Duality

Building blocks for Threshold FHE

Andreea Alexandru
aalexandru@dualitytech.com

A. Al Badawi, N. Genise, D. Micciancio, Y. Polyakov,
S. Ramanathapuram Vancheeswaran, V. Vaikuntanathan

MPTS 2023: NIST Workshop on Multi-Party Threshold Schemes 28 Sep 2023

Quick overview of Fully Homomorphic Encryption (FHE)

- Correctness: Dec(Enc(x)) =(≈) x ; Dec(Eval(f, Enc(x))) =(≈) f(x)
- Complex algorithms: (functional) bootstrapping
- Compactness + efficiency: key/modulus switching, RNS representation, relinearization
- Lattice-based schemes [Gen09, Bra12, FV12, GHS13, BGV14, DM15, CGGI16, CKKS17]

- Typical single-server use case
  - Trusted client generates the keys, encrypts and decrypts
  - Server might or might not operate with secrets

Andreea Alexandru aalexandru@dualitytech.com

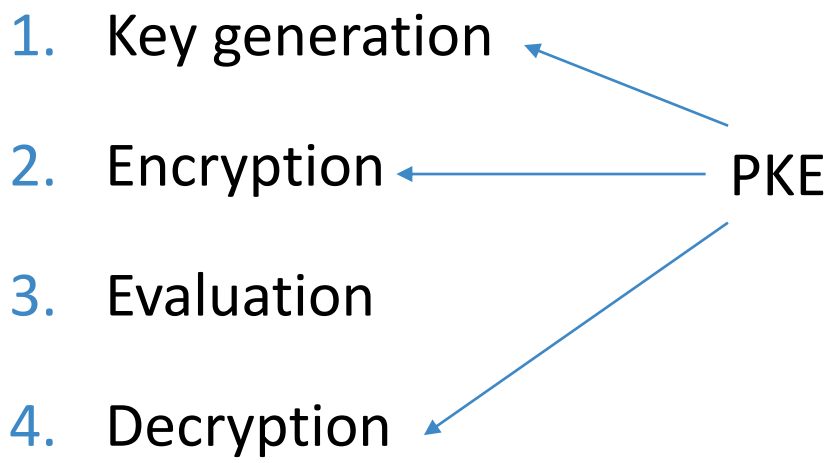
Quick overview of Threshold FHE (ThFHE)

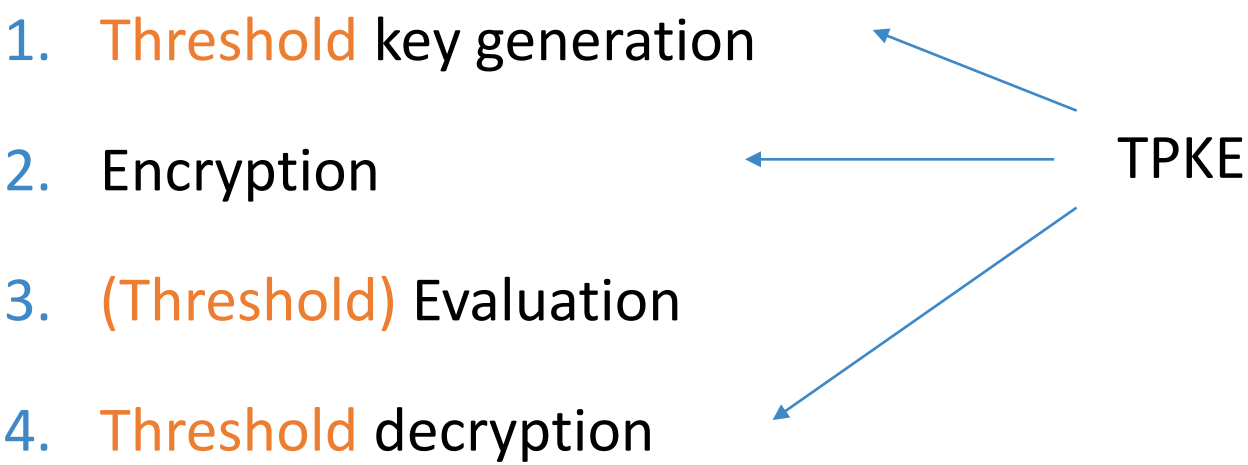
- Multiple types of multi-party FHE
  - Multi-key FHE, Threshold FHE, Hybrid
- Goal: multiple parties emulate both the client and the server
- [BD10, AJL+12, LATV12, BGG+18, CCS19, SPT+21, MBH23, CCK23]

- Typical threshold FHE use case: each party has some local secret input
  - Parties **jointly** generate the secret and public keys
  - Each party evaluates the function (can be both **non-interactive** and **interactive**)
  - Parties **jointly** decrypt the result

Andreea Alexandru aalexandru@dualitytech.com

FHE -> Threshold FHE





Static vs Adaptive Corruptions

Trusted vs Untrusted Setup

Honest vs Dishonest Majority

Passive vs Active Security

Game- vs Simulation-based Definition

Synchronous vs Asynchronous Communication

Pre-Q vs PQ resilience

Andreea Alexandru aalexandru@dualitytech.com

Background: Security notions for PKE

- IND-CPA: encryption oracle access
- IND-CCA1: a priori decryption oracle access or “lunchtime attack”
- IND-CCA2: decryption oracle access

Security notions for TPKE

- The adversary has access to partial decryptions
- IND-TCPA, IND-TCCA [FPS01]: encryption + partial decryption oracle access, + decryption oracle access
- Smudging/Noise flooding/Sanitization [DS16, MW16]
- Threshold PKE: threshold key gen + threshold decryption
  - **Not trivial** to thresholdize existing lattice-based PKE schemes [BGGK17, BGG+18, CS19, KLO+19, DLN+21, CCMS21, CHI+21, BTT22, ASY22, GKS23]
  - Issues: secret sharing of key, growth of parameters, complex algorithms, transforms, etc.

Is TPKE a building block for ThFHE?

Yes… and no.
Evaluation brings new challenges!

Background: “Passive” security notions for FHE

- IND-CPA’: encryption + evaluation oracle access **(careful in the modular approach)**
- IND-CPA^D [LM21, LMSS22]: oracle access to “encrypt-evaluate-decrypt”
- Circuit privacy [Gen09, OPCPC14, BdPMW16, KS23]: all ciphertexts have the same distribution
- funcCPA [AV21, AGHV22]: oracle access for “decrypt-evaluate-encrypt”

Andreea Alexandru aalexandru@dualitytech.com

Standardizing passive ThFHE

- Security of threshold PKE does not automatically imply security of threshold FHE
- IND-TCPA’ [BS23, KS23]: encryption + evaluation + partial decryption oracle access
- Real/Ideal functionality [DPSZ12]

Gadgets & building blocks

- Passive security definitions for ThFHE: IND-TCPA’, passive MPC, (thresholdized?) funcCPA
- Noise flooding/sanitization/smudging
- Cryptographic closeness: statistical distance [AJL+12], bit-security distance [MW18, LMSS22], Rényi divergence [BLRL+18, BS23, CSS+23]

Andreea Alexandru aalexandru@dualitytech.com

More protocol-gadgets for passive ThFHE

- Key generation
  - Secret sharing schemes
- Interactive masked decryption
  - => Interactive bootstrapping/scheme switching [CLO+13, SPT+21, MBH23, GGP+23]
  - Useful to make evaluation more efficient and to translate to other cryptographic schemes

What about active security?

Slower, but on its way?

Background: Active security notions for (Th)FHE

- IND-CCA1: a priori decryption oracle access
  - Practical FHE schemes require encryptions (of functions) of the secret key -> incompatible with the decryption oracle; other constructions in [CRRV17]
- IND-CCA2: decryption oracle access
  - No HE can satisfy this
- Targeted malleability [PR08, BSW11]: allow decryptions of some function families
- IND-CVA [LMNV10, CGG16, CCCM22, CCCM23]: oracle access for plaintext validity
- Malicious security [VKH23]: correctness, completeness, soundness
- IND-TCPA + threshold verifiability + decryption simulatability [BGG+18, ABGS22]
- Real/ideal functionality with active security [DDE+23, Sma23]

Standardizing active ThFHE

- Threshold additively/somewhat HE, FHE with active security [DKL+13, KPR18, RST+22, ABGS22, CMS+23, DDE+23]

Gadgets & building blocks

- Active security definition for ThFHE
- Honest majority to help with verifiable computation
- Non interactive zero-knowledge proofs (PQ) / Homomorphic signatures

Andreea Alexandru aalexandru@dualitytech.com

References

[ABGS22] Aranha, D.F., Baum, C., Gjøsteen, K. and Silde, T., 2022. Verifiable mix-nets and distributed decryption for voting from lattice-based assumptions. *Cryptology ePrint Archive*.

[AGHV22] Akavia, A., Gentry, C., Halevi, S. and Vald, M., 2022. Achievable CCA2 relaxation for homomorphic encryption. In *Theory of Cryptography Conference* (pp. 70-99). Cham: Springer Nature Switzerland.

[AJL+12] Asharov, G., Jain, A., López-Alt, A., Tromer, E., Vaikuntanathan, V. and Wichs, D., 2012. Multiparty computation with low communication, computation and interaction via threshold FHE. In *Advances in Cryptology–EUROCRYPT 2012: 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques. Proceedings 31* (pp. 483-501). Springer Berlin Heidelberg.

[ASY22] Agrawal, S., Stehle, D. and Yadav, A., 2022. *Round-optimal lattice-based threshold signatures*. revisited. Cryptology ePrint Archive, Paper 2022/634.

[AV21] Akavia, A. and Vald, M., 2021. On the privacy of protocols based on CPA-secure homomorphic encryption. *Cryptology ePrint Archive*.

[BD10] Bendlin, R. and Damgård, I., 2010. Threshold decryption and zero-knowledge proofs for lattice-based cryptosystems. In *Theory of Cryptography Conference* (pp. 201-218). Springer Berlin Heidelberg.

[BdPMW16] Bourse, F., Del Pino, R., Minelli, M. and Wee, H., 2016. FHE circuit privacy almost for free. In *Annual International Cryptology Conference* (pp. 62-89). Springer Berlin Heidelberg.

[BGGK17] Boneh, D., Gennaro, R., Goldfeder, S. and Kim, S., 2017. A lattice-based universal thresholdizer for cryptographic systems. *Cryptology ePrint Archive*.

[BGG+18] Boneh, D., Gennaro, R., Goldfeder, S., Jain, A., Kim, S., Rasmussen, P.M. and Sahai, A., 2018. Threshold cryptosystems from threshold fully homomorphic encryption. In *Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Proceedings, Part I 38* (pp. 565-596). Springer International Publishing.

[BGV+14] Brakerski, Z., Gentry, C. and Vaikuntanathan, V., 2014. (Leveled) fully homomorphic encryption without bootstrapping. *ACM Transactions on Computation Theory (TOCT)*, *6*(3), pp.1-36.

[BLRL+18] Bai, S., Lepoint, T., Roux-Langlois, A., Sakzad, A., Stehlé, D. and Steinfeld, R., 2018. Improved security proofs in lattice-based cryptography: using the Rényi divergence rather than the statistical distance. *Journal of Cryptology*, *31*, pp.610-640.

[Bra12] Brakerski, Z., 2012. Fully homomorphic encryption without modulus switching from classical GapSVP. In *Annual Cryptology Conference* (pp. 868-886). Springer Berlin Heidelberg.

References

[BS23] Boudgoust, K. and Scholl, P., 2023. Simple threshold (fully homomorphic) encryption from LWE with polynomial modulus. *Cryptology ePrint Archive*.

[BSW11] Boneh, D., Segev, G. and Waters, B., 2012. Targeted malleability: homomorphic encryption for restricted computations. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference* (pp. 350-366).

[BTT22] Boschini, C., Takahashi, A. and Tibouchi, M., 2022. MuSig-L: lattice-based multi-signature with single-round online phase. In *Annual International Cryptology Conference* (pp. 276-305). Cham: Springer Nature Switzerland.

[CCCM22] Chaturvedi, B., Chakraborty, A., Chatterjee, A. and Mukhopadhyay, D., 2022. A Practical Full Key Recovery Attack on TFHE and FHEW by Inducing Decryption Errors. *Cryptology ePrint Archive*.

[CCCM23] Chaturvedi, B., Chakraborty, A., Chatterjee, A. and Mukhopadhyay, D., 2023. vr^2 FHE-Securing FHE from Reaction-based Key Recovery Attacks. *Cryptology ePrint Archive*.

[CCK23] Cheon, J.H., Cho, W. and Kim, J., 2023. Improved Universal Thresholdizer from Threshold Fully Homomorphic Encryption. *Cryptology ePrint Archive*.

[CCMS21] Cong, K., Cozzo, D., Maram, V. and Smart, N.P., 2021. Gladius: LWR based efficient hybrid public key encryption with distributed decryption. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 125-155). Cham: Springer International Publishing.

[CCS19] Chen, H., Chillotti, I. and Song, Y., 2019. Multi-key homomorphic encryption from TFHE. In *Advances in Cryptology–ASIACRYPT 2019: 25th International Conference on the Theory and Application of Cryptology and Information Security, Proceedings, Part II 25* (pp. 446-472). Springer International Publishing.

[CGG16] Chillotti, I., Gama, N. and Goubin, L., 2016. Attacking FHE-based applications by software fault injections. *Cryptology ePrint Archive*.

[CGGI16] Chillotti, I., Gama, N., Georgieva, M. and Izabachene, M., 2016. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. In *Advances in Cryptology–ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security, Proceedings, Part I 22* (pp. 3-33). Springer Berlin Heidelberg.

[CHI+21] Chen, M., Hazay, C., Ishai, Y., Kashnikov, Y., Micciancio, D., Riviere, T., Shelat, A., Venkitasubramaniam, M. and Wang, R., 2021. Diogenes: Lightweight scalable RSA modulus generation with a dishonest majority. In *2021 IEEE Symposium on Security and Privacy (SP)* (pp. 590-607). IEEE.

[CKKS17] Cheon, J.H., Kim, A., Kim, M. and Song, Y., 2017. Homomorphic encryption for arithmetic of approximate numbers. In *Advances in Cryptology–ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Proceedings, Part I 23* (pp. 409-437). Springer International Publishing.

References

[CLO+13] Choudhury, A., Loftus, J., Orsini, E., Patra, A. and Smart, N.P., 2013, December. Between a Rock and a Hard Place: Interpolating between MPC and FHE. In *International conference on the theory and application of cryptology and information security* (pp. 221-240). Springer Berlin Heidelberg.

[CMS+23] Chatel, S., Mouchet, C., Sahin, A.U., Pyrgelis, A., Troncoso, C. and Hubaux, J.P., 2023. PELTA--Shielding Multiparty-FHE against Malicious Adversaries. *Cryptology ePrint Archive*.

[CRRV17] Canetti, R., Raghuraman, S., Richelson, S. and Vaikuntanathan, V., 2017. Chosen-ciphertext secure fully homomorphic encryption. In *IACR International Workshop on Public Key Cryptography* (pp. 213-240). Springer Berlin Heidelberg.

[CS19] Cozzo, D. and Smart, N.P., 2019. Sharing the LUOV: threshold post-quantum signatures. In *IMA International Conference on Cryptography and Coding* (pp. 128-153). Cham: Springer International Publishing.

[CSS+22] Chowdhury, S., Sinha, S., Singh, A., Mishra, S., Chaudhary, C., Patranabis, S., Mukherjee, P., Chatterjee, A. and Mukhopadhyay, D., 2022. Efficient threshold FHE with application to real-time systems. *Cryptology ePrint Archive*.

[DDE+23] Dahl, M., Demmler, D., Elkazdadi, S., Meyre, A., Orfila, J.B., Rotaru, D., Smart, N.P., Tap, S. and Walter, M., 2023. Noah's Ark: Efficient Threshold-FHE Using Noise Flooding. *Cryptology ePrint Archive*.

[DKL+13] Damgård, I., Keller, M., Larraia, E., Pastro, V., Scholl, P. and Smart, N.P., 2013. Practical covertly secure MPC for dishonest majority–or: breaking the SPDZ limits. In *Computer Security–ESORICS 2013: 18th European Symposium on Research in Computer Security. Proceedings 18* (pp. 1-18). Springer Berlin Heidelberg.

[DLN+21] Devevey, J., Libert, B., Nguyen, K., Peters, T. and Yung, M., 2021. Non-interactive CCA2-secure threshold cryptosystems: achieving adaptive security in the standard model without pairings. In *IACR International Conference on Public-Key Cryptography* (pp. 659-690). Cham: Springer International Publishing.

[DM15] Ducas, L. and Micciancio, D., 2015. FHEW: bootstrapping homomorphic encryption in less than a second. In *Annual international conference on the theory and applications of cryptographic techniques* (pp. 617-640). Springer Berlin Heidelberg.

[DOTT22] Damgård, I., Orlandi, C., Takahashi, A. and Tibouchi, M., 2022. Two-round n-out-of-n and multi-signatures and trapdoor commitment from lattices. *Journal of Cryptology*, *35*(2), p.14.

[DPSZ12] Damgård, I., Pastro, V., Smart, N. and Zakarias, S., 2012. Multiparty computation from somewhat homomorphic encryption. In *Annual Cryptology Conference* (pp. 643-662). Springer Berlin Heidelberg.

References

[DS16] Ducas, L. and Stehlé, D., 2016. Sanitization of FHE ciphertexts. In *Advances in Cryptology–EUROCRYPT 2016: 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Proceedings, Part I 35* (pp. 294-310). Springer Berlin Heidelberg.

[EHO+13] Emura, K., Hanaoka, G., Ohtake, G., Matsuda, T. and Yamada, S., 2013. Chosen ciphertext secure keyed-homomorphic public-key encryption. In *Public-Key Cryptography–PKC 2013: 16th International Conference on Practice and Theory in Public-Key Cryptography. Proceedings 16* (pp. 32-50). Springer Berlin Heidelberg.

[FPS01] Fouque, P.A., Poupard, G. and Stern, J., 2001. Sharing decryption in the context of voting or lotteries. In *Financial Cryptography: 4th International Conference, Proceedings 4* (pp. 90-104). Springer Berlin Heidelberg.

[FV12] Fan, J. and Vercauteren, F., 2012. Somewhat practical fully homomorphic encryption. *Cryptology ePrint Archive*.

[Gen09] Gentry, C., 2009. *A fully homomorphic encryption scheme*. Ph.D. Thesis, Stanford University.

[GGP+23] Geva, R., Gusev, A., Polyakov, Y., Liram, L., Rosolio, O., Alexandru, A., Genise, N., Blatt, M., Duchin, Z., Waissengrin, B. and Mirelman, D., 2023. Collaborative privacy-preserving analysis of oncological data using multiparty homomorphic encryption. *Proceedings of the National Academy of Sciences*, *120*(33), p.e2304415120.

[GHS13] Gentry, C., Sahai, A. and Waters, B., 2013. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In *Advances in Cryptology–CRYPTO 2013: 33rd Annual Cryptology Conference. Proceedings, Part I* (pp. 75-92). Springer Berlin Heidelberg.

[GKS23] Gur, K.D., Katz, J. and Silde, T., 2023. Two-Round Threshold Lattice Signatures from Threshold Homomorphic Encryption. *Cryptology ePrint Archive*.

[KLO+19] Kraitsberg, M., Lindell, Y., Osheter, V., Smart, N.P. and Talibi Alaoui, Y., 2019. Adding distributed decryption and key generation to a ring-LWE based CCA encryption scheme. In *Information Security and Privacy: 24th Australasian Conference, ACISP 2019, Proceedings 24* (pp. 192-210). Springer International Publishing.

[KPR13] Keller, M., Pastro, V. and Rotaru, D., 2018. Overdrive: making SPDZ great again. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 158-189). Cham: Springer International Publishing.

[KS23] Kluczniak, K. and Santato, G., 2023. On Circuit Private, Multikey and Threshold Approximate Homomorphic Encryption. *Cryptology ePrint Archive*.

[LATV12] López-Alt, A., Tromer, E. and Vaikuntanathan, V., 2012. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing* (pp. 1219-1234).

References

[LM21] Li, B. and Micciancio, D., 2021. On the security of homomorphic encryption on approximate numbers. In *Advances in Cryptology–EUROCRYPT 2021: 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Proceedings, Part I 40* (pp. 648-677). Springer International Publishing.

[LMSS22] Li, B., Micciancio, D., Schultz, M. and Sorrell, J., 2022. Securing approximate homomorphic encryption using differential privacy. In *Annual International Cryptology Conference* (pp. 560-589). Cham: Springer Nature Switzerland.

[LMSV10] Loftus, J., May, A., Smart, N.P. and Vercauteren, F., 2012. On CCA-secure somewhat homomorphic encryption. In *Selected Areas in Cryptography: 18th International Workshop, SAC 2011, Toronto, ON, Canada, 2011, Revised Selected Papers 18* (pp. 55-72). Springer Berlin Heidelberg.

[MBH23] Mouchet, C., Bertrand, E. and Hubaux, J.P., 2023. An efficient threshold access-structure for rlwe-based multiparty homomorphic encryption. *Journal of Cryptology*, *36*(2), p.10.

[MW16] Mukherjee, P. and Wichs, D., 2016. Two round multiparty computation via multi-key FHE. In *Advances in Cryptology–EUROCRYPT 2016: 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Proceedings, Part II 35* (pp. 735-763). Springer Berlin Heidelberg.

[MW18] Micciancio, D. and Walter, M., 2018. On the bit security of cryptographic primitives. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 3-28). Cham: Springer International Publishing.

[OPCPC14] Ostrovsky, R., Paskin-Cherniavsky, A. and Paskin-Cherniavsky, B., 2014. Maliciously circuit-private FHE. In *Annual Cryptology Conference* (pp. 536-553). Springer Berlin Heidelberg.

[PM08] Prabhakaran, M. and Rosulek, M., 2008. Homomorphic encryption with CCA security. In *International Colloquium on Automata, Languages, and Programming* (pp. 667-678). Springer Berlin Heidelberg.

[RST+22] Rotaru, D., Smart, N.P., Tanguy, T., Vercauteren, F. and Wood, T., 2022. Actively secure setup for SPDZ. *Journal of Cryptology*, *35*(1), p.5.

[Sma23] Smart, N.P., 2023. Practical and Efficient FHE-based MPC. *Cryptology ePrint Archive*.

[SET22] Sato, S., Emura, K. and Takayasu, A., 2022. Keyed-fully homomorphic encryption without indistinguishability obfuscation. In *International Conference on Applied Cryptography and Network Security* (pp. 3-23). Cham: Springer International Publishing.

[SPT+21] Sav, S., Pyrgelis, A., Troncoso-Pastoriza, J.R., Froelicher, D., Bossuat, J.P., Sousa, J.S. and Hubaux, J.P., 2021. POSEIDON: Privacy-Preserving Federated Neural Network Learning. In *28Th Annual Network And Distributed System Security Symposium (Ndss 2021), Internet Soc*.

[VKH23] Viand, A., Knabenhans, C. and Hithnawi, A., 2023. Verifiable fully homomorphic encryption. *arXiv preprint arXiv:2301.07041*.

Duality

Thank you!

Andreea Alexandru

aalexandru@dualitytech.com