A Unified Framework for Benchmarking Symmetric Cryptography in MPC



Problem Statement. The distributed evaluation of symmetric ciphers using Secure Multi-Party Computation (MPC) is one of the most common MPC use-cases and benchmarks as well as a vantage point for furthering MPC research for other use-cases. This cipher evaluation is critical in two distinct domains: (1) Client-server MPC, where clients use symmetric encryption to upload data with minimal bandwidth, deferring decryption to the MPC committee; and (2) MPC-in-the-Head (MPCitH) post-quantum signatures, which require efficient MPC evaluation of block ciphers or hash functions to generate zero-knowledge proofs. [1] While the design of special-purpose (e.g. lightweight, arithmetic-oriented) ciphers is accelerating, MPC lacks a unified ecosystem for evaluating them. Recent advances rely on highly specialized, disjointed implementations, such as using RMFEs to pack Boolean ciphers like Ascon [2]. This fragmentation prevents the direct integration and fair benchmarking of diverse ciphers under identical MPC network conditions. As NIST standardizes Multi-Party Threshold Cryptography (MPTC, [1]), an extensible, comparative framework is essential.

Thesis goal. The goal of this thesis is to design and implement a generalized framework in MP-SPDZ [3] for the distributed evaluation of symmetric ciphers. The student will first study MPC communication complexity, secret-sharing schemes, and recent optimizations (like RMFE embeddings [2]) to design unified algebraic/boolean interfaces. Next, they will build a modular architecture supporting different ciphers through re-usable compontents for encryption and decryption. Finally, the framework will be used to benchmark a traditional lightweight cipher (e.g., Ascon) against another cipher (e.g. Skinny, AES), evaluating communication complexity and execution time.

Practicalities

Promotor:	Bart Preneel		
	Another promotor		
Daily supervisor:	Peter Schwarz	peter.schwarz@esat.kuleuven.be	office B01.28
	Aysajan Abidin	aysajan.abidin@esat.kuleuven.be	office 01.13
Nature of the work:	30% literature, 20% theoretical work, 50% software		
Number of students:	1		

References

[1] Luís T. A. N. Brandão, Rene Peralta, "NIST First Call for Multi-Party Threshold Schemes" *NIST IR*, 2026

[2] P. Schwarz et al., "Evaluating Ascon in Secure Multi-Party Computation using RMFEs," *ePrint*, 2025.

[3] M. Keller, "MP-SPDZ: A Versatile Framework for Multi-Party Computation," *CCS*, 2020.

 © 2026 – 2027 COSIC