Mobile authentication scheme based on QKD and IBE

Meiling Chu¹, Meng Wu²
¹School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China
²College of Telecommunications & Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210023, China

Corresponding author and e-mail: Meng Wu, wum@njupt.edu.cn

Abstract. In order to handle the safety problems in mobile communication systems, a mobile identity authentication scheme based on QKD and IBE is proposed. First, the quantum key distribution technology is introduced to handle the safety problems between the private key generator and the cloud services. Next, the IBE algorithm is introduced to encrypt IMSI which makes the scheme more flexible and more efficient. Finally, the quantum time parameter is proposed to manage users’ secret key. Comparing with the existing schemes, the proposed scheme can make full use of the advantages of the QKD and IBE. The mobile identity authentication scheme based on QKD and IBE can be more safe and more efficient.

1. Introduction
With the continuous development of mobile networks and the rapid update of mobile devices, users can easily access a wealth of mobile services by smart mobile devices. [1] Typical applications include mobile payment systems. Users only need to carry a smart phone when going out without a wallet [2]. While enjoying the convenience brought by mobile services, users also face serious threats: network attackers always try to hack users' devices to obtain personal benefits. For example, an attacker may pretend to be a valid user to conduct fraudulent transactions in a mobile payment system. Once successful, he can access the service for free [3]. The arrival of the next generation of mobile networks will not only realize the communication between people, but also the communication between things, between people and things, which will make the "Internet of Everything" [4] truly realized. This will usher in more mobile network users, so the issue of identity authentication of mobile network users needs more attention.

In the mobile network defined by 3GPP [5], users have many identities, such as International Mobile Subscriber Identity (IMSI), International Mobile Equipment Identity (IMEI), Mobile Station International Subscriber Directory Number (MSISDN) and so on. [6] Among these user identities, the International Mobile Subscriber Identity (IMSI) is the focus of the identity authentication process, because the IMSI must be used when a user of a mobile network needs to communicate with other mobile networks. When IMSI first accesses the service network, it lacks confidentiality protection. At the 2019 Network and Distributed System Security Seminar (NDSS), researchers Tian Cong et al. [7] pointed out the network vulnerabilities of 4G and 5G LTE protocols, that is, remote attackers bypass the security protection implemented by 4G and 5G re-enable IMSI capture devices such as "Singrays" to intercept user calls and track their location. Even though 3GPP and academia have made a lot of
efforts to solve this problem, for example, 3GPP [5] stipulates that in order to prevent IMSI-Catcher from intercepting mobile phone users, in most cases, the communication between mobile phones and the network will use randomly generated temporary Identification code (TMSI) of mobile users instead of IMSI. However, Arapinis et al. [8] pointed out that TMSI needs to be encrypted for transmission, the identity authentication process will still be attacked due to the lack of precise instructions. It can be seen that it is a challenging problem to find out a mobile network identity authentication scheme to hide the IMSI.

At present, most identity authentication schemes are based on classic encryption systems. The security of traditional public key cryptosystems such as RSA and elliptic curve cryptosystems depends on the difficulty of factorization of large integers or discrete logarithms. However, these mathematical problems mentioned above can be easily solved by applying Shor's algorithm with quantum computers [9]. In the near future, these schemes are vulnerable to attacks from cyber-catchers equipped with quantum computers. [10] Therefore, an identity authentication scheme based on quantum encryption will be more critical than ever. Quantum encryption [11] allows the exchange of keys to follow the laws of physics, which uses qubits instead of bits to transmit encryption keys. The most famous field in quantum cryptography is quantum key distribution. [12] A shared key is established between two parties without any others to know the key, which transmitted by quantum communication. And then, encrypt the actual data using classical encryption techniques. The main advantages of quantum key distribution are that it is safe and immune to quantum attacks, because its strength lies not in the complexity of mathematics, but in its physical properties. Quantum information cannot be copied, and the measurement of quantum information changes the state of quantum information permanently. [13]

These physical properties prevent any eavesdropper from reading and copying quantum information. Domestic and foreign scholars have done a lot of research on mobile network identity authentication. Cui et al. [14] proposed a blockchain-based IoT multi-sensor network authentication scheme. A hybrid blockchain model is formed between different nodes, which realizes mutual authentication of node identities in various communication scenarios, but cannot withstand quantum attacks. Malik et al. [15] proposed a blockchain-based vehicle network authentication and revocation framework. This framework not only reduces the reliance on the authentication of trusted institutions, reduces the computational and communication costs, but also can update quickly the status of deactivated vehicles in the shared blockchain ledger, and provides distributed and decentralized security. However, when vehicles get their fake ids from a certification authority (CA) out of sync, network catchers can pretend to be fake base stations to obtain information about user identities. Yao et al. [16] proposed a certificate status verification scheme based on blockchain and with privacy protection function, which is used for the storage and management of massive terminal certificates. This scheme effectively prevents attackers from tampering with the terminal identification, but it has large the credential storage burden. Poh et al. [17] proposed a plan to protect privacy, namely, the Home of Privacy. It supports authentication, secure data storage and query smart home systems. This scheme is a new type of lightweight entity and key exchange protocol. However, network attackers can still steal user privacy information through parameters in user positioning. Zhang et al. [18] introduced a robust and universal 5G HetNets seamless switching authentication protocol. This mutual authentication and key protocol utilizes the trapdoor collision property of the chameleon hash function to support anonymous handovers. But the authentication protocol is not very user-friendly, nor is it absolutely safe. Shen et al. [19] proposed a content-centric group user authentication scheme to ensure the security and accuracy of shared data. Regular operations in the network will not be affected or damaged by events that occur during the authentication process. However, as the number of users increases, the amount of calculation for updating and revoking the user identity list will cause the authentication system to have high latency and be vulnerable to attacks. Karati et al. [20] proposed a lightweight identity-based authentication data sharing protocol to provide secure data sharing between geographically dispersed physical devices and clients. Under the assumption of the hardness of the strong DiffieHellman (SDH) problem, it is proved that the protocol can resist the selected ciphertext attack (CCA). However, it does not prove that the protocol can resist other attacks. Ma et al. [21]
proposed eye movement and identity verification based on iris recognition. Remote operators use recorded eye movement trajectories and randomly selected iris images for identity verification. This scheme provides secure identity verification. But there are no attacks that can be resisted through formal security analysis.

2. Quantum key distribution
Quantum key distribution is a highly secure communication method based on the basic principles of quantum mechanics. The quantum key distribution proposed based on the principle of quantum non-cloning [22] is unbreakable. The important role of quantum key distribution is that any third party that tries to eavesdrop on the key will be noticed by the communicating parties. Quantum key distribution protocols mainly include BB84, B92 and E91 [23]. Among them, the earliest and most common protocol is BB84. The BB84 protocol [24] was proposed by Bennett and Brassard in 1984, using two pairs of state bases that are not orthogonal to each other and cannot be completely identified. Alice randomly generates a bit, then randomly selects a base to prepare a quantum state, and then transmits the prepared quantum state to Bob through a quantum channel and repeats this process many times. Bob does not know which basis Alice chose when preparing the quantum state. He can randomly select the basis to measure the received quantum state. Bob measures each quantum state he receives and records the selected basis and measurement result. After Bob has measured all the quantum states, he and Alice communicate through a common classical channel. Alice announces the basis chosen when preparing each quantum state. Alice and Bob compare their chosen bases, discard the bits whose bases are different from each other, and restore the remaining bits to their shared key. Using this method to establish a key, it is impossible to eavesdrop on the quantum state in transmission without leaving a trace.

3. Identity-based encryption
Identity-based encryption is a public key encryption method proposed by Shamir in 1984 [25]. Compared with public key encryption commonly used PKI or certificate mechanisms to authenticate public keys, identity-based encryption methods are more flexible and convenient. Because there is no need for any pre-distributed public key in identity-based encryption. The user can simply use the publicly available identity information or any string derived from the user’s identity to generate a public key and encrypt the data. The public key and private key of the recipient are respectively calculated with from the identity of the recipient and the public key and private key of the trusted third party. Whenever the sender and receiver agree on the security context, the sender does not need to authenticate the receiver's public key. On the other hand, it requires a trusted third-party PKG, because PKG knows the private keys of all recipients. The job of PKG is to calculate the corresponding private key based on the public key. The private key of the recipient must be provided to the recipient by the PKG. Unless the identity revoked, it is impossible to revoke the public key in identity-based encryption. In terms of security, Dan Boneh et al. [26] proposed an identity-based encryption scheme based on the Diffie-Hellman problem in 2001. The scheme was based on Weir pairing and proved that it has better ciphertext security in the random oracle model. Clifford Cocks [27] also proposed a new public key cryptosystem in 2001, in which the user's public key is a publicly known value, such as his identity. The cryptosystem is proved to be related to the difficulty of solving the quadratic residual degree problem.

4. Mobile network identity authentication scheme based on quantum key distribution and identity encryption
Based on quantum key distribution technology, combined with identity-based encryption methods, this paper proposes a mobile network identity authentication scheme, as follows.

4.1. Framework design of mobile network identity authentication scheme based on quantum key distribution and identity encryption.
The framework design of mobile network identity authentication scheme based on quantum key distribution and identity encryption is shown in Figure 1. Use quantum key distribution technology and identity-based encryption algorithm to hide IMSI, combined with existing quantum encryption and cloud computing-based solutions [28-30], strengthen the security of user information list transmission through quantum key distribution technology. Using the "quantum time" with quantum physical security characteristics to regularly update the user's private key, combined with the identity encryption algorithm to hide the user's identity IMSI, to achieve a safe and efficient mobile network identity authentication scheme in a cloud computing environment.

**Figure 1.** The framework design.

The framework of the mobile network identity authentication scheme based on quantum key distribution and identity encryption is composed of network users, service networks, PKG, QTG-CLOUD and QKD equipment. Their functions are as follows:

**Network user:** Use the IMSI of the user's own device as the id to calculate the public key and obtain the private key named $\tilde{s}_s i_i T_i$, generated by the PKG, which is defined as follows.

$$\tilde{s}_s i_i T_i = \begin{cases} s_{k_{IMSI,T_0}} & i = 0(\text{generated by PKG}) \\ s_{k_{IMSI,T_i}} & i \geq 0(\text{updated by } Q_{T_i}) \end{cases}$$

The user’s initial private key is generated by PKG. Later in the process of mutual authentication between the user and the service network, QTG-CLOUD updates the quantum time $Q_{T_{id,T_i}}$ corresponding to the user id in each time period and sends it to the user. The user’s private key updates as the quantum time updates.

**Service network:** In the 3GPP network protocol, the authentication server knows the key only in the home network and SIM, the service network cannot authenticate the SIM, so the service network and the SIM initiate a challenge-response protocol, which authenticates the SIM and establishes a session key. The service network obtains the private key $s_{k_{SIM,T_i}}$ from the PKG, and the definition is the same as the private key obtained by the network user.
$$sk_{id,T_i} = \begin{cases} sk_{\text{snid},T_0}, & i = 0 \text{(generate by PKG)} \\ sk_{\text{snid},T_i}, & i \geq 0 \text{(update with } Q_{T_i}) \end{cases}$$

PKG: The home network is responsible for completing the work of the key generator, generating and distributing private keys for network users and service networks. PKG and QTG-CLOUD transmit user's private information such as user update list and revocation list through quantum channel to strengthen the security of the scheme.

QTG-CLOUD: The "quantum time" generator is combined with the cloud. The "quantum time" generator generates and distributes "quantum time" to realize the update of some private keys. The computing tasks of updating users' privacy information such as user update list and undo list transmitted between PKG and QTG-Cloud are completed by the CLOUD.

QKD equipment: Generate quantum keys required for PKG and QTG-CLOUD to transmit user privacy information on quantum channels, which can solve the problem of excessive cloud burden and security attacks. A quantum key distribution device used BB84 protocol [24], which was first proposed and widely used.

4.2. Algorithm description of mobile network identity authentication scheme based on quantum key distribution and identity encryption

The algorithm of the mobile network identity authentication scheme based on quantum key distribution and identity encryption is divided into two stages. The first stage is the generation and distribution of the private key of the user and the service network, as shown in Figure 2, and the second stage is the inquiry-response process of the user and the service network, shown in Figure 3. We use the pi-calculus language [31] to model and introduce the algorithms of these two stages in detail. The pi-calculus language is a formal language, introduced by Abadi and Fournet [31], used to model concurrent processes, especially to simplify reasoning about encryption protocols.

Algorithm 1: Generation and distribution of private keys for users and service networks

1: Init $\equiv d < \text{id}$

2: $d_{ue} \equiv d(x).f_0(^{\text{IMSI}/id}.^{Q_{T_i}}/Q_T)$

3: PKG $\equiv v \ e_{\text{pid}}.v \ d_{\text{pid}}.v \ d_{ue}.d(x).\overline{p\nu} < e_{\text{pid}},d_{\text{pid}},d_{ue},.du(y)$

4: QTG $\equiv v \ id.v \ T_i.T(x).f_0(id,T_i).\overline{q\nu} < Q_{T_i},.\overline{q\nu} < Q_{T_i},.dq(y)$

5: SN $\equiv v \ snid.d(x).\overline{p\nu} < snid,.ds(y)$

6: PKG $\equiv v \ e_{\text{pid}}.v \ d_{\text{snid}}.d(x).\overline{p\nu} < e_{\text{pid}},d_{\text{snid}},.ds(y)$

Step 1.1 PKG generates a public-private key pair $e_{\text{pid}}$ and $d_{\text{pid}}$, and the initial private key $sk_{\text{IMSI},T_0}$ of the network user. In this solution, the home network replaces the PKG. As a trusted third party, the PKG knows the IMSI of the network user and each updated quantum time $Q_{T_i}$

Step 1.2 PKG will distribute the generated primary private key $sk_{\text{IMSI},T_0}$ and PKG public key $e_{\text{pid}}$ to network users. After that, the user's private key is related to the quantum time of each update.

Step 1.3 The QTG part of QTG-CLOUD generates quantum time $Q_{T_i}$ and sends it to the service network.

Step 1.4 The QTG part of QTG-CLOUD generates quantum time $Q_{T_i}$ and sends it to network user. The user whose ID IMSI is revoked will not receive quantum time $Q_{T_i}$

Step 1.5 The service network sends the service network identification $snid$ to PKG.

Step 1.6 PKG generates $sk_{\text{snid},T_0}$, the initial private key of the service network. After that, the private key of the service network is related to each updated quantum time.
Step 1.7 PKG distributes the generated initial private key $s k_{\text{snid},T_0}$ and PKG public key $e_{\text{pid}}$ to the service network.

**Figure 2.** Generation and distribution of private keys of users and service networks.

**Algorithm 2: The challenge-response process of users and service networks**

1: $\text{SN} \leftarrow v \text{snid}.d(x).\overline{u} < \text{snid} >.d(y)$
2: $\text{UE} \leftarrow v \text{id}.v \text{QT}.v \text{hash}.d(x).h(x).\overline{u} < \text{enc}(1MSI/_{/ id}.\text{QT}_{\text{TMST},T}, hash1, e_{\text{snid}})$ >. $d(u(y))$
3: $\text{SN} \leftarrow v d_{\text{snid}}.d(x).\overline{u} \overline{s}$
4: if $\text{dec}(d_{\text{snid}}.\text{enc}(1MSI/_{/ id}.\text{QT}_{\text{TMST},T}, hash1, e_{\text{snid}})) == M$
5: jump to 9th line
6: else $v \text{snid}.d(x).\overline{p} < \text{snid}, \text{enc}(1MSI/_{/ id}.\text{QT}_{\text{TMST},T}, hash1, e_{\text{snid}}) >.d(y)$
7: $\text{PKG} \leftarrow v \text{AV}.v \text{id}.v d_{\text{snid}}.d(x).\overline{p} \overline{s} < \text{AV}.1MSI/_{/ id}.d_{\text{snid}} >.d(p(y))$
8: $\text{UE} \leftarrow d(x)\overline{u} \overline{s} < \text{KPS} - \text{AKA(SN)}.d(u(y))$
9: $\text{SN} \leftarrow v d_{\text{snid}}.d(x).\overline{u} \overline{s}$
10: $< \text{senc}(1MSI/_{/ id}.\text{QT}_{\text{TMST},T}, hash1, hash2, d_{\text{snid}}), \text{enc}(\text{hash2}, e_{\text{ue}})$ >. $d(s(y))$
11: if $\text{dec}(\text{senc}(1MSI/_{/ id}.\text{QT}_{\text{TMST},T}, hash1, hash2, d_{\text{snid}}, e_{\text{snid}})) >. d(s(y))$
12: $\text{UE} \leftarrow v d_{\text{ue}}.d(x).\overline{u} \overline{s} < \text{senc}(1MSI/_{/ id}.\text{QT}_{\text{TMST},T}, hash1, hash2, d_{\text{snid}}) >. d(s(y))$
13: $\text{Success}$
14: else $\text{Fail}$
Step 2.1 The service network broadcasts its own identification snid.
Step 2.2 5G network users send $E(\text{IMSI}||Qt_{id,T},||\text{Hash1},e_{snid})$ to the service network.
Step 2.3 If the service network can find the private key $d_{snid}$ that meets the requirements, skip to Step 2.8, otherwise continue to Step 2.4.
Step 2.4 The service network sends its own identification snid and $E(\text{IMSI}||Qt_{id,T},||\text{Hash1},e_{snid})$ to PKG.
Step 2.5 PKG generates vector AV for KPS-AKA authentication.
Step 2.6 PKG sends AV, IMSI, $sk_{snid,T_t}$ to the service network.
Step 2.7 The user and the service network perform EAP-AKA authentication.
Step 2.8 The service network decrypts the message from the user in Step 2.2 and calculates the user's public key.
Step 2.9 The service network sends $S(\text{IMSI}||\text{Hash1}||\text{Hash2},sk_{snid,T_t})$ and $E(\text{Hash2},e_{ue})$ to the user. The user verifies the signature with the public key of the service network.
Step 2.10 The user sends a signature $S(\text{IMSI}||\text{Hash1}||\text{Hash2},sk_{IMSI,T_t})$ to the service network, and the service network uses the user's public key to verify the signature. If the user and the service network can authenticate each other, it means that the authentication is successful.

![Diagram showing the request-response process for users and service networks.]

**Figure 3.** The request-response process for users and service networks.
5. Simulation experiment and analysis
We analyzed and verified the security and efficiency of the mobile network identity authentication scheme based on quantum key distribution and identity encryption by comparing with the existing schemes and combining with the Matlab tool simulation scheme.

5.1. Security
Compared with the existing schemes, the proposed mobile network identity authentication scheme has advantages in security: it can prevent attackers from cracking attacks and stealing user identity information; it can prevent illegal users from using fake base stations to create fake private keys to impersonate legitimate users.

5.1.1. Prevent attackers from cracking and stealing user identity information. In traditional mobile system identity authentication schemes, most of them are modeled under the assumption that the transmission channel is safe. However, this is not the case in reality. Considering the ever-changing complexity of the network, it still occurs that attackers crack the system and steal user identity information. And the security of the traditional mobile system identity authentication scheme is greatly reduced. In the proposed mobile network identity authentication scheme, quantum key distribution technology is introduced to distribute quantum keys to the key generator and quantum time generator-cloud. The quantum key is used to encrypt the list of user identity information. The key generator and quantum time generator-cloud can be transmitted through a quantum channel. According to quantum no-cloning theorem and other quantum physical characteristics in Heisenberg's uncertainty principle [32], we can effectively prevent attackers from cracking attacks and stealing User identity information to improves the security of existing solutions.

5.1.2. Prevent illegal users from using fake base stations to create fake private keys to impersonate legitimate users. In the proposed mobile network identity authentication scheme, "quantum time" with quantum physical characteristics is introduced to replace the traditional time parameters based on identity encryption, which effectively reduces the possibility of illegal users creating fake private keys. In addition, the "quantum time" logo is constantly updated over time, which coincides with the highest security requirement of classic encryption algorithms, "one time one secret". Illegal users cannot steal the "quantum time" parameters or create a fake private key to impersonate a legitimate user.

5.2. High efficiency
In order to verify the efficiency of the QKD-IBE certification scheme, here is a performance comparison between the scheme [33-35] and the QKD-IBE certification scheme. $T_p$, $T_e$, $T_s$, $T_h$ respectively represent the time cost of point multiplication, modular exponentiation, symmetric encryption and hashing. Other lightweight calculations such as $\oplus$ and $|$ are not considered. For the sake of generality, it is assumed that the output size of points on the elliptic curve, random numbers, timestamps, user identification IDs, keys, and hash functions are all 160 bits, and the size of points in the limited group is 1024 bits. The calculation and communication costs of the authentication phase are mainly considered, because this phase is the main part of the scheme, and the execution frequency is much higher than other phases.
Table 1. Computation cost comparison in different schemes.

|                | computation overhead       | service network     |
|----------------|---------------------------|---------------------|
| Byun [33]      | $5T_u + T_s + 5T_h$       | $5T_u + T_s + 3T_h$ |
| Wang [34]      | $3T_p + 7T_h$             | $4T_p + 6T_h$       |
| Khan [35]      | $2T_s + 3T_h$             | $4T_s + 4T_h$       |
| QKD-IBE        | $3T_s + 3T_h$             | $5T_s + 4T_h$       |

![Figure 4. Communication overhead comparison in different schemes.](image)

It can be seen from Table 1 and Figure 4 that the QKD-IBE scheme is much more efficient than Byun’s scheme [33], but it is slightly less efficient than the scheme of Wang and Khan et al. [34-35]. Considering that the QKD-IBE scheme has overcome various security deficiencies [34-35], it can avoid sacrificing some extra efficiency. All in all, since the proposed scheme maintains all the advantages and eliminates the current safety flaws, it is safer, so it is very promising in practical applications. The mobile network identity authentication technology is an important guarantee for the security of data transmission in the Internet, the Internet of Things and various heterogeneous networks. The identity authentication technology realizes the integrity protection of the identity and privacy information of all devices or users connected to the network and the integrity of information transmission. This is the security core of all networks. In a heterogeneous network environment, the resources of users or devices are more severely restricted. Identity authentication technology based on traditional cryptosystems is no longer secure, and identity authentication technology based on quantum key distribution is more promising.

6. Conclusions

This paper uses quantum distribution technology and identity-based encryption methods to propose a mobile network identity authentication scheme. The framework design and authentication algorithm process of the authentication scheme are given, and the safety and efficiency of the authentication scheme are discussed by comparing with the existing schemes and combining the simulation scheme with Matlab tools. Compared with the classic mobile network identity authentication scheme, the security of we proposed mobile network identity authentication scheme based on quantum distribution technology and identity encryption method is significantly improved.
Compared with the classic mobile network identity authentication scheme that uses a pseudonym to hide the IMSI or encrypts the IMSI based on public key encryption to ensure the security of the authentication process, the QKD-IBE authentication scheme introduces quantum distribution technology and identity-based encryption methods. Quantum encryption guarantees the higher security of the authentication scheme with its "non-clonability". The identity-based encryption method does not need to pre-distribute the public key, and directly uses the mobile user's unified identity identifier IMSI as the public key, making the authentication scheme more flexible and convenient.

References
[1] Zhu H, Hu J, Chang S, et al. ShakeIn: Secure user authentication of smartphones with single-handed shakes[J]. IEEE transactions on mobile computing, 2017, 16(10): 2901-2912.
[2] Zhang Y, Xu C, Li H, et al. PROTECT: efficient password-based threshold single-sign-on authentication for mobile users against perpetual leakage[J]. IEEE Transactions on Mobile Computing, 2020.
[3] Miao Y, Ma J, Liu X, et al. Practical attribute-based multi-keyword search scheme in mobile crowdsourcing[J]. IEEE Internet of Things Journal, 2017, 5(4): 3008-3018.
[4] Ji Xinxing, Huang Kaizhi, Jin Liang, et al. Research overview of 5G safety Technology [J]. mobile communication, 2019.
[5] Ahn S, Park S I, Lee J Y, et al. Cooperation Between LDM-Based Terrestrial Broadcast and Broadband Unicast: On Scalable Video Streaming Applications [J]. IEEE Transactions on Broadcasting, 2020.
[6] Saxena N, Shen H, Komninos N, et al. BVPSMS: A batch verification protocol for end-to-end secure SMS for mobile users [J]. IEEE Transactions on Dependable and Secure Computing, 2018.
[7] Tian Cong, WU Zhen, LUO Wei, et al. Research on side Channel Attack and Defense Methods based on 4G and 5G Networks [C]/ 2019 Guangdong Communication Youth Forum. 0.
[8] Arapinis M, Mancini L I, Ritter E, et al. Privacy through Pseudonymity in Mobile Telephony Systems[C]/NDSS. 2014.
[9] Xin G, Han J, Yin T, et al. VPQC: A Domain-Specific Vector Processor for Post-Quantum Cryptography Based on RISC-V Architecture [J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2020.
[10] Zhang X, Zhao J, Xu C, et al. DOPIV: Post-quantum secure identity-based data outs ourcing with public integrity verification in cloud storage [J]. IEEE Transactions on Services Computing, 2019.
[11] Abd El-Latif A A, Abd-El-Atty B, Mazurczyk W, et al. Secure data encryption based on quantum walks for 5G Internet of Things scenario[J]. IEEE Transactions on Network and Service Management, 2020, 17(1): 118-131.
[12] Geihs M, Nikiforov O, Demirel D, et al. The status of quantum-key-distribution-based long-term secure internet communication [J]. IEEE Transactions on Sustainable Computing, 2019.
[13] Cao Y, Zhao Y, Li J, et al. Multi-Tenant Provisioning for Quantum Key Distribution Networks with Heuristics and Reinforcement Learning: A Comparative Study[J]. IEEE Transactions on Network and Service Management, 2020, 17(2): 946-957.
[14] He D. An efficient remote user authentication and key agreement protocol for mobile client – server environment from pairings [J]. Ad Hol Networks, 2012, 10(6): 1009-1016.
[15] Ni J, Lin X, Shen X S. Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT[J]. IEEE Journal on Selected Areas in Communications, 2018, 36(3): 644-657.
[16] YAO Shixiong, CHEN Jing, HE Kun, et al. PBCert: Privacy-Preserving Blockchain-based Certificate Status Validation Toward Mass Storage Management[J]. IEEE Access, 2018, 7: 6117-6128.
[17] Yu J, Wang G, Mu Y, et al. An efficient generic framework for three-factor authentic cation with provably secure instantiation[J]. IEEE transactions on information forensics and security, 2014, 9(12): 2302-2313.

[18] Zhang Y, Xu C, Li H, et al. PROTECT: efficient password-based threshold single-sign-on authentication for mobile users against perpetual leakage[J]. IEEE Transactions on Mobile Computing, 2020.

[19] Luo Y, Cao J, Ma M, et al. DIAM: Diversified Identity Authentication Mechanism for 5G Multi-Service System[C]//2019 International Conference on Computing, Networking and Communications (ICNC). IEEE, 2019: 418-424.

[20] Karati A, Amin R, Islam S K H, et al. Provably secure and lightweight identity-based authenticated data sharing protocol for cyber-physical cloud environment [J]. IEEE Transactions on Cloud Computing, 2018.

[21] Ma Z, Yang Y, Liu X, et al. Emir-auth: Eye-movement and iris based portable remote authentication for smart grid[J]. IEEE Transactions on Industrial Informatics, 2019.

[22] Wootters W K, Zurek W H. A single quantum cannot be cloned[J]. Nature, 1982, 299(5886): 802-803.

[23] Wikipedia. Quantum key distribution[EB/OL]. (2020-9-16)[2020-11-4].://en.wikipedia.org/wiki/Quantum_key_distribution

[24] Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol[J]. Physical review letters, 2000, 85(2): 441.

[25] Shamir A. Identity-based cryptosystems and signature schemes[C]//Workshop on the theory and application of cryptographic techniques. Springer, Berlin, Heidelberg, 1984: 47-53.

[26] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[C]//Annual international cryptology conference. Springer, Berlin, Heidelberg, 2001: 213-229.

[27] Cocks C. An identity based encryption scheme based on quadratic residues[C]//IMA international conference on cryptography and coding. Springer, Berlin, Heidelberg, 2001: 360-363.

[28] Wang X A, Ma J, Xhafa F, et al. Cost-effective secure E-health cloud system using identity based cryptographic techniques[J]. Future Generation Computer Systems, 2017, 67: 242-254.

[29] Li J, Li J, Chen X, et al. Identity-based encryption with outsourced revocation in cloud computing[J]. Ieee Transactions on computers, 2013, 64(2): 425-437.

[30] Han Jiawei, Liu Yanheng, SUN Xin, et al. Identity Encryption Scheme based on Quantum Key and Cloud Service [J].Journal of Jilin University (Engineering Science), 2018, 48(2): 551-557.

[31] Abadi M, Fournet C. Mobile values, new names, and secure communication [J]. ACM Sigplan Notices, 2001, 36(3): 104-115.

[32] Raviteja P, Hong Y, Viterbo E, et al. Practical pulse-shaping waveforms for reduced-cyclic-prefix OTFS[J]. IEEE Transactions on Vehicular Technology, 2018, 68(1): 957-961.

[33] Byun J W. Privacy preserving smartcard-based authentication system with provable security [J]. Security and Communication Networks, 2015, 8(17): 3028-3044.

[34] Wang D, Cheng H, He D, et al. On the challenges in designing identity-based privacy-preserving authentication schemes for mobile devices [J]. IEEE Systems Journal, 2016, 12(1): 916-925.

[35] Khan M, Niemi V. Concealing IMSI in 5G network using identity based encryption[C]//International Conference on Network and System Security. Springer, Cham, 2017: 544-554.