Isogenies for Post-Quantum Cryptography

Introduction:

- Public key cryptography is crucial for securing everyday communications, but current systems will be broken by large-scale quantum computers .
- Supersingular isogeny-based cryptography is a proposal for public key cryptosystems that are believed to remain secure even in the presence of quantum computers .
- The most famous cryptosystem based on supersingular isogenies is the supersingular isogeny Diffie-Hellman (SIDH) key exchange .
- This paper aims to explain the theoretical background of supersingular isogeny-based cryptography and evaluate the practicality of SIDH key exchange .
- The paper discusses how isogenies in SIDH give rise to non-backtracking walks in supersingular isogeny graphs and performs simulations to describe their behavior .
- It also provides an optimized and efficient software implementation of SIDH key exchange in Rust and compares its performance with other state-of-the-art implementations .
- The paper focuses on isogeny-based cryptography as a post-quantum candidate and highlights its potential as a viable alternative in the field of cryptography .

Barriers:

- The paper highlights the barrier of quantum computers, which have the potential to break current public key

cryptosystems, including widely used systems like RSA and DSA **[1]**.

- It emphasizes the need for post-quantum cryptography solutions that can remain secure even in the presence of large-scale quantum computers .
- The paper discusses the challenge of optimizing and efficiently implementing the supersingular isogeny Diffie-Hellman (SIDH) key exchange, aiming to assess its practicality **[2]**.
- It mentions the complexity of isogeny graphs and the behavior of non-backtracking walks in these graphs, which require simulations to study and understand **[2]**.
- The paper acknowledges the possibility of complications in isogeny graphs, such as non-equivalent isogenies having equivalent dual isogenies and the occurrence of loops, which can impact the security and efficiency of the cryptosystem **[3]**.
- It also highlights the importance of evaluating the performance of the SIDH key exchange implementation in comparison to existing state-of-the-art implementations **[2]**.

Applications:

- Isogeny-based cryptography, specifically the supersingular isogeny Diffie-Hellman (SIDH) key exchange, is discussed as a promising candidate for post-quantum cryptography .
- The primary application mentioned is the use of SIDH key exchange for secure communication in the presence of large-scale quantum computers .

- The paper also mentions additional protocols based on supersingular isogenies, although specific applications are not elaborated upon **[1]**.
- Isogeny-based cryptography is highlighted as a potential alternative to current public key cryptosystems, such as RSA and DSA, which are vulnerable to quantum attacks .
- The focus of the paper is on evaluating the practicality and performance of SIDH key exchange, suggesting its potential application in real-world scenarios **[2]**.
- The optimized and efficient software implementation of SIDH key exchange in Rust is presented, indicating its potential for practical use **[2]**.
- The paper also discusses the current status of hardware and software implementations of SIDH, suggesting its potential for implementation in various systems

Research scope:

- The paper focuses on explaining the theoretical background of supersingular isogeny-based cryptography and evaluating the current status of the supersingular isogeny Diffie-Hellman (SIDH) key exchange in practice **[1]**.
- It discusses the construction and evaluation of isogenies, as well as the construction of supersingular elliptic curves .
- The paper explores the structure of supersingular isogeny graphs and the behavior of non-backtracking walks in these graphs, including simulations to estimate various distributions of isogeny walks in SIDH key exchange **[2]**.

- It addresses the computational problems that supersingular isogeny cryptography, specifically SIDH key exchange, is based on .
- The paper also covers the best known attacks against isogeny problems and SIDH key exchange, along with proposed countermeasures .
- Additionally, the paper reviews the current status of hardware and software implementations of SIDH, including optimizations that can be applied to these implementations **[3]**.
- The research scope of isogeny-based cryptography in this paper encompasses both theoretical aspects and practical evaluations of SIDH key exchange.

Mathematical background:

- Isogeny-based cryptography is based on the theory of elliptic curves and isogenies, which are maps between elliptic curves that preserve certain algebraic properties.
- The cryptographic primitive used in isogeny-based cryptography is similar to the classical Diffie-Hellman key exchange, where two parties compute a shared secret over a public channel. **[1]**
- Isogeny-based cryptography specifically focuses on supersingular elliptic curves, which have special properties that make them suitable for cryptographic applications. **[2]**
- The security of isogeny-based cryptography relies on the difficulty of computing isogenies between supersingular elliptic curves, as well as the hardness of certain computational problems related to these curves. **[3] [2]**

- Isogeny-based cryptography offers a promising candidate for post-quantum cryptography due to its relatively short key sizes and the belief that it will remain secure even in the presence of large-scale quantum computers. **[2]**
- The mathematical foundations of isogeny-based cryptography were pioneered by Couveignes and Stolbunov, who introduced the concept of using isogenies on ordinary curves as a cryptographic primitive.

Security analysis:

- Isogeny-based cryptography offers a promising candidate for post-quantum cryptography due to its resistance against attacks from quantum computers.
- The security of isogeny-based cryptography relies on the difficulty of computing isogenies between supersingular elliptic curves.**[1]**
- The paper discusses various attacks against supersingular isogeny-based cryptography, specifically the SIDH key exchange. These include classical and quantum algorithms to solve isogeny problems, the claw problem, active adaptive attacks against static keys, passive attacks against torsion points, and side-channel attacks.
- The paper also reviews the best known attacks against isogeny problems and SIDH key exchange, along with proposed countermeasures to mitigate these attacks.**[2]**
- The current status of hardware and software implementations of SIDH is reviewed, along with

optimizations that can be applied to these implementations.**[3]**

- The research evaluates the practicality and performance of the SIDH key exchange through simulations and comparisons with state-of-the-art implementations.

Implementation aspects:

- The paper discusses the implementation of the supersingular isogeny Diffie-Hellman (SIDH) key exchange in practice.
- It provides an optimized and efficient software implementation of SIDH key exchange in Rust, which is compared with currently available state-of-the-art implementations to assess its practicality **[1]**.
- The current status of both hardware and software implementations of SIDH is reviewed, including their performance and optimizations that can be applied **[2]**.
- The research evaluates the performance of the software implementation through simulations and comparisons with other implementations, aiming to assess its practicality **[1]**.
- The paper also discusses the compression and key validation techniques suitable for SIDH key exchange, which are important aspects of the implementation **[2]**.
- The focus is on providing an efficient and practical implementation of SIDH key exchange, considering its potential as a post-quantum alternative for secure communication

Conclusion and future work:

- The paper presents conclusions about supersingular isogeny cryptography, specifically the SIDH key exchange, as a viable post-quantum alternative.
- The research evaluates the theoretical background and practical implementation of supersingular isogeny-based cryptography, highlighting its potential for secure communication.
- The optimized and efficient software implementation of SIDH key exchange in Rust is compared with state-of-the-art implementations, assessing its practicality and performance.
- The paper discusses the current status of hardware and software implementations of SIDH, along with optimizations that can be applied.
- Future works in isogeny-based cryptography may involve further research on the security analysis of isogeny problems and SIDH key exchange, exploring potential vulnerabilities and proposing additional countermeasures.
- Additionally, ongoing efforts may focus on improving the efficiency and performance of isogeny-based cryptographic algorithms, making them more practical for real-world applications.