TU Graz

SCIENCE
PASSION
TECHNOLOGY

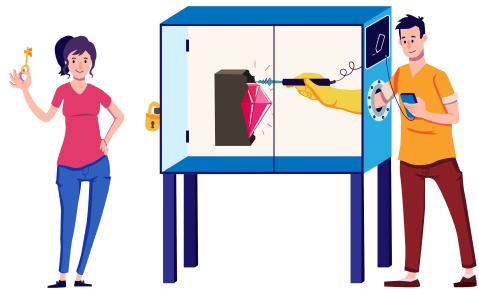
Open Source Framework for Hybrid Homomorphic Encryption

Lukas Helminger, Daniel Kales, Christian Rechberger, **Roman Walch**

FSE 2020 Rump Session

Hybrid Homomorphic Encryption

- Evaluate symmetric ciphers under homomorphic encryption
- Why?
  - Ciphertext expansion prevention
  - See also Dasta talk from Monday
- Relevant metrics:
  - Multiplicative depth (AND-depth)
  - ANDs per encrypted bit

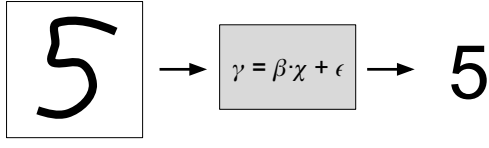


HHE Schemes

- So far:
  - Many candidate schemes
  - Many different HE libraries
  - But: No meaningful comparison done/possible
- Which scheme is best suited for
  - ... which metric?
  - ... which HE library?
  - ... which use case afterwards?

Benchmarking Framework

- No meaningful comparison done/possible → until now!
- We build a open-source Framework:
  - Compares candidate schemes in different libraries
  - Benchmarks use cases afterwards
  - Easy integration of new designs
- Small use cases from Privacy-Preserving Machine Learning
  - E.g. linear regression to identify handwritten digits



Benchmarking Framework – Status

- So far:
  - Implementations of candidate ciphers in three different libraries
  - Small benchmarks

	SEAL	HElib	TFHE
Rasta	✓	✓	✓
Agrasta	✓	✓	✓
Dasta	✗	✗	✗
FiLIP	✓	✓	✓
Kreyvium	✓	✓	✓
LowMC	✓	✓	✓

Benchmarking Framework – Status (cont.)

- Up next:
  - Implement missing ciphers
  - Extensive Benchmarks
  - Compare to orthogonal approach
    - E.g. LWEs $\rightarrow$ RLWE [CDKS20]
  - Publish Code
    - Will be available at `https://github.com/IAIK/hybrid-HE-framework`

TU Graz

SCIENCE
PASSION
TECHNOLOGY

Open Source Framework for Hybrid Homomorphic Encryption

Lukas Helminger, Daniel Kales, Christian Rechberger, **Roman Walch**

FSE 2020 Rump Session

Bibliography I

[20] **Microsoft SEAL (release 3.5)**. https://github.com/Microsoft/SEAL. Microsoft Research, Redmond, WA. Apr. 2020.

[ARS+15] Martin R. Albrecht, Christian Rechberger, Thomas Schneider, Tyge Tiessen, and Michael Zohner. **Ciphers for MPC and FHE**. EUROCRYPT (1). Vol. 9056. Lecture Notes in Computer Science. Springer, 2015, pp. 430–454.

[CCF+16] Anne Canteaut, Sergiu Carpov, Caroline Fontaine, Tancrède Lepoint, Maria Naya-Plasencia, Pascal Paillier, and Renaud Sirdey. **Stream Ciphers: A Practical Solution for Efficient Homomorphic-Ciphertext Compression**. FSE. Vol. 9783. Lecture Notes in Computer Science. Springer, 2016, pp. 313–333.

[CDKS20] Hao Chen, Wei Dai, Miran Kim, and Yongsoo Song. **Efficient Homomorphic Conversion Between (Ring) LWE Ciphertexts**. IACR Cryptology ePrint Archive 2020 (2020), p. 15.

Bibliography II

[CGGI16] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. **TFHE: Fast Fully Homomorphic Encryption Library**. https://tfhe.github.io/tfhe/. August 2016.

[DEG+18] Christoph Dobraunig, Maria Eichlseder, Lorenzo Grassi, Virginie Lallemand, Gregor Leander, Eik List, Florian Mendel, and Christian Rechberger. **Rasta: A Cipher with Low ANDdepth and Few ANDs per Bit**. CRYPTO (1). Vol. 10991. Lecture Notes in Computer Science. Springer, 2018, pp. 662–692.

[HL20] Phil Hebborn and Gregor Leander. **Dasta - Alternative Linear Layer for Rasta**. IACR Trans. Symmetric Cryptol. 2020.3 (2020), pp. 46–86.

[HS14] Shai Halevi and Victor Shoup. **Algorithms in HElib**. CRYPTO (1). Vol. 8616. Lecture Notes in Computer Science. Springer, 2014, pp. 554–571.

[MCJS19] Pierrick Méaux, Claude Carlet, Anthony Journault, and François-Xavier Standaert. **Improved Filter Permutators for Efficient FHE: Better Instances and Implementations**. INDOCRYPT. Vol. 11898. Lecture Notes in Computer Science. Springer, 2019, pp. 68–91.