Homomorphic Encryption (Design and optimization)

- Cheon, Jung Hee, et al. "Homomorphic Multiple Precision Multiplication for CKKS and Reduced Modulus Consumption." *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*. 2023. [CCS]
- Kluczniak, Kamil. "NTRU-v-um: secure fully homomorphic encryption from NTRU with small modulus." *Proceedings of the 2022 ACM SIGSAC conference on computer and communications security*. 2022. [CCS]
- Mouchet, Christian, et al. "Multiparty homomorphic encryption from ring-learning-with-errors." *Proceedings on Privacy Enhancing Technologies* 2021.4 (2021): 291-311. [PET]
- Viand, Alexander, et al. "{HECO}: Fully Homomorphic Encryption Compiler." *32nd USENIX Security Symposium (USENIX Security 23)*. 2023 [SEC]
- Lee, Yongwoo, et al. "{ELASM}:{Error-Latency-Aware} Scale Management for Fully Homomorphic Encryption." *32nd USENIX Security Symposium (USENIX Security 23)*. 2023. [SEC]
- Viand, Alexander, Patrick Jattke, and Anwar Hithnawi. "SoK: Fully homomorphic encryption compilers." *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2021. [S&P]

Secure Multi-party Computing

- Escudero, Daniel, et al. "Turbopack: honest majority MPC with constant online communication." *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*. 2022. [CCS]
- Boyle, Elette, et al. "Practical fully secure three-party computation via sublinear distributed zero-knowledge proofs." *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 2019. [CCS]
- Ishaq, Muhammad, Ana L. Milanova, and Vassilis Zikas. "Efficient MPC via program analysis: A framework for efficient optimal mixing." *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 2019. [CCS]
- Wong, Harry WH, Jack PK Ma, and Sherman SM Chow. "Secure Multiparty Computation of Threshold Signatures Made More Efficient." *ISOC Network and Distributed System Security Symposium–NDSS 2024*. 2024. [NDSS]
- Klinger, Andreas, Vincent Ehrmanntraut, and Ulrike Meyer. "Estimating the Runtime and Global Network Traffic of SMPC Protocols." *Proceedings of the Fourteenth ACM Conference on Data and Application Security and Privacy*. 2024. [SPY]

Private Set Intersection/Union

- Jia, Yanxue, et al. "Shuffle-based private set union: Faster and more secure." *31st USENIX Security Symposium (USENIX Security 22)*. 2022. [SEC]
- Zhang, En, et al. "Efficient multi-party private set intersection against malicious adversaries." *Proceedings of the 2019 ACM SIGSAC conference on cloud computing security workshop*. 2019. [CCS]
- Rosulek, Mike, and Ni Trieu. "Compact and malicious private set intersection for small sets." *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. 2021. [CCS]
- Cong, Kelong, et al. "Labeled PSI from homomorphic encryption with reduced computation and communication." *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. 2021. [CCS]
- Le, Phi Hung, Samuel Ranellucci, and S. Dov Gordon. "Two-party private set intersection with an untrusted third party." *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 2019. [CCS]
- Gao, Jiahui, Ni Trieu, and Avishay Yanai. "Multiparty private set intersection cardinality and its applications." *Proceedings on Privacy Enhancing Technologies* (2024). [PET]
- Vos, Jelle, Mauro Conti, and Zekeriya Erkin. "Sok: Collusion-resistant multi-party private set intersections in the semi-honest model." *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2024. [S&P]
- Kerschbaum, Florian, Erik-Oliver Blass, and Rasoul Akhavan Mahdavi. "Faster secure comparisons with offline phase for efficient private set intersection." *arXiv preprint arXiv:2209.13913* (2022). [NDSS]
- Bui, Dung, and Geoffroy Couteau. "Improved private set intersection for sets with small entries." *IACR International Conference on Public-Key Cryptography*. Cham: Springer Nature Switzerland, 2023. [Other]
- Su, Jiuheng, Zhili Chen, and Xiaomin Yang. "Multi-Party Private Set Intersection: A Circuit-Based Protocol with Jaccard Similarity for Secure and Efficient Anomaly Detection in Network Traffic." *Proceedings of the 2024 3rd International Conference on Cryptography, Network Security and Communication Technology*. 2024. [Other]
- Chase, Melissa, and Peihan Miao. "Private set intersection in the internet setting from lightweight oblivious PRF." *Advances in Cryptology–CRYPTO 2020: 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17–21, 2020, Proceedings, Part III 40*. Springer International Publishing, 2020.[Other]

Secure Federate Learning

- Arazzi, Marco, et al. "Turning privacy-preserving mechanisms against federated learning." *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*. 2023. [CCS]
- Mansouri, Mohamad, et al. "Sok: Secure aggregation based on cryptographic schemes for federated learning." *Proceedings on Privacy Enhancing Technologies* (2023). [PET]
- Zhang, Chengliang, et al. "{BatchCrypt}: Efficient homomorphic encryption for {Cross-Silo} federated learning." *2020 USENIX annual technical conference (USENIX ATC 20)*. 2020. [SEC]
- Rathee, Mayank, et al. "Elsa: Secure aggregation for federated learning with malicious actors." *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2023. [S&P]
- Sav, Sinem, et al. "POSEIDON: Privacy-preserving federated neural network learning." *arXiv preprint arXiv:2009.00349* (2020). [NDSS]
- N. Yan *et al.*, "Efficient and Straggler-Resistant Homomorphic Encryption for Heterogeneous Federated Learning," *IEEE INFOCOM 2024 - IEEE Conference on Computer Communications*, Vancouver, BC, Canada, 2024, pp. 791-800, doi: 10.1109/INFOCOM52122.2024.10621440. [INFOCOM]

Application

- Akhavan Mahdavi, Rasoul, et al. "Level up: Private non-interactive decision tree evaluation using levelled homomorphic encryption." *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*. 2023. [CCS]
- Tu, Binbin, et al. "Fast unbalanced private set union from fully homomorphic encryption." *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*. 2023. [CCS]
- Yang, Kang, et al. "Ferret: Fast extension for correlated OT with small communication." *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*. 2020. [CCS]
- Choi, Seung Geol, et al. "Compressed oblivious encoding for homomorphically encrypted search." *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. 2021. [CCS]
- Ren, Liangqin, et al. "PrivDNN: A Secure Multi-Party Computation Framework for Deep Learning using Partial DNN Encryption." *Proceedings on Privacy Enhancing Technologies* 3 (2024): 1-18. [PET]
- Gao, Jiahui, Son Nguyen, and Ni Trieu. "Toward A Practical Multi-party Private Set Union." *Cryptology ePrint Archive* (2023). [PET]

- Hamada, Koki, et al. "Efficient decision tree training with new data structure for secure multi-party computation." *arXiv preprint arXiv:2112.12906* (2021). [PET]
- Iliashenko, Ilia, et al. "Homomorphically counting elements with the same property." *Proceedings on Privacy Enhancing Technologies* (2022). [PET]
- Gálvez, Rafa, Veelasha Moonsamy, and Claudia Diaz. "Less is More: A privacy-respecting Android malware classifier using federated learning." *arXiv preprint arXiv:2007.08319* (2020). [PET]
- Lu, Wen-jie, et al. "Squirrel: A Scalable Secure {Two-Party} Computation Framework for Training Gradient Boosting Decision Tree." *32nd USENIX Security Symposium (USENIX Security 23)*. 2023. [SEC]
- Steffen, Samuel, et al. "Zeestar: Private smart contracts by homomorphic encryption and zero-knowledge proofs." *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2022. [S&P]
- Folkerts, Lars, Charles Gouert, and Nektarios Georgios Tsoutsos. "REDsec: Running encrypted discretized neural networks in seconds." *Cryptology ePrint Archive* (2021). [NDSS]
- Hesamifard, Ehsan, Hassan Takabi, and Mehdi Ghasemi. "Deep neural networks classification over encrypted data." *Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy*. 2019. [SPY]
- Wibawa, Febrianti, et al. "Homomorphic encryption and federated learning based privacy-preserving cnn training: Covid-19 detection use-case." *Proceedings of the 2022 European Interdisciplinary Cybersecurity Conference*. 2022.[Other]
- Lee, Seewoo, et al. "HETAL: efficient privacy-preserving transfer learning with homomorphic encryption." *International Conference on Machine Learning*. PMLR, 2023. [ICML]
- Lou, Qian, and Lei Jiang. "Hemet: A homomorphic-encryption-friendly privacy-preserving mobile neural network architecture." *International conference on machine learning*. PMLR, 2021.[ICML]
- Choi, Hyunmin, Simon S. Woo, and Hyoungshick Kim. "Blind-Touch: Homomorphic Encryption-Based Distributed Neural Network Inference for Privacy-Preserving Fingerprint Authentication." *Proceedings of the AAAI Conference on Artificial Intelligence*. Vol. 38. No. 20. 2024. [AAAI]

Conference Legend:

CCS: ACM CCS

S&P: IEEE Security and Privacy (Oakland)

SEC: Usenix Security

NDSS: Usenix Network and Distributed System Security

ICML: International Conference in Machine Learning

INFOCOM: IEEE International Conference on Computer Communication

SPY: ACM conference on Data and Application security and Privacy

PET: Privacy Enhancing Technology

AAAI: The Association for the Advancement of Artificial Intelligence