Verifiable and Privacy-Preserving Computation via FHE, MPC, and ZKP

Context

The evolution of cryptography can be broadly characterized through three interconnected stages. The first stage, Secure Communication, focused on ensuring that transmitted messages were accessible only to intended recipients, leading to the development of encryption protocols for private and authenticated exchange. The second stage, Secure Storage, emerged with the rise of cloud computing, emphasizing the protection of data in public and hybrid infrastructures through encryption, secret sharing, and fine-grained access control. The third and most transformative stage, Secure Computation, enables computation on data without revealing its content. Techniques such as Fully Homomorphic Encryption (FHE), Secure Multiparty Computation (MPC), and Zero-Knowledge Proofs (ZKPs) have revolutionized privacy-preserving computation, shifting the paradigm from protecting data in transit or at rest to enabling its secure utility in use. Fully Homomorphic Encryption (FHE) [Gen09] is a groundbreaking cryptographic primitive that allows arbitrary computation directly on encrypted data without decryption. Originating from Gentry's 2009 breakthrough, FHE provides the foundation for privacy-preserving computation in untrusted environments such as cloud or outsourced platforms. Despite its transformative potential, FHE still faces significant challenges, including ciphertext noise growth, bootstrapping overhead, and efficient key management issues that are particularly relevant under post-quantum assumptions. Secure Multiparty Computation (MPC) extends these guarantees to collaborative settings, allowing multiple parties to jointly compute a function over their private inputs without revealing them. Initially introduced by Yao [Yao82, Yao86] for the two-party case under semi-honest adversaries, MPC was later generalized by Goldreich et al. [GMW19] to support multiple parties and fully malicious adversaries. MPC has since become a cornerstone of distributed privacy-preserving computation, underpinning protocols for secure aggregation, federated learning, and threshold cryptography. Zero-Knowledge Proofs (ZKPs) [GMR19] allow a prover to convince a verifier of the correctness of a statement without revealing any additional information beyond its validity. ZKPs interact with both FHE and MPC in two crucial ways. First, they enable verifiable computation over encrypted data, allowing a verifier to ensure that a homomorphic evaluation was correctly performed on ciphertexts, thereby guaranteeing integrity without revealing plaintexts. Second, ZKPs intersect with MPC through paradigms such as MPC-in-the-Head (MPCitH) and VOLE-in-the-Head (VOLEitH), which transform MPC executions into efficient non-interactive zero-knowledge proofs and form the foundation of practical post-quantum digital signature schemes.

Objectives

The goal of this research is to advance the state of verifiable and privacy-preserving computation by integrating the strengths of FHE, MPC and ZKP. Specifically, the project aims to design cryptographic frameworks that enable computation on encrypted data while ensuring correctness, privacy, and post-quantum security.

The proposed work will focus on the following specific objectives:

Achieving MPC using FHE

Most Secure Multiparty Computation (MPC) protocols rely on private communication channels among participating parties and employ secret-sharing techniques [Sha79] to securely compute functions over distributed inputs. However, these protocols often assume that all parties remain online throughout the computation and possess sufficient computational resources to perform cryptographic operations. FHE provides an attractive alternative by enabling computation directly on encrypted data, thus reducing the need for synchronous interaction and continuous participation among parties. When multiple data owners are involved in a computation, integrating FHE with distributed trust

becomes essential to avoid reliance on a single trusted third party (TTP) for key generation or decryption. This challenge is addressed by two major paradigms *Threshold FHE* and *Multi-Key FHE* which distribute trust and computation among multiple entities. In a **Threshold FHE (Th-FHE)** scheme, the key generation process produces a single public key, while each party holds a share of the corresponding secret key. Key generation can be performed collaboratively through an MPC protocol or with partial assistance from a TTP. The scheme typically adopts a t-out-of-n access structure, where any subset of t parties (with $t \leq n$) can cooperatively decrypt ciphertexts, ensuring fault tolerance and resistance against collusion among fewer than t participants. In contrast, **Multi-Key FHE (MK-FHE)** adopts a decentralized configuration in which each party independently generates its own key pair and encrypts data using its public key. During evaluation, the server expands ciphertexts to accommodate multiple encryption keys, enabling computations across inputs encrypted under different keys. While this model eliminates the need for shared secret material, it introduces significant space and time complexity due to ciphertext expansion, and its performance degrades as the number of participants increases. Recent research has focused on improving scalability, reducing communication cost, and enabling dynamic participation. Chen et al. [CCS19] and Kwak et al. [KMS24] explored multi-key extensions of the TFHE scheme using blind rotation to optimize bootstrapping. Morten et al. [DDEK$^+$23] proposed the "switch-and-squash" bootstrapping method to reduce server interaction while maintaining decryption share size. Other works, including Boudgoust and Scholl [BS23] and Passelègue and Stehlé [PS25], targeted communication and decryption bottlenecks by designing compact ciphertext and key-share representations. Despite these advancements, most current schemes either assume full participation ($t = N$) or depend on trusted setup procedures, limiting their adaptability in dynamic, heterogeneous environments. Smart [Sma23] proposed a reactive MPC protocol resilient to active adversaries but without support for dynamic group changes.

Our goal is to design new constructions and improvements for existing schemes that enhance scalability, enable dynamic participation, and reduce trust and communication overhead in FHE-based MPC frameworks.

Achieving Verifiability in FHE through ZKP and SNARKs

A conventional approach to achieving verifiability in FHE is to combine an FHE scheme with a Verifiable Computation (VC) system. However, this integration is highly non-trivial. FHE schemes natively operate over polynomial rings, whereas VC protocols particularly SNARKs are optimized for arithmetic over finite fields. Bridging this algebraic mismatch introduces substantial overhead in proof size, common reference string (CRS) size, and computational cost for both the prover and verifier. A complementary direction of research investigates *authenticated homomorphic computation*, wherein data is accompanied by cryptographic authentication tags that remain valid under homomorphic operations. Notable constructions include homomorphic Message Authentication Codes (MACs) [GW13, CF13, FGP14] and homomorphic signatures [BF11], both ensuring data integrity through algebraic compatibility between messages and their authenticators. Three primary paradigms have been explored for integrating MACs with FHE: Encrypt-and-MAC (EaM), Encrypt-then-MAC (EtM), and MAC-then-Encrypt (MtE). Each offers distinct trade-offs in terms of security, expressiveness, and efficiency. For example, EaM requires MACs that inherently support homomorphic operations, while EtM applies MACs to ciphertexts, demanding homomorphic-friendly hash functions [FGP14]. MtE, though conceptually simpler, incurs significant verification costs due to the need for recomputation [GW13]. Homomorphic signature schemes extend these principles by enabling *public verification* of computations performed on signed data. In such schemes, a client signs data before outsourcing it to an untrusted server, which can perform computations and update the signatures accordingly. Verification ensures that the correct function was applied without revealing the underlying data. Fully Homomorphic Signatures (FHS) generalize this capability to arbitrary computations, with recent designs leveraging SNARKs for recursive verification and succinct proof generation [GVW15]. Recent SNARK-based FHS constructions employ extractable SNARKs and recursive proof composition to support multi-hop computation with compact signatures. While these approaches are powerful, they typically rely on strong knowledge assumptions, trusted setup phases, or non-falsifiable security assumptions. An alternative approach focuses on verifying computations *directly on ciphertexts* using general-purpose SNARKs [FGP14,KVMGH23]. This methodology offers stronger privacy guarantees but faces critical challenges: (i) FHE ciphertexts lie in polynomial rings $R_q = \mathbb{Z}_q[X]/(X^N + 1)$, which are incompatible with the prime fields underlying standard SNARKs;

and (ii) FHE-specific operations such as modulus switching, key switching, and rescaling are inherently non-arithmetic, making them expensive to emulate in SNARK-friendly formats. To address these challenges, specialized SNARKs supporting R_q-arithmetic [BCFK21, GNSV23] have been proposed. These systems enable native handling of ring-based operations but often suffer from large setup parameters, high prover costs, or restrictions on supported computation types. A promising recent direction is the *HE-IOP paradigm* [ACGSV25], which confines the use of homomorphic encryption to the information-theoretic component of a SNARK, namely the Interactive Oracle Proof (IOP). This approach achieves efficiency and supports full FHE functionality, including bootstrapping. However, it remains incompatible with approximate HE schemes such as CKKS [CKKS17], and typically assumes a private-verifier model to preserve semantic security.

Our goal is to design novel constructions and optimizations that bridge the gap between FHE and verifiable computation frameworks. Specifically, we aim to enhance the efficiency, scalability, and compatibility of FHE–SNARK integrations by developing verifiable FHE frameworks that support dynamic participation, public verification, and broader applicability across both exact and approximate HE schemes.

Constructing ZKPs and Digital Signatures using MPC

To standardize and promote quantum-resistant public-key algorithms, the National Institute of Standards and Technology (NIST) initiated the Post-Quantum Cryptography (PQC) Standardization Process in 2016. After three rounds of evaluation, NIST selected CRYSTALS-Kyber (ML-KEM) as the key encapsulation mechanism, and CRYSTALS-Dilithium (ML-DSA) and SPHINCS+ (SLH-DSA) as digital signature schemes for standardization. However, the underlying security assumptions of these standardized schemes SPHINCS+ relying on hash-function hardness and Dilithium on structured lattice problems highlight the limited cryptographic diversity among PQC primitives. To address this, NIST issued a new call in July 2022 for additional digital signature proposals emphasizing alternative assumptions, compact signatures, and efficient verification. From 50 initial submissions, 40 schemes were accepted into the first round, and by October 2024, 14 candidates had advanced to the second round. Notably, a significant proportion of these candidates leverage techniques from zero-knowledge proofs [GMR19], particularly the *MPC-in-the-Head* (MPCitH) paradigm, which has emerged as a key design framework. The MPCitH paradigm, introduced by Ishai et al. [IKOS07], allows a prover to internally simulate a MPC protocol by generating and committing to the views of multiple virtual parties. The verifier then challenges the prover to open a subset of these views, using the privacy and correctness guarantees of the underlying MPC protocol to ensure zero-knowledge and soundness. This transformation enables the construction of non-interactive zero-knowledge proofs of knowledge via the Fiat–Shamir heuristic [FS86]. Moreover, it allows the design of digital signature schemes that rely solely on symmetric primitives, thereby eliminating the costly public-key operations typically required in traditional designs. Schemes such as Picnic [CDG$^+$17], Banquet [BdSGK$^+$21], BBQ [dSGDMOS19], and Helium [KZ22] demonstrate the practicality and post-quantum resilience of this approach. Despite its conceptual simplicity and versatility, MPCitH-based signature schemes tend to produce large signatures due to the need to reveal multiple MPC views. To overcome this inefficiency, several refinements have been proposed. The *VOLE-in-the-Head* (VOLEitH) paradigm, introduced by Baum et al. [BBdSG$^+$23b], replaces explicit MPC input sharing with structured randomness generated via vector oblivious linear evaluation (VOLE). This design significantly reduces communication overhead while maintaining public verifiability and compatibility with efficient symmetric-key primitives such as AES. The FAEST signature scheme [BBdSG$^+$23a] exemplifies this advancement, achieving compact signatures of approximately 5 KB for 128-bit security and offering faster verification times. In parallel, the *Threshold-Computation-in-the-Head* (TCitH) paradigm [FR23] extends MPCitH to support secret sharing and secure computation over arithmetic circuits. This framework enhances scalability and enables threshold-style verification, opening new avenues for constructing robust, efficient, and post-quantum-secure digital signature schemes grounded in MPC and zero-knowledge principles.

Our goal is to design optimized constructions of digital signatures based on ZKP and MPC frameworks that achieve improved scalability, compactness, and post-quantum security, while minimizing reliance on strong setup assumptions and enhancing compatibility with real-world deployment environments.

Organization

This Post-doc position will take place within the PEPR Quantique PQ-TLS project, which aims to develop efficient post-quantum primitives for practical industrial use.

Candidates for the Post-doc position must hold a PhD and have experience in cryptography. The selected candidate will be integrated in the CAPSULE team at the Inria Center at the University of Rennes and supervised by Dr Yixin Shen, researcher at Inria Rennes.

References

ACGSV25. D. F. Aranha, A. Costache, A. Guimarães, and E. Soria-Vazquez. Heliopolis: Verifiable computation over homomorphically encrypted data from interactive oracle proofs is practical. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 302–334. Springer, 2025.

BBdSG+23a. C. Baum, L. Braun, C. D. de Saint Guilhem, M. Klooß, C. Majenz, S. Mukherjee, E. Orsini, S. Ramacher, C. Rechberger, L. Roy, et al. Faest: algorithm specifications. Technical report, Technical report, National Institute of Standards and Technology, 2023.

BBdSG+23b. C. Baum, L. Braun, C. D. de Saint Guilhem, M. Klooss, E. Orsini, L. Roy, P. Scholl, et al. Publicly verifiable zero-knowledge and post-quantum signatures from vole-in-the-head. In *Advances in cryptology–CRYPTO 2023: 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings. Part V*. Springer, 2023.

BCFK21. A. Bois, I. Cascudo, D. Fiore, and D. Kim. Flexible and efficient verifiable computation on encrypted data. In *IACR International Conference on Public-Key Cryptography*, pages 528–558. Springer, 2021.

BdSGK+21. C. Baum, C. D. de Saint Guilhem, D. Kales, E. Orsini, P. Scholl, and G. Zaverucha. Banquet: short and fast signatures from aes. In *IACR International Conference on Public-Key Cryptography*, pages 266–297. Springer, 2021.

BF11. D. Boneh and D. M. Freeman. Homomorphic signatures for polynomial functions. In *Advances in Cryptology–EUROCRYPT 2011: 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings 30*, pages 149–168. Springer, 2011.

BS23. K. Boudgoust and P. Scholl. Simple threshold (fully homomorphic) encryption from lwe with polynomial modulus. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 371–404. Springer, 2023.

CCS19. H. Chen, I. Chillotti, and Y. Song. 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*, pages 446–472. Springer, 2019.

CDG+17. M. Chase, D. Derler, S. Goldfeder, C. Orlandi, S. Ramacher, C. Rechberger, D. Slamanig, and G. Zaverucha. Post-quantum zero-knowledge and signatures from symmetric-key primitives. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1825–1842, 2017.

CF13. D. Catalano and D. Fiore. Practical homomorphic macs for arithmetic circuits. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 336–352. Springer, 2013.

CKKS17. J. H. Cheon, A. Kim, M. Kim, and Y. Song. 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*, pages 409–437. Springer, 2017.

DDEK+23. M. Dahl, D. Demmler, S. El Kazdadi, A. Meyre, J.-B. Orfila, D. Rotaru, N. P. Smart, S. Tap, and M. Walter. Noah's ark: Efficient threshold-fhe using noise flooding. In *Proceedings of the 11th Workshop on Encrypted Computing & Applied Homomorphic Cryptography*, pages 35–46, 2023.

dSGDMOS19. C. D. de Saint Guilhem, L. De Meyer, E. Orsini, and N. P. Smart. Bbq: using aes in picnic signatures. In *International Conference on Selected Areas in Cryptography*, pages 669–692. Springer, 2019.

FGP14. D. Fiore, R. Gennaro, and V. Pastro. Efficiently verifiable computation on encrypted data. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*, pages 844–855, 2014.

FR23. T. Feneuil and M. Rivain. Threshold computation in the head: Improved framework for post-quantum signatures and zero-knowledge arguments. *Cryptology ePrint Archive*, 2023.

FS86. A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Conference on the Theory and Application of Cryptographic Techniques*, pages 186–194. Springer, 1986.

Gen09. C. Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 169–178, 2009.

GMR19. S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof-systems. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, pages 203–225. 2019.

GMW19. O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game, or a completeness theorem for protocols with honest majority. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, pages 307–328. 2019.

GNSV23. C. Ganesh, A. Nitulescu, and E. Soria-Vazquez. Rinocchio: Snarks for ring arithmetic. *Journal of Cryptology*, 36(4):41, 2023.

GVW15. S. Gorbunov, V. Vaikuntanathan, and D. Wichs. Leveled fully homomorphic signatures from standard lattices. In *Proceedings of the forty-seventh annual ACM symposium on Theory of computing*, pages 469–477, 2015.

GW13. R. Gennaro and D. Wichs. Fully homomorphic message authenticators. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 301–320. Springer, 2013.

IKOS07. Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai. Zero-knowledge from secure multiparty computation. In *Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing*, pages 21–30, 2007.

KMS24. H. Kwak, S. Min, and Y. Song. Towards practical multi-key tfhe: parallelizable, key-compatible, quasi-linear complexity. In *IACR International Conference on Public-Key Cryptography*, pages 354–385. Springer, 2024.

KVMGH23. C. Knabenhans, A. Viand, A. Merino-Gallardo, and A. Hithnawi. vfhe: Verifiable fully homomorphic encryption. In *Proceedings of the 12th Workshop on Encrypted Computing & Applied Homomorphic Cryptography*, pages 11–22, 2023.

KZ22. D. Kales and G. Zaverucha. Efficient lifting for shorter zero-knowledge proofs and post-quantum signatures. *Cryptology ePrint Archive*, 2022.

PS25. A. Passelègue and D. Stehlé. Low communication threshold fully homomorphic encryption. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 297–329. Springer, 2025.

Sha79. A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

Sma23. N. P. Smart. Practical and efficient fhe-based mpc. In *IMA International Conference on Cryptography and Coding*, pages 263–283. Springer, 2023.

Yao82. A. C. Yao. Protocols for secure computations. In *23rd annual symposium on foundations of computer science (sfcs 1982)*, pages 160–164. IEEE, 1982.

Yao86. A. C.-C. Yao. How to generate and exchange secrets. In *27th annual symposium on foundations of computer science (Sfcs 1986)*, pages 162–167. IEEE, 1986.