Research on Secure Mobile Payment System Based on NTRU-MPS

Zhang Man

Chongqing Technology and Business Institute, Chongqing, China

Abstract: This paper aims to explore and implement a mobile payment system based on the NTRU-MPS signature algorithm to enhance the security and efficiency of mobile payments. By designing a salted hash mechanism and applying it to the registration and login process, the robustness of user authentication is enhanced. Additionally, the seamless integration of NTRU-MPS digital certificate technology into the mobile payment system realizes encrypted verification and signature authentication of transaction data, effectively defending against quantum computing threats and traditional security attacks.

Keywords: NTRU-MPS; Mobile Payment; Salted Hash; Digital Certificate; Security

1. Introduction

With the rapid development of mobile internet technology and the widespread adoption of smart devices, mobile payment has emerged as an indispensable payment method in modern society due to its convenience, immediacy, and efficiency. However, this highly digitized and networked transaction mode also presents a series of severe security challenges. Issues such as user data leaks, transaction fraud, and middle attacks occur frequently, posing threats not only to users' property security but also affecting the healthy development of the entire payment industry. Furthermore, as quantum computing technology continues to make breakthroughs and advancements, traditional encryption algorithms based on mathematical challenges such as large integer factorization and discrete logarithms like RSA and ECC are facing unprecedented quantum computing threats. Quantum computers, with their formidable parallel processing capabilities, are expected to significantly reduce the time required to crack these classical encryption algorithms in the coming years, putting the existing security framework of mobile payments at risk of becoming ineffective.

Therefore, researching and applying post-quantum cryptography algorithms has become an inevitable choice to ensure the security of mobile payments and address the challenges posed by quantum computing [1]. Post-quantum cryptography algorithms are a class of encryption algorithms that can maintain security in a quantum computing environment. They are based on different mathematical challenges, such as lattice theory, coding theory, and multivariate polynomials, which are considered to be equally difficult to solve efficiently on quantum computers.

2. NTRU-MPS Algorithm

As an important representative in post-quantum cryptography, NTRU-MPS demonstrates tremendous potential in resource-constrained applications with high security requirements such as mobile payments due to its small key size, efficient computational speed, and robust quantum resistance. NTRU-MPS leverages the trapdoor properties of multivariate polynomial functions to construct a signing scheme, enabling both the signature generation and verification processes to be fast and secure. To fully exploit the advantages of NTRU-MPS, this paper innovatively proposes combining it with WPKI (Wireless Public Key Infrastructure) technology to build a novel security framework for mobile payments. WPKI, as an extension of traditional PKI [2] in wireless environments, aims to provide identity authentication, data integrity, and confidentiality protection for devices and services in wireless communication networks. By integrating NTRU-MPS into the WPKI system, we can implement post-quantum cryptography-based digital certificate issuance, verification, and key management within the mobile payment system, thereby ensuring the security and integrity of transaction data during transmission and effectively defending against quantum computing and traditional security threats.

Specifically, this framework will encompass multiple stages, including user identity registration, certificate issuance, transaction signing, and verification. During the registration phase, NTRU-MPS is utilized to generate a public-private key pair for the user, and a digital certificate containing the user's public key is issued by the CA (Certificate Authority) of WPKI. During the transaction process, NTRU-MPS is employed to sign the transaction data, and the verification mechanism of WPKI ensures the validity of the signature and the authenticity of the identities of both parties involved in the transaction. Additionally, leveraging the key management mechanism of WPKI, the user's public-private key pair and certificate are regularly updated, further enhancing the security of the system.

Applying the combination of NTRU-MPS and WPKI technology in mobile payment systems can not only enhance the system's quantum-resistant capabilities but also improve the security and efficiency of the transaction process, providing a solid security guarantee for the healthy development of the mobile payment industry.

3. NTRU-MPS-based Mobile Payment System

The WPKI secure mobile payment system architecture based on NTRU-MPS aims to establish an efficient, secure, and quantum-resistant mobile payment environment. This system integrates the advanced post-quantum cryptography algorithm [3] NTRU-MPS with Wireless Public Key Infrastructure (WPKI) technology. Through the close collaboration of multiple components, including mobile payment user terminals, payment servers, and Certificate Authorities, it realizes key functions such as user identity authentication, transaction data encryption, signature verification, and key management.

3.1 Components and Their Functions

3.1.1. Mobile Payment User Terminal

Identity Registration and Authentication: When users first use the system, they need to submit registration information through the mobile payment user terminal, including identity information, contact details, etc. the mobile payment user terminal encrypts the user information and sends it to the CA for identity authentication [4]· and receives a digital certificate containing the user's public key issued by the CA. Afterward, before each login or transaction, users must use the NTRU-MPS signature algorithm to sign the login information or transaction requests to ensure the authenticity and integrity of the requests.

Transaction Request Initiation: After selecting a product or service, the user generates a transaction request through the mobile payment user terminal, including details of the product, transaction amount, user's public key, and other information. Subsequently, the mobile payment user terminal uses the NTRU-MPS private key to sign the transaction request and sends the signed transaction request to the payment server.

Transaction Result Reception: the mobile payment user terminal receives the transaction result returned by the payment server, including notifications of whether the payment was successful or not, transaction details, and other information. Simultaneously, the mobile payment user terminal uses the NTRU-MPS public key to verify the signature returned by the payment server, ensuring the legitimacy and authenticity of the transaction result.

3.1.2. Payment Server

Transaction Request Processing: the payment server receives signed transaction requests from the mobile payment user terminal. It first verifies the legitimacy and integrity of the request. By querying the user's public key through the WPKI system, the server uses this public key to validate the signature of the transaction request. Once the verification is successful, the payment server proceeds to execute transaction logic, including fund transfer, inventory update, and other operations.

Transaction Result Generation and Return: After completing the transaction, the payment server generates the transaction result and signs it using the NTRU-MPS private key. Then, it returns the signed transaction result to both the mobile payment user terminal and the merchant terminal to ensure that both parties receive accurate and error-free transaction information.

Secure Communication: Communication between the payment server, mobile payment user terminal, merchant terminal, and CA is conducted through encrypted channels to ensure the confidentiality and integrity of data during transmission.

3.1.3. Certificate Authority (CA)

Identity Authentication and Certificate Issuance: the CA is responsible for receiving registration information from the mobile payment user terminal and conducting rigorous identity authentication. Upon successful authentication, the CA uses its private key to generate a digital certificate containing the user's public key and issues it to the mobile payment user terminal. the certificate includes information such as the user's identity, public key, and the validity period of the certificate.

Certificate Management: the CA is also responsible for managing certificate revocation, updates, and queries. In the event of a user's private key compromise or a certificate expiration, the CA will revoke the certificate and notify the affected users and system components. Additionally, the CA provides certificate lookup services to enable other system components to verify the validity of user certificates when needed.

3.2 Interaction Process

User Registration and Authentication: the user submits registration information to the CA through the mobile payment user terminal for identity authentication. Upon successful authentication, the CA issues a digital certificate containing the user's public key to the mobile payment user terminal.

Transaction Request Generation and Signing: After selecting a product or service, the user generates a transaction request through the mobile payment user terminal and signs the request using the NTRU-MPS private key.

Transaction Request Submission: the mobile payment user terminal sends the signed transaction request to the payment server.

Transaction Request Processing and Verification: Upon receiving the transaction request, the payment server queries the user's public key through the WPKI system and verifies the legitimacy and integrity of the signature. If the verification is successful, the payment server proceeds with the transaction logic.

Transaction Result Generation and Return: After completing the transaction, the payment server generates the transaction result and signs it with the NTRU-MPS private key. It then returns the signed transaction result to both the mobile payment user terminal and the merchant terminal.

Transaction Result Verification and Display: the mobile payment user terminal and merchant terminal receive the transaction result and verify the validity of the signature using the NTRU-MPS public key. Once the verification is successful, the transaction result is displayed for the user to view.

3.3 Registration and Login Security Authentication

In designing the security authentication mechanism for a registration and login system, incorporating both salted hashing and NTRU-MPS for dual verification can significantly enhance the security of user identity authentication, effectively defending against security threats such as password guessing and replay attacks.

3.3.1. Salted Hashing Mechanism

Salted hashing is primarily used to protect user passwords stored in databases, preventing them from being easily cracked in the event of a breach. the specific implementation steps are as follows:

Generate Salt: During user registration, the system uses a strong random number generator to create a sufficiently long random string as the salt value. This salt value should be comparable in length to or longer than the output of the hash function to enhance security.

Hash Password with Salt: Combine the user's input password with the salt value, and then apply a secure hash function to the combined string. the resulting hash value will be stored in the database as the encrypted form of the user's password.

Storage: Store the salt value and hash value separately in corresponding fields of the user record in the database.

Verification: When a user logs in, the system retrieves the salt value and hash value associated with the account from the database. It combines the user's input password with the retrieved salt value and hashes it again. the newly generated hash value is then compared with the hash value stored in the database. If they are identical, the password verification is successful.

Even for the same password, due to the unique salt value, the resulting hash value will be different, increasing the difficulty of cracking. Additionally, the encrypted password cannot be decrypted back to its original form, further protecting user privacy.

3.3.2. NTRU-MPS Signature Mechanism

The NTRU-MPS signature mechanism is used during the registration and login process to verify the integrity of messages and the identity of the sender, thus preventing security threats such as replay attacks. the implementation steps are as follows:

Key Generation: During the registration process, the system generates a pair of NTRU-MPS public and private keys for each user. the public key is used to verify signatures, while the private key is used to generate signatures.

Registration Information Signing: After the user submits their registration information, the system signs the registration information using the user's private key. the signature is then sent along with the registration information to the server for verification and storage.

Signature Verification: When the server receives the registration information and the signature, it uses the user's public key to verify the validity of the signature.

If the signature verification passes, the registration information is considered authentic and unmodified, and the registration process continues.

Login Verification: During user login, the system may also require the user to sign the login request and send the signed request to the server. the server then uses the user's public key to verify the signature of the login request, ensuring the authenticity of the request and preventing replay attacks.

NTRU-MPS signatures are based on lattice cryptography, which offers high security and computational efficiency. Through signature verification, the integrity of messages and the identity of the sender can be ensured, effectively defending against security threats such as replay attacks.

3.3.3. Combination of Dual Verification

Combining the salted hashing mechanism with the NTRU-MPS signature mechanism enables dual verification of user identity during the registration and login process, ensuring the security and authenticity of user information. Specifically, during registration, the system not only encrypts the user's password using the salted hashing mechanism but also verifies the integrity and authenticity of the registration information using the NTRU-MPS signature mechanism. During login, the system verifies both the correctness of the user-entered password and the validity of the signature of the login request, ensuring that only legitimate users can successfully log in.

This dual verification mechanism significantly enhances the security of user identity authentication, effectively preventing security threats such as password guessing and replay attacks.

4. Summary

In mobile payment systems, NTRU-MPS digital certificate technology is designed as one of the core security components, integrated into various stages such as user registration, device binding, transaction authentication, data encryption and decryption. the Certificate Authority is responsible for generating and distributing NTRU-MPS-based public and private key pairs, and creating digital certificates that contain the public key, user identity information, validity period, and other content. These certificates are signed using the CA's private key to ensure their authenticity and immutability. the mobile payment app incorporates an NTRU-MPS support module, enabling users to store their private keys, manage certificates, and use their private keys for signature authentication or decryption operations during transactions.

Furthermore, the mobile payment app is also capable of verifying signatures from the payment platform or other participants, ensuring data integrity and trustworthiness of its sources. As the intermediary in transactions, the payment platform utilizes NTRU-MPS technology to validate the validity of user certificates, decrypt transaction request data, and re-encrypt and sign transaction results, thereby ensuring the security and integrity of data transmission. Backend services, including databases and business logic processing services, are designed to support NTRU-MPS encryption and decryption operations, safeguarding the storage and processing of sensitive data.

The NTRU algorithm is based on lattice theory [5], and its security does not rely on traditional challenges such as large number factorization or discrete logarithms, making it considered effective in resisting the threat of quantum computing. This enables digital certificate technology based on NTRU-MPS to maintain high security even in the future era of quantum computing. Combining the salted hashing mechanism with the NTRU-MPS signature mechanism, this dual verification mechanism significantly enhances the security of user identity authentication, effectively defending against traditional security threats such as man-in-the-middle attacks, replay attacks, and data tampering.

Acknowledgments

Project: Chongqing Municipal Education Committee's Scientific and Technological Research Project in 2020.

Research and Implementation of a Secure and Efficient Mobile Payment System Based on Resistance to Quantum Computing Attacks, Project Number: KJQN202004008.

References

[1] Silverman J H. Almost inverses and fast NTRU key creation [R]. NTRU cryptosystems technical report 014, 1999.

[2] Gama N, Howgrave-Grahamn, Nguyenpq. Symplectic lattice reduction and NTRU [C]. In: Advances in Cryptology—Eurocrypt 2006. Springer Berlin Heidelberg, 2006:233–253.

[3] Howgrave-Graham N, Nguyen P Q, Pointcheval D, et al. the impact of decryption failures on the security of NTRU encryption [C]. In: Advances in Cryptology—CRYPTO 2003. Springer Berlin Heidelberg, 2003:226–246.

[4] Duan Ran, Gu Chunxiang, Zhu Yuefei, et al. Efficient Identity-Based Fully Homomorphic Encryption Scheme on NTRU Lattice [J]. Journal on Communications, 2017, 38(1):66-75.

[5] Hoffstein J, Howgrave-Graham N, Pipher J, et al. NTRU-Sign: digital signatures using the NTRU lattice [C]//RSA Conference on the Cryptographers'Track, 2002:122-140.