Setup-free threshold multikey FHE with short ciphertexts

Antoine Urban, Telecom Paris, Institut Polytechnique de Paris

Keywords: Multiparty computation, FHE, Lattice cryptography, Threshold cryptography

1. Background & Use Cases

Secure multiparty computation (MPC) allows a set of N players holding private inputs x_i to securely compute any arithmetic circuit on these inputs, even if up to $t < N/2$ players, denoted as "corrupted", are fully controlled by an adversary $\mathcal{A}$ which we assume to be computationally bounded. We focus on the specific case of an asynchronous communication network, with access to one synchronous broadcast at the beginning. This model covers the case where players would publish encryptions of their inputs on a public ledger, and, after a timeout, the actual MPC computation is done asynchronously on the published encrypted inputs.

In this model (denoted as *almost-asynchronous*), Beerliova-Hirt-Nielsen [BHN10] proposed a MPC protocol that tolerates up to $t < N/2$ corruptions. However, their construction requires a trusted third party during setup. Later, Gordon et al. [DLS15] presented a threshold FHE scheme without trusted setup, but that produces large ciphertexts (of size $O((nN)^2)$ where n denotes a large lattice parameter). *Our goal is to build a more efficient scheme by reducing the size of the ciphertexts.* To this end, advances have been made in two opposite directions: *i*) [Che+19; CCS19] built setup-free multikey FHE schemes, but the ciphertexts are at least linear in size in the number of players and do not support threshold operations, and, *ii*) [Mou+21; Kim+20] built FHE schemes with constant size of ciphertext, but that require an interactive setup and doesn't support threshold operations. Our aim is to link these two lines of research.

2. Setup-free threshold multikey FHE with short ciphertexts

In this presentation, we address the aforementioned limitation by presenting a new *Threshold Multikey Fully Homomorphic Encryption* (TMFHE) scheme that requires only a *transparent setup*, and, produces a threshold *constant-size ciphertexts* (i.e. with only a $O(n)$ dependence) after transformation (down from $O((nN)^2)$ [DLS15]). Informally, we first recall the structure, presented in [DLS15], of a threshold encryption with $t < N/2$ corrupt players among N participants that allows:

- (For any *Input Owner*, denoted Alice), to generate a threshold ciphertext c between N players at threshold $t < N/2$, even though the N players have never interacted. We only require that each of them has published a public key; notably, they have not generated a shared secret key beforehand.
- The N participants to collectively transform, whatever the behavior of t malicious players, the ciphertext c into a ciphertext c' of constant size, without any intervention of Alice. This takes only 2 interactions, of which the first one is *independent* of c. Last but not least, we are able to do FHE operations on all ciphertexts c' obtained from several different Alices.

Our construction encompasses three main ingredients.

- First, we leverage the key homomorphic properties of a RLWE-based [LPR13] cryptosystem (eg BFV [FV12]), to build a multikey construction with short ciphertexts. The intuition is that we can use this property to define a common key as a sum of the individual player' keys.
- Second, we notice that the ciphertext transformation of [DLS15] doesn't easily adapt to the ring setting. Thus, we formalize an innovative solution to implement an *almost non-interactive delayed linear combination* functionality that we use to create a scheme that adapts to the players that behave correctly.
- Third, we leverage linear secret sharing over rings [Abs+19] (in our case $Z/qZ[X]/(X^n + 1)$) to build a threshold and setup-free construction. Importantly, the linearity of the secret sharing is what allows the key homomorphism to be used, without the necessary intervention of the malicious players.

December 6, 2021

References

[BHN10] Zuzana Beerliová-Trubíniová, Martin Hirt, and Jesper Buus Nielsen. "On the theoretical gap between synchronous and asynchronous MPC protocols". In: *Proceedings of the 29th Annual ACM Symposium on Principles of Distributed Computing, PODC 2010, Zurich, Switzerland, July 25-28, 2010*. 2010.

[FV12] Junfeng Fan and Frederik Vercauteren. "Somewhat practical fully homomorphic encryption." In: *IACR Cryptol. ePrint Arch.* 2012 (2012), p. 144.

[LPR13] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. "On Ideal Lattices and Learning with Errors over Rings". In: *J. ACM* 60.6 (Nov. 2013). ISSN: 0004-5411. DOI: 10.1145/2535925. URL: https://doi.org/10.1145/2535925.

[DLS15] S. Dov Gordon, Feng-Hao Liu, and Elaine Shi. "Constant-Round MPC with Fairness and Guarantee of Output Delivery". In: *Advances in Cryptology – CRYPTO 2015*. Ed. by Rosario Gennaro and Matthew Robshaw. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 63–82. ISBN: 978-3-662-48000-7.

[Abs+19] Mark Abspoel et al. "Efficient Information-Theoretic Secure Multiparty Computation over Z/p^kZ via Galois Rings". In: *Theory of Cryptography - 17th International Conference, TCC*. 2019.

[CCS19] Hao Chen, Ilaria Chillotti, and Yongsoo Song. "Multi-key homomorphic encryption from TFHE". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2019, pp. 446–472.

[Che+19] Hao Chen et al. "Efficient multi-key homomorphic encryption with packed ciphertexts with application to oblivious neural network inference". In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 2019, pp. 395–412.

[Kim+20] E. Kim et al. "How to Securely Collaborate on Data: Decentralized Threshold HE and Secure Key Update". In: *IEEE Access* 8 (2020), pp. 191319–191329. DOI: 10.1109/ACCESS.2020.3030970.

[Mou+21] Christian Mouchet et al. "Multiparty homomorphic encryption from ring-learning-with-errors". In: *Proceedings on Privacy Enhancing Technologies* 2021.4 (2021), pp. 291–311.