Poznan University of Technology

Blockchain Technology And Quantum Computation
Post Quantum Cryptography

Jakub Piotr Hamerliński

Blockchain Technology And Quantum Computation
Post Quantum Cryptography

01. The threats of quantum computing to current cryptographic mechanisms
02. Post-quantum cryptographic mechanisms, including lattice-based cryptography, hash-based cryptography, and code-based cryptography
03. Research directions for post-quantum cryptography
04. Possibilities of quantum cryptography: quantum key distribution, quantum coin tossing
05. Practical implementation of quantum cryptography

The threats of quantum computing to current cryptographic mechanisms

Post Quantum Cryptography

The threats of quantum computing to current cryptographic mechanisms

The development of powerful quantum computers poses significant threats to current cryptographic mechanisms used to secure data and communication. Here's a brief and compact overview of the threats:

01. Breaking Public Key Cryptography: Quantum computers can efficiently solve mathematical problems that are the foundation of many widely used public key cryptographic algorithms. For example, Shor's algorithm can factorize large numbers and solve the discrete logarithm problem efficiently. This means that widely deployed cryptographic systems, such as RSA and ECC, could be easily broken by quantum computers, rendering the encrypted data vulnerable to decryption.

Post Quantum Cryptography

The threats of quantum computing to current cryptographic mechanisms

02. Key Distribution: Quantum computers have implications for the security of key distribution protocols. While classical cryptographic protocols like Diffie-Hellman key exchange or symmetric key distribution mechanisms may still be secure against classical attacks, they become vulnerable to quantum attacks. Quantum key distribution (QKD) protocols provide a solution, as they rely on the laws of quantum mechanics to establish secure keys. However, the implementation and scalability of QKD systems pose practical challenges.

Post Quantum Cryptography

The threats of quantum computing to current cryptographic mechanisms

03. Cryptographic Hash Functions: Quantum computers could potentially break cryptographic hash functions, which are used for various purposes, including integrity checks, digital signatures, and password storage. Grover's algorithm provides a quadratic speedup for searching an unsorted database, enabling the brute-force search of hash functions with greater efficiency. This threatens the security provided by hash functions and the integrity of digital signatures.

Post Quantum Cryptography

The threats of quantum computing to current cryptographic mechanisms

04. Blockchain Technology: Quantum computers could impact the security of blockchain technology, particularly if it relies on classical cryptographic algorithms. Quantum attacks on blockchain systems could include breaking the security of digital signatures, manipulating transaction records through chain reorganization attacks, or compromising the privacy of transactions. Post-quantum cryptographic algorithms and quantum-resistant approaches need to be developed and integrated into blockchain systems to withstand potential quantum threats.

Post Quantum Cryptography

The threats of quantum computing to current cryptographic mechanisms

To address these threats, ongoing research and development focus on post-quantum cryptography, which aims to develop new cryptographic algorithms that are resistant to attacks from both classical and quantum computers. Implementing these quantum-resistant algorithms and transitioning to quantum-safe cryptographic systems is crucial to ensure the long-term security of sensitive data and communication in the face of quantum computing advancements.

Post-quantum cryptographic mechanisms

Post Quantum Cryptography

Post-quantum cryptographic mechanisms

Post-quantum cryptographic mechanisms refer to cryptographic algorithms and schemes designed to be resistant against attacks from both classical and quantum computers. Here's a brief description of some post-quantum cryptographic mechanisms:

Post Quantum Cryptography

Post-quantum cryptographic mechanisms

01. Lattice-based Cryptography: Lattice-based cryptography relies on mathematical problems involving lattices, which are grid-like structures in higher-dimensional spaces. These problems, such as the Learning With Errors (LWE) problem, are believed to be hard to solve even for quantum computers. Lattice-based cryptography offers a wide range of cryptographic primitives, including encryption, key exchange, and digital signatures.

Post Quantum Cryptography

Post-quantum cryptographic mechanisms

02. Isogeny-based Cryptography: Isogeny-based cryptography utilizes mathematical properties of elliptic curves and isogenies, which are mappings between elliptic curves with special properties. These cryptographic schemes are based on the hardness of solving the isogeny problem and offer post-quantum security. Notable examples include the Supersingular Isogeny Diffie-Hellman (SIDH) key exchange and the SIKE digital signature scheme.

Post Quantum Cryptography

Post-quantum cryptographic mechanisms

03. Multivariate-based Cryptography: Multivariate-based cryptography employs mathematical equations and systems of multivariate polynomials. The security of these schemes relies on the difficulty of solving systems of multivariate polynomial equations. Multivariate-based cryptography offers encryption and digital signatures and can withstand quantum attacks by requiring solving large systems of polynomial equations.

Post Quantum Cryptography

Post-quantum cryptographic mechanisms

04. Hash-based Cryptography: Hash-based cryptography uses cryptographic hash functions as the foundation for various cryptographic operations. These schemes rely on the properties of hash functions, such as collision resistance and preimage resistance, to provide security. Hash-based cryptographic schemes, such as the Merkle signature scheme, are considered post-quantum secure as they require quantum computers to break the underlying hash functions.

Post Quantum Cryptography

Post-quantum cryptographic mechanisms

05. Code-based Cryptography: Code-based cryptography is based on error-correcting codes, which are used to encode and decode information. These cryptographic schemes rely on the hardness of decoding encoded information from linear error-correcting codes. Notable examples include the McEliece encryption and the Niederreiter encryption schemes.

Post Quantum Cryptography

Post-quantum cryptographic mechanisms

These post-quantum cryptographic mechanisms offer alternatives to the traditional cryptographic algorithms vulnerable to attacks from quantum computers. They provide a foundation for secure communication, digital signatures, and other cryptographic operations in a post-quantum era, where the security of classical cryptographic mechanisms may be compromised.

Research directions for post-quantum cryptography

Post Quantum Cryptography

Research directions for post-quantum cryptography

Research directions for post-quantum cryptography involve exploring new cryptographic algorithms and protocols that can resist attacks from both classical and quantum computers. Here are some key research directions in post-quantum cryptography:

Post Quantum Cryptography

Research directions for post-quantum cryptography

01. Development of New Mathematical Assumptions: Researchers are investigating new mathematical problems and assumptions that can form the basis of post-quantum cryptographic algorithms. These include problems from various mathematical areas, such as lattice theory, coding theory, multivariate polynomials, and isogenies. The goal is to identify mathematical problems that are believed to be hard for both classical and quantum computers to solve.

Post Quantum Cryptography

Research directions for post-quantum cryptography

02. Exploration of Quantum-Resistant Cryptographic Primitives: Researchers are designing and analyzing cryptographic primitives that are specifically resistant to attacks from quantum computers. This includes developing post-quantum secure encryption schemes, digital signature algorithms, key exchange protocols, and hash functions. The focus is on creating new cryptographic building blocks that can be used to construct secure post-quantum systems.

Post Quantum Cryptography

Research directions for post-quantum cryptography

03. Standardization Efforts: There are ongoing standardization efforts by organizations such as NIST (National Institute of Standards and Technology) to evaluate and select post-quantum cryptographic algorithms. The goal is to establish a set of standardized post-quantum cryptographic algorithms that can be widely adopted and implemented across various systems and protocols.

Post Quantum Cryptography

Research directions for post-quantum cryptography

04. Practical Implementations and Efficiency: Researchers are working on optimizing and improving the efficiency of post-quantum cryptographic algorithms to ensure their practicality and suitability for real-world applications. This involves developing efficient algorithms, reducing the computational and communication overhead, and addressing performance limitations associated with post-quantum cryptography.

Post Quantum Cryptography

Research directions for post-quantum cryptography

05. Security Analysis and Evaluations: Thorough security analysis and evaluations of post-quantum cryptographic algorithms are essential to ensure their resistance against both classical and quantum attacks. Researchers are conducting extensive analysis, including cryptanalysis and security proofs, to validate the security properties and strengths of post-quantum cryptographic schemes.

Post Quantum Cryptography

Research directions for post-quantum cryptography

06. Post-Quantum Cryptography and Quantum Computing Interactions: Researchers are exploring the interaction between post-quantum cryptography and quantum computing. This includes investigating the potential impact of quantum computers on post-quantum cryptographic schemes, the development of quantum-safe encryption schemes suitable for use in quantum computing environments, and the use of quantum technologies to enhance post-quantum cryptographic protocols.

Post Quantum Cryptography

Research directions for post-quantum cryptography

These research directions aim to develop robust and secure post-quantum cryptographic solutions that can withstand attacks from quantum computers and ensure the long-term security of data and communication in a world where quantum computing becomes prevalent.

Possibilities of quantum cryptography: quantum key distribution, quantum coin tossing

Post Quantum Cryptography

Possibilities of quantum cryptography: quantum key distribution, quantum coin tossing

The possibilities of quantum cryptography center around leveraging the principles of quantum mechanics to enhance the security of communication and data protection. Here are two key possibilities in quantum cryptography:

Post Quantum Cryptography

Possibilities of quantum cryptography: quantum key distribution, quantum coin tossing

Quantum Key Distribution (QKD): Quantum key distribution enables the secure exchange of cryptographic keys between two parties over an insecure channel. QKD utilizes the properties of quantum mechanics, such as the no-cloning theorem and the uncertainty principle, to provide information-theoretic security. By encoding information in quantum states, any attempt to intercept or measure these states would disrupt their quantum properties, thereby indicating the presence of an eavesdropper. QKD protocols, such as the BB84 and E91 protocols, establish a shared secret key between the communicating parties, ensuring secure communication channels.

Post Quantum Cryptography

Possibilities of quantum cryptography: quantum key distribution, quantum coin tossing

Quantum Coin Tossing: Quantum coin tossing is a cryptographic protocol that allows two parties to fairly generate a random bit in a way that prevents either party from biasing the result. In classical coin tossing, it is impossible to ensure fairness if one party has more control or information than the other. However, with the use of quantum mechanics, quantum coin tossing protocols enable a fair outcome by exploiting the properties of quantum states and measurements. Quantum coin tossing has implications in scenarios where a fair and unbiased random bit is required, such as cryptographic key generation or fair gambling protocols.

Practical implementation of quantum cryptography

Post Quantum Cryptography

Practical implementation of quantum cryptography

01. Quantum Hardware: Quantum cryptography requires the use of quantum hardware to generate, manipulate, and measure quantum states. This typically involves technologies like quantum key distribution (QKD) systems or other quantum devices capable of preparing and measuring quantum bits (qubits) accurately.

Post Quantum Cryptography

Practical implementation of quantum cryptography

02. Quantum Key Distribution (QKD) Protocols: QKD protocols, such as the BB84 or E91 protocols, form the basis of practical quantum cryptography implementations. These protocols enable the secure distribution of cryptographic keys over insecure channels by utilizing the principles of quantum mechanics to detect any eavesdropping attempts.

Post Quantum Cryptography

Practical implementation of quantum cryptography

03. Quantum Channel: The communication channel between the sender and the receiver plays a crucial role in quantum cryptography. It should provide sufficient protection against external interference and maintain the integrity of the quantum states being transmitted. Technologies such as fiber optics or free-space optical communication can be used to establish secure quantum channels.

Post Quantum Cryptography

Practical implementation of quantum cryptography

04. Security Analysis and Authentication: Practical implementation of quantum cryptography requires a rigorous security analysis to ensure the system's resilience against potential attacks. Techniques such as authentication and error detection/correction codes are employed to enhance the security and reliability of the quantum communication.

Post Quantum Cryptography

Practical implementation of quantum cryptography

05. Post-processing and Classical Cryptography: Quantum cryptography often involves post-processing steps to extract the final cryptographic key from the exchanged quantum states. Classical cryptographic algorithms, such as symmetric encryption or hashing, are often used in combination with quantum cryptography to provide additional security and functionalities.

Post Quantum Cryptography

Practical implementation of quantum cryptography

06. Infrastructure and Deployment: Quantum cryptography systems require a well-designed infrastructure for deployment, including the integration of quantum hardware, secure communication networks, and cryptographic protocols. Implementations can vary depending on the specific requirements, ranging from small-scale laboratory setups to larger-scale networks.

Post Quantum Cryptography

Practical implementation of quantum cryptography

07. Practical Limitations: Practical implementation of quantum cryptography faces challenges such as noise, decoherence, and the need for error correction. Mitigating these limitations requires advancements in quantum hardware, error correction techniques, and robust engineering solutions.

Post Quantum Cryptography

Practical implementation of quantum cryptography

In summary, the practical implementation of quantum cryptography involves the use of quantum hardware, QKD protocols, secure communication channels, security analysis, post-processing, and a well-designed infrastructure. Overcoming practical challenges and advancing quantum technologies are essential for realizing the full potential of quantum cryptography in real-world applications.

Sources

Sources

The threats of quantum computing to current cryptographic mechanisms:

01. "A Survey of Quantum Attacks Exploiting the Algebraic Structure of Cryptographic Primitives" by Jean-Charles Faugère, Ludovic Perret, and Mathieu Renault.
02. "Quantum Computation and Cryptography: A Tutorial" by Michele Mosca and Alexander Russell.
03. "Quantum Computing and Cryptography: A Survey" by An Braeken, Roel Maes, and Ingrid Verbauwhede.
04. "Quantum Computing and Cryptography: Challenges and Opportunities" by Michele Mosca.

Sources

Post-quantum cryptographic mechanisms:

01. "Post-Quantum Cryptography: Current State and Future Directions" by Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen.
02. "Post-Quantum Cryptography" by Peter J. Schwabe.
03. "NIST Post-Quantum Cryptography Standardization" by Dustin Moody, Daniel A. C. Smith, and Rachel Player.
04. "Post-Quantum Cryptography: Current Landscape and Challenges Ahead" by Christiane Peters.

Sources

Research directions for post-quantum cryptography:

01. "Post-Quantum Cryptography: From Theory to Practice" by Tsuyoshi Takagi and Daiki Miyahara.
02. "Post-Quantum Cryptography: A New Frontier in Information Security" by Michele Mosca.
03. "Post-Quantum Cryptography and Quantum Fault-Tolerance" by Daniel Gottesman and John Preskill.
04. "Quantum Cryptography: From Theory to Practice" by Vadim Lyubashevsky.

Sources

Possibilities of quantum cryptography:

01. "Quantum Cryptography: Public Key Distribution and Coin Tossing" by Gilles Brassard and Louis Salvail.
02. "Quantum Cryptography and Secret-Key Distillation" by Stefano Pirandola.
03. "Quantum Cryptography: Uncertainty in the Service of Privacy" by Gilles Brassard.
04. "Quantum Cryptography: A Review" by Artur Ekert.

Sources

Practical implementation of quantum cryptography:

01. "Quantum Cryptography: A Practical Introduction" by Norbert Lütkenhaus.
02. "Practical Quantum Cryptography" by Paul D. Townsend.
03. "Quantum Key Distribution: Practical Aspects and New Challenges" by Tommaso Gagliardoni and Giuseppe Vallone.
04. "Quantum Key Distribution with High-Speed Data Encryption for Secure Communication" by Zhiliang Yuan et al.

Thank you

Feel free to reach me via LinkedIn

Fin