Updated description to initial draft submission to thesis.fr from march 2025

June to September 2025:
Description de l'avancée de la thèse
Point sur les travaux effectués, difficultés rencontrées, ...

Verified through manual computation and implementation significant improvements for works of interest in the area of ZKP and Verifiable FHE.
Contributed special new findings in the area of Finite Field Set Membership Proofs, ideas
which qualified for standalone publication and which could be applied to allow significant contributions in recent works.

Updated from end of September 2025
Résumé du projet de thèse en français

La cryptographie avancée nécessite une sécurité post-quantique et bénéficie grandement de constructions simplifiant le schéma et l'analyse de sécurité. Outre la diversité des hypothèses mathématiques, telles que les treillis et les codes, des primitives permettant une simplicité globale sont fortement souhaitées. Ce travail s'intéresse plus particulièrement aux primitives à clés symétriques, qui permettent une grande modularité de conception et pour lesquelles de nouvelles constructions peuvent être proposées. Cette thèse porte sur les schémas cryptographiques avancés, post-quantiques et sécurisés, dont les principales constructions sont construites à partir de primitives à clés symétriques. Plus précisément, ce travail vise à améliorer et à innover l'état de l'art en matière de preuves cryptographiques (PC), de chiffrement homomorphe (HE) et de chiffrement entièrement homomorphe (FHE), ainsi que de cryptographie post-quantique (PQC) à partir de primitives à clés symétriques, d'algèbre abstraite et d'autres techniques telles que les protocoles de calcul multipartite simulés (MPC). La thèse prend CP comme point de départ et vise à couvrir et à contribuer à d'autres domaines connexes, tels que FHE, PQC et l'algèbre abstraite, de manière autonome.

Les constructions et applications des preuves cryptographiques elles-mêmes impliquent d'autres primitives avancées, telles que les codes correcteurs d'erreurs pour le codage et l'efficacité, la caractérisation NP pour les langages autorisant les propriétés homomorphes ou les évaluations aveugles, les protocoles MPC et leurs variantes simulées (par exemple, MPC-in-the-Head et VOLE-in-the-Head), le chiffrement homomorphe et classique (utilisant le chiffrement comme engagement), les preuves oracle interactives polynomiales (PIOP ou simplement IOP) et les schémas d'engagements polynomiaux (PCS) pour la compilation. Bien

que les schémas cryptographiques modernes ou classiques issus de la cryptographie symétrique et à clé publique permettent de construire des schémas avec des objectifs de sécurité souhaités tels que l'intégrité, la confidentialité, l'authentification et la disponibilité, ils ne permettent pas un calcul vérifiable avec d'autres propriétés souhaitées telles que la concision et la divulgation de connaissance, avec différents niveaux de sécurité selon les applications. Il s'agit du domaine des preuves cryptographiques : une solution relevant du calcul préservant la confidentialité (PPC) qui garantit l'intégrité des données (preuve de calcul), l'anonymat des calculs externalisés et les applications générales de traitement de données (modèles client-serveur traditionnels ou distribués). Ce travail s'intéresse particulièrement au calcul vérifiable pour les instances de chiffrement et les schémas de signature compatibles avec zk-SNARK, qui offrent de nombreuses autres applications avancées telles que les signatures en anneau et agrégées optimisées, les identifiants anonymes (identité de l'utilisateur et divulgation sélective), le partage de secrets et l'exportation de clés. De plus, nous étudions les applications distribuées telles que les réseaux P2P incluant les blockchains et toute application de validation de transaction avec zk-SNARK transparents.

Pour les contributions connexes ou autonomes à d'autres domaines, tels que l'HE ou les algèbres spéciales, y compris les espaces vectoriels avec applications à la cryptographie, l'objectif est d'améliorer les travaux existants et d'en apporter de nouveaux. L'objectif est notamment d'aborder l'HE et FHE pour l'arithmétique approximative ainsi que bootstrapping et d'exploiter au maximum l'arithmétique sous-jacente pour enrichir les idées. Il existe un fort désir de développer des HE et FHE pratiques prenant en charge l'arithmétique approximative, car leurs applications sont plus vastes que celles des schémas qui prenant en charge que les entiers seulement. De plus, l'optimisation de bootstrapping constitue l'élément le plus coûteux et le plus sophistiqué en termes de calcul pour HE/FHE car l'objectif est d'augmenter efficacement le module du texte chiffré afin d'éviter la réduction modulaire et la perte des résultats en clair lors des calculs, l'objectif principal étant un calcul théoriquement illimité. Comme le montre CASA: A Compact and Scalable Accelerator for Approximate Homomorphic Encryption, l'amélioration de l'arithmétique sous-jacente peut avoir un impact significatif sur les performances globales. La conception de nouveaux protocoles pour ces primitives avancées est également fortement souhaitée. En outre, le travail de thèse s'intéresse également à la recherche de domaines quantiques, de transferts inconscients et de signatures aveugles qui complètent bien le parcours du doctorant.

Depuis l'appel lancé en 2016 par le National Institute of Standards and Technology (NITS) en faveur d'algorithmes post-quantiques sécurisés,
a accordé une attention particulière sur la cryptographie à clé publique, il est bien connu que les investissements et les efforts mondiaux en informatique quantique

menacent les algorithmes classiques fondamentaux qui protègent nos communications numériques actuelles. Malgré les travaux en cours et les avancées potentielles pour construire des ordinateurs quantiques dotés des qubits fonctionnels nécessaires pour déchiffrer les primitives cryptographiques classiques, la dernière décennie a été consacrée à la préparation et à l'application d'analogues de la cryptographie post-quantique. Cela est dû en partie au théorème de Mosca, qui vise à éviter la collecte de textes chiffrés facilement déchiffrables ultérieurement. La classe d'algorithmes la plus vulnérable est celle des primitives de cryptographie à clé publique, telles que les signatures numériques et les algorithmes d'échange de clés. En réalité, tous les problèmes mathématiques sur lesquels reposent les algorithmes classiques ont des solutions en temps polynomial, du moins pour certains groupes ou variantes, dans le régime quantique. La plupart des SNARK reposent sur la cryptographie à courbe elliptique et les appariements qui ne sont pas sécurisés post-quantique. Outre les preuves cryptographiques basées sur des fonctions de hachage cryptographiques standard qui permettent la sécurité post-quantique, ce travail envisage de contribuer au domaine de la cryptographie post-quantique (PQC) en tant que domaine autonome avec des contributions telles que, SMALL : Scalable Matrix OriginAted Large Integer PoLynomial Multiplication Accelerator for Lattice-Based Post-Quantum Cryptography, à des constructions plus générales ou nouvelles.

Outre les algorithmes post-quantiques sécurisés basés sur les réseaux, d'autres catégories d'algorithmes post-quantiques sécurisés, basés sur les paradigmes de hachage et de MPC-in-the-head, présentent un intérêt particulier. Parmi les principaux exemples, on peut citer HSS, LMS, XMSS, XMSS^MT, SPHINCS+, Picnic et FAEST. Outre leurs cas d'utilisation courants, ces algorithmes conviennent aux applications de signature de code pour lesquelles d'autres schémas tels que Falcon et Dilithium ne reposent pas sur le pré-hachage des données. De plus, les algorithmes basés sur le hachage, similaires aux constructions CP à partir de fonctions de hachage, présentent l'avantage que la sécurité repose uniquement sur la fonction de hachage cryptographique sous-jacente utilisée et offrent de nombreuses possibilités d'optimisation. En revanche, l'analyse de sécurité et les composants des alternatives basées sur les réseaux sont plus complexes. Par exemple, Falcon utilise des FPU qui peuvent présenter des risques de canaux auxiliaires ultérieurement. D'ailleurs, la CNSA 2.0 recommande LMS et XMSS pour la signature de code; les deux avec un RFC et au moins plus d'une décennie d'exposition. Les algorithmes basés sur le hachage utilisent intensivement la fonction de hachage cryptographique sous-jacente qui peut être excessivement lente sous certains paramètres et cas d'utilisation. Par exemple, LMS pourrait faire des millions à des milliards d'appels de hachage pour les arbres les plus grands (15 à 25). L'incorporation, la conception ou l'application de techniques de co-conception peuvent avoir une amélioration totale du schéma en question comme c'est le cas pour Legendre avec les protocoles MPC. De plus, une conception soignée peut être requise pour des cas d'utilisation spécifiques où

des algorithmes avec ou sans état peuvent être requis. Ce travail vise à contribuer à l'optimisation des signatures numériques sécurisées post-quantiques basées sur des primitives symétriques, en se concentrant sur des constructions compatibles SNARK et qui permettent d'autres primitives cryptographiques avancées très souhaitées. Un exemple principal est LOQUAT: A SNARK-Friendly Post-Quantum Signature based on the Legendre PRF with Applications in Ring and Aggregate Signatures. En plus des applications dans différents contextes, tels que les signatures en anneau et agrégées, LOQUAT tire parti de la fonction pseudo-aléatoire de Legendre (PRF) et est plus efficace en ce qui concerne l'opération de vérification par rapport aux alternatives de signature post-quantique basées sur des clés symétriques. Dans le contexte des signatures en anneau basées sur l'ID et des signatures agrégées basées sur SNARK, LOQUAT démontre une amélioration remarquable dans le domaine de la cryptographie avancée préservant la confidentialité dans la sphère de la cryptographie post-quantique basée sur des clés symétriques. De plus, il existe de nombreuses opportunités d'explorer les contributions dans les schémas de signature de seuil à travers le paradigme MPC-in-the-head et similaires. Ce travail vise à améliorer les primitives à clé symétrique en améliorant leurs applications existantes, en repensant les schémas existants (par exemple, en explorant des alternatives potentielles à la PRF ultra-efficace de Legendre pour MPC) et en concevant de nouveaux OWF. Les applications incluent l'application de techniques de fusion, l'amélioration des calculs d'appartenance à l'ensemble et le protocole CP global pour améliorer des travaux tels que Phecda : Post-Quantum Transparent zkSNARKs from Improved Polynomial Commitment et VOLE-in-the-Head avec application dans le calcul vérifiable publiquement et vérifiable pour les schémas de cryptage homomorphe approximatifs ainsi que proposer des schémas nouveaux et originaux.

En résumé, cette thèse vise à améliorer les CP (notamment les zkSNARK et zkSTARK) sous tous leurs aspects de conception, notamment l'optimisation des calculs pour des algèbres spécifiques et l'arithmétique sous-jacente, ainsi que la conception de nouveaux protocoles. De plus, elle vise à contribuer à d'autres primitives avancées dans la construction et l'application des CP, ainsi qu'à des domaines spécifiques, tels que la FHE, la PQC et les corps finis. Nous envisageons des explorations potentielles, telles que le quantique pour la démonstration d'algorithmes quantiques sans calculs quantiques, et envisageons la contribution potentielle aux preuves relativistes à partir de la non-localité quantique avec des notions de sécurité renforcées. De manière exhaustive, ce travail croise les domaines de la cryptographie post-quantique, de la cryptographie à clé symétrique et de la cryptographie avancée afin d'améliorer et de contribuer à différents domaines, notamment les zk-SNARK et les zk-STARK, FHE, l'algèbre abstraite et les signatures distribuées. La thèse s'intéresse particulièrement à l'adressage d'instances prenant en compte le calcul vérifiable pour le chiffrement et les signatures numériques, les primitives compatibles SNARK issues des OWF, l'amélioration de l'appartenance à un ensemble, bootstrapping pour FHE et le

PQC. Les contributions envisagées s'inscrivent dans une perspective théorique et implémentée, à travers les principes de conception et l'exploration d'optimisations globales des systèmes, incluant l'arithmétique sous-jacente. De plus, la thèse considère les améliorations et les implémentations dans tous les domaines d'implémentation, tant au niveau logiciel que matériel et de la co-conception.

Résumé du projet de thèse en anglais

Thesis Summary (English and French)

Advanced cryptography necessitates post-quantum security and benefits much from constructions that simplify the scheme and security analysis. Besides variety in mathematical assumptions such as lattices and codes, primitives that allow for overall simplicity, are much desired. In particular this work considers symmetric-key-based primitives which permit high modularity in design and for which novel constructions can be proposed. This thesis is concerned with advanced cryptographic schemes that are post-quantum secure and for which the main constructions are built from symmetric-key-based primitives. Specifically, this work is focused on improving and innovating the state-of-the-art in Cryptographic Proofs (CP), homomorphic encryption (HE) and Fully Homomorphic Encryption (FHE), and Post-Quantum Cryptography (PQC) from symmetric-key primitives, abstract algebra, and other techniques such as, simulated Multi-Party Computation protocols (MPC). The thesis takes CP as a starting point and aims to span and contribute to other related areas, such as FHE, PQC, and Abstract Algebra, in a standalone manner.

The constructions and applications for cryptographic proofs themselves involve other advanced primitives, such as error-correcting codes for encoding and efficiency, NP characterisation for languages that allow for homomorphic properties or blind evaluations, MPC protocols and simulated variants (e.g., MPC-in-the-Head and VOLE-in-the-Head), Homomorphic and classical encryption (using encryption as commitments), Polynomial Interactive Oracle Proofs (PIOP or simply IOP) and Polynomial Commitments Schemes (PCSs) for compilation. Though modern or classical cryptographic schemes from symmetric and public key cryptography allow us to build schemes with desired security objectives such as, integrity, confidentiality, authentication, and availability, they do not allow verifiable computation with other desired properties such as, succinctness and zero-knowledge with various levels of security according to the applications. This is the playground of cryptographic proofs—a solution within the sphere of Privacy-Preserving Computation (PPC) that permits data integrity (proof of computation), anonymity for outsourced computation, and general data processing applications (traditional client-server or distributed models). This work is particularly interested in verifiable computation for instances of encryption and zk-SNARK-friendly signature schemes which in turn have a number of other advanced applications

such as, optimized ring and aggregated signatures, anonymous credentials (user identity and selective disclosure), secret sharing, and key export. Moreover, we consider distributed applications such as, p2p networks which include blockchains and any transaction validation applications with transparent zk-SNARKs .

For related or standalone contributions to other areas, such as HE or special algebras, including vectors spaces with applications to cryptography, the plan is to improve existing works and contribute new works. In particular, the objective is to address HE and FHE for approximate arithmetic as well as bootstrapping therein and to leverage as much as possible the underlying arithmetic to improve ideas. There is much desire for practical FHE and HE that supports approximate arithmetic because the applications are more vast than working with schemes that support only integers. Moreover, optimizing bootstrapping constitutes the most computationally expensive and sophisticated element for FHE/HE as the objective is an efficient means for raising the ciphertext modulus to avoid modular reduction and losing the plaintext results in computation with main goal of theoretically boundless computation. As CASA: A Compact and Scalable Accelerator for Approximate Homomorphic Encryption shows, improvements in the underlying arithmetic can have significant impacts on the overall performance. Designing new protocols for any of the advanced primitives is also much desired. In addition, the thesis work is also interested in pursuing quantum areas, oblivious transfers, and blind signatures which complement well the background of the doctorante.

It is well known since the 2016 National Institute of Standards and Technology call for post-quantum secure algorithms with emphasis on public-key cryptography, that global investment and efforts in quantum computing poses a threat to the core classical algorithms that safeguard our current digital communications. Despite the work in progress and potential leap to construct quantum computers with the required functional qubits capable of breaking classical cryptographic primitives, the last decade or so has been dedicated to preparing for and applying post-quantum cryptography analogues. In part, this is due to Mosca’s theorem as an effort to avoid collection of ciphertexts that could be easily decrypted later. The most vulnerable class of algorithms are public-key cryptography primitives, such as digital signatures and key exchange algorithms. In fact, all the mathematical problems on which the classical algorithms are based have polynomial-time solutions, at least for some groups or variants, in the quantum regime. Most SNARKs are based on elliptic curve cryptography and pairings which are not post-quantum secure. Besides cryptographic proofs based on standard cryptographic hash functions that allow post-quantum security, this work considers contributing to the area of Post-Quantum Cryptography (PQC) as a standalone area with contributions such as, SMALL : Scalable Matrix OriginAted Large Integer PoLynomial Multiplication Accelerator for Lattice-Based Post-Quantum Cryptography, to more general or new constructions.

Besides the main focus on lattice-based post-quantum secure algorithms, there are other categories of post-quantum secure algorithms of much interest based on the hash-based and MPC-in-the-head paradigms. Primary examples are HSS, LMS, XMSS, XMSS^MT, SPHINCS+, Picnic, and FAEST. In addition to the common use cases, these algorithms are suitable for code-signing applications for which other schemes such as, Falcon and Dilithium are not due to the pre-hash of data. Moreover, the hash-based algorithms similar to CP constructions from hash functions, have the advantage that the security relies solely on the underlying cryptographic hash function used and present ample opportunity for optimization. In contrast, the security analysis and components of the lattice-based alternatives is more involved. For instance, Falcon makes use of FPUs which may present side-channel risks later on. In fact, the CNSA 2.0 recommends LMS and XMSS for code-signing; both with an RFC and at least more than a decade of exposure. Hash-based algorithms make heavy use of the underlying cryptographic hash function which may be prohibitively slow under some parameters and use cases. For example, LMS might make millions to trillions of hash calls for the taller trees (15 to 25). Incorporating, designing, or applying co-design techniques, can have a total improvement on the scheme in question as is the case for Legendre with MPC protocols. In addition, overall careful design might be required for specific use cases where stateful or stateless algorithms might be required. This work aims to contribute to the optimization of post-quantum secure digital signatures based on symmetric primitives, with focus on constructions that are SNARK-friendly and which allow for other much desired advanced cryptographic primitives. A primary example is LOQUAT: A SNARK-Friendly Post-Quantum Signature based on the Legendre PRF with Applications in Ring and Aggregate Signatures. In addition to applications in different contexts, such as ring and aggregate signatures, LOQUAT takes advantage of the Legendre Pseudorandom Function (PRF) and is more efficient with respect to the verification operation in comparison to symmetric-key-based post-quantum signature alternatives. In the context of ID-based ring signatures and SNARK-based aggregate signatures, LOQUAT demonstrates outstanding improvement in the area of advanced privacy-preserving cryptography within the sphere of symmetric-key-based post-quantum cryptography. Moreover, there is ample opportunity to explore contributions in threshold signature schemes through the MPC-in-the-head paradigm and similar. This work aims to improve symmetric-key primitives by improving their existing applications, re-designing existing schemes (e.g., exploring potential alternatives to the ultra efficient Legendre PRF for MPC), and designing novel OWFs. The applications include applying merging techniques, improving set membership computations, and the overall CP protocol to improve works such as Phecda: Post-Quantum Transparent zkSNARKs from Improved Polynomial Commitment and VOLE-in-the-Head with Application in Publicly Verifiable and Verifiable Computation for Approximate Homomorphic Encryption Schemes as well as propose new and original schemes.

In summary, this thesis considers improving the CPs (spefifically zkSNARKs and zkSTARKs) from all designs aspects, which includes optimizing computations for specific algebras and the underlying arithmetic as well as the design of new protocols. Moreover, the thesis aims to contribute to other advanced primitives in the constructions and applications of CPs as well as standalone areas in themselves, including FHE, PQC, and Finite Fields. We consider potential explorations, such as quantum for the case of proving quantum algorithms without quantum computations and consider the prospective of contributions to relativistic proofs from quantum non-locality with stronger security notions. In a comprehensive manner, this work intersects the areas of Post-Quantum Cryptography, Symmetric-Key Cryptography, and Advanced Cryptography to improve and contribute to different areas which includes zk-SNARKS and zk-STARKs, FHE, Abstract Algebra, and Distributed Signatures. The thesis has special interest on addressing instances considers verifiable computation for encryption and digital signatures, SNARK- friendly primitives from OWFs, improved Set Membership, bootstrapping for FHE, and PQC. The contributions intended are from the theoretical and implementation perspectives through design principles and exploring a holistic optimizations of the systems which includes the underlying arithmetic. Moreover, the thesis considers improvements and implementations from all implementation domains in software, hardware, and co-designs.