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

Jung Hee Cheon  Keewoo Lee
(Seoul National University & Crypto Lab Inc.)  (Seoul National University)
Sketch

- **Formal & Unified Study of “Polynomial Packing”**
  - ... which appears in various contexts:
  - HE & SHE-based MPC (HE Packing), IT-MPC (RMFE), Correlation Extractor, ZK...

- **Upper Bounds & Impossibility Results**
  - Packing Density, Level-Consistency, & Surjectivity

- **Implications**
  - SHE-based MPC over $\mathbb{Z}_{2^k}$, HE Packing, RMFE
Definition
Definition

Polynomial Packing

\[ R^n \quad \xrightarrow{\text{Pack}} \quad R = \mathbb{Z}_{p^k}[x]/f(x) \quad \xleftarrow{\text{Unpack}} \quad \mathcal{R} = \mathbb{Z}_{p^t}[x]/f(x) \]

Degree-\(D\) Packing

\[ R^n \quad \xrightarrow{\text{Pack}} \quad \mathcal{R} \quad \xleftarrow{\text{Unpack}} \quad \mathcal{R} \]

\[ P(\cdot): \text{(Multivariate) Polynomial of Degree } \leq D \]

* Packing Density = \(\log(|R|^n) / \log(|\mathcal{R}|)\)
Remark: Unpack may differ for each multiplicative level.

Definition 3.2 (Degree-$D$ Packing). Let $\mathcal{P} = (\text{Pack}_i, \text{Unpack}_i)_{i=1}^D$ be a collection of packing methods for $\mathbb{R}^n$ into $\mathbb{R}$. 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 $\text{Unpack}_i(a(x)) = a, \text{Unpack}_i(b(x)) = b$ for $a, b \in \mathbb{R}^n$, then $\text{Unpack}_i(a(x) \pm b(x)) = a \pm b$ holds;

- If $a(x), b(x)$ satisfy $\text{Unpack}_s(a(x)) = a, \text{Unpack}_t(b(x)) = b$ for $a, b \in \mathbb{R}^n$ and $s, t \in \mathbb{Z}^+$ such that $s + t = i$, then $\text{Unpack}_i(a(x) \cdot b(x)) = a \odot b$ holds.
Contexts & Examples
Homomorphic Encryption

- HE supports computation on encrypted data.

Diagram:

- $m$ is encrypted to $Enc(m)$ using $Enc$.
- $P(\cdot)$ transforms $Enc(m)$ to $Enc(P(m))$.
- $Eval_P$ evaluates $Enc(P(m))$.
- $Dec$ decrypts $Enc(P(m))$ to $P(m)$.
- $P(m)$ is decrypted to $m$.
- HE supports computation on encrypted data.
- Concurrent HE schemes are often based on RLWE for efficiency.
  - e.g. BGV, FV
Homomorphic Encryption

- HE supports computation on encrypted data.
- Concurrent HE schemes are often based on RLWE for efficiency.
  - e.g. BGV, FV
  - Practical Usability?
HE Packing [Smart-Vercauteren;PKC10]

\[ R^n \uparrow \mathcal{P} \downarrow \]

\[ \mathbb{Z}_t[x]/\Phi_M(x) \]

\[ m(x) \]

\[ \text{Enc}(m(x)) \]

\[ \mathcal{P} \]

\[ \mathcal{P}(\overrightarrow{m}) \]

\[ \text{Pack} \]

\[ \text{Eval}_\mathcal{P} \]

\[ \text{Unpack} \]

\[ \text{Dec} \]

\[ \text{Enc}(\mathcal{P}(m(x))) \]
HE Packing: Examples

- **Traditional Packing Method** [Smart-Vercauteren;PKC10]
  - $(\mathbb{F}_p^d)^r \rightarrow \mathbb{Z}_p[x]/\Phi_M(x) : \text{Degree-}\infty, \text{Density} = 1$
  - $(\mathbb{Z}_p)^{\varphi(M)} \rightarrow \mathbb{Z}_p[x]/\Phi_M(x)$, if $\Phi_M(x)$ fully splits mod $p : \text{Degree-}\infty, \text{Density} = 1$

- **HELib Packing for } \mathbb{Z}_{p^k}\text{-messages**} [Gentry-Halevi-Smart;PKC12], [Halevi-Shoup;Eurocrypt15]
  - $(\mathbb{Z}_{p^k})^r \rightarrow \mathbb{Z}_{p^k}[x]/\Phi_M(x) : \text{Degree-}\infty, \text{Density} = 1/d$

- **Recent Developments in SHE-based MPC over } \mathbb{Z}_{2^k}\text{ (SPDZ-family)}**
  - Overdrive2k [Orsini-Smart-Vercauteren;CT-RSA20] : \text{Degree-2, Density} \approx 1/5
  - MHzz2k [Cheon-Kim-Lee;Crypto21] : \text{Degree-2, Density} \approx 1/2

\[ \Phi_M(x) = \prod_{i=1}^r F_i(x) \mod p \& \deg F_i = d \]
Using “Large Field” is often required due to:

1. **Mathematical Structures**
   - **Shamir Secret Sharing**: We can interpolate at most \( q \) points over \( \mathbb{F}_q \)

2. **Security**
   - **Linear MAC**: \( MAC_\alpha(x) := \alpha \cdot x \) over \( \mathbb{F}_q \) has soundness error \( 1/q \)
Reverse Multiplication-Friendly Embedding (RMFE)

- Embed algebraic structure of copies of small field (e.g. $\mathbb{F}_2^n$) into a larger field (e.g. $\mathbb{F}_{2^d}$).
- Essentially, RMFEs are **Degree-2** packings from $\mathbb{F}_q^n$ into $\mathbb{F}_{q^d} \cong \mathbb{F}_q[x]/f(x)$.
- Now a Standard Tool in IT-MPC (e.g. [DLN;Crypto19], [DLSV;Euro20], [PS;Euro21], ...)
- Also used in ZK (e.g. [BMRS;Crypto21], [CG;FC22])
Theorems & Implications
Packing Density

- **Theorem**
  - Roughly speaking, density of degree-$D$ packing method $\leq 1/D$
  - For $d = \text{deg. of irreducible quotient poly.}$, 
    \[ \text{[packing density]} \leq \frac{1}{D} + \frac{1}{d} \left(1 - \frac{1}{D}\right) \]

- **Implications**
  1. MHz2k [CKL;Crypto21] achieves near-optimal density (as a degree-2 packing for $\mathbb{Z}_{2^k}$)
  2. ($\mathbb{F}_{p^k}$ Version) New and more general proof for upper bound on rate of RMFE
  3. First upper bound on rate of RMFE over Galois rings [Cramer-Rambaud-Xing;Crypto21]
Level-Consistency

- Motivation
  - FHE, Homomorphic computation between different mult. levels (e.g. Reshare Protocol)

- Theorem
  - If level-consistency holds,
    \[ n \leq \lceil \text{# of distinct irreducible factors of quotient poly. \mod p} \rceil \]

- Implications
  1. Optimality of HELib packing with respect to packing density and level-consistency
  2. Impossibility of Efficient Level-Consistent HE Packing for \( \mathbb{Z}_{2^k} \)
  3. Importance of “Constant Packing Trick” of MHZ2k for Level-dependent packings
Surjectivity

- **Motivation**
  - Malicious “Packer” might leverage invalid packings in protocols.

- **Theorem**
  - If surjectivity holds,

\[ n \leq \lceil \text{# of distinct linear factors of quotient poly. mod } p^k \rceil \]

- **Implications**
  1. Impossibility of Surjective HE Packing for \( \mathbb{Z}_{2^k} \)
  2. Necessity of ZKPoMK in HE-based MPC over \( \mathbb{Z}_{2^k} \) (First conceptualized in MHz2k)
Summary

- **Formal & Unified Study of Polynomial Packing**
  - which appears in various contexts:
    - HE & SHE-based MPC (HE Packing), IT-MPC (RMFE), Correlation Extractor, ZK...

- **Upper Bounds & Impossibility Results**
  - Packing Density, Level-consistency, and Surjectivity
Summary

- Implications on SHE-based MPC over $\mathbb{Z}_{2^k}$ (c.f. MHz2k [CKL;Crypto21])
  1. MHz2k achieves near-optimal packing density
  2. Importance of “Constant Packing Trick” of MHz2k for Level-dependent packings
  3. Necessity of ZKPoMK in HE-based MPC over $\mathbb{Z}_{2^k}$ (First conceptualized in MHz2k)

- Implication on HE Packing
  1. Optimality of HELib packing with respect to packing density and level-consistency

- Implications on RMFE
  1. New and more general proof for upper bound on rate of RMFE
  2. First upper bound on rate of RMFE over Galois rings (c.f. [CRX;Crypto21])
Conclusion

1. Packing is not a question asked before secure computation.
   - Messages are “static” (e.g. PKE): No need to worry about structure of messages.

2. Packing is a question shared by secure computation primitives.
   - Messages are “dynamic” (HE, MPC, ZK): Algebraic structure of messages matters.

3. There might be more questions of like this!
   - Especially when we try to apply secure computation to real-life problems.
Thank You!

* ePrint: ia.cr/2021/1033
* E-mail: activecondor@snu.ac.kr
* Webpage: keewoolee.github.io