ for arbitrary $D' > D$.*

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

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

Definition 3.2.4 (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 $i \in [D]$.

3.2.3 Surjectivity

We define and examine the concept of *surjectivity*, which is a favorable property for a packing method to have.

Definition 3.2.5 (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*[1] 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.

The following proposition says that the definition of surjectivity trivially extends to all levels. The fact plays an important role in proving our main result.

Proposition 3.2.6. *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 does not exist* $a(x) \in \mathcal{R}$ *such that* $\mathsf{Unpack}_i(a(x)) = \perp$*, for all* $i \in [D]$*.*

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

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 $\mathsf{Unpack}_D(\cdot)$. □

3.3 Decomposition Lemmas

In this section, 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 $\mathbb{Z}_{p^t}[x]/f(x)$.

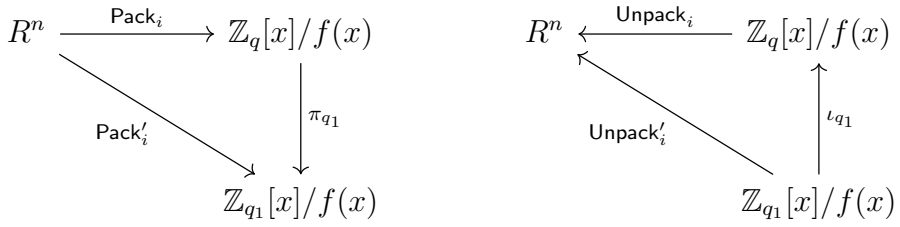
Proposition 3.3.1. *Let R be a ring with characteristic p and $\mathcal{R}$ be a ring with characteristic q. There exists a degree-0 packing method $(\mathsf{Pack}, \mathsf{Unpack})$ for R^n into $\mathcal{R}$ only if p divides q.*

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 3.1.3. Meanwhile, $q \cdot a(x) = 0$ in $\mathcal{R}$. Thus, $q \cdot \mathbf{1} = \mathbf{0}$ in R^n, again by Remark 3.1.3. □

Proposition 3.3.2. *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. 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.

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



(a) Pack'_i (b) Unpack'_i

Figure 3.1: Definitions of Pack'_i and Unpack'_i in Prop. 3.3.2

- $(\mathrm{Inv}_{q_1}(q_2) \cdot q_2) \cdot a_2(x) = \mathrm{Inv}_{q_1}(q_2) \cdot 0 = 0 \in \mathbb{Z}_{q_2}[x]/f(x)$

Thus, if $\mathsf{Unpack}_i(a(x)) = \mathsf{Unpack}_i(a_1(x), a_2(x)) = \boldsymbol{a}$ then $\mathsf{Unpack}_i(a_1(x), 0) = \boldsymbol{a}$.

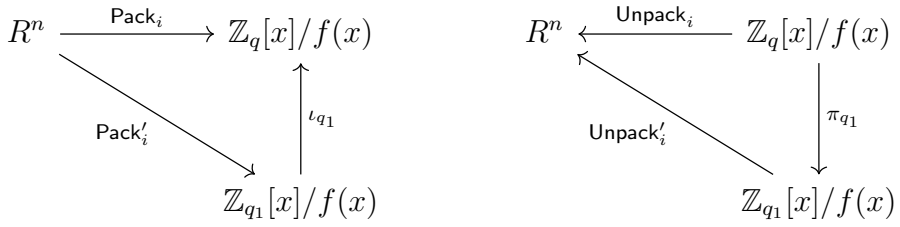
Let π_{q_1} and ι_{q_1} denote the projection and injection between $\mathbb{Z}_q[x]/f(x)$ and $\mathbb{Z}_{q_1}[x]/f(x)$ respectively. Then, for all $a(x) \in \mathbb{Z}_q[x]/f(x)$, $\mathsf{Unpack}_i(a(x))$ is fully determined by $\pi_{q_1}(a(x))$, given it does not output a failure $\perp$.

Define $\mathsf{Pack}'_i := \pi_{q_1} \circ \mathsf{Pack}_i$ and $\mathsf{Unpack}'_i := \mathsf{Unpack}_i \circ \iota_{q_1}$ (Fig. 3.1). Then, it is straightforward that $(\mathsf{Pack}'_i, \mathsf{Unpack}'_i)_{i=1}^D$ is a degree-D packing method for R^n into $\mathbb{Z}_{q_1}[x]/f(x)$.

On the other hand, suppose that $(\mathsf{Pack}'_i, \mathsf{Unpack}'_i)_{i=1}^D$ is a degree-D packing method for R^n into $\mathbb{Z}_{q_1}[x]/f(x)$. Define $\mathsf{Pack}_i := \iota_{q_1} \circ \mathsf{Pack}'_i$ and $\mathsf{Unpack}_i := \mathsf{Unpack}'_i \circ \pi_{q_1}$ (Fig. 3.2). Then, it is straightforward that $(\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^D$ is a degree-D packing method for R^n into $\mathbb{Z}_q[x]/f(x)$. □

Proposition 3.3.3. *Let $p = p_1 \cdot p_2$ and $q = q_1 \cdot q_2$, where $p_1 | q_1$, $p_2 | q_2$ 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. 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



(a) Pack_i (b) Unpack_i

Figure 3.2: Definitions of Pack_i and Unpack_i in Prop. 3.3.2

$1 \leq i \leq D$. 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.

- $(\mathrm{Inv}_{q_1}(q_2) \cdot q_2) \cdot \boldsymbol{a}_1 = (\mathrm{Inv}_{p_1}(q_2) \cdot q_2) \cdot \boldsymbol{a}_1 = \boldsymbol{a}_1 \in \mathbb{Z}_{p_1}^n$
- $(\mathrm{Inv}_{q_1}(q_2) \cdot q_2) \cdot \boldsymbol{a}_2 = \mathrm{Inv}_{q_1}(q_2) \cdot \boldsymbol{0} = \boldsymbol{0} \in \mathbb{Z}_{p_2}^n$
- $(\mathrm{Inv}_{q_1}(q_2) \cdot q_2) \cdot a_1(x) = 1 \cdot a_1(x) = a_1(x) \in \mathcal{R}_1$
- $(\mathrm{Inv}_{q_1}(q_2) \cdot q_2) \cdot a_2(x) = \mathrm{Inv}_{q_1}(q_2) \cdot 0 = 0 \in \mathcal{R}_2$

That is, if $\mathsf{Unpack}_i(a_1(x), a_2(x)) = (\boldsymbol{a}_1, \boldsymbol{a}_2)$ then $\mathsf{Unpack}_i(a_1(x), 0) = (\boldsymbol{a}_1, \boldsymbol{0})$. The similar holds for $j = 2$.

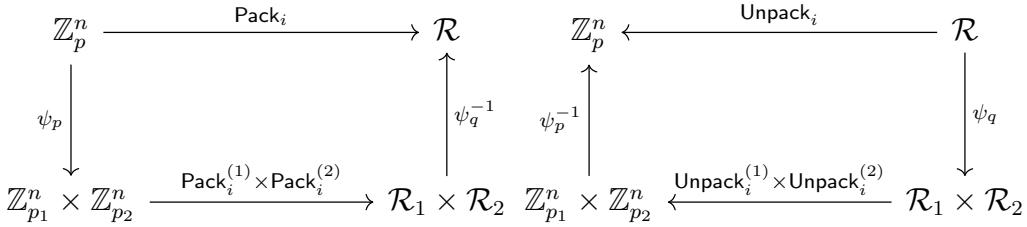
Let π_{p_j} and ι_{p_j} denote the projection and injection between $\mathbb{Z}_p^n$ and $\mathbb{Z}_{p_j}^n$ respectively. Also let π_{q_j} and ι_{q_j} denote the projection and injection between $\mathcal{R}$ and $\mathcal{R}_j$ respectively. Then, for all $a(x) \in \mathcal{R}$, $\pi_{p_j} \circ \mathsf{Unpack}_i(a(x))$ is fully determined by $\pi_{q_j}(a(x))$, given it does not output a failure $\perp$.

Define $\mathsf{Pack}_i^{(j)} := \pi_{q_j} \circ \mathsf{Pack}_i \circ \iota_{p_j}$ and $\mathsf{Unpack}_i^{(j)} := \pi_{p_j} \circ \mathsf{Unpack}_i \circ \iota_{q_j}$ (Fig. 3.3). Then, it is straightforward that $(\mathsf{Pack}_i^{(j)}, \mathsf{Unpack}_i^{(j)})_{i=1}^D$ is a degree-D packing method for $\mathbb{Z}_{p_j}^n$ into $\mathcal{R}_j$.

On the other hand, suppose $(\mathsf{Pack}_i^{(j)}, \mathsf{Unpack}_i^{(j)})_{i=1}^D$ are degree-D packing methods for $\mathbb{Z}{p_j}^n$ into $\mathcal{R}_j$, for $j = 1, 2$. Let ψ_p denote the CRT ring

(a) $\mathsf{Pack}_i^{(j)}$ (b) $\mathsf{Unpack}_i^{(j)}$

Figure 3.3: Definitions of $\mathsf{Pack}_i^{(j)}$ and $\mathsf{Unpack}_i^{(j)}$ in Prop. 3.3.3



(a) Pack_i (b) Unpack_i

Figure 3.4: Definitions of Pack_i and Unpack_i in Prop. 3.3.3

isomorphism from $\mathbb{Z}_p^n$ to $\mathbb{Z}_{p_1}^n \times \mathbb{Z}_{p_2}^n$. Also, let ψ_q denote the CRT ring isomorphism from $\mathcal{R}$ to $\mathcal{R}_1 \times \mathcal{R}_2$. Define $\mathsf{Pack}_i := \psi_q^{-1} \circ (\mathsf{Pack}_i^{(1)} \times \mathsf{Pack}_i^{(2)}) \circ \psi_p$ and $\mathsf{Unpack}_i := \psi_p^{-1} \circ (\mathsf{Unpack}_i^{(1)} \times \mathsf{Unpack}_i^{(2)}) \circ \psi_q$ (Fig. 3.4). Then, it is straightforward that $(\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^D$ is a degree-D packing method for $\mathbb{Z}_p^n$ into $\mathcal{R}$. □

According to Prop. 3.3.1 and 3.3.2, 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. 3.3.1, 3.3.2, and 3.3.3. 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. 3.3.2, 3.3.3). We note that level-consistency (Def. 3.2.2) and subjectivity (Def. 3.2.5) are preserved by the constructions in Prop. 3.3.2 and 3.3.3.

Chapter 4

Constructions

In this chapter, we introduce previous constructions of homomorphic packing (Section 4.1) and propose a new efficient packing method (Section 4.2). We also analyze and compare these homomorphic packing methods regarding properties defined in Section 3.2 (Section 4.3).

4.1 Previous Constructions

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 [DPSZ12]. Most of definitions and statements in this thesis are motivated from these examples.

4.1.1 HElib Packing

In Example 3.1.6, 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 proposed by Gentry-Halevi-Smart [GHS12] and generalized by Halevi-Shoup [HS15] to optimize *bootstrapping* procedure for fully homomorphic encryption (particularly, for HElib [HEl]). In this work, 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 $1/d$.

4.1.2 Overdrive2k Packing

To design an efficient HE-based MPC protocol over $\mathbb{Z}_{2^k}$, Overdrive2k [OSV20] 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. 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 $\mathbb{Z}_{p^k}[x]/f(x)$.

4.1.3 Notes on Overdrive2k Packing

There are other cryptography literature those considering similar problems of Overdrive2k packing [Lip12, BMN17, DLSV20]. They are also interested in embedding several elements into a larger polynomial ring for amortizing computations while providing one multiplication. Even though the authors of Overdrive2k did not present detailed discussions, behind the scene of [Lip12, BMN17, DLSV20], and Overdrive2k [OSV20], there is one of the central problems in additive number theory.

3-free Set Problem. A set of numbers no three of which form an arithmetic progression is called 3-free set (a.k.a. progression-free set or Salem-Spencer Set). Especially, we are most interested in 3-free subset of $[n]$. We denote the size of a largest 3-free subset of $[n]$ by $r_3(n)$.

After Erdős and Turán first considered 3-free set and stated the famous Erdős-Turán conjecture on arithmetic progression [ET36], 3-free set, its variants, and its generalizations have been researched extensively. The strongest lower bound on $r_3(n)$ until now is given by Behrend [Beh46]: $r_3(n) = n/e^{O(\sqrt{\log n})}$. On the other hand, an upper bound by Bloom [Blo16] is known: $r_3(n) = O(n(\log\log n)^4/\log n)$. Meanwhile, a recent manuscript by Bloom and Sisask [BS21] claimed a proof of a stronger upper bound: $r_3(n) = O(\frac{n}{\log^{1+c} n})$ for some $c > 0$.

Recall that Overdrive2k considered the following problem to embed ring

elements as much as they can into a polynomial ring. Consider a subset A of $\{0, 1, \cdots, d-1\}$ 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. We denote the solution to this problem for d by $\rho_3(d)$. Clearly, this problem is closely related to 3-free sets. It is easy to see that $\rho_3(d) = r_3(\lfloor \frac{d+1}{2} \rfloor)$.

Constructing 3-free Sets. There is an elementary method constructing 3-free sets via ternary representations of nonnegative integers. If we construct a set composed of ternary numbers that use only the digits 0 and 1, not 2, such a set must be a 3-free set. If two of its elements a_1 and a_2 are the first and the second of an arithmetic progression of length three, the third a_3 must have the digit two at the position of the least significant digit where a_1 and a_2 differ. Using this method, we can obtain a 3-free subset of $[n]$ with size approximately $n^{\log_3(2)} \approx n^{0.631}$, which is considerably smaller than the lower bound by Behrend. Observing the paper, the authors of Overdrive2k seem to have only considered this ternary construction.

Note that ternary construction can be naturally extended to $(D+1)$-ary construction, yielding a degree-D packing method of density roughly

$$\frac{(d/D)^{\log_{D+1}(2)}}{d}.$$

Meanwhile, Behrend's contruction does not well extend to be used for degree-D packing methods. We also note that constructing an optimal 3-free subset requires an intense amount of computation at the current stage of research. The optimal solutions are known only for small input n's: Gasarch, Glenn, and Kruskal [GGK08] found the exact size of the largest 3-free subset of $[n]$ for $n \leq 187$.

Generalized 3-free Set Problem. To achieve a better packing density, Block, Maji, and Nguyen [BMN17] proposed a generalized version of the 3-

free set problem. The idea is to consider two subsets A and B of $\{0, 1, \cdots, d-1\}$ with $A = \{a_1, \cdots, a_m\}$ and $B = \{b_1, \cdots, b_m\}$ so that $a_i + b_i \neq a_j + b_k$ for all $(i, i) \neq (j, k)$ and $a_i + b_j < d$ for all i, j. The generalized problem is to find the maximum value of $m = |A| = |B|$ with A and B for given d. We denote the solution to this generalized problem for d by $\hat{\rho_3}(d)$. Obviously, $\hat{\rho_3}(d)$ is greater than $\rho_3(d)$. Applying the solution of generalized 3-free set problem on polynomial multiplication, we can use two different embedding methods for right operands and left operands and directly improve the capacity of Overdrive2k. However, the asymmetric nature of the generalized problem significantly reduces freedom in homomorphic computations between packed plaintexts. Therefore, we exclude this approach from the scope of our study.

4.2 New Packing Method for $\mathbb{Z}_{2^k}$-Messages

In this section, we present a new and efficient $\mathbb{Z}_{2^k}$-message packing method for contemporary SHE schemes, e.g. BGV [BGV12]. Since the conventional plaintext packing method of using the isomorphism $\mathbb{Z}_t[x]/\Phi_M(x) \cong \mathbb{Z}_t^{\varphi(M)}$ does not work when $t = 2^k$, an alternative method is required to provide high parallelism.

To tackle this problem, unlike previous approaches which packed messages in coefficients of a polynomial (Section 4.1.2), we pack messages in evaluation points of a polynomial. Here, we detour the impossibility[1] of interpolation on $\mathbb{Z}_{2^k}$ by introducing a *tweaked* interpolation on $\mathbb{Z}_{2^k}$.

[1]For example, over $\mathbb{Z}_{2^k}$, a polynomial $f(x)$ of degree 2 such that $f(0) = f(1) = 0$ and $f(2) = 1$ does not exist.

4.2.1 Tweaked Interpolation

The crux of our packing method is the following lemma: we can perform interpolation on $\mathbb{Z}_{2^k}$ if we 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.

Lemma 4.2.1 (Tweaked Interpolation on $\mathbb{Z}_{2^k}$)**.** *Let $\mu_0, \mu_1, \ldots, \mu_n$ be elements in $\mathbb{Z}_{2^k}$. Assume that an integer δ is not smaller than $\nu_2(n!)$, the multiplicity of 2 in the factorization of $n!$. Then, there exists a polynomial $\Lambda(x) \in \mathbb{Z}_{2^{k+\delta}}[x]$ of degree at most n such that*

$$\Lambda(i) = \mu_i \cdot 2^\delta \qquad \forall i \in [0, n].$$

Proof. Recall that, for $i \in [0, n]$, an i-th Lagrange polynomial on $[0, n]$ is defined as $\lambda_i(x) := \prod_{j \in [0,n] \setminus \{i\}} \frac{x-j}{i-j} \in \mathbb{Q}[x]$. Lagrange polynomial satisfies

$$\lambda_i(x) = \begin{cases} 0 & \text{if } \ x \in [0, n] \text{ and } x \neq i, \\ 1 & \text{if } \ x = i. \end{cases}$$

Note that $2^\delta \lambda_i(x)$ has no multiples of 2 in denominators of its coefficients since $\delta \geq \nu_2(n!)$. Then, we can identify $2^\delta \lambda_i(x)$ as a polynomial over $\mathbb{Z}_{2^{k+\delta}}$ of degree at most n, since the denominator of each coefficient is now invertible in $\mathbb{Z}_{2^{k+\delta}}$. Let $\tilde{\lambda}_i(x) \in \mathbb{Z}_{2^{k+\delta}}[x]$ denote the polynomial. Then,

$$\tilde{\lambda}_i(x) = \begin{cases} 0 & \text{if } \ x \in [0, n] \text{ and } x \neq i, \\ 2^\delta & \text{if } \ x = i. \end{cases}$$

Now, $\Lambda(x) := \sum_{i=0}^{n} \mu_i \cdot \tilde{\lambda}_i(x) \in \mathbb{Z}_{2^{k+\delta}}[x]$ satisfies the claimed property. □

4.2.2 Packing Method from Tweaked Interpolation

Our tweaked interpolation on $\mathbb{Z}_{2^k}$ gives an efficient *degree-2* homomorphic packing for $\mathbb{Z}_{2^k}$-messages into $\mathbb{Z}_{2^{k+2\delta}}[x]/\Phi_M(x)$. Notice the extra δ added

to preserve packed messages: after multiplying two polynomials constructed from tweaked interpolation, the resulting polynomial carries a factor of $2^{2\delta}$. In bird's eye view, our new packing method applies tweaked interpolation on each CRT slots (Eq. (2.1), Section 2.2), while preventing degree overflow and modulus overflow when multiplying two packed polynomials. Recall the isomorphism Eq. (2.1) and the notation $\varphi(M) = r \cdot d$ of $\Phi_M(x)$ (Section 2.2).

Theorem 4.2.2 (Tweaked Interpolation Packing)**.** *Let $\{\mu_{ij}\}_{i,j}$ be $\mathbb{Z}_{2^k}$-messages for $i \in [r]$ and $j \in [0, \lfloor \frac{d-1}{2} \rfloor]$. For integers δ, t satisfying $\delta \geq \nu_2(\lfloor \frac{d-1}{2} \rfloor !)$ and $t \geq k+\delta$, there exists $L(x) \in \mathbb{Z}_{2^t}[x]/\Phi_M(x)$ satisfying the following properties:*

> *Let $L_i(x)$ be the projection of $L(x)$ onto the i-th slot $\mathbb{Z}_{2^t}[x]/F_i(x)$. Then, for each i and j,*
>
> (i) $\deg(L_i(x)) \leq \lfloor \frac{d-1}{2} \rfloor$,
>
> (ii) $L_i(j) = \mu_{ij} \cdot 2^\delta \mod 2^{k+\delta}$.

We call such $L(x)$ a tweaked interpolation packing *of $\{\mu_{ij}\}$.*

Proof. By Lemma 4.2.1, the condition on δ guarantees that there exists $L_i(x) \in \mathbb{Z}_{2^{k+\delta}}[x] \subset \mathbb{Z}_{2^t}[x]$ of degree not greater than $\lfloor \frac{d-1}{2} \rfloor$ such that $L_i(j) = \mu_{ij} \cdot 2^\delta \mod 2^{k+\delta}$ for all $j \in [0, \lfloor \frac{d-1}{2} \rfloor]$. Now, we can define $L(x) \in \mathbb{Z}_{2^t}[x]/\Phi_M(x)$ as the isomorphic image of $(L_1(x), \cdots, L_r(x)) \in \prod_{i=1}^r \mathbb{Z}_{2^t}[x]/F_i(x)$ from the CRT isomorphism; $L(x)$ satisfies the property. □

The next theorem suggests that the tweaked interpolation packing (Theorem 4.2.2) homomorphically preserves the messages under (multiplicative) depth-1 arithmetic circuits. This property implies that we can naturally plug our packing method into the two-level BGV scheme with a plaintext space $\mathbb{Z}_{2^{k+2\delta}}[x]/\Phi_M(x)$ and exploit it for MPC preprocessing phase.

Theorem 4.2.3 (Degree-2 Homomorphism)**.** *Let $L(x)$ and $R(x)$ be polynomials in $\mathbb{Z}_{2^{k+2\delta}}[x]/\Phi_M(x)$ which are tweaked interpolation packings (Theorem 4.2.2, $t = k + 2\delta$) of $\mathbb{Z}_{2^k}$-messages $\{\mu_{ij}^L\}$ and $\{\mu_{ij}^R\}$, respectively. For $\alpha \in \mathbb{Z}_{2^k}$, let $\tilde{\alpha}$ denote an element of $\mathbb{Z}_{2^{k+2\delta}}$ such that $\tilde{\alpha} = \alpha \pmod{2^k}$. Then,*

(a) *$L(x) + R(x)$ is a tweaked interpolation packing of $\{\mu_{ij}^L + \mu_{ij}^R\}$.*

(b) *$\tilde{\alpha} \cdot L(x)$ is a tweaked interpolation packing of $\{\alpha \cdot \mu_{ij}^L\}$.*

(c) *From $LR(x) := L(x) \cdot R(x)$, one can decode homomorphically multiplied $\mathbb{Z}_{2^k}$-messages $\{\mu_{ij}^L \cdot \mu_{ij}^R\}$.*

Proof. Properties (a) and (b) are straightforward from the linearity of projection map and evaluation map, together with the fact that additions and scalar multiplications preserves the degree of polynomial.

To prove (c), let $L_i(x)$, $R_i(x)$, and $LR_i(x)$ respectively be the projection of $L(x)$, $R(x)$, and $LR(x)$ onto the i-th slot $\mathbb{Z}_{2^{k+2\delta}}[x]/F_i(x)$. Then,

$$LR_i(x) = L_i(x) \cdot R_i(x) \qquad \text{in } \mathbb{Z}_{2^{k+2\delta}}[x]/F_i(x).$$

Note that the above equation holds also in $\mathbb{Z}_{2^{k+2\delta}}[x]$: Since the degree of $L_i(x)$ and $R_i(x)$ are at most $\lfloor \frac{d-1}{2} \rfloor$, the sum of their degree is less than the degree d of $F_i(x)$. Therefore,

$$LR_i(j) = L_i(j) \cdot R_i(j) = \mu_{ij}^L \cdot \mu_{ij}^R \cdot 2^{2\delta} \pmod{2^{k+2\delta}},$$

from which one can decode the desired values. □

Remark 4.2.4. We call the packing structure of $LR(x)$ in Theorem 4.2.3(c) the *level-zero* tweaked interpolation packing, whereas the original packing in Theorem 4.2.2 is called *level-one* packing. We omit the level when the packing is of level-one.

Table 4.1: Comparisons on degree-2 packing methods for $\mathbb{Z}_{2^k}$-messages

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

Packing Density. Let $\kappa_k(d)$ denote the packing density of tweaked interpolation packing method for $\mathbb{Z}_{2^k}$-messages when the cyclotomic polynomial $\Phi_M(x)$ splits into irreducible factors of degree d. Then,

$$\kappa_k(d) = \frac{k \cdot \lfloor \frac{d+1}{2} \rfloor}{\left(k + 2\nu_2(\lfloor \frac{d-1}{2} \rfloor !)\right) d} \approx \frac{k}{2(k+d)},$$

where the approximation follows from $\nu_2(\lfloor \frac{d-1}{2} \rfloor !) \approx \frac{d}{2}$ and $\lfloor \frac{d+1}{2} \rfloor \approx \frac{d}{2}$.

Remark 4.2.5. For a fixed $\mathbb{Z}_{2^k}$, the packing density of our method (Theorem 4.2.2) depends only on d: it is better to use $\Phi_M(x)$ with smaller d. When d is sufficiently smaller than k, the packing density approaches $\frac{1}{2}$.

Remark 4.2.6. 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

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

4.3 Analysis and Comparison

In this section, we analyze and compare the homomorphic packing methods previously given in this chapter, with respect to properties defined in Section 3.2. This section is summarized in Table 4.1.

Notice that, in HElib packing which is of degree-∞, packing algorithms and unpacking algorithms are identical for all levels, i.e., *level-consistent*

(Def. 3.2.2). However, in Overdrive2k and our new packing, the packing algorithm differs for each level, i.e., *level-dependent*. 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.[2]

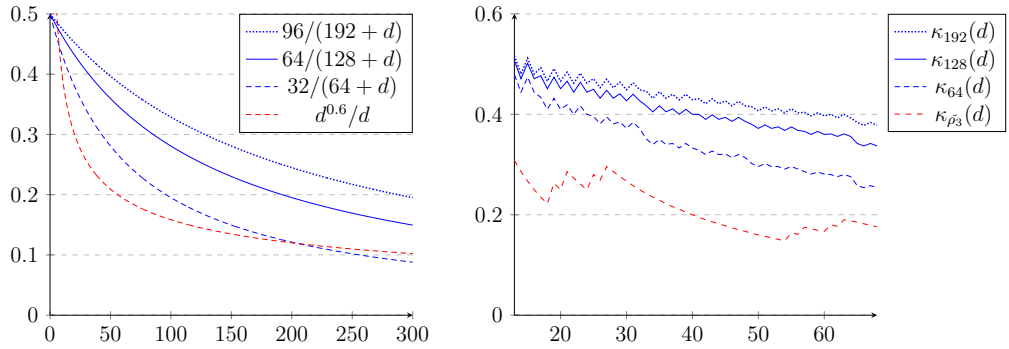
One big difference between our new packing from the previous packings is that it uses a larger modulus for plaintext than that of messages. The other packing methods are sort of coefficient packing, making it no use of increasing the modulus for polynomial ring. This difference will serve as one of the topics in Section 6.1 (e.g. Example 6.1.6).

Note that our new degree-2 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 6.1, we will show that our packing method achieves a certain form of near-optimality (Example 6.1.6).

We now examine common features of these methods. Note that there are *invalid* packings regarding to these packing methods, i.e., they are non-*surjective* packings (Def. 3.2.5). 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.

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*. However, we shed light on the possibility that this CRT approach might be hindering us to achieve a better packing density (Example 6.1.11).

[2] In Section 6.2, we prove the impossibility of designing efficient $\mathbb{Z}_{2^k}$-message packings while satisfying level-consistency.



(a) Rough plots

(b) Exact plots on $13 \leq d \leq 68$

Figure 4.1: Comparison of packing densities on each method according to d

Concrete Efficiency. Let $\kappa_{\tilde{\rho}_3}(d)$ denote the packing density of Overdrive2k packing [OSV20] for given d (Section 4.1.2). In Fig. 4.1a, the rough plots of packing densities according to d are presented: the lowest one is the plot of $d^{0.6}/d$ which was mentioned as a rough estimate of $\kappa_{\tilde{\rho}_3}(d)$ in [OSV20]. The graph suggests that our method has higher packing density than theirs when k is not too small compared to d. For practical parameters, this is always the case: in Fig. 4.1b, the exact plots of packing densities on $13 \leq d \leq 68$ demonstrates that the density of our method is higher than that of Overdrive2k.

Chapter 5

Application to MPC over $\mathbb{Z}_{2^k}$

In this chapter, we apply our new homomorphic packing method for $\mathbb{Z}_{2^k}$-messages (Section 4.2) to secure multi-party computation (MPC). This chapter illustrates how homomorphic packing can be utilized in secure computation and provides a rich context for the implications of the limitations proved later in Chapter 6. To focus on these purposes, we only present the high-level idea of our protocol in this thesis. For formal descriptions and more detailed discussions, please refer to [CKL21].

5.1 Background on MPC and SPD$\mathbb{Z}_{2^k}$

Secure Multi-Party Computation (MPC) aims to jointly compute a function f on input $(x_1, \cdots, x_n)$ each held by n parties $(P_1, \cdots, P_n)$, without revealing any information other than the desired output to each other. Through steady development from the feasibility results in 1980s (e.g., [BOGW88]), MPC research is now at the stage of improving practicality and developing applications to diverse use-cases: auction [BCD+09], secure statistical analysis [BJSV15], privacy-preserving machine learning [DEF+19], etc.

Among various settings of MPC, the most important setting in practice is

the actively corrupted dishonest majority case: corrupted majority is the only meaningful goal in two-party computation (2PC), and modeling the security threat as passive (honest-but-curious) adversaries is often unsatisfactory in real-life applications. At the same time, however, it is notoriously difficult to handle actively corrupted majority efficiently. It is a well-known fact that lightweight information-theoretically secure primitives are not sufficient in this setting and we need rather heavier primitives [CK89].

A seminal work BeDOZa [BDOZ11] observed that one can push the use of heavy public key machinery into a preprocessing phase, without knowing input values and functions to compute. Meanwhile in an online phase, one can securely compute a function using only lightweight primitives. This paradigm, so-called *preprocessing model*, spotlighted the possibility of designing an efficient MPC protocol even in actively corrupted dishonest majority setting. From then, there have been active and steady research on improving efficiency of MPC protocol in this setting: [DPSZ12, DKL+13, KOS16, KPR18, BCS20, RRKK23].

All previously mentioned works consider MPC only over finite fields where arithmetic message authentication code (MAC), the main ingredients of the protocols, is easily defined. Recently, SPD$\mathbb{Z}_{2^k}$ [CDE+18] initiated a study of efficient MPC over $\mathbb{Z}_{2^k}$ in actively corrupted dishonest majority setting by introducing an arithmetic MAC for $\mathbb{Z}_{2^k}$-messages. This is to leverage the fact that integer arithmetic on modern CPUs is done modulo 2^k, e.g. $k = 32, 64, 128$; using MPC over $\mathbb{Z}_{2^k}$, one can naturally deal with such arithmetic. Also, there is no need to emulate modulo prime p operations on CPUs, simplifying the online phase implementation. The authors of SPD$\mathbb{Z}_{2^k}$ claimed that these advantages are much beneficial than the loss from the modified MAC for $\mathbb{Z}_{2^k}$. The claim was convinced by implementation and experimental results [DEF+19].

In regard to the cost of the preprocessing phase, however, there still re-

mains a substantial gap between the finite field case and the $\mathbb{Z}_{2^k}$ case. Particularly, the authors of SPD$\mathbb{Z}_{2^k}$, which is based on oblivious transfer (OT), left an open problem to design an efficient preprocessing phase for MPC over $\mathbb{Z}_{2^k}$ from lattice-based homomorphic encryption (HE). The motivation here is that the HE-based approach has proved the best performance in the finite field case.

The main difficulty is that the conventional message packing method using the isomorphism of cyclotomic ring $\mathbb{Z}_t[x]/\Phi_M(x) \cong \mathbb{Z}_t^{\varphi(M)}$ does not work when t is not prime, especially when $t = 2^k$. This makes it hard to fully leverage the batching technique of HE and causes inefficiency compared to the finite field case. Followup works, Overdrive2k [OSV20] and Mon$\mathbb{Z}_{2^k}$a [CDRFG20], proposed more efficient preprocessing phases for MPC over $\mathbb{Z}_{2^k}$, yet they do not give a satisfactory solution to this problem.

5.2 Overview of Our Protocol

We propose an MPC over $\mathbb{Z}_{2^k}$ from Somewhat HE (SHE) in actively corrupted dishonest majority setting. It is based on our new efficient homomorphic packing method for $\mathbb{Z}_{2^k}$-messages (Section 4.2) and non-trivial adaptations of techniques used in the finite field case to the $\mathbb{Z}_{2^k}$ case.

Note that the core of an SHE-based MPC preprocessing phase is the triple (or *authenticated* Beaver's triple [Bea92]) generation protocol which consists of the following building blocks (see Section 5.3):

- a *packing* method for SHE which enables parallelism of the protocol and enhances amortized performance;
- the *reshare* protocol which re-encrypts a *level-0* ciphertext to a *fresh* ciphertext allowing two-level SHE to be sufficient for the generation of authenticated triples;

- and *ZKPoPK* (zero-knowledge proof of plaintext knowledge) which guarantees that ciphertexts are validly generated from a plaintext and restricts adversaries from submitting maliciously generated ciphertexts.

We present improvements on all of these building blocks for $\mathbb{Z}_{2^k}$-messages and integrate them into our new preprocessing phase, which is compatible with the online phase of SPD$\mathbb{Z}_{2^k}$.

Our New Packing Method for $\mathbb{Z}_{2^k}$-messages. Under the plaintext ring of degree N, our homomorphic packing method (Section 4.2) achieves near $N/2$-fold parallelism while providing degree-2 homomorphism, enough for the preprocessing phase. Previously, the best solution over $\mathbb{Z}_{2^k}$ of Overdrive2k [OSV20] (Section 4.1.2) only achieved roughly $N/5$-fold parallelism. Thus, our homomorphic packing method directly offers 2.5x improvement in the overall (amortized) performance of the preprocessing phase. (See Section 4.3.)

Reshare Protocol for Level-dependent Packings. A seeming problem is that it is difficult to design a *level-consistent* packing method for $\mathbb{Z}_{2^k}$-messages with high parallelism (Section 4.3), while the previous reshare protocol for messages in finite fields (with *level-consistent* packing) should be modified to be utilized in this setting.[1] To this end, in the reshare protocol of Overdrive2k [OSV20], an extra masking ciphertext with ZKPoPK, which is the most costly part, is provided. We propose a new reshare protocol for *level-dependent* packings, which resolves this problem and closes the gap between the field case and the $\mathbb{Z}_{2^k}$ case (Section 5.4). Concretely, in our triple generation, the total number of ZKPoPK is *five* as using the original reshare,

[1] In Section 6.2, we prove the impossibility of designing 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 our trick.

whereas Overdrive2k requires *seven*. From this aspect, we gain an additional 1.4x efficiency improvement in total communication cost.

Better ZKPoPKs over $\mathbb{Z}[x]/\Phi_p(x)$. When the messages are in $\mathbb{Z}_{2^k}$, using power-of-two cyclotomic rings $\mathbb{Z}[x]/\Phi_{2^m}(x)$ introduces a huge inefficiency in packing, since $\Phi_{2^m}(x)$ has only one irreducible factor in $\mathbb{Z}_{2^k}[x]$ (Section 2.2). Thus, it is common to use *odd* cyclotomic rings for $\mathbb{Z}_{2^k}$-messages. In this case, however, we cannot leverage known efficient ZKPoPKs over the ciphertexts regarding $\mathbb{Z}[x]/\Phi_{2^m}(x)$, such as TopGear [BCS20].

To this end, we develop an efficient ZKPoPK over $\mathbb{Z}[x]/\Phi_p(x)$ where p is a prime . This new protocol is an adaptation of TopGear to the $\mathbb{Z}_{2^k}$ case. The essence of our protocol is that the core properties of power-of-two cyclotomic rings, which was observed in [BCK+14], hold similarly also in prime cyclotomic rings.[2] This fact not only improves the amortized communication cost, latency, and memory consumption of our ZKPoPK, but can also has ramifications on works derived from [BCK+14].

ZKP of Message Knowledge. When the message space is $\mathbb{Z}_p$ for a moderate-sized prime p, we can take M to satisfy $p = 1 \pmod M$ so that the plaintext space $\mathbb{Z}_p[x]/\Phi_M(x)$ is *isomorphic* to $\mathbb{Z}_p^{\varphi(M)}$, a product of the message space. In this case, we can effortlessly use the conventional packing method (Example 3.1.6) where any plaintext from $\mathbb{Z}_p[x]/\Phi_M(x)$ is a valid encoding for some messages from $\mathbb{Z}_p^{\varphi(M)}$. That is, we can use a *surjective* packing method (Section 4.3) when dealing with $\mathbb{Z}_p$-messages.

However, this is not the case for $\mathbb{Z}_{2^k}$-messages. As remarked in Section 4.3, our new packing method and previous methods for $\mathbb{Z}_{2^k}$-messages are not

[2] In fact, we can prove that the similar property also holds in cyclotomic rings with $M = p^s q^t$, where p and q are prime. [CKKL22] This allows us more freedom in the choice of cyclotomic ring and, thus, better performance.

surjective except for trivial cases. In fact, we will see that this is inevitable for $\mathbb{Z}_{2^k}$-messages. (See Section 6.3.)

Thus, to achieve malicious security, HE-based protocols with $\mathbb{Z}_{2^k}$-messages must guarantee that each ciphertext encrypts a *valid plaintext* with respect to a specific packing method, in addition to the guarantee of valid encryption. This is an intricacy of the $\mathbb{Z}_{2^k}$-message case, which differs from the $\mathbb{Z}_p$-message case where ZKPoPK (for the guarantee of valid encryption) is sufficient [DPSZ12, DKL+13, KPR18, BCS20].

In this regard, extending ZKPoPK, we conceptualize *Zero-Knowledge Proof of Message Knowledge (ZKPoMK)*, which guarantees that the given ciphertext is encrypting a plaintext that is a *valid encoding* for some messages with respect to a specific packing method. Indeed, we also propose a ZKPoMK for our new packing method (Section 4.2) and plug it into our MPC protocol.

Performance. We can summarize the improvements by our packing (Section 4.2) and reshare protocol (Section 5.4) as follows: (i) Our new homomorphic packing achieves near 1/2 packing density, 2.5x compared to 1/5 of Overdrive2k [OSV20], (ii) Our reshare protocol requires only 5 ZKPoPKs which is 1.4x less than 7 ZKPoPKs of Overdrive2k. In total, we can expect that the amortized communication costs of our protocol will show 3.5x improvements from Overdrive2k. Concretely, in our preprocessing phase, the amortized communication costs for triple generation[3] (in kbit) over $\mathbb{Z}_{2^{32}}$ and $\mathbb{Z}_{2^{64}}$, respectively, are 27.4 and 43.3 which outperforms the current best results, 59.1 of Mon$\mathbb{Z}_{2^k}$a [CDRFG20] and 153.3 of Overdrive2k [OSV20], respectively showing 2.2x and 3.5x improvements.

[3]We assume a two-party case, and similar improvements occur in multi-party cases.

5.3 Authenticated Triple Generation

In this section, we describe how to put all the tools together to construct an MPC protocol for $\mathbb{Z}_{2^k}$-messages. Since our MPC protocol follows the online phase of SPD$\mathbb{Z}_{2^k}$ [CDE+18], the goal of our preprocessing phases is to generate *authenticated triples* with respect to SPD$\mathbb{Z}_{2^k}$-MAC. That is, n parties together securely generate secret shares $[a]_i, [b]_i, [c]_i$ and $[\alpha a]_i, [\alpha b]_i, [\alpha c]_i$ in $\mathbb{Z}_{2^{\tilde{k}}}$ such that $\sum_i [a]_i = a \bmod 2^k$, $\sum_i [\alpha a]_i = \alpha a \bmod 2^{\tilde{k}}$, and similar for the others, satisfying $c = ab \bmod 2^k$. Here, $\tilde{k} := k+s$ with s as a security parameter[4], and $\alpha \in \mathbb{Z}_{2^{\tilde{k}}}$ is a single global MAC key of which share $[\alpha]_i \in \mathbb{Z}_{2^s}$ is given to the i-th party. Then, in the online phase, the parties can securely compute any arithmetic circuit via Beaver's trick [Bea92, CDE+18] with these authenticated triples.

Overview of Authenticated Triple Generation. We give an overview of our preprocessing phase, focusing on the triple generation protocol, which follows the standard methods of SPDZ [DPSZ12] (and Overdrive2k [OSV20]) exploiting *two-level* SHE and zero-knowledge proofs (ZKP) on it. We remark that message packing of SHE enable the parties to generate multiple authenticated triples (represented by vectors) in one execution of the triple generation protocol, significantly reducing the amortized costs.

First, each party P_i generates and broadcasts HE ciphertexts $\mathfrak{ct}_{\boldsymbol{a}_i}$ and $\mathfrak{ct}_{\boldsymbol{b}_i}$ each encrypting the *vectors* $[\boldsymbol{a}]_i$ and $[\boldsymbol{b}]_i$ of random shares from $\mathbb{Z}_{2^{\tilde{k}}}$; we omit the superscript$^{(1)}$ for level-one ciphertexts. Then, all parties run ZKPoMK on $\mathfrak{ct}_{\boldsymbol{a}} = \sum_i \mathfrak{ct}_{\boldsymbol{a}_i}$ and $\mathfrak{ct}_{\boldsymbol{b}} = \sum_i \mathfrak{ct}_{\boldsymbol{b}_i}$ to guarantee that each ciphertext is generated correctly. Next, all parties compute a ciphertext $\mathfrak{ct}_{\boldsymbol{c}}^{(0)} := \mathfrak{ct}_{\boldsymbol{a}} \boxtimes \mathfrak{ct}_{\boldsymbol{b}}$ whose underlying message is the Hadamard product $\boldsymbol{c} = \boldsymbol{a} \odot \boldsymbol{b}$. Similarly, given ciphertexts $\mathfrak{ct}_{\alpha_i}$, all parties can also compute $\mathfrak{ct}_{\alpha\boldsymbol{a}}^{(0)}$ and $\mathfrak{ct}_{\alpha\boldsymbol{b}}^{(0)}$ with homomorphic

[4] SPD$\mathbb{Z}_{2^k}$-MAC provides $\mathsf{sec} = s - \log(s+1)$-bit security [CDE+18, Theorem 1].

operations on the ciphertexts. The parties, however, cannot directly compute $\mathfrak{ct}_{\alpha \boldsymbol{c}}$ from ciphertext multiplication between $\mathfrak{ct}_{\boldsymbol{c}}^{(0)}$ and $\mathfrak{ct}_{\alpha}$ since the former is of level-zero.

Thus, the parties perform so-called *reshare* protocol [DPSZ12] which, given $\mathfrak{ct}_{\boldsymbol{c}}^{(0)}$ as the input, outputs a *level-one* ciphertext $\mathfrak{ct}_{\boldsymbol{c}}$ having the same message as the input and/or the random shares $[\boldsymbol{c}]_i$ of the message to each party. Roughly, it proceeds by decrypting the masked input $\mathsf{ModSwitch}(\mathfrak{ct}_{\boldsymbol{f}}) \boxplus \mathfrak{ct}_{\boldsymbol{c}}^{(0)}$ to get a (masked) message $\boldsymbol{f}+\boldsymbol{c}$, then subtracting the mask $\mathfrak{ct}_{\boldsymbol{f}}$ from the fresh encryption $\mathfrak{ct}_{\boldsymbol{f}+\boldsymbol{c}}$ of the message, resulting in $\mathfrak{ct}_{\boldsymbol{c}} = \mathfrak{ct}_{\boldsymbol{f}+\boldsymbol{c}} \boxminus \mathfrak{ct}_{\boldsymbol{f}}$. Then, parties can compute $\mathfrak{ct}_{\alpha \boldsymbol{c}}^{(0)} := \mathfrak{ct}_{\boldsymbol{c}} \boxtimes \mathfrak{ct}_{\alpha}$. Here, ZKPs for the masking ciphertext $\mathfrak{ct}_{\boldsymbol{f}}$ is also required.

Finally, parties jointly perform *distributed decryption* on the ciphertexts $\mathfrak{ct}_{\alpha \boldsymbol{a}}$, $\mathfrak{ct}_{\alpha \boldsymbol{b}}$, and $\mathfrak{ct}_{\alpha \boldsymbol{c}}$ to get random shares of the underlying messages: $[\alpha \boldsymbol{a}]_i$, $[\alpha \boldsymbol{b}]_i$, and $[\alpha \boldsymbol{c}]_i$. The parties already have the other components of the triple ($[\boldsymbol{a}]_i$, $[\boldsymbol{b}]_i$, and $[\boldsymbol{c}]_i$), so the authenticated triple is generated.

5.4 Reshare for Level-dependent Packings

When designing a packing method for $\mathbb{Z}_{2^k}$-messages with high parallelism, it is hard to not get a *level-dependent* packing, e.g., the Overdrive2k [OSV20] packing (Section 4.1.2) and our new homomorphic packing (Section 4.2, Remark 4.2.4). However, this leads to a complication in the reshare protocol for $\mathbb{Z}_{2^k}$-messages, which does not occur in the case of a finite field $\mathbb{Z}_p$ with *level-consistent* packing from the isomorphism $\mathbb{Z}_p[x]/\Phi_{2^m}(x) \cong \mathbb{Z}_p^{\varphi(2^m)}$. In particular, the reshare protocol of Overdrive2k [OSV20] exploits an extra masking ciphertext with ZKPoPK on it, which is the most costly part, to remedy the issue.

In this section, we propose a new reshare protocol for *level-dependent* packings, which resolves this complication: our protocol extends the previous

reshare protocol of the finite field case to operate also with level-dependent packings *without any extra cost*. Our result closes the gap between the finite field and the $\mathbb{Z}_{2^k}$ cases which originates from the level-dependency.

The Problem of Level-dependent Packings. Recall that the goal of the reshare protocols is, for an input level-zero ciphertext, to output shares of the underlying message along with a *level-one* ciphertext having the same message as the input (Section 5.3). The complication, with a level-dependent packing, is that we have to manage not only the *ciphertext level* but also the *packing level*.

Recall that one masking ciphertext $\mathfrak{ct}_f$ is used twice in the reshare protocol for the finite field case: once to mask the input ciphertext of level-zero and once to reconstruct the fresh ciphertext of level-one by subtracting it (Section 5.3). While the difference of ciphertext levels can be managed easily with modulus-switching, that of the packing levels seems to be problematic.

Solution of Overdrive2k. To resolve this problem, Overdrive2k [OSV20] provides two masking ciphertexts having the *same messages* but in *different packing*: one with level-zero packing and the other with level-one packing. This approach requires an extra ZKPoPK with the additional broadcast of the masking ciphertext, doubling the cost of the reshare protocol. It results in substantial increase of cost in the whole preprocessing protocol. In the triple generation protocol, the number of ZKPoPK with broadcasts of ciphertexts is *five* using the original reshare protocol in the field case, whereas Overdrive2k requires *seven* due to their reshare protocol, resulting roughly a 1.4x reduction in efficiency.[5]

[5]The number of ZKPoPK is counted regarding the *correlated* sacrifice technique [KOS16].

Our Solution. The crux of our reshare protocol for level-dependent packings is the idea of generating the ciphertext $\mathfrak{ct}_\alpha$ of the MAC key $\alpha \in \mathbb{Z}_{2^s}$ by treating α as a constant in the cyclotomic ring $\mathbb{Z}_{2^t}/\Phi_M(x)$, i.e. $\mathfrak{ct}_\alpha = \mathsf{Enc}(\alpha)$ for $\alpha \in \mathbb{Z}_{2^t}/\Phi_M(x)$ *without* any packing structure. Then, we actually do *not* need the fresh ciphertext to be of packing level-one: it is okay to be of packing level-zero. This is because, whereas multiplying $\mathfrak{ct}_\alpha$ to a ciphertext consumes a ciphertext level, multiplying α to a plaintext does not consume a packing level, i.e. multiplying α is a linear operation in the aspect of packing (Theorem 4.2.3(b)).

Chapter 6

Limitations

In this chapter, we explore several mathematical limitations of homomorphic packing, regarding packing density (Def. 3.2.1), level-consistency (Def. 3.2.2), and surjectivity (Def. 3.2.5). Our results on the limitations of homomorphic packing have several implications on HE packing, HE-based MPC, and RMFE. In particular, our results justify our approaches and design choices for the packing method (Section 4.2) and the MPC protocol (Chapter 5).

6.1 Packing Density

In this section, we examine upper bounds on packing density (Def. 3.2.1) of degree-D packing methods for $\mathbb{Z}_{p^k}$ and $\mathbb{F}_{p^k}$, where p is a prime (See Section 3.3). Our main result is that, when a packing method provides somewhat homomorphism upto degree-D polynomials, the packing density is roughly upper bounded by $1/D$ (Thm. 6.1.5 and 6.1.14). The results have implications in our new packing method (Example 6.1.6) and RMFE (Example 6.1.7 and 6.1.18).

6.1.1 Algebraic Background

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

Proposition 6.1.1. *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 Section 6.1.4 □

Remark 6.1.2. 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. 6.1.1.

6.1.2 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 6.1.2. 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 6.1.3. *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 3.1.3), 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 6.1.2). □

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 6.1.6 - 6.1.12). The following is a small remark on packings of non-zero elements modulo p in this setting.

Remark 6.1.4. 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, $\mathsf{Unpack}_i(p^{k-1} \cdot a(x)) = \mathsf{Unpack}_i(0) = \boldsymbol{0} \neq p^{k-1} \cdot \boldsymbol{a}$, contradicting the linear homomorphic property (Remark 3.1.3). 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. 6.1.3 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 6.1.5. *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 $\mathcal{A}^{(r,s)} := \{a_1(x)^r \cdot a_j(x)^s\}_{1<j\leq n}$. That is, $\mathcal{A}^{(0,D)} = \{a_2(x)^D, \cdots, a_n(x)^D\}$, $\mathcal{A}^{(D,0)} = \{a_1(x)^D\}$, 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 3.1.3): $\mathcal{A}_1 = \{a_2(x), \cdots, a_n(x)\}$ (See also Prop. 6.1.3).

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 6.1.4) 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 $\sum_{a_\alpha(x) \in \mathcal{A}} (c_\alpha \cdot a_\alpha(x)) = 0$, 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 6.1.2). □

The following are direct consequences of our theorem.

Example 6.1.6. Degree-D packing methods for $\mathbb{Z}_{p^k}$-messages to $\mathbb{Z}_{p^k}[x]/f(x)$, 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 4.3). 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, our new packing method already nearly reaches the optimal packing density for packing methods for $\mathbb{Z}_{p^k}$-messages into $\mathbb{Z}_{p^k}[x]/f(x)$ (Section 4.2). 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 our new packing method, the only possibility is choosing $t > k$ or not employing the CRT approach. (See also Example 6.1.12)

Example 6.1.7 (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. 6.1.5. 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 6.1.8. 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. 6.1.3, 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. 6.1.5. 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 6.1.9. 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 6.1.8, 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.

The following theorem is a bit more general version of Thm. 6.1.5 which has no restriction on the quotient polynomial. However, it assumes the existence of a unit of $\mathcal{R}$ which unpacks to an element of $\mathbb{Z}_{p^k}^n$.

Theorem 6.1.10. *Let* $(\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^D$ *be a degree-*D *packing method for* $\mathbb{Z}_{p^k}^n$ *into* $\mathcal{R} := \mathbb{Z}_{p^k}[x]/f(x)$*. Suppose a linear combination of* $\{a_i(x)\}_{i\in I}$ *is a unit in* $\mathcal{R}$*, where each* $a_i(x) \in \mathcal{R}$ *satisfies* $\mathsf{Unpack}_1(a_i(x)) = \boldsymbol{e}_i$*. Then,* $d \geq D \cdot (n - |I|) + |I|$ *holds.*

Sketch. Assume $u(x) := \sum_{i\in I} c_i \cdot a_i(x)$ is a unit, for some $c_i \in \mathbb{Z}_{p^k}$. The proof is exactly same as that of Thm. 6.1.5, but with only difference in the definition of $\mathcal{A}^{(r,s)}$ and $\mathcal{A}$. Here, we define $\mathcal{A}^{(r,s)} := \{u(x)^r \cdot a_j(x)^s\}_{j\notin I}$ and $\mathcal{A} := \mathcal{A}_D \cup \{a_i(x)^D\}_{i\in I}$. □

The following are some consequences of Thm. 6.1.10.

Example 6.1.11. We can revisit upper bound on packing density of *CRT* packings (Section 4.3) using Thm. 6.1.10. Consider degree-D CRT packing methods $(\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^{D}$ for $\mathbb{Z}_{p^k}$-messages into $\mathcal{R} := \mathbb{Z}_{p^k}[x]/f(x)$, where $f(x)$ factors into r distinct irreducible factors modulo p. Let $f(x) = \prod_{i=1}^{r} f_i(x)$ via Hensel lifting.

By Remark 6.1.4, for each $i \in [r]$, we have $a^{(i)}(x)$ such that (i) $a^{(i)}(x)$ is a unit modulo $f_\imath(x)$ if and only if $\imath = i$ and (ii) $\mathsf{Unpack}_1(a^{(i)}(x)) = \boldsymbol{e}_j$ for some distinct $j \in [n]$. Then, $\sum_{i=1}^{r} a^{(i)}(x)$ is a unit in $\mathcal{R}$. That is, we have $|I| = r$ for Thm. 6.1.10, yielding the upper bound $\frac{1}{D} + \frac{r}{\deg(f)} \cdot (1 - \frac{1}{D})$ previously shown in Example 6.1.6.

Example 6.1.12. Suppose one wants to design a degree-D packing method for $\mathbb{Z}_{p^k}$-messages into $\mathbb{Z}_{p^k}[x]/f(x)$ which has a packing density substantially larger than $1/D$. The only possibility is designing a packing method where every unit element of $\mathbb{Z}_{p^k}[x]/f(x)$ unpacks to elements of $\mathbb{Z}_{p^k}^n$ with very few zero coordinates or fails to unpack at level-1.

6.1.3 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. 6.1.3. Unlike the simple and plausible statement, the proof is quite involved. In particular, it depends on Remark 6.1.2. 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 6.1.13. *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 3.1.3), 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 6.1.2). □

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 6.1.18 - 6.1.21).

Our main result in this subsection is the following theorem, which is a finite field analogue of Thm. 6.1.5. 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. 6.1.13 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 6.1.14. *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. Let $(\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^D$ be a degree-D packing method for $\mathbb{F}_{p^k}^n$ into $\mathcal{R}$. For each $i \in [n]$ and $j \in [k]$, choose $a_{ij}(x) \in \mathcal{R}$ such that $\mathsf{Unpack}_1(a_{ij}(x)) =$

$\beta_j \cdot \boldsymbol{e}_i$. For each $s \in \mathbb{Z}^+$, fix a basis $\mathcal{B}_s := \{\beta^{(s)_j}\}_j$ of $\langle \beta_1^s, \cdots, \beta_k^s \rangle$. Then, there exist $a_{ij}^{(s)}(x) \in \mathcal{R}$ such that (i) $\mathsf{Unpack}_s(a_{ij}^{(s)}(x)) = \beta_j^{(s)} \cdot \boldsymbol{e}_i$ and (ii) $a_{ij}^{(s)}(x)$ is a linear combination of $\{a_{ij}(x)^s\}_{j\in[k]}$. Let us denote $\mathcal{A}^{(r,s)} := \{a_{11}(x)^r \cdot a_{ij}^{(s)}(x)\}_{1<i\leq n \ \&\ j\in[|\mathcal{B}_s|]}$.

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 3.1.3): $\mathcal{A}_1 = \{a_{ij}(x)\}_{1<i\leq n \ \&\ j\in[k]}$ (See also Prop. 6.1.3).

Suppose $\mathcal{A}_t$ is linearly independent for some $t < D$. View $\mathcal{A}_{t+1}$ as $\mathcal{A}^{(0,t+1)} \cup a_{11}(x) \cdot \mathcal{A}_t$. Suppose $\sum_{a_\alpha(x)\in\mathcal{A}_{t+1}}(c_\alpha \cdot a_\alpha(x)) = 0$, for some $c_\alpha \in \mathbb{Z}_p$. 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 $a_{11}(x)\cdot\mathcal{A}_t$ 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:

$$\sum_{a_\alpha(x)\in a_{11}(x)\cdot\mathcal{A}_t} (c_\alpha \cdot a_\alpha(x)) = 0.$$

Meanwhile, since $a_{11}(x)$ is non-zero (and hence a unit in $\mathcal{R}$) (Remark 3.1.3) and $\mathcal{A}_t$ is linearly independent by induction hypothesis, $c_\alpha = 0$ must also hold for all $a_\alpha(x) \in a_{11}(x) \cdot \mathcal{A}_t$. Thus, $\mathcal{A}_t$ is linearly independent in $\mathcal{R}$ for all $t \leq D$.

Step 2: Now consider the set $\mathcal{A} := \mathcal{A}_D \cup \{a_{1j}^{(D)}(x)\}_{j\in[|\mathcal{B}_D|]}$, which coincides with $\{a_{ij}^{(D)}(x)\}_{i\in[n] \ \&\ j\in[|\mathcal{B}_D|]} \cup a_{11}(x) \cdot \mathcal{A}_{D-1}$. Suppose $\sum_{a_\alpha(x)\in\mathcal{A}}(c_\alpha \cdot a_\alpha(x)) = 0$, for some $c_\alpha \in \mathbb{Z}_p$. Then, by linear homomorphic property at level-D, $c_\alpha = 0$ must hold for all $a_\alpha(x) \in \{a_{ij}^{(D)}(x)\}_{i\in[n] \ \&\ j\in[|\mathcal{B}_D|]}$, since elements of $a_{11}(x) \cdot \mathcal{A}_{D-1}$ unpack to $\mathbf{0}$ and $\{a_{ij}^{(D)}(x)\}_{i\in[n] \ \&\ j\in[|\mathcal{B}_D|]}$ unpacks to a linearly

independent set by construction. Subsequently, we have again the following equality:

$$\sum_{a_\alpha(x)\in a_{11}(x)\cdot\mathcal{A}_{D-1}} (c_\alpha \cdot a_\alpha(x)) = 0.$$

Meanwhile, since $a_{11}(x)$ 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 $a_\alpha(x) \in a_{11}(x)\cdot\mathcal{A}_{D-1}$. Thus, $\mathcal{A}$ is linearly independent, and therefore $d \geq |\mathcal{A}|$ must hold. □

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 6.1.15. *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 6.1.16. *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. 6.1.14 on the basis $\{1, \beta, \beta^2, \cdots, \beta^{k-1}\}$ with the help of Prop. 6.1.15. □

Remark 6.1.17. Since $\gcd(p^k - 1, t) \leq t$, we have $\sigma^{(t)}_{p^k} \geq \log_p(\frac{p^k-1}{t})$. Subsequently, we have a very rough bound of $\sigma^{(t)}_{p^k} \gtrsim k - \log_p(t)$. Applying this bound to Cor. 6.1.16, we have the following bound.

$$d \geq k \cdot (D \cdot (n-1) + 1) - \log_p(D \cdot (D!)^{n-1})$$

The following are some consequences of our main result.

Example 6.1.18 (RMFE)**.** Note that $\sigma^{(1)}_{p^k}$ and $\sigma^{(2)}_{p^k}$ are always k. Then, by Cor. 6.1.16, 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 [CXY20]). However, previous proofs do not extend to higher-degree cases (See Example 6.1.20) or to the Galois ring case (See Example 6.1.7).

Example 6.1.19 (Degree-2 Packing)**.** By Example 6.1.18, 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 4.3). 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. 6.1.13. Thus, only possibility is not employing the CRT approach (See also Remark 6.1.23).

Example 6.1.20 (Degree-3 Packing)**.** Note that $\sigma^{(3)}_{p^k}$ is always k, except the case of $p^k = 4$. Then, by Cor. 6.1.16, 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. 6.1.13. Thus, only possibility is choosing $t = 2$ or not employing the CRT approach (See also Remark 6.1.23).

Example 6.1.21. By the same arguments as in Example 6.1.8 and 6.1.9, 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.

The following theorem is a bit more general version of Thm. 6.1.14 which has no restriction on the quotient polynomial. However, it assumes the existence of a unit of $\mathcal{R}$ which unpacks to an element of $\mathbb{F}_{p^k}^n$.

Theorem 6.1.22. *Let $\mathcal{B} := \{\beta_1, \cdots, \beta_k\}$ be a basis of $\mathbb{F}_{p^k}$ as a $\mathbb{F}_p$-vector space. Let $(\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^D$ be a degree-D packing method for $\mathbb{F}_{p^k}^n$ into $\mathcal{R} := \mathbb{Z}_p[x]/f(x)$. Suppose a linear combination of $\{a_{ij}(x)\}_{i \in I \ \& \ j \in [k]}$ is a unit in $\mathcal{R}$, where each $a_{ij}(x) \in \mathcal{R}$ satisfies $\mathsf{Unpack}_1(a_{ij}(x)) = \beta_j \cdot \boldsymbol{e}_i$. Then, the following inequality holds.*

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

Sketch. Assume $u(x) := \sum_{i\in I \ \&\ j\in[k]} c_{ij}\cdot a_{ij}(x)$ is a unit, for some $c_i \in \mathbb{Z}_p$. The proof is exactly same as that of Thm. 6.1.14, but with only difference in the definition of $\mathcal{A}^{(r,s)}$ and $\mathcal{A}$. Here, we define $\mathcal{A}^{(r,s)} := \{u(x)^r \cdot a_{ij}^{(s)}(x)\}_{i\notin I \ \&\ j\in[|\mathcal{B}_s|]}$ and $\mathcal{A} := \mathcal{A}_D \cup \{a_{ij}^{(D)}(x)\}_{i\in I \ \&\ j\in[|\mathcal{B}_D|]}$. □

Remark 6.1.23. As Cor. 6.1.16, and Rem. 6.1.17, we can apply Prop. 6.1.15 to have a more concrete version of Thm. 6.1.22. The theorem has analogous consequences of Example 6.1.11 and 6.1.12.

6.1.4 Proof of Prop. 6.1.1

We believe the following proposition is a classic fact in algebra. Nonetheless, since we could not find a proper reference containing the statement, we give a proof. Our proof is a more or less verbatim of the proof given in [Con] for the analogous fact on principal ideal *domains* (PID).

Proposition 6.1.24. *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. A free R-module of rank n is isomorphic to R^n, so we can assume the free R-module is R^n without loss of generality. We proceed by induction on n. The case where $n = 0$ is trivial. The case where $n = 1$ is true since R is a PIR: every R-submodule of R is a principal ideal, i.e. can be finitely generated with 1 generator.

Suppose the statement is proved for all free R-modules of rank not larger than n. Let M be a submodule of R^{n+1}. Let $\pi : R^{n+1} \to R^n$ be the projection which maps an element of R^{n+1} to its first n coordintes. First consider the image of $\pi|_M$, the restriction of π to M. Indeed, the image is $\pi_M(R^{n+1}) = \pi(M)$, which is a submodule of R^n and therefore has at most n generators by the inductive hypothesis. Thus, we can put $\pi(M) = \sum_{i=1}^{k} R\cdot \boldsymbol{b}_i$ for some $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_k \in R^n$ where $k \leq n$. Let $\boldsymbol{b}_i = \pi(\boldsymbol{a}_i)$ for some $\boldsymbol{a}_i \in M$. Then,

$\pi_M(R^{n+1}) = \pi(M) = \sum_{i=1}^{k} R \cdot \pi(\boldsymbol{a}_i)$. And $\ker(\pi|_M) = M \cap \ker(\pi)$. Notice $\ker(\pi) \cong R$ as R-modules. Since R is a PIR, $\ker(\pi|_M) = R \cdot \boldsymbol{a}_0$ for some $\boldsymbol{a}_0 \in M$.

We will show $M = \sum_{i=0}^{k} R \cdot \boldsymbol{a}_i$, and therefore M can be generated by $k+1$ generators $\boldsymbol{a}_0, \cdots, \boldsymbol{a}_k$ with $k+1 \leq n+1$. It is clear that $\sum_{i=0}^{k} R \cdot \boldsymbol{a}_i \subset M$. For the other direction, choose an arbitrary $\boldsymbol{a} \in M$. Then, from the above discussions, $\pi|_M(\boldsymbol{a}) = r_1\pi(\boldsymbol{a}_1) + \cdots + r_k\pi(\boldsymbol{a}_k) = \pi(r_1\boldsymbol{a}_1 + \cdots + r_k\boldsymbol{a}_k)$ for some $r_1, \cdots, r_k \in R$. Therefore $\boldsymbol{a} - \sum_{i=1}^{k} r_i\boldsymbol{a}_i \in \ker(\pi|_M)$, and $\boldsymbol{a} - \sum_{i=1}^{k} r_i\boldsymbol{a}_i = r_0\boldsymbol{a}_0$ for some $r_0 \in R$. Thus $\boldsymbol{a} = r_0\boldsymbol{a}_0 + r_1\boldsymbol{a}_1 + \cdots + r_k\boldsymbol{a}_k \in \sum_{i=0}^{k} R \cdot \boldsymbol{a}_i$, and $M \subset \sum_{i=0}^{k} R \cdot \boldsymbol{a}_i$. □

6.2 Level-consistency

In this section, we examine the concept of level-consistency. 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 3.3). They limit the achievable efficiency of level-consistent packing methods, yielding the impossiblity of designing an efficient packing methods while satisfying level-consistency. The results justify the use of *level-dependent* packings in SPDZ-like MPC protocols over $\mathbb{Z}_{2^k}$ and highlights the usefulness of the reshare protocol for level-dependent packings proposed in Section 5.4 (Example 6.2.7, 6.2.8, and 6.2.9). Our results also implies that the HElib packing (Section 4.1.1) is essentially the optimal method to use in *fully* homomorphic encryption(FHE) (Example 6.2.6).

6.2.1 Idempotents and Nilpotents

A crucial tool when dealing with a level-consistent packing method is idempotents. We extensively leverage the concept of idempotents and their prop-

erties when proving our main results on level-consistency. Here, we list and prove the properties of idempotents related to level-consistent packing methods, which are used afterwards.

The following proposition on idempotents is a classic result in finite ring theory. Nevertheless, for completeness, we give a proof.

Proposition 6.2.1. *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. Consider the sequence $(a^i)_{i\in\mathbb{Z}^+}$ of R-elements. Since R is finite, there is an element of R which appears infinitely many times in the sequence. Thus, we can choose $i, j \in \mathbb{Z}^+$ satisfying $a^i = a^j$ and $2i \leq j$. Letting $s = j - i$ proves the proposition: $a^s = a^{j-2i}a^i = a^{j-2i}a^j = a^{2s}$. □

The following proposition says that any idempotent $\boldsymbol{a}$ must have an idempotent packing $a(x)$, regarding to a level-consistent method.

Proposition 6.2.2. *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. 3.2.3). 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. 6.2.1, 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. □

The following proposition is a slight generalization of the property of Galois rings having only 0 and 1 as idempotents.

Proposition 6.2.3. *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. Suppose $a(x) \in \mathcal{R}$ is idempotent. Then, $f(x)$ divides $a(x)^2 - a(x)$ in $\mathbb{Z}_{p^t}[x]$, and therefore $g(x)^\ell$ divides $a(x)(a(x)-1)$ in $\mathbb{F}_p[x]$. Since $g(x)$ is irreducible and $a(x)$ and $a(x)-1$ are coprime in $\mathbb{F}_p[x]$, $a(x)$ equals 0 or 1 in $\mathcal{R}/p\mathcal{R}$.

Suppose $a(x) = 1$ in $\mathcal{R}/p\mathcal{R}$. We can represent $a(x)$ as $1 + p^s \cdot \tilde{a}(x)$ for some $t \geq s > 0$, where $\tilde{a}(x)$ is not divisible by p. Then, $0 = a(x)^2 - a(x) = p^{2s} \cdot \tilde{a}(x)^2 + p^s \cdot \tilde{a}(x)$ in $\mathcal{R}$. Since $s > 0$ and $p \nmid \tilde{a}(x)$, s must be t and therefore $a(x) = 1$ in $\mathcal{R}$. We can similarly show that if $a(x) = 0$ in $\mathcal{R}/p\mathcal{R}$ then $a(x) = 0$ in $\mathcal{R}$. □

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 6.2.4. *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. 3.2.3). Then, $\boldsymbol{a}^s = \mathsf{Unpack}(a(x)^s) = \mathsf{Unpack}(0) = \mathbf{0}$ holds. □

6.2.2 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. 6.2.2, 6.2.3).

Theorem 6.2.5. *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 $n \leq r$.*

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. 6.2.3, 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. 6.2.2, 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 $n \leq r$ holds. □

The following are some consequences of Thm. 6.2.5. We begin with an optimality result for HElib packing (Section 4.1.1).

Example 6.2.6. Essentially, Thm. 6.2.5 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 [GHS12, HS15, CH18].

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 6.2.7. 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 6.2.8. 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 6.2.9. When $M = 2^s \cdot M'$, where M' is an odd, $\Phi_M(x) = \Phi_{M'}(x)^{2^{s-1}}$ 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.

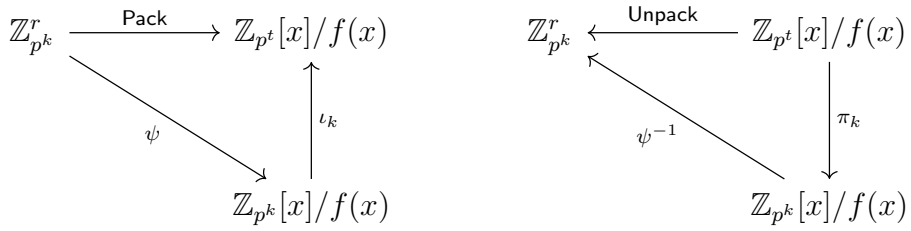
Thm. 6.2.5 also yields the impossibility of level-consistent RMFEs over Galois ring for $\mathbb{Z}_{p^k}$-messages.

Example 6.2.10. 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. 6.2.5 is also a sufficient one.

Theorem 6.2.11. *If there are r distinct irreducible factors of $f(x) \in \mathbb{Z}_{p^t}[x]$ in $\mathbb{F}_p[x]$, then there exists 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.



(a) Pack (b) Unpack

Figure 6.1: Definitions of Pack and Unpack in Thm. 6.2.11

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. 6.1). Then, it is straightforward that (Pack, Unpack) is a level-consistent packing method. □

Corollary 6.2.12. *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 $\mathbb{Z}_{p^t}[x]/f(x)$ if and only if $n \leq r$.*

Proof. Straightforward from Thm. 6.2.5 and 6.2.11. □

6.2.3 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. 6.2.5 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 6.2.13. *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. See Section 6.2.4. □

The following are some consequences of Thm. 6.2.13. 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 6.2.14. 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 6.2.15. 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 6.2.16. 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. 6.2.13 also yields the impossibility of level-consistent RMFEs.

Example 6.2.17. 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. 6.2.13 is also a sufficient one.

Theorem 6.2.18. *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. Let $g(x) \in \mathbb{F}_p[x]$ be the product of r distinct irreducible factors of $f(x)$ in $\mathbb{F}_p[x]$ whose degrees are multiples of k. Then, there is a ring monomorphism $\psi : \mathbb{F}_{p^k}^r \to \mathbb{F}_p[x]/g(x)$. Define the function $\psi^{-1} : \mathbb{F}_p[x]/g(x) \to \mathbb{F}_{p^k}^r \cup \{\perp\}$ as the following.

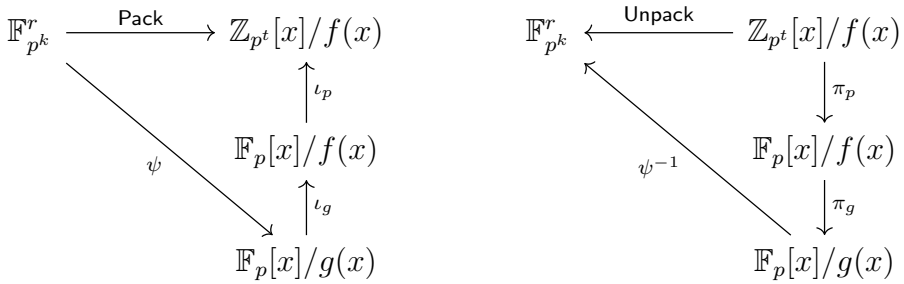
$$\psi^{-1}(a(x)) = \begin{cases} \boldsymbol{a}, & \text{if there is } \boldsymbol{a} \in \mathbb{F}_{p^k}^r \text{ such that } \psi(\boldsymbol{a}) = a(x) \\ \perp, & \text{otherwise} \end{cases}$$

Let π_p and ι_p denote the projection and injection between $\mathbb{Z}_{p^k}[x]/f(x)$ and $\mathbb{F}_p[x]/f(x)$, and let π_g and ι_g denote those of $\mathbb{F}_p[x]/f(x)$ and $\mathbb{F}_p[x]/g(x)$ respectively.

Define $\mathsf{Pack} := \iota_p \circ \iota_g \circ \psi$ and $\mathsf{Unpack} := \psi^{-1} \circ \pi_h \circ \pi_p$ (Fig. 6.2). Then, it is straightforward that $(\mathsf{Pack}, \mathsf{Unpack})$ is a level-consistent packing method. □

Corollary 6.2.19. *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 $\mathbb{Z}_{p^t}[x]/f(x)$ if and only if $n \leq r$*

Proof. Straightforward from Thm. 6.2.13 and 6.2.18. □



(a) Pack (b) Unpack

Figure 6.2: Definitions of Pack and Unpack in Thm. 6.2.18

6.2.4 Proof of Thm. 6.2.13

In this subsection, we prove Thm. 6.2.13. The proof is elementary, but consists of a number of steps. As mentioned, idempotents (Prop. 6.2.2) and nilpotents (Prop. 6.2.4) are at the core of the proof. Even if they are not directly referred, many parts of the proof are motivated from the concepts. Also notice the crucial role of one-to-one property in the proof of Lem. 6.2.24.

Theorem 6.2.13. *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. Straightforward from Lem. 6.2.21, 6.2.22, 6.2.23, and 6.2.24. □

Lemma 6.2.21. *Suppose there exists a level-consistent packing method for $\mathbb{F}_{p^k}^n$ into $\mathbb{Z}_{p^t}[x]/f(x)$. Then, there exists a level-consistent packing method for $\mathbb{F}_{p^k}^n$ into $\mathbb{F}_p[x]/f(x)$.*

Proof. Let $(\mathsf{Pack}, \mathsf{Unpack})$ be a level-consistent packing method for $\mathbb{F}_{p^k}^n$ into $\mathbb{Z}_{p^t}[x]/f(x)$. Suppose $a(x), b(x) \in \mathbb{Z}_{p^t}[x]/f(x)$ satisfy $\mathsf{Unpack}(a(x)) = \boldsymbol{a}$ and $\mathsf{Unpack}(b(x)) = \boldsymbol{b}$ for some $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_{p^k}^n$. If $a(x) = b(x)$ modulo p, then $\boldsymbol{a} = \boldsymbol{b}$ since (i) $\mathsf{Unpack}(a(x) - b(x)) = \boldsymbol{a} - \boldsymbol{b}$, (ii) $a(x) - b(x)$ is

nilpotent in $\mathbb{Z}_{p^t}[x]/f(x)$, and (iii) $\mathbf{0}$ is the only nilpotent element in $\mathbb{F}_{p^k}^n$ (Prop. 6.2.4). Thus, for all $a(x) \in \mathbb{Z}_{p^t}[x]/f(x)$, $\mathsf{Unpack}(a(x))$ is fully determined by $a(x) \bmod p$, given it does not output a failure $\perp$.

Let $\mathsf{Pack}' = \pi_p \circ \mathsf{Pack}$ where π_p denotes the projection from $\mathbb{Z}_{p^t}[x]/f(x)$ to $\mathbb{F}_p[x]/f(x)$. Let $\mathsf{Unpack}' : \mathbb{F}_p[x]/f(x) \to \mathbb{F}_{p^k}^n \cup \{\perp\}$ be defined as the following.

$$\mathsf{Unpack}(a(x)) = \begin{cases} \boldsymbol{a}, & \text{if there is } \tilde{a}(x) \in \mathbb{Z}_{p^t}[x]/f(x) \text{ such that} \\ & \pi_p(\tilde{a}(x)) = a(x) \text{ and } \mathsf{Unpack}(\tilde{a}(x)) = \boldsymbol{a} \text{ for} \\ & \text{some } \boldsymbol{a} \in \mathbb{F}_{p^k}^n \\ \perp, & \text{otherwise} \end{cases}$$

Then, it is straightforward that $(\mathsf{Pack}', \mathsf{Unpack}')$ is a level-consistent packing method. □

Lemma 6.2.22. *Suppose there exists a level-consistent packing method for $\mathbb{F}_{p^k}^n$ into $\mathbb{F}_p[x]/f(x)$. Then, there exists a level-consistent packing method 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 $f(x)$.*

Proof. Let $(\mathsf{Pack}, \mathsf{Unpack})$ be a level-consistent packing method for $\mathbb{F}_{p^k}^n$ into $\mathbb{F}_p[x]/f(x)$. Note that $a(x) \in \mathbb{F}_p[x]/f(x)$ is nilpotent if and only if it is divisible by $\hat{g}(x)$. We can use the same argument used in the proof of Lem. 6.2.21 with the help of Prop. 6.2.4. Then, for all $a(x) \in \mathbb{F}_p[x]/f(x)$, $\mathsf{Unpack}(a(x))$ is fully determined by $a(x) \bmod \hat{g}(x)$, given it does not output a failure $\perp$. Consequently, we can design a level-consistent packing method $(\mathsf{Pack}', \mathsf{Unpack}')$ for $\mathbb{F}_{p^k}^n$ into $\mathbb{F}_p[x]/\hat{g}(x)$ as in the proof of Lem. 6.2.21. □

Lemma 6.2.23. *Suppose there exists a level-consistent packing method for $\mathbb{F}_{p^k}^n$ into $\mathbb{F}_p[x]/\hat{g}(x)$ where $\hat{g}(x)$ is square-free. Then, there exists a factor $g(x)$ of $\hat{g}(x)$ which allows a level-consistent one-to-one packing method for $\mathbb{F}_{p^k}^n$ into $\mathbb{F}_p[x]/g(x)$.*

Proof. Let $(\mathsf{Pack}, \mathsf{Unpack})$ be a level-consistent packing method for $\mathbb{F}_{p^k}^n$ into $\mathcal{R} := \mathbb{F}_p[x]/\hat{g}(x)$. Let $\hat{g}(x)$ factorizes into r distinct irreducible polynomials $\{\hat{g}_i(x)\}_{i=1}^r$. We identify $\mathcal{R}$ with $\prod_{i=1}^r \mathbb{F}_p[x]/\hat{g}_i(x)$.

Step 1: For a subset $A \subset [r]$, let $e_A(x) \in \mathcal{R}$ denote the element which is 1 modulo $\hat{g}_i(x)$ for $i \in A$ and 0 modulo $\hat{g}_i(x)$ for $i \notin A$. Note that $e_{A\cup B}(x) = e_A(x)+e_B(x)-e_A(x)\cdot e_B(x)$. Thus, if $\mathsf{Unpack}(e_A(x)) = \mathbf{0}$ and $\mathsf{Unpack}(e_B(x)) = \mathbf{0}$, then $\mathsf{Unpack}(e_{A\cup B}(x))$ is also $\mathbf{0}$ by the level-consistency. We can therefore choose the maximal set $I \subset [r]$ such that $\mathsf{Unpack}(e_I(x)) = \mathbf{0}$.

Step 2: Let $g(x) := \prod_{i\notin I} \hat{g}_i(x)$. Consider the ideal $Z \subset \mathcal{R}$ generated by $e_I(x)$, which coincides with $g(x) \cdot \mathcal{R}$. Then, for any $a(x) \in Z$, $\mathsf{Unpack}(a(x))$ outputs $\mathbf{0}$ or a failure $\perp$, since $a(x) \cdot e_I(x) = a(x)$. Thus, for all $a(x) \in \mathcal{R}$, $\mathsf{Unpack}(a(x))$ is fully determined by $a(x) \bmod g(x)$, given it does not output a failure $\perp$.

Step 3: Let $a(x) \in \mathcal{R}$ satisfies $\mathsf{Unpack}(a(x)) = \mathbf{0}$. Suppose $a(x)$ is non-zero modulo $\hat{g}_i(x)$ if $i \in A$ and 0 modulo $\hat{g}_i(x)$ if $i \notin A$, for some $A \subset [r]$. Since $\mathbb{F}_p[x]/\hat{g}_i(x)$ are fields, there exists $s \in \mathbb{Z}^+$ such that $a(x)^s = e_A(x)$. By definition, $A \subset I$ holds. Thus, for any $a(x) \in \mathcal{R}$ satisfying $\mathsf{Unpack}(a(x)) = \mathbf{0}$, it holds that $a(x) \in Z$, i.e. $a(x) = 0 \pmod{g(x)}$.

Step 4: Following the proof of Lem. 6.2.21 together with Step 2, we can design a level-consistent packing method $(\mathsf{Pack}', \mathsf{Unpack}')$ for $\mathbb{F}_{p^k}^n$ into $\mathbb{F}_p[x]/g(x)$. Moreover, such $(\mathsf{Pack}', \mathsf{Unpack}')$ is a one-to-one packing method by Step 3. □

Lemma 6.2.24. *Let $g(x) \in \mathbb{F}_p[x]$ be square-free and r be the number of distinct irreducible factors of $g(x)$ whose degrees are multiples of k. There exists a level-consistent one-to-one packing method for $\mathbb{F}_{p^k}^n$ into $\mathbb{F}_p[x]/g(x)$, only if $r \le n$.*

Proof. Let $\mathcal{P} = (\mathsf{Pack}, \mathsf{Unpack})$ be a level-consistent one-to-one packing method for $\mathbb{F}_{p^k}^n$ into $\mathcal{R} := \mathbb{F}_p[x]/g(x)$. Let $g(x)$ factorizes into $\hat{r}$ distinct irreducible polynomials $\{g_i(x)\}_{i=1}^{\hat{r}}$ and let $d_i := \deg(g_i)$. We identify $\mathcal{R}$ with $\prod_{i=1}^{r} \mathbb{F}_p[x]/g_i(x)$. For a subset $A \subset [\hat{r}]$, let $e_A(x) \in \mathcal{R}$ denote the element which is 1 modulo

$g_i(x)$ for $i \in A$ and 0 modulo $g_i(x)$ for $i \notin A$. Let $\boldsymbol{e}_i \in \mathbb{F}_{p^k}^n$ denote the element with 1 in its i-th coordinate and 0 in the others.

Since $\mathcal{P}$ is one-to-one, there is only one element which unpacks to $\boldsymbol{e}_i$, which we can set as $e_{A_i}(x)$ for some $A_i \subset [\hat{r}]$ by Prop. 6.2.2 and 6.2.3. Moreover, $A_i \cap A_j = \emptyset$ for distinct i, j since $e_{A_i}(x) \cdot e_{A_j}(x)$ must be 0 to be unpacked to $\mathbf{0}$ by one-to-one property.

Let $u \in \mathbb{F}_{p^k}$ be a multiplicative generator of $\mathbb{F}_{p^k}$, and let $u_i(x) \in \mathcal{R}$ be the element which unpacks to $u \cdot \boldsymbol{e}_i$. Observe that $u_i(x) \bmod g_j(x)$ is non-zero if and only if $j \in A_i$, since $(u \cdot \boldsymbol{e}_i)^{p^k-1} = \boldsymbol{e}_i$ and consequently $u_i(x)^{p^k-1} = e_{A_i}(x)$. Moreover, for $j \in A_i$, the multiplicative order s of $u_i(x) \bmod g_j(x)$ in $\mathbb{F}_p[x]/g_j(x) \cong \mathbb{F}_{p^{d_j}}$ must divide $p^k - 1$.

Meanwhile, if the multiplicative order s is less than $p^k - 1$, then $u_i(x)^s = e_{A_i}(x) = 1 \pmod{g_j(x)}$. This contradicts the one-to-one property, since there must be another element of $\mathcal{R}$, a power of $u_i(x)^s - e_{A_i}(x)$, which unpacks to $\boldsymbol{e}_i$ and is 0 modulo $g_j(x)$. Consequently, $s = p^k - 1$ must hold. To allow such conditions on the orders, d_j's must be multiples of k for $j \in A_i$. Thus, for each $\boldsymbol{e}_i$, we can choose distinct $g_j(x)$ whose degree is a multiple of k, and $r \leq n$ holds. □

6.3 Surjectivity

In this section, we examine the concept of surjectivity. 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 3.3). They limit the achievable efficiency of surjective packing methods, yielding the impossiblity of designing an efficient packing methods while satisfying surjectivity. The results justify the use of *non*-surjective packings and the need of ZKPoMK in SPDZ-like MPC protocols over $\mathbb{Z}_{2^k}$ as done in Chapter 5 (Example 6.3.3, 6.3.4, and 6.3.5).

6.3.1 Zero-Set Ideal

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 6.3.1 (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. 3.2.6 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. 3.2.6 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 $\mathcal{R}$. □

6.3.2 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 6.3.2. *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 $n \leq \check{r}$.*

Proof. See Section 6.3.4. □

The following are some consequences of Thm. 6.3.2. 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 6.3.3. When $M = 2^m$, by Prop. 2.2.2, 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 6.3.4. 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 6.3.5. 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 6.3.4, 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.

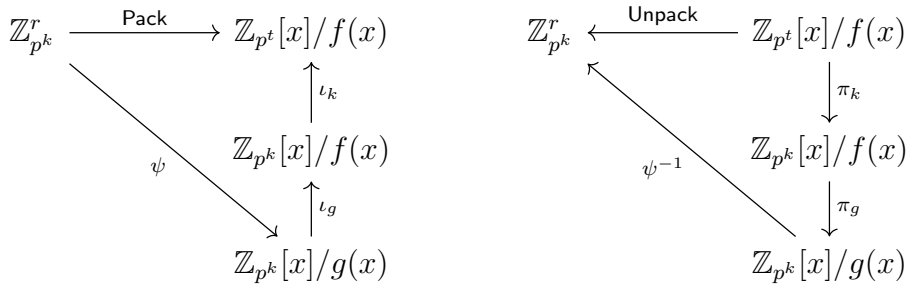
Thm. 6.3.2 also yields the impossibility of surjective RMFEs over Galois ring for $\mathbb{Z}_{p^k}$-messages.

Example 6.3.6. 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. 6.3.2 is also a sufficient one.

Theorem 6.3.7. *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 level-consistent 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 $\psi : \mathbb{Z}_{p^k}^r \xrightarrow{\cong} \mathbb{Z}_{p^k}[x]/g(x)$.



(a) Pack (b) Unpack

Figure 6.3: Definitions of Pack and Unpack in Thm. 6.3.7

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. 6.3). Then, it is straightforward that $(\mathsf{Pack}, \mathsf{Unpack})$ is a level-consistent surjective packing method. □

Corollary 6.3.8. *Let 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 $\mathbb{Z}_{p^t}[x]/f(x)$ if and only if $n \leq r$.*

Proof. Straightforward from Thm. 6.3.2 and 6.3.7. □

The following corollary suggests that surjectivity is a somewhat stronger notion than level-consistency for $\mathbb{Z}_{p^k}$-message packings.

Corollary 6.3.9. *For $D > 1$, if there exists a degree-D surjective packing method for $\mathbb{Z}_{p^k}^n$ into $\mathbb{Z}_{p^t}[x]/f(x)$, then there exists a level-consistent surjective packing method for $\mathbb{Z}_{p^k}^n$ into $\mathbb{Z}_{p^t}[x]/f(x)$.*

Proof. Straightforward from Thm. 6.3.2 and 6.3.7. □

6.3.3 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. 6.3.2 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 6.3.10. *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. See Section 6.3.5. □

The following are some consequences of Thm. 6.3.10. 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 6.3.11. 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 6.3.12. 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 6.3.13. 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 6.3.12.

Thm. 6.3.10 also yields the impossibility of surjective RMFEs.

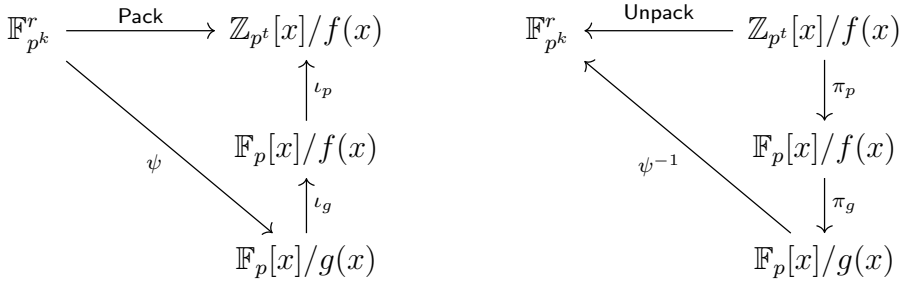
Example 6.3.14. In $\mathbb{F}_{p^d} \cong \mathbb{Z}_p[x]/f(x)$ with a degree-d irreducible $f(x)$, we cannot pack even a single copy of $\mathbb{F}_{p^k}$ while satisfying surjectivity and degree-2 homomorphism, if $k \neq d$. That is, there is no meaningful surjective RMFE.

On the other side, we have the following theorem with a constructive proof, which asserts that the necessary condition in Thm. 6.3.10 is also a sufficient one.

Theorem 6.3.15. *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 level-consistent surjective packing method $\mathbb{F}_{p^k}^r$ into $\mathbb{Z}_{p^t}[x]/f(x)$.*

Proof. Let $g(x) \in \mathbb{F}_p[x]$ be the product of r distinct degree-k irreducible factors of $f(x)$ in $\mathbb{F}_p[x]$. Then, there is a ring isomophism $\psi : \mathbb{F}_{p^k}^r \xrightarrow{\cong} \mathbb{F}_p[x]/g(x)$. Let π_p and ι_p denote the projection and injection between $\mathbb{Z}_{p^k}[x]/f(x)$ and $\mathbb{F}_p[x]/f(x)$, and let π_g and ι_g denote those of $\mathbb{F}_p[x]/f(x)$ and $\mathbb{F}_p[x]/g(x)$ respectively.

Define $\mathsf{Pack} := \iota_p \circ \iota_g \circ \psi$ and $\mathsf{Unpack} := \psi^{-1} \circ \pi_h \circ \pi_p$ (Fig. 6.4). Then, it is straightforward that $(\mathsf{Pack}, \mathsf{Unpack})$ is a level-consistent surjective packing method. □



(a) Pack (b) Unpack

Figure 6.4: Definitions of Pack and Unpack in Thm. 6.3.15

Corollary 6.3.16. *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 for $\mathbb{F}_{p^k}^n$ into $\mathbb{Z}_{p^t}[x]/f(x)$ if and only if $n \leq r$.*

Proof. Straightforward from Thm. 6.3.10 and 6.3.15. □

The following corollary suggests that surjectivity is a somewhat stronger notion than level-consistency, also in the $\mathbb{F}_{p^k}$ case.

Corollary 6.3.17. *For $D > 1$, if there exists a degree-D surjective packing method for $\mathbb{F}_{p^k}^n$ into $\mathbb{Z}_{p^t}[x]/f(x)$, then there exists a level-consistent surjective packing method for $\mathbb{F}_{p^k}^n$ into $\mathbb{Z}_{p^t}[x]/f(x)$.*

Proof. Straightforward from Thm. 6.3.10 and 6.3.15. □

6.3.4 Proof of Thm. 6.3.2

In this subsection, we prove Thm. 6.3.2. The proof is elementary, but consists of a number of steps. As mentioned, Prop. 6.3.1 plays an important role in the proof.

Theorem 6.3.2. *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 $n \leq \check{r}$.*

Proof. Straightforward from Lem. 6.3.19, 6.3.20, and 6.3.21. □

Lemma 6.3.19. *For $D > 1$, if there exists a degree-D surjective packing method for $\mathbb{Z}_{p^k}^n$ into $\mathbb{Z}_{p^t}[x]/f(x)$, then there exists a degree-D surjective packing method for $\mathbb{Z}_{p^k}^n$ into $\mathbb{Z}_{p^k}[x]/f(x)$.*

Proof. 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. 3.2.6), $\mathsf{Unpack}_i(p^k \cdot b(x)) = \mathbf{0}$ holds. Thus, at any level-i and for all $a(x) \in \mathbb{Z}_{p^t}[x]/f(x)$, $\mathsf{Unpack}_i(a(x))$ is fully determined by $a(x) \bmod p^k$.

Let $\mathsf{Pack}'_i = \pi_k \circ \mathsf{Pack}_i$ and $\mathsf{Unpack}'_i = \mathsf{Unpack}_i \circ \iota_k$, where 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. Then, it is straightforward that $(\mathsf{Pack}'_i, \mathsf{Unpack}'_i)_{i=1}^D$ is a degree-D surjective packing method. □

For the remaining parts of this subsection, let $f(x)$ be a monic polynomial in $\mathbb{Z}_{p^k}[x]$, and let $\mathcal{R} := \mathbb{Z}_{p^k}[x]/f(x)$. Let $f(x)$ be factorized into $\prod_{i=1}^r g_i(x)^{\ell_i}$ in $\mathbb{F}_p[x]$, where 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 $f(x) = \prod_{i=1}^r f_i(x)$, where $f_i(x) \in \mathbb{Z}_{p^k}[x]$ is the Hensel lift of $g_i(x)^{\ell_i}$ satisfying $f_i(x) = g_i(x)^{\ell_i} \pmod p$. Let $d_j := \deg(f_i)$. Then, we can identify $\mathcal{R}$ with $\prod_{i=1}^r \mathbb{Z}_{p^k}[x]/f_i(x)$ via the CRT ring isomorphism. We denote as $\mathcal{R}_i$ for the subring of $\mathcal{R}$ which is isomorphic to $\mathbb{Z}_{p^k}[x]/f_i(x)$ according to the CRT isomorphism. Let Z be the zero-set ideal defined in Prop. 6.3.1

Lemma 6.3.20. *Let $(\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^D$ be a degree-D surjective packing method for $\mathbb{Z}_{p^k}^n$ into $\mathcal{R}$, for some $D > 1$. For each standard unit vector $\boldsymbol{e}_i \in \mathbb{Z}_{p^k}^n$, there exists $a_i(x)$ such that $\mathsf{Unpack}_1(a_i(x)) = \boldsymbol{e}_i$ and $a_i(x) \in \mathcal{R}_j$ for some $j \in [r]$. Moreover, such $a_i(x)$ is a unit in $\mathcal{R}_j$, and such j is distinct for all i's.*

Proof. Let $a_i(x)$ satisfy $\mathsf{Unpack}_1(a_i(x)) = \boldsymbol{e}_i$, and let $A_i \subset [r]$ be the set of j's such that $a_i(x)$ is non-zero modulo $f_j(x)$. Without loss of generality, assume that $a_i(x)$ has the smallest such subset of $[r]$, among the elements satisfying $\mathsf{Unpack}_1(\cdot) = \boldsymbol{e}_i$.

Step 1: Suppose, for $j \in A_i$, $a_i(x) \pmod{f_j(x)}$ is a non-unit in $\mathbb{Z}_{p^k}[x]/f_j(x)$. Let $\mathsf{Unpack}_1(e_j(x))$ outputs an element in $\mathbb{Z}_{p^k}^n$ with c_i in its i-th coordinate. Then, at level-1, $(e_j(x) - c_i \cdot a_i(x))$ unpacks to an element with 0 in its i-th coordinate. Thus, the following holds.

$$\mathsf{Unpack}_2\Big(a_i(x) \cdot \big(e_j(x) - c_i \cdot a_i(x)\big)\Big) = \mathbf{0}$$

That is, $a_i(x) \cdot (e_j(x) - c_i \cdot a_i(x)) \in Z$. Meanwhile, notice that $(e_j(x) - c_i \cdot a_i(x)) \pmod{f_j(x)}$ is a unit, since $\mathbb{Z}_{p^k}[x]/f_j(x)$ is a local ring. Therefore, $a_i(x) \cdot e_j(x) \in Z$ and $a_i(x) - a_i(x) \cdot e_j(x)$ unpacks to $\boldsymbol{e}_i$ at level-1, contradicting the assumption on the size of A_i. Thus, for all $j \in A_i$, $a_i(x) \pmod{f_j(x)}$ must be a multiplicative unit in $\mathbb{Z}_{p^k}[x]/f_j(x)$.

Step 2: Consider $e_j(x) \cdot a_i(x) \in \mathcal{R}_j$, and let $\mathsf{Unpack}_1(e_j(x) \cdot a_i(x))$ outputs an element in $\mathbb{Z}_{p^k}^n$ with $\tilde{c}_i$ in its i-th coordinate. Then, at level-1, $(e_j(x) \cdot a_i(x) - \tilde{c}_i \cdot a_i(x))$ unpacks to an element with 0 in its i-th coordinate. Thus, the following holds.

$$\mathsf{Unpack}_2\Big(a_i(x) \cdot \big(e_j(x) \cdot a_i(x) - \tilde{c}_i \cdot a_i(x)\big)\Big) = \mathbf{0}$$

That is, $a_i(x)^2 \cdot (e_j(x) - \tilde{c}_i) \in Z$, and therefore $a_i(x) \cdot (e_j(x) - \tilde{c}_i) \in Z$ since $a_i(x) \pmod{f_\jmath(x)}$ is a multiplicative unit in $\mathbb{Z}_{p^k}[x]/f_\jmath(x)$ for all $\jmath \in A_i$ by Step 1. Consequently, it holds that $\mathsf{Unpack}_1(e_j(x) \cdot a_i(x)) = \mathsf{Unpack}_1(\tilde{c}_i \cdot a_i(x)) = \tilde{c}_i \cdot \boldsymbol{e}_i$.

Suppose $\tilde{c}_i \in \mathbb{Z}_{p^k}$ is a non-unit. Then, $(1 - \tilde{c}_i)$ is a unit, and $(1 - \tilde{c}_i)^{-1} \cdot (a_i(x) - e_j(x) \cdot a_i(x))$ unpacks to $\boldsymbol{e}_i$ at level-1 contradicting the assumption on the size of A_i. Thus, $\tilde{c}_i$ is a unit. Then, $\tilde{c}_i^{-1} \cdot e_j(x) \cdot a_i(x)$ unpacks to $\boldsymbol{e}_i$ at level-1 satisfying the desired conditions.

Step 3: Suppose $a_{i'}(x)$ is also in $\mathcal{R}_j$ and unpacks to a standard unit vector $\boldsymbol{e}_{i'}$ at level-1. Then, $a_i(x) \cdot a_{i'}(x)$ unpacks to $\mathbf{0}$ at level-2, and therefore $a_i(x) \cdot a_{i'}(x) \in Z$. However, since $a_i(x)$ and $a_{i'}(x)$ are both units in $\mathcal{R}_j$, all elements of $\mathcal{R}_j$ must be included in Z, leading to a contradiction. □

Lemma 6.3.21. *Let* $(\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^D$ *be a degree-D surjective packing method for* $\mathbb{Z}_{p^k}^n$ *into* $\mathcal{R}$*, for some* $D > 1$*. If there exists* $a_i(x) \in \mathcal{R}_j$ *which satisfies* $\mathsf{Unpack}_1(a_i(x)) = \boldsymbol{e}_i$ *for a standard unit vector* $\boldsymbol{e}_i \in \mathbb{Z}_{p^k}^n$*, then* $f_j(x)$ *has a linear factor in* $\mathbb{Z}_{p^k}[x]$*.*

Proof. Consider $x \cdot a_i(x) \in \mathcal{R}_j$. Suppose $\mathsf{Unpack}_1(x \cdot a_i(x))$ outputs an element in $\mathbb{Z}_{p^k}^n$ with c_i in its i-th coordinate. Then, at level-1, $(x \cdot a_i(x) - c_i \cdot a_i(x))$ unpacks to an element with 0 in its i-th coordinate. Thus, the following holds.

$$\mathsf{Unpack}_2\Big(\big(x \cdot a_i(x) - c_i \cdot a_i(x)\big) \cdot a_i(x)\Big) = \mathsf{Unpack}_2\Big((x - c_i) \cdot a_i(x)^2\Big) = \mathbf{0}$$

That is, $(x - c_i) \cdot a_i(x)^2 \in Z$, and therefore $(x - c_i) \cdot e_j(x) \in Z$ as $a_i(x)$ is a unit in $\mathcal{R}_j$ (Lem. 6.3.20).

Now consider $(x - c_i) \in \mathbb{Z}_{p^k}[x]/f_j(x)$ and the ideal $\langle x - c_i \rangle \subset \mathbb{Z}_{p^k}[x]/f_j(x)$ generated by it. The ideal $\langle x - c_i \rangle$ contains at least $p^{k \cdot (d_j - 1)}$ elements, namely $(x - c_i) \cdot h(x)$'s for $h(x) \in \mathbb{Z}_{p^k}[x]$ with $\deg(h) < d_j - 1$, which are multiples of $(x - c_i)$ in $\mathbb{Z}[x]$. On the other hand, $\langle x - c_i \rangle$ cannot contain more than $p^{k \cdot d_j}/p^k$ elements: this is because $\mathcal{R}_j$ must contain p^k distinct elements modulo Z, namely $c \cdot a_i(x)$'s for $c \in \mathbb{Z}_{p^k}$. Thus, $|\langle x - c_i \rangle| = p^{k \cdot (d_j - 1)}$ holds. In particular, it must hold that $(x - c_i)^{d_j} - f_j(x)$ is a multiple of $(x - c_i)$ in $\mathbb{Z}[x]$. Consequently, $f_j(x)$ has a linear factor $(x - c_i)$ in $\mathbb{Z}_{p^k}[x]$. □

6.3.5 Proof of Thm. 6.3.10

In this subsection, we prove Thm. 6.3.10. The proof is elementary, but consists of a number of steps. As mentioned, Prop. 6.3.1 plays an important role in the proof.

Theorem 6.3.10. *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. Straightforward from Lem. 6.3.23, 6.3.24, and 6.3.25. □

Lemma 6.3.23. *For $D > 1$, if there exists a degree-D surjective packing method for $\mathbb{F}_{p^k}^n$ into $\mathbb{Z}_{p^t}[x]/f(x)$, then there exists a degree-D surjective packing method for $\mathbb{F}_{p^k}^n$ into $\mathbb{F}_p[x]/f(x)$.*

Proof. 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, $\mathsf{Unpack}_i(p \cdot b(x)) = \mathbf{0}$ holds. Thus, at any level-i and for all $a(x) \in \mathbb{Z}_{p^t}[x]/f(x)$, $\mathsf{Unpack}_i(a(x))$ is fully determined by $a(x) \bmod p$.

Let $\mathsf{Pack}'_i = \pi_p \circ \mathsf{Pack}_i$ and $\mathsf{Unpack}'_i = \mathsf{Unpack}_i \circ \iota_p$, where π_p and ι_p denote the projection and injection between $\mathbb{Z}_{p^t}[x]/f(x)$ and $\mathbb{F}_p[x]/f(x)$ respectively. Then, it is straightforward that $(\mathsf{Pack}'_i, \mathsf{Unpack}'_i)_{i=1}^D$ is a degree-D surjective packing method. □

Lemma 6.3.24. *For $D > 1$, if there exists a degree-D surjective packing method for $\mathbb{F}_{p^k}^n$ into $\mathcal{R} := \mathbb{F}_p[x]/f(x)$, then there exists $g(x) \in \mathbb{F}_p[x]$ which divides $f(x)$, is of degree $k \cdot n$, and allows a degree-D packing method for $\mathbb{F}_{p^k}^n$ into $\mathbb{F}_p[x]/g(x)$.*

Proof. Let $(\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^D$ be a degree-D surjective packing method for $\mathbb{F}_{p^k}^n$ into $\mathcal{R}$. By Prop. 6.3.1, the sets Z_i consisting of elements $a(x) \in \mathcal{R}$ such that $\mathsf{Unpack}_i(a(x)) = \mathbf{0}$ coincide with an ideal $Z = \check{g}(x) \cdot \mathcal{R}$ for some $\check{g}(x) \in \mathbb{F}_p[x]$ which divides $f(x)$, as cR is a principal ideal ring. Let $g(x) := f(x)/\check{g}(x)$. Then, $\mathcal{R}/Z \cong \mathbb{F}_p[x]/g(x)$, and therefore $\deg(g) = k \cdot n$ since $|\mathcal{R}/Z| = p^{kn}$. Furthermore, at any level-i and for all $a(x) \in \mathbb{F}_p[x]/f(x)$, $\mathsf{Unpack}_i(a(x))$ is fully determined by $a(x) \bmod g(x)$.

Let $\mathsf{Pack}'_i = \pi_g \circ \mathsf{Pack}_i$ and $\mathsf{Unpack}'_i = \mathsf{Unpack}_i \circ \iota_g$, where π_g and ι_g denote the projection and injection between $\mathbb{F}_p[x]/f(x)$ and $\mathbb{F}_p[x]/g(x)$ respectively. Then, it is straightforward that $(\mathsf{Pack}'_i, \mathsf{Unpack}'_i)_{i=1}^D$ is a degree-D packing method. □

Lemma 6.3.25. *For $D > 1$, there exists a degree-D packing method for $\mathbb{F}_{p^k}^n$ into $\mathcal{R} := \mathbb{F}_p[x]/g(x)$, where $g(x) \in \mathbb{F}_p[x]$ is a polynomial of degree $k \cdot n$, only if $g(x)$ factors into n distinct degree-k irreducible polynomials.*

Proof. **Step 1:** Let $(\mathsf{Pack}_i, \mathsf{Unpack}_i)_{i=1}^D$ be a degree-D packing method for $\mathbb{F}_{p^k}^n$ into $\mathcal{R}$. Since $|\mathbb{F}_{p^k}^n| = |\mathcal{R}|$, all Pack_i and Unpack_i are bijective, and $0 \in \mathcal{R}$ is the only element which packs $\mathbf{0}$ at each level-i. Thus, $a(x) \cdot b(x) = 0$ if and only if $\boldsymbol{a} \odot \boldsymbol{b} = \mathbf{0}$, where $\boldsymbol{a} := \mathsf{Unpack}_1(a(x))$ and similar for $\boldsymbol{b}$, since $\mathsf{Unpack}_1(a(x)) \odot \mathsf{Unpack}_1(b(x)) = \mathsf{Unpack}_2(a(x) \cdot b(x))$.

Step 2: Suppose $g(x)$ is not square-free. Then, there exists a non-zero $a(x) \in \mathcal{R}$ such that $a(x)^2 = 0$. By Step 1, $\boldsymbol{a}^2 = \mathbf{0}$, where $\boldsymbol{a} := \mathsf{Unpack}_1(a(x))$. However, there is no non-zero $\boldsymbol{a} \in \mathbb{F}_{p^k}^n$ satisfying $\boldsymbol{a}^2 = \mathbf{0}$. Thus, $g(x)$ is square-free. Let $g(x)$ factorizes into r distinct irreducible polynomials $\{g_i(x)\}_{i=1}^r$ and let $d_i := \deg(g_i)$. We identify $\mathbb{F}_p[x]/g(x)$ with $\prod_{i=1}^r \mathbb{F}_p[x]/g_i(x)$.

Step 3: Note that for any $\boldsymbol{a} \in \mathbb{F}_{p^k}^n$ with s zero-coordinates, there are p^{ks} elements in $\mathbb{F}_{p^k}^n$ whose Hadamard product with $\boldsymbol{a}$ is $\mathbf{0}$. Then, consider $\check{e}_i(x) \in \mathbb{F}_p[x]/g(x)$ which corresponds to the vector of polynomials in $\prod_{i=1}^r \mathbb{F}_p[x]/g_i(x)$ with 0 in its i-th coordinate and 1 in the others. Observe that there are p^{d_i} elements in $\mathbb{F}_p[x]/g(x)$ whose product with $\check{e}_i(x)$ is 0. By Step 1 and the above facts, $p^{d_i} = p^{ks}$ for some s. Thus, the degree d_i is a positive multiple of k and we can let $d_i := kc_i$ where $\sum_{i=1}^r c_i = n$.

Step 4: By Step 1, the number of zero-divisors in $\mathbb{F}_{p^k}^n$ and $\mathcal{R}$ must be same. The number of elements which are not zero-divisors in $\mathbb{F}_{p^k}^n$ is $(p^k - 1)^n$. Meanwhile, the number of elements which are not zero-divisors in $\mathcal{R}$ is

$\prod_{i=1}^{r}(p^{d_i}-1)$. Thus, the following must hold.

$$\prod_{i=1}^{r}(p^{d_i}-1) = (p^k-1)^n = \prod_{i=1}^{r}(p^k-1)^{c_i}$$

Observe that $p^{d_i}-1 \geq (p^k-1)^{c_i}$ holds, where the equality holds if and only if $c_i = 1$. Thus, $d_i = k$ for all $1 \leq i \leq r$. □

Bibliography

[BCD+09] Peter Bogetoft, Dan Lund Christensen, Ivan Damgård, Martin Geisler, Thomas Jakobsen, Mikkel Krøigaard, Janus Dam Nielsen, Jesper Buus Nielsen, Kurt Nielsen, Jakob Pagter, Michael Schwartzbach, and Tomas Toft. Secure Multiparty Computation Goes Live. In Roger Dingledine and Philippe Golle, editors, *Financial Cryptography and Data Security*, pages 325–343, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg. 35

[BCK+14] Fabrice Benhamouda, Jan Camenisch, Stephan Krenn, Vadim Lyubashevsky, and Gregory Neven. Better zero-knowledge proofs for lattice encryption and their application to group signatures. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology – ASIACRYPT 2014*, pages 551–572, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg. 39

[BCS20] Carsten Baum, Daniele Cozzo, and Nigel P. Smart. Using TopGear in Overdrive: A More Efficient ZKPoK for SPDZ. In Kenneth G. Paterson and Douglas Stebila, editors, *Selected Areas in Cryptography – SAC 2019*, pages 274–302, Cham, 2020. Springer International Publishing. 36, 39, 40

BIBLIOGRAPHY

[BDGM19] Zvika Brakerski, Nico Döttling, Sanjam Garg, and Giulio Malavolta. Leveraging Linear Decryption: Rate-1 Fully-Homomorphic Encryption and Time-Lock Puzzles. In Dennis Hofheinz and Alon Rosen, editors, *Theory of Cryptography*, pages 407–437, Cham, 2019. Springer International Publishing. 5

[BDOZ11] Rikke Bendlin, Ivan Damgård, Claudio Orlandi, and Sarah Zakarias. Semi-homomorphic Encryption and Multiparty Computation. In Kenneth G. Paterson, editor, *Advances in Cryptology – EUROCRYPT 2011*, pages 169–188, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg. 36

[Bea92] Donald Beaver. Efficient Multiparty Protocols Using Circuit Randomization. In Joan Feigenbaum, editor, *Advances in Cryptology — CRYPTO '91*, pages 420–432, Berlin, Heidelberg, 1992. Springer Berlin Heidelberg. 37, 41

[Beh46] F. A. Behrend. On sets of integers which contain no three terms in arithmetical progression. *Proc. Nat. Acad. Sci. U.S.A.*, 32:331–332, 1946. 26

[BGV12] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (Leveled) Fully Homomorphic Encryption without Bootstrapping. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, ITCS '12, page 309–325, New York, NY, USA, 2012. Association for Computing Machinery. 1, 28

[BJSV15] Dan Bogdanov, Marko Jõemets, Sander Siim, and Meril Vaht. How the Estonian Tax and Customs Board Evaluated a Tax

Fraud Detection System Based on Secure Multi-party Computation. In Rainer Böhme and Tatsuaki Okamoto, editors, *Financial Cryptography and Data Security*, pages 227–234, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg. 35

[Blo16] T. F. Bloom. A quantitative improvement for Roth's theorem on arithmetic progressions. *J. Lond. Math. Soc. (2)*, 93(3):643–663, 2016. 26

[BMN17] Alexander R. Block, Hemanta K. Maji, and Hai H. Nguyen. Secure Computation Based on Leaky Correlations: High Resilience Setting. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology – CRYPTO 2017*, pages 3–32, Cham, 2017. Springer International Publishing. 4, 11, 26, 27

[BMN18] Alexander R. Block, Hemanta K. Maji, and Hai H. Nguyen. Secure Computation with Constant Communication Overhead Using Multiplication Embeddings. In Debrup Chakraborty and Tetsu Iwata, editors, *Progress in Cryptology – INDOCRYPT 2018*, pages 375–398, Cham, 2018. Springer International Publishing. 3, 11

[BOGW88] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88, page 1–10, New York, NY, USA, 1988. Association for Computing Machinery. 35

[BS21] Thomas F. Bloom and Olof Sisask. Breaking the logarithmic barrier in Roth's theorem on arithmetic progressions, 2021. 26

[CCXY18] Ignacio Cascudo, Ronald Cramer, Chaoping Xing, and Chen Yuan. Amortized Complexity of Information-Theoretically Secure MPC Revisited. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology – CRYPTO 2018*, pages 395–426, Cham, 2018. Springer International Publishing. 3, 11

[CDE+18] Ronald Cramer, Ivan Damgård, Daniel Escudero, Peter Scholl, and Chaoping Xing. SPD$\mathbb{Z}_{2^k}$: Efficient MPC mod 2^k for Dishonest Majority. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology – CRYPTO 2018*, pages 769–798, Cham, 2018. Springer International Publishing. 2, 36, 41

[CDRFG20] Dario Catalano, Mario Di Raimondo, Dario Fiore, and Irene Giacomelli. Mon$\mathbb{Z}_{2^k}$a: Fast Maliciously Secure Two Party Computation on $\mathbb{Z}_{2^k}$. In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *Public-Key Cryptography – PKC 2020*, pages 357–386, Cham, 2020. Springer International Publishing. 37, 40

[CG20] Ignacio Cascudo and Jaron Skovsted Gundersen. A Secret-Sharing Based MPC Protocol for Boolean Circuits with Good Amortized Complexity. In Rafael Pass and Krzysztof Pietrzak, editors, *Theory of Cryptography*, pages 652–682, Cham, 2020. Springer International Publishing. 3, 11

[CG22] Ignacio Cascudo and Emanuele Giunta. On Interactive Oracle Proofs for Boolean R1CS Statements. In Ittay Eyal and Juan Garay, editors, *Financial Cryptography and Data Secu-*

rity, pages 230–247, Cham, 2022. Springer International Publishing. 4, 11

[CH18] Hao Chen and Kyoohyung Han. Homomorphic Lower Digits Removal and Improved FHE Bootstrapping. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018*, pages 315–337, Cham, 2018. Springer International Publishing. 61

[CIV18] Wouter Castryck, Ilia Iliashenko, and Frederik Vercauteren. Homomorphic SIM^{2}D Operations: Single Instruction Much More Data. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018*, pages 338–359, Cham, 2018. Springer International Publishing. 2

[CJLL17] Jung Hee Cheon, Jinhyuck Jeong, Joohee Lee, and Keewoo Lee. Privacy-Preserving Computations of Predictive Medical Models with Minimax Approximation and Non-Adjacent Form. In Michael Brenner, Kurt Rohloff, Joseph Bonneau, Andrew Miller, Peter Y.A. Ryan, Vanessa Teague, Andrea Bracciali, Massimiliano Sala, Federico Pintore, and Markus Jakobsson, editors, *Financial Cryptography and Data Security*, pages 53–74, Cham, 2017. Springer International Publishing. 2

[CK89] B. Chor and E. Kushilevitz. A Zero-One Law for Boolean Privacy. In *Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing*, STOC '89, page 62–72, New York, NY, USA, 1989. Association for Computing Machinery. 36

BIBLIOGRAPHY

[CKKL22] Jung Hee Cheon, Dongwoo Kim, Duhyeong Kim, and Keewoo Lee. On the scaled inverse of $(x^i - x^j)$ modulo cyclotomic polynomial of the form $\phi_{p^s}(x)$ or $\phi_{p^s q^t}(x)$. *Journal of the Korean Mathematical Society*, 59(3):621–634, 2022. 39

[CKKS17] Jung Hee Cheon, Andrey Kim, Miran Kim, and Yongsoo Song. Homomorphic Encryption for Arithmetic of Approximate Numbers. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017*, pages 409–437, Cham, 2017. Springer International Publishing. 2

[CKL21] Jung Hee Cheon, Dongwoo Kim, and Keewoo Lee. MHz2k: MPC from HE over $\mathbb{Z}_{2^k}$ with New Packing, Simpler Reshare, and Better ZKP. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology – CRYPTO 2021*, pages 426–456, Cham, 2021. Springer International Publishing. 6, 7, 35

[CL22] Jung Hee Cheon and Keewoo Lee. Limits of Polynomial Packings for $\mathbb{Z}_{p^k}$ and $\mathbb{F}_{p^k}$. In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology – EUROCRYPT 2022*, pages 521–550, Cham, 2022. Springer International Publishing. 7

[CLPX18] Hao Chen, Kim Laine, Rachel Player, and Yuhou Xia. High-Precision Arithmetic in Homomorphic Encryption. In Nigel P. Smart, editor, *Topics in Cryptology – CT-RSA 2018*, pages 116–136, Cham, 2018. Springer International Publishing. 2

[Con] Keith Conrad. Modules over a PID. https://kconrad.math.uconn.edu/blurbs/linmultialg/modulesoverPID.pdf. 57

[CRX21] Ronald Cramer, Matthieu Rambaud, and Chaoping Xing. Asymptotically-good arithmetic secret sharing over $\mathbb{Z}/p^{\ell}\mathbb{Z}$ with strong multiplication and its applications to efficient mpc. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology – CRYPTO 2021*, pages 656–686, Cham, 2021. Springer International Publishing. 3, 12

[CXY20] Ronald Cramer, Chaoping Xing, and Chen Yuan. On the Complexity of Arithmetic Secret Sharing. In Rafael Pass and Krzysztof Pietrzak, editors, *Theory of Cryptography*, pages 444–469, Cham, 2020. Springer International Publishing. 3, 11, 55

[DEF+19] Ivan Damgård, Daniel Escudero, Tore Frederiksen, Marcel Keller, Peter Scholl, and Nikolaj Volgushev. New Primitives for Actively-Secure MPC over Rings with Applications to Private Machine Learning. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 1102–1120, 2019. 35, 36

[DKL+13] Ivan Damgård, Marcel Keller, Enrique Larraia, Valerio Pastro, Peter Scholl, and Nigel P. Smart. Practical Covertly Secure MPC for Dishonest Majority – Or: Breaking the SPDZ Limits. In Jason Crampton, Sushil Jajodia, and Keith Mayes, editors, *Computer Security – ESORICS 2013*, pages 1–18, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg. 36, 40

[DLN19] Ivan Damgård, Kasper Green Larsen, and Jesper Buus Nielsen. Communication Lower Bounds for Statistically Secure MPC, With or Without Preprocessing. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryp-*

tology – CRYPTO 2019, pages 61–84, Cham, 2019. Springer International Publishing. 3, 11

[DLSV20] Anders Dalskov, Eysa Lee, and Eduardo Soria-Vazquez. Circuit Amortization Friendly Encodingsand Their Application to Statistically Secure Multiparty Computation. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2020*, pages 213–243, Cham, 2020. Springer International Publishing. 3, 11, 26

[DPSZ12] Ivan Damgård, Valerio Pastro, Nigel P. Smart, and Sarah Zakarias. Multiparty Computation from Somewhat Homomorphic Encryption. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology – CRYPTO 2012*, pages 643–662, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg. 1, 2, 24, 36, 40, 41, 42

[ET36] Paul Erdös and Paul Turán. On Some Sequences of Integers. *J. London Math. Soc.*, 11(4):261–264, 1936. 26

[FV12] Junfeng Fan and Frederik Vercauteren. Somewhat Practical Fully Homomorphic Encryption. Cryptology ePrint Archive, Paper 2012/144, 2012. https://eprint.iacr.org/2012/144. 1

[Gen09] Craig Gentry. Fully Homomorphic Encryption Using Ideal Lattices. In *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, STOC '09, page 169–178, New York, NY, USA, 2009. Association for Computing Machinery. 1

[GGK08] William Gasarch, James Glenn, and Clyde P. Kruskal. Finding large 3-free sets I: The small n case. *Journal of Computer and System Sciences*, 74(4):628–655, 2008. Carl Smith Memorial Issue. 27

[GH19] Craig Gentry and Shai Halevi. Compressible FHE with Applications to PIR. In Dennis Hofheinz and Alon Rosen, editors, *Theory of Cryptography*, pages 438–464, Cham, 2019. Springer International Publishing. 5

[GHS12] Craig Gentry, Shai Halevi, and Nigel P. Smart. Better Bootstrapping in Fully Homomorphic Encryption. In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, *Public Key Cryptography – PKC 2012*, pages 1–16, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg. 2, 6, 25, 61

[HEl] HElib. https://github.com/homenc/HElib. 25

[HS15] Shai Halevi and Victor Shoup. Bootstrapping for HElib. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology – EUROCRYPT 2015*, pages 641–670, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg. 6, 25, 61

[KOS16] Marcel Keller, Emmanuela Orsini, and Peter Scholl. MASCOT: Faster Malicious Arithmetic Secure Computation with Oblivious Transfer. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, page 830–842, New York, NY, USA, 2016. Association for Computing Machinery. 36, 43

[KPR18] Marcel Keller, Valerio Pastro, and Dragos Rotaru. Overdrive: Making SPDZ Great Again. In Jesper Buus Nielsen and Vin-

cent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018*, pages 158–189, Cham, 2018. Springer International Publishing. 36, 40

[KSK+18] Andrey Kim, Yongsoo Song, Miran Kim, Keewoo Lee, and Jung Hee Cheon. Logistic regression model training based on the approximate homomorphic encryption. *BMC Medical Genomics*, 11(4):23–31, 2018. 1

[Lip12] Helger Lipmaa. Progression-Free Sets and Sublinear Pairing-Based Non-Interactive Zero-Knowledge Arguments. In Ronald Cramer, editor, *Theory of Cryptography*, pages 169–189, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg. 26

[LPR10] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On Ideal Lattices and Learning with Errors over Rings. In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, pages 1–23, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg. 1

[OSV20] Emmanuela Orsini, Nigel P. Smart, and Frederik Vercauteren. Overdrive2k: Efficient Secure MPC over $\mathbb{Z}_{2^k}$ from Somewhat Homomorphic Encryption. In Stanislaw Jarecki, editor, *Topics in Cryptology – CT-RSA 2020*, pages 254–283, Cham, 2020. Springer International Publishing. 2, 6, 7, 25, 26, 34, 37, 38, 40, 41, 42, 43

[PS21] Antigoni Polychroniadou and Yifan Song. Constant-Overhead Unconditionally Secure Multiparty Computation Over Binary Fields. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology – EUROCRYPT 2021*, pages

812–841, Cham, 2021. Springer International Publishing. 3, 11

[RRKK23] Pascal Reisert, Marc Rivinius, Toomas Krips, and Ralf Kuesters. Overdrive LowGear 2.0: Reduced-Bandwidth MPC without Sacrifice. In *Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security*, ASIA CCS '23, page 372–386, New York, NY, USA, 2023. Association for Computing Machinery. 36

[SV10] Nigel P. Smart and Frederik Vercauteren. Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes. In Phong Q. Nguyen and David Pointcheval, editors, *Public Key Cryptography – PKC 2010*, pages 420–443, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg. 2

[SV14] Nigel P. Smart and Frederik Vercauteren. Fully homomorphic SIMD operations. *Des. Codes Cryptogr.*, 71(1):57–81, 2014. 2

[Wan03] Zhe-Xian Wan. *Lectures on finite fields and Galois rings*. World Scientific Publishing Co., Inc., River Edge, NJ, 2003. 9

국문초록

암호학에서는 안전성 혹은 기능성을 위해 종종 크고 복잡한 수학적 구조를 사용한다. 반면 우리는 일상에서 작고 단순한 대수적 구조 위에서 주로 계산한다. 이러한 불일치와 관련하여, 대수적 구조를 보존하면서 큰 구조에 여러 개의 메시지를 채워 넣는 기법이 암호학의 다양한 세부분야에서 독립적으로 연구되어 왔다. 대표적으로 동형암호에서의 패킹기법과 정보이론적으로 안전한 다자간계산(MPC)에서의 역곱셈친화적 임베딩(RMFE)이 있다.

본 논문에서는 암호학의 다양한 맥락에서 등장하는 관련 개념들을 포괄하여 새롭게 동형팩킹을 정의한다. 통합된 정의를 바탕으로 기존의 기법들을 분석하고 동형패킹의 성능에 대한 몇 가지 수학적 한계를 증명한다.

또한, 새로운 동형패킹 방법을 고안하고 이를 활용하여 $\mathbb{Z}_{2^k}$를 메시지공간으로 갖는 효율적인 동형암호 기반 MPC 프로토콜을 설계한다. 증명한 동형패킹의 한계는 새로운 동형팩킹과 MPC 프로토콜의 설계방식을 정당화한다.

주요어: 암호학, 동형팩킹, 동형암호, 다자간계산, 역곱셈친화적 임베딩, $\mathbb{Z}_{2^k}$
학　번: 2017-28540

감사의 글

6년간의 대학원 생활을 마무리하는 글을 쓰고 있자니 시원섭섭합니다. 이 기회를 빌려 저의 삶에 크고 작은 자국을 남겨주신 모든 분께 감사의 말을 전하고 싶습니다. 좁은 지면 탓에 일일이 언급할 수 없고, 이유 없이 마음이 바빠 일일이 연락드리지는 못하지만, 지금껏 만난 소중한 인연들에 늘 감사하며 살아가고 있습니다.

제일 먼저, 박사과정 동안 저를 지도해 주신 천정희 교수님. 항상 진심으로 저를 대해주셔서 감사했습니다. 박사과정 내내 정말 많이 배웠습니다. 쉽지는 않겠지만, 교수님의 바람대로 청출어람 할 수 있도록 정진하겠습니다. 바쁘신 와중에 저의 학위논문심사를 위해 귀한 시간을 내어주신 현동훈 교수님, 이주영 교수님, 서재홍 교수님, 송용수 교수님께도 감사드립니다.

짧지 않은 대학원 생활이 외롭거나 지루하지 않을 수 있었던 것은 옆에서 함께 달려준 연구실 동료들 덕분임을 압니다. 학부생 인턴 때부터 함께 한 원희 형, 노르웨이 여행메이트 형민이 형, 가장 많은 대화를 나눈 재현이 형, 과몰입안하는(?) 민식이 형, 왠지 모르게 애착이 가는 용동이, 의젓한 막내 태성이까지 모두 고맙습니다. 덕분에 마지막까지 즐거웠습니다.

아무것도 모르던 풋내기 학부생 인턴이 박사학위를 받는 데까지 연구실 선배들의 도움도 컸습니다. 늘 밝은 미소로 대해주시는 미란 누나부터, 저의 첫 학회 참석과 LA 여행을 함께해 준 희원이 형, 끊임없는 아이디어와 집념이 대단한 창민이 형, 다양한 방면에서 꾸준히 영감과 도움을 주는 용수 형, 만날 때마다 저를 챙겨주려는 마음이 느껴지는 규형이 형, 암호 연구의 첫 단추를 끼워준 인턴 멘토이자 몰타 여행을 함께한 진혁이 형과 주희 누나, [수학적 알고리즘] 조교를 함께했던 안드레이, 대화할 때마다 경청해 주시고 함께 있으면 늘 유쾌한 용하 형, 의외의 섬세함으로 저를 살펴주었던 지승이 형, 희로애락을 함께한 최고의 coworker 동우 형, 가장 많은 자극과 영향을 받은 두형이 형, 판데믹에 랩장을 맡아 고생이 많았던 승완이 형까지 모두 감사합니다. 어깨너머로 많이 배웠습니다.

연구실에서 함께 생활한 기간이 없음에도 학회 등에서 마주치면 반갑게 안부를 물어주시는 연구실 선배님들께도 감사드립니다. 특히, 재홍 선배, 성욱 선배, 형태 선배, 태찬 선배 감사합니다.

연구실 선후배 외에도, 논문 공저자들을 포함하여 암호학을 통해 맺은 인연들 모두 소중하게 여기고 있습니다. 특히, 대화할 때마다 지적 자극을 주는 민기 형 고맙습니다. 이 지면을 빌려 준영이에게도 응원의 말을 전합니다.

장안중, 용인외고, 자유전공학부, 수리과학부 대학원, 혹은 그 밖의 인연으로 만나 저와 함께 걸어준 친구들과 선생님들 모두 감사합니다. 특히, 박사과정 동안 동거동락한 룸메이트 경성이 형에게 고맙다는 말을 전합니다. 늘 웃는 얼굴로 행정업무를 도와주신 김한나 선생님께도 감사드립니다.

흔들리거나 길을 잃은 것 같은 때 가장 먼저 찾게 되는 아버지, 혹여나 방해될까 늘 한 발짝 뒤에서 조용히 기도해 주시는 어머니, 그리고 동생 기주에게 고맙고 사랑한다는 말을 전합니다. 마지막으로, 만일 살아계셨다면, 제가 박사가 된 것에 저보다 더 기뻐해 주셨을 저의 조부모님들께 감사드립니다.