Abstract

The growing reliance on digital communication, cloud platforms, and data-driven services has made strong cryptographic protection essential for modern computing systems. At the same time, rapid progress in quantum computing has raised concerns about the long-term security of many public-key cryptographic algorithms that are currently widely deployed, including RSA and elliptic-curve cryptography. If large-scale quantum computers become practical, these traditional systems could become vulnerable. This situation has motivated significant research into post-quantum cryptography as well as new approaches for protecting sensitive information during storage and computation, even when the underlying infrastructure cannot be fully trusted.

This thesis investigates how secure and efficient hardware platforms can be designed to support next-generation cryptographic techniques. The research focuses on two closely related directions. The first addresses post-quantum cryptographic primitives that enable secure communication in the presence of quantum adversaries. The second explores fully homomorphic encryption, which allows computations to be carried out directly on encrypted data without revealing the underlying information.

On the communication side, the thesis introduces unified hardware architectures for lattice-based cryptographic schemes that were selected during the NIST post-quantum standardization process. These architectures support both key encapsulation mechanisms and digital signature algorithms within a shared hardware framework. By reusing common computational components, the designs enable compact and efficient implementations across multiple security levels. In addition, the thesis proposes lightweight masking techniques that protect polynomial arithmetic from side-channel attacks while preserving the efficiency advantages of compact hardware multipliers.

For privacy-preserving computation, the thesis presents hardware acceleration strategies for fully homomorphic encryption. A scalable chiplet-based accelerator architecture is proposed to improve performance while reducing development complexity and manufacturing costs compared with conventional monolithic hardware solutions. The work also investigates hybrid homomorphic encryption approaches that combine symmetric cryptography with homomorphic computation, thereby reducing communication overhead and improving performance for privacy-preserving applications.

Beyond performance and architectural improvements, the thesis also examines the security of cryptographic implementations. It analyzes potential vulnerabilities such as side-channel leakage and fault attacks in modern cryptographic systems, demonstrating new attack scenarios and presenting countermeasures that strengthen the resilience of practical implementations.

Background and Motivation

Modern digital infrastructure depends heavily on cryptography to guarantee secure communication, authenticate users and systems, and protect sensitive information. Public-key cryptography plays a particularly important role in enabling secure interactions over open networks. For instance, protocols such as TLS rely on public-key algorithms to establish encrypted communication channels between clients and servers, while software distribution systems use digital signatures to verify the authenticity of updates and applications.

However, many of the public-key algorithms currently in use are based on mathematical problems that could become solvable with sufficiently powerful quantum computers. Shor's algorithm, for example, shows that large-scale quantum computers would be capable of efficiently breaking cryptographic systems such as RSA and elliptic-curve cryptography. Although practical quantum computers capable of performing such attacks do not yet exist, their potential development represents a serious long-term risk for existing digital security systems.

In response to this challenge, researchers and standardization bodies have begun developing post-quantum cryptographic algorithms that remain secure against both classical and quantum adversaries. At the same time, the increasing use of cloud computing has raised new privacy concerns. Sensitive data is often processed on remote servers, which means that information may be exposed during computation even if it is encrypted during transmission and storage.

Fully homomorphic encryption offers a promising solution to this problem by enabling computations to be performed directly on encrypted data. However, the computational cost of such techniques remains extremely high, limiting their practical deployment.

This thesis addresses these challenges by exploring efficient hardware implementations of post-quantum cryptography and homomorphic encryption systems, with the goal of improving both security and performance in real-world environments.

Objectives

The primary objectives of this research are:

- To design efficient hardware architectures capable of supporting post-quantum cryptographic algorithms.
- To improve the performance of privacy-preserving computation using fully homomorphic encryption.
- To study implementation-level security threats, including side-channel and fault-injection attacks.
- To develop countermeasures and secure design techniques for practical cryptographic systems.
- To facilitate the deployment of advanced cryptographic technologies in modern computing platforms.

Research Contributions

Efficient Hardware Architectures for Post-Quantum Cryptography

A major contribution of this thesis is the development of unified hardware architectures that support several lattice-based post-quantum cryptographic schemes within a single design framework. These architectures integrate the key computational components required for both key encapsulation mechanisms and digital signature algorithms.

By sharing building blocks such as polynomial arithmetic units, cryptographic hash functions, and memory structures, the proposed architectures significantly reduce hardware area and energy consumption. At the same time, they remain flexible enough to support different parameter sets and security levels, ensuring that the designs can adapt as cryptographic standards evolve.

Secure Implementations and Side-Channel Protection

While algorithmic security is essential, real-world cryptographic systems must also be protected against implementation-level attacks. Side-channel attacks, for example, exploit information leaked through physical characteristics of a device, such as power consumption or electromagnetic emissions.

To address this challenge, the thesis introduces lightweight masking techniques designed specifically for polynomial arithmetic used in lattice-based cryptography. These techniques protect sensitive computations while preserving the performance advantages of compact hardware multipliers commonly used in high-performance cryptographic accelerators. The effectiveness of these countermeasures is evaluated using established leakage assessment techniques to ensure that the resulting implementations provide strong resistance against side-channel attacks.

Hardware Acceleration for Fully Homomorphic Encryption

Fully homomorphic encryption makes it possible to perform computations on encrypted data without revealing the underlying plaintext. Although this capability enables powerful privacy-preserving applications, the computational overhead associated with FHE operations remains extremely high compared to traditional computation.

To improve performance, this thesis proposes specialized hardware accelerator architectures tailored for homomorphic encryption workloads. In particular, a chiplet-based accelerator design is introduced to enable scalable and cost-efficient implementations.

By distributing computational tasks across multiple interconnected processing units, the proposed architecture increases parallelism and improves throughput while reducing the complexity and cost associated with manufacturing large monolithic chips.

Hybrid Homomorphic Encryption and Client-Side Optimization

The thesis also explores hybrid homomorphic encryption approaches that combine symmetric encryption with homomorphic computation. In this paradigm, data is first encrypted using a fast symmetric cipher, and the server performs homomorphic operations that effectively decrypt the data within the encrypted domain.

This strategy reduces the computational burden on client devices while still maintaining strong privacy guarantees. Efficient hardware implementations of these hybrid schemes are presented, demonstrating

substantial performance improvements for applications such as privacy-preserving machine learning and secure data processing.

Security Analysis and Cryptographic Attacks

In addition to proposing new system architectures, the thesis examines potential vulnerabilities in modern cryptographic constructions. The research demonstrates novel attack strategies that exploit fault injections and weaknesses in hybrid homomorphic encryption implementations.

These analyses highlight the importance of considering realistic attack models when designing cryptographic systems. The work also proposes countermeasures that help strengthen the security of practical implementations against such threats.

Application-Level Optimizations

To further improve the practicality of encrypted computation, the thesis introduces new techniques for optimizing frequently used operations, such as matrix multiplication, in encrypted environments. These optimizations reduce the number of expensive cryptographic operations required for large-scale computations, improving efficiency in applications including privacy-preserving machine learning.

Impact and Significance

The results of this thesis contribute to the broader transition toward quantum-resistant cryptographic systems and more secure cloud computing infrastructures. By combining efficient hardware implementations with security analysis and application-level optimization, the research advances the state of the art in both post-quantum cryptography and privacy-preserving computation. The proposed architectures and techniques help bridge the gap between theoretical cryptographic research and the practical deployment of secure systems in real-world environments.

Conclusion

This thesis demonstrates that efficient and secure hardware implementations are essential for enabling the next generation of cryptographic technologies. Through contributions spanning architecture design, security analysis, and application-level optimization, the research provides a comprehensive hardware-centric perspective on building cryptographic systems suitable for the post-quantum era.

The findings support the practical deployment of post-quantum cryptography and homomorphic encryption, helping ensure secure communication and strong privacy protection in future digital infrastructures.