Hybrid PETs: A Project Summary for the 2026 CISE CAREER Workshop

PI: Jonathan Takeshita, Assistant Professor, Old Dominion University (jtakeshi@odu.edu)

Privacy-preserving computation techniques allow data to be operated upon while it is encrypted or obscured, separating knowledge and computation. These techniques have advanced greatly in the past decade, but still face challenges. General cryptographic methods such as Secure Multiparty Computation (MPC) and Fully Homomorphic Encryption have the disadvantages high computational complexity and communication overhead [1]. Purpose-built protocols can be much more efficient, but often lack features beyond high performance [2, 3]. Trusted Execution Environments rely on hardware capabilities to provide security, but struggle with a conflict between scalability and strong integrity [1, 4]. Prior work has shown that in some specific scenarios, the differing capabilities of these technologies can be exploited, allowing the strengths of one to cover the weaknesses of the other. Concrete examples of this in my prior work include:

- Combining SGX and HE for privacy in both the linear high-scale and nonlinear portions of machine learning computations [5].
- Using trusted hardware to reduce MPC communication rounds [6].
- Enabling fault tolerance for post-quantum Private Stream Aggregation (PSA) with trusted hardware [2].

In my future work, I aim to seek out scenarios that can benefit from novel integrations of Privacy-Enhancing Technologies (PETs), and to derive and apply bespoke combinations of PETs to improve performance, scalability, utility, and robustness. I am a few years from applying for a CAREER award, and I am seeking feedback on refining ideas in this line of inquiry. In particular, there are three main research thrusts I am interested in pursuing:

1. PSA for FL: State-of-the-art quantum-secure PSA protocols have the potential to greatly improve the speed of secure federated learning (FL). Mathematical compatibility between post-quantum PSA and FHE allows for the possibility of private post-aggregation computation, by converting a PSA penultimate result (i.e., aggregated but not decrypted) to a FHE ciphertext. However, there are technical obstacles: PSA noise must be removed from the FHE ciphertext or otherwise mitigated.
2. High-trust TEEs for integrity-guaranteed FHE: Ongoing work in my group is showing how to use limited-scale TEEs with stronger integrity such as Intel SGX for large-scale AI (e.g., LLMs) by exploiting untrusted memory for well-structured data (e.g., matrices) [1]. These methods can also be applied to polynomial arithmetic, which shows a clear path to using SGX-like TEEs for to ensure integrity for outsourced FHE computation.
3. Probabilistic integrity: When using PETs, malleable ciphertexts such as those in FHE mean that a recipient of a ciphertext must trust that the sender has honestly performed homomorphic calculations. Using a "canary-in-the-coal-mine" strategy [5], we can (to a high probability) detect malicious mutation with minimal overhead or implementation.

References

[1] J. Takeshita, "Towards improving and integrating homomorphic cryptography and trusted hardware," Ph.D. dissertation, University of Notre Dame, 2025.
[2] J. Takeshita, Z. Carmichael, R. Karl, and T. Jung, "TERSE: Tiny Encryptions and Really Speedy Execution for Post-Quantum Private Stream Aggregation," in *International Conference on Security and Privacy in Communication Systems*. Cham: Springer Nature Switzerland, Oct. 2022, pp. 331–352.
[3] J. Takeshita, R. Karl, T. Gong, and T. Jung, "SLAP: Simpler, Improved Private Stream Aggregation from Ring Learning with Errors," *Journal of Cryptology*, vol. 36, no. 2, 2023.
[4] P.-L. Aublin, M. Mahhouk, and R. Kapitza, "Towards TEEs with Large Secure Memory and Integrity Protection Against HW Attacks," in *5th Workshop on System Software for Trusted Execution (SysTEX 2022)*, 2022.
[5] J. Takeshita, C. McKechney, J. Pajak, A. Papadimitriou, R. Karl, and T. Jung, "GPS: Integration of Graphene, Palisade, and SGX for large-scale aggregations of distributed data," *Cryptology ePrint Archive*, 2021.
[6] R. Karl, H. Burchfield, J. Takeshita, and T. Jung, "Developing non-interactive mpc with trusted hardware for enhanced security," *International Journal of Information Security*, vol. 21, no. 4, pp. 777–797, 2022.