SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

December 2024, Vol. 67, Iss. 12, 222501:1–222501:7
https://doi.org/10.1007/s11432-024-4177-5

Lattice-based access authentication scheme for quantum communication networks

Min WANG[1*] & Gui-Lu LONG[1,2,3,4*]

[1]*Beijing Academy of Quantum Information Sciences, Beijing* 100193*, China;*
[2]*State Key Laboratory of Low-dimensional Quantum Physics and Department of Physics, Tsinghua University, Beijing* 100084*, China;*
[3]*Frontier Science Center for Quantum Information, Beijing* 100084*, China;*
[4]*Beijing National Research Center for Information Science and Technology, Beijing* 100084*, China*

Received 18 April 2024/Revised 18 June 2024/Accepted 21 August 2024/Published online 7 November 2024

Abstract Access authentication scheme plays a foundational role in ensuring the security of communication networks. However, an access authentication scheme with high security and efficiency is still lacking in quantum communication networks. In this paper, we propose a lattice-based access authentication scheme for quantum communication networks in the manner of real-time interaction with the network control center, which could achieve properties of mutual authentication, conditional anonymity, data confidentiality, unforgeability, undeniability, and data integrity. We utilize the digital signature algorithm CRYSTALS-Dilithium and the key-establishment algorithm CRYSTALS-KYBER, both of which have been selected for standardization by the National Institute of Standards and Technology, to realize secure access authentication for users of the quantum communication networks. Specifically, in the quantum secure direct communication network, key-establishment is replaced by the verification of signatures encoded in quantum states. Our results demonstrate the feasibility of establishing a quantum-secure communication network.

Keywords quantum communication, quantum network, access authentication, post-quantum cryptography, network control center

1 Introduction

Benefiting from significant advancements in information technology, communication networks have evolved from local terrestrial systems to integrated space-air-ground platforms, meeting the escalating demands for information exchange. Within these networks, an access authentication scheme with high security and efficiency stands as a cornerstone to ensure the secure information exchange. Recently, numerous access authentication schemes have emerged with properties such as mutual authentication, key establishment, data integrity, unforgeability, and undeniability [1].

In large-scale communication networks, public-key cryptosystems serve as fundamental components of access authentication schemes. The security of traditional access authentication schemes is based on some number-theoretic problems, for instance, the factoring problem. However, the rapid advancement of quantum computing raises concerns about the security of schemes based on the Rivest-Shamir-Adleman (RSA) algorithm and the elliptic curve cryptosystems (ECC) algorithms. To avoid compromising the security of communication networks, substantial research has focused on quantum cryptography [2–4] and post-quantum cryptography (PQC) [5]. Quantum cryptography utilizes quantum principles, such as quantum superposition and entanglement, to construct the quantum communication network. PQC, also known as quantum-resistant cryptography, addresses the security challenges of public-key cryptographic algorithms by tackling computationally difficult problems, even for quantum computers. Achievements have been made in both scientific fields. The quantum communication network has been demonstrated in several studies [6–14]. Recently, researchers have made progress on high-efficiency authentication with the universal hashing authentication code and quantum digital signatures in a local-scale network [15,16].

* Corresponding author (email: wangmin@baqis.ac.cn, gllong@tsinghua.edu.cn)

© Science China Press 2024

Meanwhile, the National Institute of Standards and Technology (NIST) has selected one public-key encryption and key-establishment algorithm and three digital signature algorithms for standardization [17]. Until now, CRYSTALS-KYBER remains the only public-key encryption and key-establishment algorithm to be standardized, and CRYSTALS-Dilithium is recommended as the primary algorithm for digital signature. However, quantum cryptography alone cannot support a quantum-secure access authentication scheme. Therefore, the integration of quantum cryptography and post-quantum cryptography emerges as an inevitable way to realize practical quantum communication networks.

As an important branch of quantum cryptography, quantum secure direct communication (QSDC) allows direct transmission of secret messages encoded in quantum states. It is meaningful to construct a large-scale QSDC network. As demonstrated in [10,18], the integration of quantum cryptography and post-quantum cryptography offers a pragmatic avenue for realizing the quantum-secure classical repeaters. However, the quantum-secure access authentication scheme for the QSDC network is still missing. Here, we propose a lattice-based access authentication scheme for quantum communication networks in the manner of real-time interaction with the network control center (NCC). Specifically, two lattice-based post-quantum algorithms, namely CRYSTALS-Dilithium and CRYSTALS-KYBER, are utilized in our access authentication scheme. Since QSDC enables the direct transmission of messages, we can realize a successful access authentication by verifying signatures encoded in quantum states. As a consequence, compared with conventional access authentication schemes, our approach obviates the need for a key-establishment process. Importantly, our access authentication scheme achieves the desired properties of mutual authentication, conditional anonymity, data confidentiality, unforgeability, undeniability, and data integrity. Together with the results in [10,18], we show that it is feasible to establish a full quantum-secure large-scale quantum network.

2 Access authentication for quantum communication networks

In a communication network, users get access to it by implementing the access authentication scheme which is composed of the digital signature algorithm and public-key encryption and key-establishment algorithm. Here, we propose a lattice-based access authentication scheme for quantum communication networks in the manner of real-time interaction with the NCC, which is suitable for space information networks [1,19,20]. NCC serves as a pivotal component in communication networks, which is responsible for registering communication devices and assigning public keys to legitimate devices. For a communication network with N users, the size of public keys stored at NCC is $O(N)$, instead of $O(N^2)$ in the directly connected network. To illustrate the scheme clearly, we assign two users (Alice and Bob) for simplicity in our description.

We take advantage of the recent achievements in post-quantum cryptography to design the access authentication scheme of the quantum communication network. To eliminate the security loopholes caused by quantum computers, NIST has initiated a public selection process for post-quantum algorithms. Until now, NIST has selected a key-establishment algorithm along with three digital signature algorithms for standardization. Notably, the primary digital signature algorithm recommended by NIST is CRYSTALS-Dilithium, while the key-establishment algorithm set for standardization is CRYSTALS-KYBER.

CRYSTALS-Dilithium [21,22], based on the "Fiat-Shamir with Aborts" approach, exhibits strong unforgeability under chosen message attacks (SUF-CMA) in the random oracle model. Its security relies on the hardness of standard learning-with-errors problems and short-integer-solution problems in module lattices (MLWE and MSIS). Both MLWE and MSIS are considered challenging problems even for quantum computers. For CRYSTALS-Dilithium, the main procedures contain key generation, signing, and verification, which are denoted as GenD(), SigD(Sk, M), and Verify(Pk, M, σ), respectively.

$$
\begin{aligned}
\mathrm{GenD}():\quad & \boldsymbol{A}' \longleftarrow R_{q'}^{k'\times l}, \quad (\boldsymbol{s}_1,\boldsymbol{s}_2) \longleftarrow S_{\eta'}^{l}\times S_{\eta'}^{k'},\\
& \boldsymbol{t}' = \boldsymbol{A}'\boldsymbol{s}_1+\boldsymbol{s}_2,\\
& \text{return} \quad (\mathrm{Pk}=(\boldsymbol{A}',\boldsymbol{t}'),\mathrm{Sk}=(\boldsymbol{s}_1,\boldsymbol{s}_2)),\\
\mathrm{SigD}(\mathrm{Sk},M):\quad & \boldsymbol{y} \longleftarrow S_{\gamma_1-1}^{l}, \quad \boldsymbol{w}_1=\mathrm{HighBits}(\boldsymbol{A}'\boldsymbol{y},2\gamma_2),\\
& c=H(M||\boldsymbol{w}_1), \quad \boldsymbol{z}=\boldsymbol{y}+c\boldsymbol{s}_1,\\
& \text{if} \quad ||\boldsymbol{z}||_\infty<\gamma_1-\beta \quad \text{and} \quad ||\mathrm{LowBits}(\boldsymbol{A}'\boldsymbol{y}-c\boldsymbol{s}_2,2\gamma_2)||_\infty<\gamma_2-\beta,\\
& \text{return} \quad \sigma=(\boldsymbol{z},c),
\end{aligned}
$$

$$\begin{aligned}\text{Verify}(\text{Pk}, M, \sigma): \quad & \boldsymbol{w}_1' = \text{HighBits}(\boldsymbol{A}'\boldsymbol{z} - c\boldsymbol{t}', 2\gamma_2),\\ & \text{accept} \quad \text{if} \quad [||\boldsymbol{z}||_\infty < \gamma_1 - \beta] \quad \text{and} \quad [c = H(M||\boldsymbol{w}_1')].\end{aligned}$$

Here, $\boldsymbol{A}'$ is a matrix with dimension of $k' \times l$, the entries of which are polynomials in the ring $R_{q'} = Z_{q'}[X]/(X^n + 1)$. $\boldsymbol{s}_1$ and $\boldsymbol{s}_2$ are secret key vectors randomly sampled from $R_{q'}$ with the coefficients at most η' (denoted as $S_{\eta'}^{l/k'}$). The algorithm first generates a polynomial vector $\boldsymbol{y}$ with coefficients at most $\gamma_1 - 1$. Then, the signer calculates $\boldsymbol{A}'\boldsymbol{y}$ and keeps the high-order bits. H is a hash function. To guarantee security and correctness, the rejection sampling is used to extract the signature $\sigma = (\boldsymbol{z}, c)$. The verification algorithm accepts the signature if two conditions are satisfied simultaneously. The first is that the coefficients of $\boldsymbol{z}$ are less than $\gamma_1 - \beta$. The second one is that c is the hash of the message and the high-order bits of $\boldsymbol{A}'\boldsymbol{z} - c\boldsymbol{t}'$.

CRYSTALS-KYBER [23,24], as an indistinguishability-under-chosen-ciphertext-attack (IND-CCA) secure key-encapsulation mechanism (KEM), follows a two-stage construction approach. It first designs an indistinguishability-under-chosen-plaintext-attack (IND-CPA) secure public-key encryption scheme and then utilizes the Fujisaki-Okamoto (FO) transform to build the IND-CCA KEM. The security of CRYSTALS-KYBER relies on the computational hardness of standard MLWE. For CRYSTALS-KYBER, the public-key encryption scheme includes key generation, encryption, and decryption, which are denoted as GenK(), EncK(Pk, M), and DecK(Sk, c), respectively.

$$\begin{aligned}\text{GenK}(): \quad & \boldsymbol{A} \longleftarrow R_q^{k\times k}, \quad (\boldsymbol{s}, \boldsymbol{e}) \longleftarrow B_\eta^k \times B_\eta^k,\\ & \boldsymbol{t} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e},\\ & \text{return} \quad (\text{Pk} = (\boldsymbol{A}, \boldsymbol{t}), \text{Sk} = \boldsymbol{s}),\\ \text{EncK}(\text{Pk}, M): \quad & (\boldsymbol{r}, \boldsymbol{e}_1, e_2) \longleftarrow B_\eta^k \times B_\eta^k \times B_\eta,\\ & \boldsymbol{u} = \boldsymbol{A}^{\mathrm{T}}\boldsymbol{r} + \boldsymbol{e}_1,\\ & v = \boldsymbol{t}^{\mathrm{T}}\boldsymbol{r} + e_2 + \lceil q/2 \rfloor \cdot M,\\ & \text{return} \quad c = (\boldsymbol{u}, v),\\ \text{DecK}(\text{Sk}, c): \quad & M' = v - \boldsymbol{s}^{\mathrm{T}}\boldsymbol{u}.\end{aligned}$$

Here, $\boldsymbol{A}$ is a matrix with dimension of $k \times k$, the entries of which are polynomials in the ring $R_q = Z_q[X]/(X^n + 1)$. $\boldsymbol{s}$ is the secret key vector, and $\boldsymbol{e}$ is the noise vector. $\boldsymbol{s}$, $\boldsymbol{e}$, $\boldsymbol{r}$, $\boldsymbol{e}_1$, and e_2 are randomly sampled from a centered binomial distribution with parameter η (denoted as B_η).

The public-key key encapsulation mechanism is described as follows:

$$\begin{aligned}\text{EncapK}(\text{Pk}): \quad & m \longleftarrow \{0,1\}^{256},\\ & (\hat{K}, r) = G(H(\text{Pk}), m),\\ & c = \text{EncK}(\text{Pk}, m; r),\\ & K = H(\hat{K}, H(c)),\\ & \text{return} \quad (c, K),\\ \text{DecapK}(\text{Sk}, c): \quad & m' = \text{DecK}(s, c),\\ & (\hat{K}', r') = G(H(\text{Pk}), m'),\\ & c' = \text{EncK}(\text{Pk}, m'; r'),\\ & \text{if} \quad c = c', \quad \text{return} \quad K = H(\hat{K}', H(c)).\end{aligned}$$

Here, m is a 256-bit random value, H and G are hash functions.

Consequently, we choose CRYSTALS-Dilithium and CRYSTALS-KYBER as foundational algorithms to design the access authentication scheme of quantum communication networks.

2.1 Access authentication scheme

The access authentication scheme follows a two-stage process, namely the registration of communication devices and the access authentication.

In the registration stage, communication devices should register at NCC in the following manner.

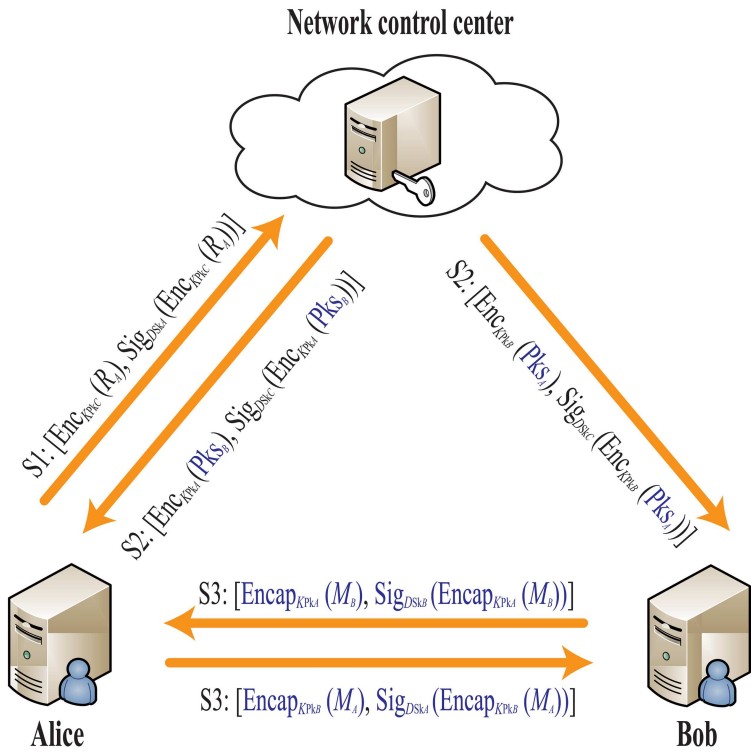

Figure 1 (Color online) Access authentication scheme for the classical secure communication network and quantum key distribution network.

Step 1. Pre-configure public keys of NCC. NCC's public keys of CRYSTALS-KYBER (K_{Pk_C}) and CRYSTALS-Dilithium (D_{Pk_C}) are pre-configured in the communication devices that intend to join into the network.

Step 2. Generate the public and private keys of participants. The participants utilize the CRYSTALS-KYBER algorithm to create the public key for encryption ($K_{\mathrm{Pk}_{A/B}}$) and the private key for decryption ($K_{\mathrm{Sk}_{A/B}}$). Simultaneously, they employ the CRYSTALS-Dilithium algorithm to create the private key for signature ($D_{\mathrm{Sk}_{A/B}}$) and the public key for verification ($D_{\mathrm{Pk}_{A/B}}$).

Step 3. Register public keys at NCC. The participant generates signatures ($\mathrm{Sigs}_{D_{\mathrm{Sk}_{A/B}}}(\mathrm{Pks}_{A/B})$) on the public keys ($\mathrm{Pks}_{A/B}$, including $K_{\mathrm{Pk}_{A/B}}$ and $D_{\mathrm{Pk}_{A/B}}$) with his/her private key of CRYSTALS-Dilithium ($D_{\mathrm{Sk}_{A/B}}$). The public keys $\mathrm{Pks}_{A/B}$ together with the signatures $\mathrm{Sigs}_{D_{\mathrm{Sk}_{A/B}}}(\mathrm{Pks}_{A/B})$ are transmitted to NCC for registration by each participant. The private keys are only known to the corresponding participant of the network. NCC is unaware of the private keys of the participants, so NCC cannot decrypt the communication message between the participants.

In the access authentication stage, as for classical secure communication network and quantum key distribution network, it follows a three-step process shown in Figure 1.

Step 1. Initiate communication request. Alice encrypts the communication request (R_A) with NCC's public key (K_{Pk_C}) and signs the ciphertext with her private key (D_{Sk_A}). Then, she sends the message ($[\mathrm{Enc}_{K_{\mathrm{Pk}_C}}(R_A), \mathrm{Sig}_{D_{\mathrm{Sk}_A}}(\mathrm{Enc}_{K_{\mathrm{Pk}_C}}(R_A))]$) to NCC. NCC verifies the signature with D_{Pk_A} and decrypts the ciphertext with K_{Sk_C} to recover the request.

Step 2. Distribute public keys of CRYSTALS-Dilithium and CRYSTALS-KYBER. According to the request, NCC encrypts Bob's public keys (Pks_B, including K_{Pk_B} and D_{Pk_B}) with Alice's public key (K_{Pk_A}), and signs the ciphertext with its private key D_{Sk_C}. Then, NCC sends the message ($[\mathrm{Enc}_{K_{\mathrm{Pk}_A}}(\mathrm{Pks}_B), \mathrm{Sig}_{D_{\mathrm{Sk}_C}}(\mathrm{Enc}_{K_{\mathrm{Pk}_A}}(\mathrm{Pks}_B))]$) to Alice. Alice verifies the signature with the pre-configured public key of CRYSTALS-Dilithium to confirm the identity of the NCC, and decrypts the received ciphertext to recover Bob's public keys (Pks_B). At the same time, NCC informs Bob of Alice's public keys ($\mathrm{Enc}_{K_{\mathrm{Pk}_B}}(\mathrm{Pks}_A), \mathrm{Sig}_{D_{\mathrm{Sk}_C}}(\mathrm{Enc}_{K_{\mathrm{Pk}_B}}(\mathrm{Pks}_A))$) in the same manner.

Step 3. Establish keys for symmetric cryptosystem. Alice and Bob launch a key exchange protocol based on key-exchange algorithm or KEM ($[\mathrm{Encap}_{K_{\mathrm{Pk}_{A/B}}}(M_{B/A}), \mathrm{Sig}_{D_{\mathrm{Sk}_{B/A}}}(\mathrm{Encap}_{K_{\mathrm{Pk}_{A/B}}}(M_{B/A}))]$) to

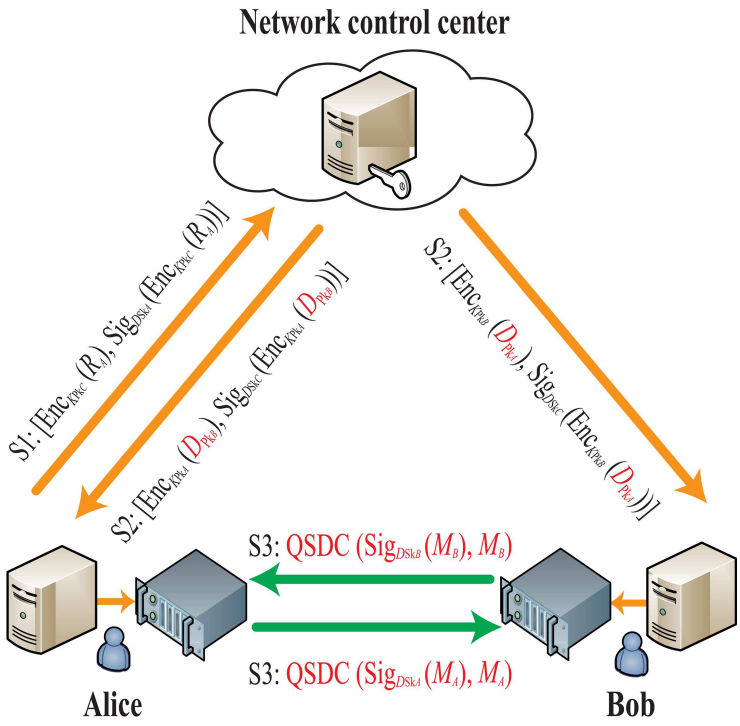

Figure 2 (Color online) Access authentication scheme for the QSDC network.

share a secret key ($M_{A/B}$) for symmetric cryptosystem such as the advanced encryption standard (AES).

However, in the access authentication stage, the QSDC network behaves differently from the classical secure communication network and quantum key distribution network. Benefiting from the direct transmission of secret messages, QSDC could partially substitute the function of key-establishment algorithm CRYSTALS-KYBER in the access authentication scheme. Specifically, only the public keys of CRYSTALS-Dilithium rather than CRYSTALS-KYBER need to be distributed in Step 2, and only the public keys of CRYSTALS-Dilithium are needed in Step 3. Furthermore, we can execute Step 3 by implementing the QSDC protocol.

Here, we implement the DL04 protocol of QSDC [25, 26] as follows: Bob randomly sends qubits generated in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ to Alice; Alice collaborates with Bob to assess the quantum bit error rate (QBER) after randomly selecting and measuring some qubits in either Z or X basis; if the QBER falls below the security threshold, Alice proceeds to encode the message using the remaining qubits, which will subsequently be transmitted back to Bob for decoding.

The proposed access authentication stage for the QSDC network is shown in Figure 2.

Step 1. Initiate communication request. The first step is identical to the classical version.

Step 2. Distribute public keys of CRYSTALS-Dilithium. According to the request, NCC encrypts Bob's public key of CRYSTALS-Dilithium (D_{Pk_B}) with Alice's public key of CRYSTALS-KYBER (K_{Pk_A}), and signs the ciphertext with its private key D_{Sk_C}. Then, NCC sends the message ([Enc$_{K_{\mathrm{Pk}_A}}$(D_{Pk_B}), Sig$_{D_{\mathrm{Sk}_C}}$(Enc$_{K_{\mathrm{Pk}_A}}$(D_{Pk_B}))]) to Alice. Alice verifies the signature to confirm the source of the message, and then decrypts the received ciphertext to recover Bob's public key of CRYSTALS-Dilithium (D_{Pk_B}). Simultaneously, NCC informs Bob of Alice's public key corresponding to CRYSTALS-Dilithium (Enc$_{K_{\mathrm{Pk}_B}}$(D_{Pk_A}), Sig$_{D_{\mathrm{Sk}_C}}$(Enc$_{K_{\mathrm{Pk}_B}}$(D_{Pk_A}))) in the same manner.

Step 3. Verify signatures encoded in quantum states. Alice prepares the qubits and transmits them to Bob. Bob sends prepared qubits to Alice for mutual authentication. Afterwards, Alice and Bob engage in communication to assess the QBER. If the QBER falls below the security threshold, Alice (Bob) proceeds to encode the message ($M_{A(B)}$) and signature on the message (Sig$_{D_{\mathrm{Sk}_{A(B)}}}$($M_{A(B)}$)) into quantum states with the remaining qubits, and transmits them to Bob (Alice), denoted as QSDC(Sig$_{D_{\mathrm{Sk}_{A(B)}}}$($M_{A(B)}$), $M_{A(B)}$). Bob and Alice decode the signature from the received qubits. The message ($M_{A/B}$) can be a string of random numbers or just a reply. Finally, Alice and Bob verify the signature to realize a successful access authentication.

In the access authentication scheme for the QSDC network, the CRYSTALS-KYBER algorithm is utilized to hide the identities of the participants which satisfies the security requirement of conditional anonymity. For a network in which anonymity is not essential, we can eliminate the use of the CRYSTALS-KYBER algorithm and only use the algorithm of CRYSTALS-Dilithium to implement the access authentication in the QSDC network.

After the successful access authentication, the DL04 protocol was implemented to transmit information securely and reliably in the QSDC network.

2.2 Security properties

(1) Mutual authentication. Mutual authentication implies that both parties involved in the communication can verify the legitimacy of the other party. Mutual authentication between participants can be achieved by verifying the signatures with the corresponding public keys of CRYSTALS-Dilithium.

(2) Conditional anonymity. Conditional anonymity indicates that in addition to the legitimate communication parties, only the NCC could disclose the identities of the participants as a third party. The identities are encrypted with NCC's public key, rendering it computationally challenging for an adversary lacking NCC's private key of CRYSTALS-KYBER to decrypt the identities.

(3) Data confidentiality. In the access authentication stage, the privacy information undergoes encryption with the public key of CRYSTALS-KYBER. Furthermore, for the QSDC network, the security of the private information is guaranteed by quantum principles in Step 3.

(4) Unforgeability. Each participant creates a signature using their respective private key of CRYSTALS-Dilithium, and the intended receiver verifies the signature. Only the legitimate participant can produce a valid signature. Thus, it is impossible for adversaries to forge a valid signature without the corresponding private key of CRYSTALS-Dilithium.

(5) Undeniability. Similarly, each participant creates a signature using their own private key of CRYSTALS-Dilithium, and then the intended receiver verifies the signature. This process ensures that only the legitimate participant can create a valid signature. Consequently, each participant cannot deny having sent the signature to the intended receiver, as the signature's validity is tied to their private key.

(6) Data integrity. Each participant signs the encrypted information with their own private key of CRYSTALS-Dilithium, and the intended receiver verifies the signature using the corresponding public key. Once the message is tampered with, the verification will fail.

Benefiting from the above security properties, our access authentication scheme is resistant to protocol attacks such as impersonation attacks, and man-in-the-middle (MitM) attacks.

3 Conclusion

In conclusion, we have proposed a lattice-based access authentication scheme for a quantum communication network in the manner of real-time interaction with the NCC. In this scheme, the digital signature algorithm CRYSTALS-Dilithium and key-establishment algorithm CRYSTALS-KYBER have been utilized. Additionally, an NCC is responsible for registering communication devices and assigning public keys to legitimate devices. Specifically, for the QSDC network, key-establishment is replaced by the verification of signatures encoded in quantum states. The proposed scheme could achieve properties of mutual authentication, conditional anonymity, data confidentiality, unforgeability, undeniability, and data integrity. Together with the results in the literature (e.g., [18]), the access authentication scheme could also assign public keys of CRYSTALS-KYBER for the secure-relayed QSDC network. In the future, we could establish a large-scale quantum-secure communication network with access authentication and secure relay.

Acknowledgements This work was supported by Young Elite Scientists Sponsorship Program by China Association for Science and Technology (Grant No. 2022QNRC001). The authors would like to thank Dr. Guang-Zhao TANG for the fruitful discussions on access authentication and post-quantum cryptography.

References

1 Ma R, Cao J, Feng D, et al. LAA: lattice-based access authentication scheme for IoT in space information networks. IEEE Internet Things J, 2020, 7: 2791–2805
2 Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, 1984. 175–179
3 Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution scheme. Phys Rev A, 2002, 65: 032302
4 Hillery M, Bužek V, Berthiaume A. Quantum secret sharing. Phys Rev A, 1999, 59: 1829–1834

5 National Institute of Standards and Technology. Announcing request for nominations for public-key post-quantum cryptographic algorithms. Federal Register, 2016. https://federalregister.gov/a/2016-30615
6 Wehner S, Elkouss D, Hanson R. Quantum internet: a vision for the road ahead. Science, 2018, 362: eaam9288
7 Li Z Z, Xu G, Chen X B, et al. Efficient quantum state transmission via perfect quantum network coding. Sci China Inf Sci, 2019, 62: 012501
8 Su X L, Wang M H, Yan Z H, et al. Quantum network based on non-classical light. Sci China Inf Sci, 2020, 63: 180503
9 Qi Z, Li Y, Huang Y, et al. A 15-user quantum secure direct communication network. Light Sci Appl, 2021, 10: 183
10 Long G L, Pan D, Sheng Y B, et al. An evolutionary pathway for the quantum internet relying on secure classical repeaters. IEEE Netw, 2022, 36: 82–88
11 Ren S Y, Wang Y, Su X L. Hybrid quantum key distribution network. Sci China Inf Sci, 2022, 65: 200502
12 Wang S, Yin Z Q, He D Y, et al. Twin-field quantum key distribution over 830-km fibre. Nat Photon, 2022, 16: 154–161
13 Zhou L, Lin J, Xie Y M, et al. Experimental quantum communication overcomes the rate-loss limit without global phase tracking. Phys Rev Lett, 2023, 130: 250801
14 Fang K, Zhao J T, Li X F, et al. Quantum NETwork: from theory to practice. Sci China Inf Sci, 2023, 66: 180509
15 Yin H L, Fu Y, Li C L, et al. Experimental quantum secure network with digital signatures and encryption. Natl Sci Rev, 2023, 10: nwac228
16 Cao X Y, Li B H, Wang Y, et al. Experimental quantum e-commerce. Sci Adv, 2024, 10: eadk3258
17 Alagic G, Apon D, Cooper D, et al. Status report on the third round of the NIST post-quantum cryptography standardization process. National Institute of Standards and Technology, 2022. https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413-upd1.pdf
18 Wang M, Zhang W, Guo J, et al. Experimental demonstration of secure relay in quantum secure direct communication network. Entropy, 2023, 25: 1548
19 Xue K, Meng W, Li S, et al. A secure and efficient access and handover authentication protocol for Internet of Things in space information networks. IEEE Int Things J, 2019, 6: 5485–5499
20 Wang C, An J P, Xing C W, et al. A review of covert communication technologies for space information networks. Sci Sin Inform, 2024, 54: 1319–1349
21 Ducas L, Kiltz E, Lepoint T, et al. CRYSTALS-Dilithium: a lattice-based digital signature scheme. IACR Trans Cryptogr Hardw Embed Syst, 2018, 2018: 238–268
22 Bai S, Ducas L, Kiltz E, et al. CRYSTALS-Dilithium algorithm specifications and supporting documentation. 2020. https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022
23 Bos J, Ducas L, Kiltz E, et al. CRYSTALS-KYBER: a CCA-secure module-lattice-based KEM. In: Proceedings of the IEEE European Symposium on Security and Privacy, London, 2018. 353–367
24 Avanzi R, Bos J, Ducas L, et al. CRYSTALS-KYBER: algorithm specifications and supporting documentation. National Institute of Standards and Technology, 2020. https://csrc.nist.gov/CSRC/media/Projects/post-quantum-cryptography/documents/round-3/submissions/Kyber-Round3.zip
25 Deng F G, Long G L. Secure direct communication with a quantum one-time pad. Phys Rev A, 2004, 69: 052319
26 Qi R, Sun Z, Lin Z, et al. Implementation and security analysis of practical quantum secure direct communication. Light Sci Appl, 2019, 8: 22