

ON ALGEBRAIC HOMOMORPHIC ENCRYPTION AND ITS APPLICATIONS TO DOUBLY-EFFICIENT PIR [OPP25]

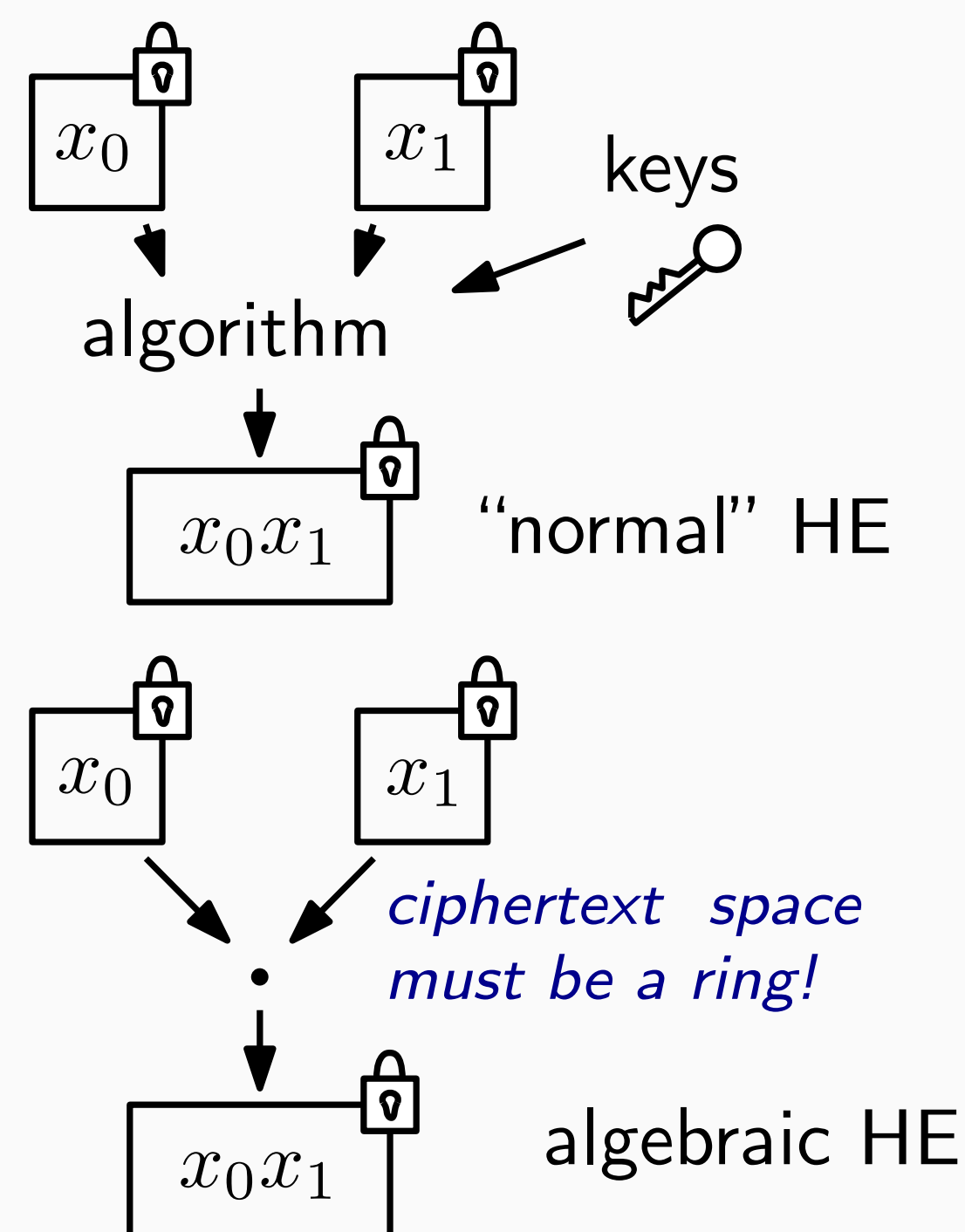


Hiroki Okada^{1,2}, Rachel Player³, Simon Pohmann³, and Christian Weinert³

¹KDDI Research ²The University of Tokyo ³Royal Holloway, University of London



ASHE



e.g. BV [BV11], but not modern schemes (BGV, BFV, CGGI)

Our contributions

- Lower bound on ASHE ciphertext size
 - Asymptotic improvements to DEPIR
 - Security proof for $\{0, 1\}$ -CRT RLWE
- See our paper [OPP25] for
- [KU11] datastructure improvements
 - Faster DEPIR, building on [OPP24]
 - Concrete attacks on $\{0, 1\}$ -CRT RLWE

Polynomial datastructure

$$f \in \mathbb{Z}[X_1, \dots, X_m]$$



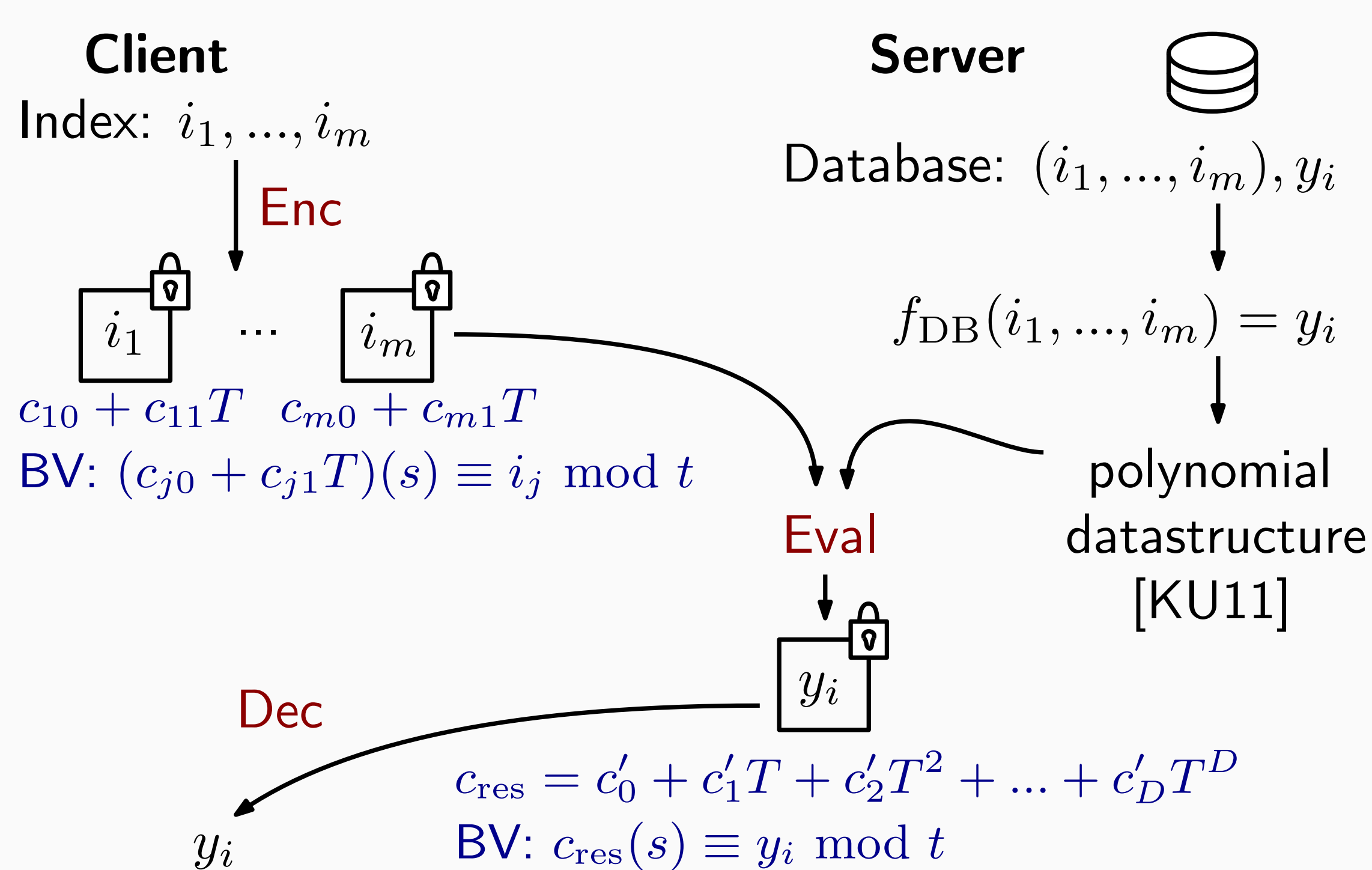
Polynomial Datastructure [KU11, Thm 5.1]

Size is $\text{poly}(m, D, \ln p)(D \ln \ln p)^m$

Evaluation takes $\tilde{O}(D^2 \log p)$

- $D = \deg_{\text{total}}(f)$
- Evaluation at points in $\mathbb{F}_p^m$

DEPIR Protocol [LMW23]



BV ring size

$$\text{RLWE ring: } R_q := \mathbb{Z}[X]/(\Phi_n(X), q) \cong \bigoplus_{0 \leq i \leq r} \bigoplus_{0 \leq j \leq \phi(n)} \mathbb{F}_{p_i}$$

$$\text{Ciphertext ring: } C := R_q[T]/(X^{D+1} - 1) \text{ "polys of deg } \leq D"$$

$$\text{Efficiency metric: } \#C \approx \exp(\ln(\max p_i) \cdot r \cdot \phi(n) \cdot D) \approx \exp(nD^2)$$

- $r \approx D$ because noise grows multiplicatively
- $\max p_i$ basically constant

We show a lower bound!

A post-quantum ASHE scheme that can evaluate polynomials of total degree D has ciphertext ring size

$$\#C \in \exp(\Omega(D))$$

Can we construct an ASHE scheme with ciphertext ring of size $\exp(O(D))$?

RLWE with $b = 0$ and NTRU

Ring LWE: Distinguish samples (b, a) from uniform!

$$a \xleftarrow{\$} R_q, \quad b = as + e, \quad e \leftarrow \underbrace{\mathcal{D}_\sigma}_{\text{discrete Gaussian}}$$

$s \in R_q$ is a short ring element, the "secret"

What if $b = 0$? $\rightsquigarrow$ **NTRU:** Distinguish e/s from uniform, where $e \leftarrow \mathcal{D}_\sigma$

Unfortunately, NTRU is "overstretched" for the q we use...

$\{0, 1\}$ -CRT RLWE

Don't set $b = 0$, but b in the " $\{0, 1\}$ -CRT set"

$$S = \{a \in R_q \mid \forall \mathfrak{p} \leq R_q : a \bmod \mathfrak{p} \in \{0, 1\}\}$$

$$= \text{preimage of } \{0, 1\}^{r \times \phi(n)} \text{ under } R_q \xrightarrow{\sim} \bigoplus_{p \mid q} \bigoplus_{0 \leq j \leq \phi(n)} \mathbb{F}_p$$

$\{0, 1\}$ -CRT RLWE: Distinguish (b, a) from uniform, where

$$b \xleftarrow{\$} S, \quad a = s^{-1}(b - e), \quad e \leftarrow \mathcal{D}_\sigma$$

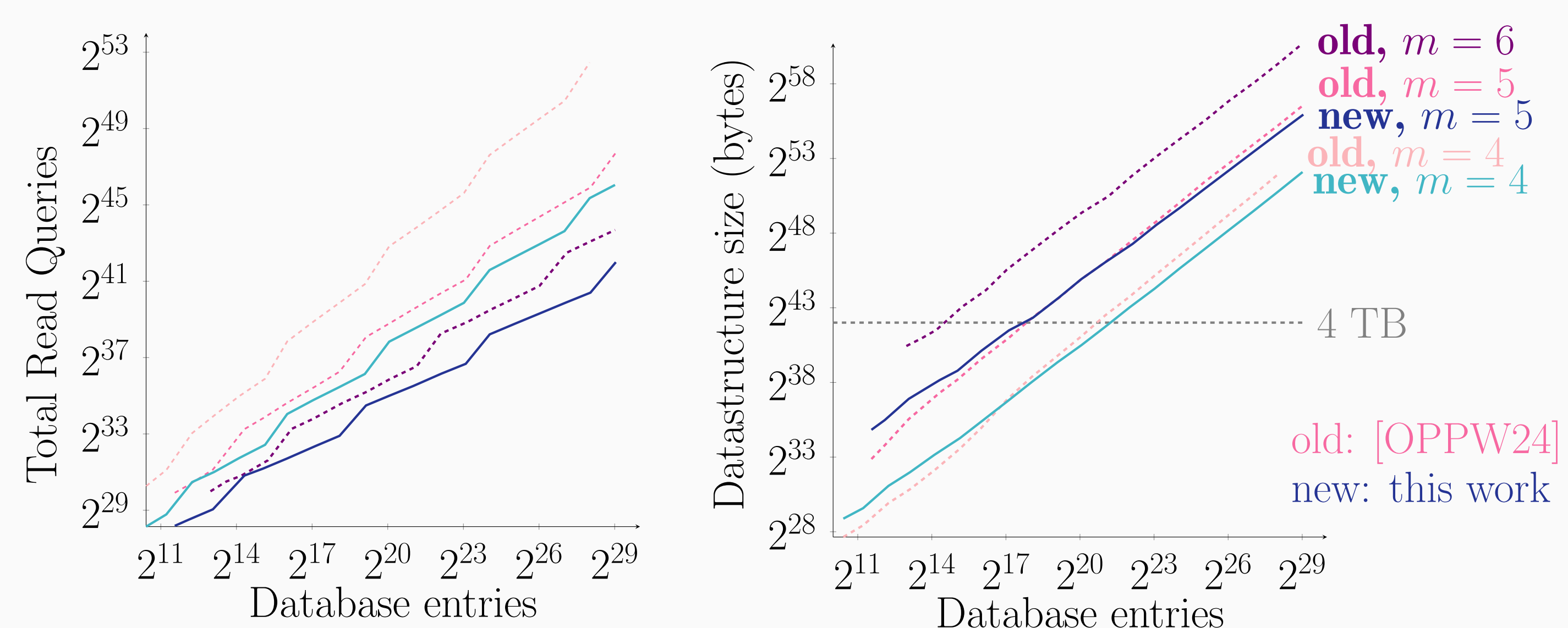
Security of $\{0, 1\}$ -CRT RLWE

Goal: Reduction from RLWE to $\{0, 1\}$ -CRT RLWE

Idea: "Round" the b of RLWE samples "to S "

- We don't know how to efficiently solve "CVP" on S
 - $\rightsquigarrow$ Use a preprocessing phase, which given R and q , computes "hint"
- S must be "evenly distributed", i.e. rounding gives low additional error
 - $\rightsquigarrow$ Generalize smoothing parameter to non-lattices (i.e. S)
 - $\rightsquigarrow$ Use Fourier analysis + probabilistic argument over random choice of q

Better DEPIR performance with $\{0, 1\}$ -CRT RLWE



References

- [BV11] Z. Brakerski and V. Vaikuntanathan. "Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages". *CRYPTO*. Vol. 6841. LNCS. 2011, pp. 505–524.
- [KU11] K. S. Kedlaya and C. Umans. "Fast Polynomial Factorization and Modular Composition". In: *SIAM J. Comput.* 40.6 (2011), pp. 1767–1802.
- [LMW23] W. Lin, E. Mook, and D. Wichs. "Doubly Efficient Private Information Retrieval and Fully Homomorphic RAM Computation from Ring LWE". *STOC*. 2023, pp. 595–608.
- [OPP24] H. Okada, R. Player, S. Pohmann, and C. Weinert. "Towards Practical Doubly-Efficient Private Information Retrieval". *FC*. Vol. 14745. LNCS. 2024, pp. 264–282.
- [OPP25] H. Okada, R. Player, S. Pohmann, and C. Weinert. "On Algebraic Homomorphic Encryption and its Applications to Doubly-Efficient PIR". *EUROCRYPT*. LNCS. To Appear. 2025.

Acknowledgements

Simon Pohmann was supported by the EPSRC and the UK Government as part of the Centre for Doctoral Training in Cyber Security at Royal Holloway, University of London (EP/S021817/1).