Duality

FHE-Related Comments on NIST First Call for Multi-Party Threshold Schemes

Yuriy Polyakov

ypolyakov@dualitytech.com

September 27, 2023

MPTS 2023: NIST Workshop on Multi-Party Threshold Schemes 2023

Public Comments

- Our initial comments were submitted in April 2023
- This talk presents updated (conceptual) comments on FHE, focusing on classes of capabilities, use cases, and security models
- Andreea Alexadru's talk presents technical details and discusses potential gadgets for Threshold FHE

Comments on NIST First Call for Multi-Party Threshold Schemes

Ahmad Al Badawi[1], Andreea Alexandru[1], Nicholas Genise[1], Daniele Micciancio[1,3], Yuriy Polyakov[1], Saraswathy R.V.[1], and Vinod Vaikuntanathan[1,2]

[1]Duality Technologies
[2]MIT
[3]UCSD

April 10, 2023

Our comments are for Fully Homomorphic Encryption (FHE) schemes based on LWE and Ring/Module LWE over power-of-two cyclotomic rings, since that is what is most commonly implemented in open-source libraries. Our comments could apply to other FHE schemes with different hardness assumptions as well (e.g., NTRU).

Background: FHE Schemes

- Practical FHE scheme instantiations target passive security
- Common FHE schemes can be separated into three categories:
  - Brakerski-Gentry-Vaikuntanathan [BGV14] (BGV) and Brakerski [Bra12]/Fan-Vercauteren [FV12] (BFV)
    - Support SIMD encrypted computations for arithmetic circuits modulo a prime power
  - Ducas-Micciancio [DM15] (DM, also called FHEW)/Chillotti-Gama-Georgieva-Izabachene [CGGI16] (CGGI, also called TFHE)
    - Support binary or small-precision arithmetic
    - Arbitrary functions are evaluated using lookup tables via functional/programmable bootstrapping
  - Cheon-Kim-Kim-Song [CKKS17] (CKKS, also called HEAAN)
    - Support SIMD fixed-point-like arithmetic circuits (for many real-number applications)
- All these schemes are based on LWE/RLWE/MLWE
  - There are also less-common variants based on NTRU
  - Thresholdization of FHE schemes in practice follows the same blueprint with key-homomorphism used for distributed key generation and masked partial decryptions for distributed decryption

Background: Current Standardization Efforts

- HomomorphicEncryption.org – open consortium of industry, government and academia to standardize homomorphic encryption
  - Founded in 2017
  - 6 meetings held from 2017 to present
  - Security recommendations are available since 2018
- ISO standardization (in progress)
  - Targeting BGV, BFV, CKKS, and CGGI
  - Technical Committee : ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection

Background: Main Active Open-Source Software Libraries

- [OpenFHE]
  - Implements in C++ single-key FHE for all five schemes
  - Supports threshold FHE for BGV, BFV, and CKKS
- [Lattigo]
  - Implements in Go single-key and threshold FHE for BGV, BFV, and CKKS
- [TFHE-rs]
  - Implements in rust the CGGI scheme (with many enhancements)

Classes of HE-Related Capabilities

- We suggest separating lattice-based HE capabilities into three classes
- Class 1: Threshold key generation and decryption
- Class 2: HE schemes with linearly-homomorphic operations/additive homomorphic encryption (AHE)
- Class 3: FHE schemes that support nonlinear operations, which may use relinearization, bootstrapping, and/or other similar techniques
  - This class should probably be further broken down into subclasses
  - Circular security should be considered in the context of Class 3
- **Targeting the first two classes should be easier, both under passive and active security**

Use Cases for HE

- **Class 1: Threshold key generation and decryption**
  - Same as for Category 1 of the NIST MPTS call
  - Can build upon the NIST PQC standardization effort + thresholdization [CCMS21]
- **Class 2: Additive homomorphic encryption**
  - Often used as a gadget in hybrid cryptosystems, e.g., MP-SPDZ uses BGV for addition and plaintext-ciphertext computations to generate Beaver triplets
  - Several other use cases are discussed in our public comments, e.g., secure voting, aggregation, some PIR schemes
- Class 3: FHE schemes
  - Certain PIR and PSI schemes, AES tranciphering, neural network & training
  - See our public comments for more details

Passive Security

- IND-CPA security is typically sufficient to achieve passive security (for data privacy) for **exact** FHE schemes, including BGV, BFV, DM, and CGGI
- IND-CPA security is not sufficient for **approximate** FHE schemes
  - Li and Micciancio showed that CKKS is not secure if access to a decryption oracle is provided, i.e., when the decryption result is shared with parties that do not have the secret key [LM21]
  - They proposed a new definition IND-CPA^D that provides access to encryption, evaluation, and decryption oracles
- Threshold FHE schemes also require access to decryption oracles (for partial decryptions) and similar solutions, i.e., **approximate encryption can be viewed as a special case of threshold FHE** [KS23]

Active Security

- What are the potential approaches for building actively-secure threshold encryption schemes based on lattices?

- Class 1: Fujisaki-Okamoto (FO) transformation (very challenging for scenarios with HE)?
  - Two of the three lattice-based finalists in the NIST PQC competition, Crystals-Kyber and Saber, built an IND-CPA secure encryption scheme and then applied the FO transform to create an IND-CCA hybrid scheme
  - There are some challenges in thresholdizing this approach; however, initial constructions for thresholdized Saber based on this approach are available [CCMS21]

- Class 2: Actively secure BGV-based threshold encryption/AHE
  - Overdrive [KPR18] employs BGV for addition and plaintext-ciphertext multiplication to generate Beaver triples, applying noise flooding for circuit privacy and zero-knowledge proofs for active security
  - Aranha et al. use actively secure threshold BGV (both threshold key generation and threshold decryption) and ZKPs to construct an efficient form of secure voting [ABGS22]

References

[ABGS22] Diego F. Aranha, Carsten Baum, Kristian Gjøsteen, and Tjerand Silde. Verifiable mix-nets and distributed decryption for voting from lattice-based assumptions. IACR Cryptol. ePrint Arch., page 422, 2022.

[BGV14] Z. Brakerski, C. Gentry, and V. Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. ACM Transactions on Computation Theory (TOCT), 6(3):1–36, 2014.

[Bra12] Z. Brakerski. Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP. In CRYPTO 2012. Pages 868 – 886.

[CCMS21] Kelong Cong, Daniele Cozzo, Varun Maram, and Nigel P. Smart. Gladius: LWR based efficient hybrid public key encryption with distributed decryption. In ASIACRYPT (4), volume 13093 of LNCS, pages 125–155. Springer, 2021.

[CGGI16]: I. Chillotti, N. Gama, M. Georgieva, and M. Izabachène. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. In Asiacrypt 2016 (Best Paper), pages 3-33.

[CKKS17] J. H. Cheon, A. Kim, M. Kim, Y. Song, Homomorphic Encryption for Arithmetic of Approximate Numbers. In ASIACRYPT 2017. Pages 409–437.

[DM15]: L. Ducas and D. Micciancio. FHEW: bootstrapping homomorphic encryption in less than a second. EUROCRYPT 2015.

[DLNPY21] Julien Devevey, Benoît Libert, Khoa Nguyen, Thomas Peters, Moti Yung: Non-interactive CCA2-Secure Threshold Cryptosystems: Achieving Adaptive Security in the Standard Model Without Pairings. Public Key Cryptography (1) 2021: 659-690

[FV12] J. Fan and F. Vercauteren. Somewhat Practical Fully Homomorphic Encryption. Cryptology ePrint Archive. Report 2012/144, 2012. http://eprint.iacr.org/2012/144.

[KPR18] Marcel Keller, Valerio Pastro, and Dragos Rotaru. Overdrive: Making SPDZ great again. In EUROCRYPT (3), volume 10822 of LNCS, pages 158–189. Springer, 2018.

[KS23] Kamil Kluczniak, Giacomo Santato: On Circuit Private, Multikey and Threshold Approximate Homomorphic Encryption. IACR Cryptol. ePrint Arch. 2023: 301 (2023)

Thank You! Have questions?

Yuriy Polyakov

ypolyakov@dualitytech.com