npj | Quantum Information

www.nature.com/npjqi

ARTICLE OPEN

Check for updates

Experimental authentication of quantum key distribution with post-quantum cryptography

Liu-Jun Wang[1,2,3,9], Kai-Yi Zhang[4,5,9], Jia-Yong Wang[6], Jie Cheng[7], Yong-Hua Yang[6], Shi-Biao Tang[7], Di Yan[4], Yan-Lin Tang[7], Zhen Liu[4], Yu Yu[4,5✉], Qiang Zhang[1,2,8✉] and Jian-Wei Pan[1,2✉]

Quantum key distribution (QKD) can provide information theoretically secure key exchange even in the era of quantum computers. However, QKD requires the classical channel to be authenticated, the current method for which is pre-sharing symmetric keys. For a QKD network of n users, this method requires $C_n^2 = n(n-1)/2$ pairs of symmetric keys to realize pairwise interconnection. In contrast, with the help of a mature public key infrastructure (PKI) and post-quantum cryptography (PQC) with quantum-resistant security, each user only needs to apply for one digital certificate from a certificate authority (CA) to achieve efficient and secure authentication for QKD. We need to assume only the short-term security of the PQC algorithm to achieve long-term security of the distributed keys. Here, we experimentally verified the feasibility, efficiency, and stability of the PQC algorithm in QKD authentication, and demonstrated the advantages when new users join the QKD network. Using the PQC public-key infrastructure, the nodes need to mutually trust only the CA to authenticate each other. QKD combined with PQC authentication will greatly promote and extend the application prospects of quantum-safe communication.

npj Quantum Information (2021)7:67 ; https://doi.org/10.1038/s41534-021-00400-7

INTRODUCTION

Recently, Google claimed to have achieved quantum supremacy[1], a major milestone towards the development of quantum computers. Quantum computing can efficiently solve classical hard problems such as integer factorization and discrete logarithms and demonstrates a quadratic speedup (over classical algorithms) in solving unstructured search problems[2,3], which poses a serious threat to the security of classical cryptographic algorithms based on the complexity of these problems. Boudot et al.[4] recently announced the factoring of RSA-240, an RSA number of 240 decimal digits or 795 bits, as well as solved a discrete logarithm of the same size. New records of this type are constantly being refreshed as the performance of computer hardware increases over time. In the era of quantum computing, there are two kinds of reliable information security mechanism: one is quantum cryptography[5], which mainly includes quantum key distribution (QKD); and the other is post-quantum cryptography (PQC), such as lattice-based cryptography and code-based cryptography, which cannot be effectively cracked by the currently known quantum computing algorithms.

QKD is unconditionally secure based on the principle of quantum mechanics[6–8]. With realistic devices, the security of QKD can also be guaranteed[9]. The experiments and practical applications of QKD have drastically developed. The secure key rate reaches 26.2 Mbps at a channel loss of 4 dB (equivalent to a 20-km-long optical fiber)[10], and the maximum key distribution distance through a practical optical fiber exceeds 500 km[11,12]. The Micius satellite has realized entanglement-based repeaterless QKD between two places on the ground at a distance of 1120 km[13]. Through a trusted relay, several quantum communication networks have been built[14–19], and the "Beijing-Shanghai backbone" quantum communication network spans 2200 km.

Currently, the hardness of most public-key cryptography is based on integer factorization and discrete logarithm problems that are difficult or intractable for conventional computers. However, Shor's[2] quantum algorithm can achieve an exponential speedup in solving these mathematical problems. In 2016, NIST published a report on PQC[20] anticipating that a quantum computer is likely to be built by 2030 that breaks 2000-bit RSA in a few hours and therefore renders the current public-key infrastructure insecure. As a result, in the same year, NIST initiated the "Post-Quantum Cryptography Standardization" process by announcing a call for proposals of quantum-resistant cryptographic primitives including public-key encryption, digital signature, and key exchange algorithms. And the process is expected to release the standardization documents by 2024.

Shannon proved that only one-time-pad encryption can achieve secure message exchange. This requires a symmetric key distribution between the two communicating parties, and the key distribution protocol must be secure; then, both parties can use the symmetric key to encrypt and decrypt messages. In the process of key distribution, the identity legitimacy of both parties must be guaranteed, which is realized by authentication. Conventional encryption and authentication methods do not have provable security and will be vulnerable against Shor algorithm with a quantum computer. PQC can be used for both encryption and authentication and is believed to be secure against Shor algorithm. However, PQC is still not an information theoretically secure method, and it is still an open question whether PQC is secure against other classical or quantum

[1]Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, China. [2]Shanghai Branch, CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai, China. [3]School of Physics and Astronomy and Yunnan Key Laboratory for Quantum Information, Yunnan University, Kunming, China. [4]Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China. [5]Shanghai Qizhi Institute, Shanghai, China. [6]CAS Quantum Network Co., Ltd, Shanghai, China. [7]QuantumCTek Co., Ltd, Hefei, China. [8]Key Laboratory of Space Active Opto-electronics Technology, Chinese Academy of Sciences, Shanghai, China. [9]These authors contributed equally: Liu-Jun Wang, Kai-Yi Zhang. ✉email: yyuu@sjtu.edu.cn; qiangzh@ustc.edu.cn; pan@ustc.edu.cn

algorithm except for Shor algorithm. Therefore, it is believed that PQC is good for short-term security (e.g., authentication) but not for long-term security (e.g., key for coding information). Here, we combine PQC and QKD to achieve the short-term security of authentication and long-term security of keys, and then secure message exchange can be realized with the symmetric keys and one-time-pad encryption.

RESULTS

QKD authentication methods

QKD includes the quantum channel that transmits photons and the classical channel used in post data processing. The unconditional security of QKD does not require the classical channel to be confidential, but requires it to be authenticated; otherwise, a man-in-the-middle attack will occur. The attacker can completely obtain the keys of both parties without being discovered, as shown in Fig. 1a. The processes of QKD that require authentication include: basis sifting, error correction verification, random number transfer needed for privacy amplification, and final key verification[21]. QKD requires two-way authentication between the two parties.

The current secure authentication method is to pre-share a small amount of symmetric seed keys and encrypt (sign) and decrypt (verify) the hash value of classical messages[21], as shown in Fig. 1b. Later, the generated quantum key can be used for authentication. This method can guarantee the information theoretical secure authentication; however, when the number of QKD network users is large, this method is not easy to operate and has the following problems. On the one hand, for a network with two arbitrary users connected, if the number of users is n, then the number of pre-shared key pairs m is

$$m = C_n^2 = \frac{n(n-1)}{2}. \quad (1)$$

Symmetric keys are generally pre-shared face to face. When the number of users is relatively large, the burden of pre-sharing keys is heavy and inefficient. For example, if $n = 100$, then $m = 4950$. At the same time, each user needs to store the authentication key pairs with all other users. The storage, synchronization and management of so many key pairs will increase the complexity and security risk of the network. One solution is to use a trusted relay to form a star-type network, each user connects and pre-shares one key pair only with the trusted relay[17,22], but this

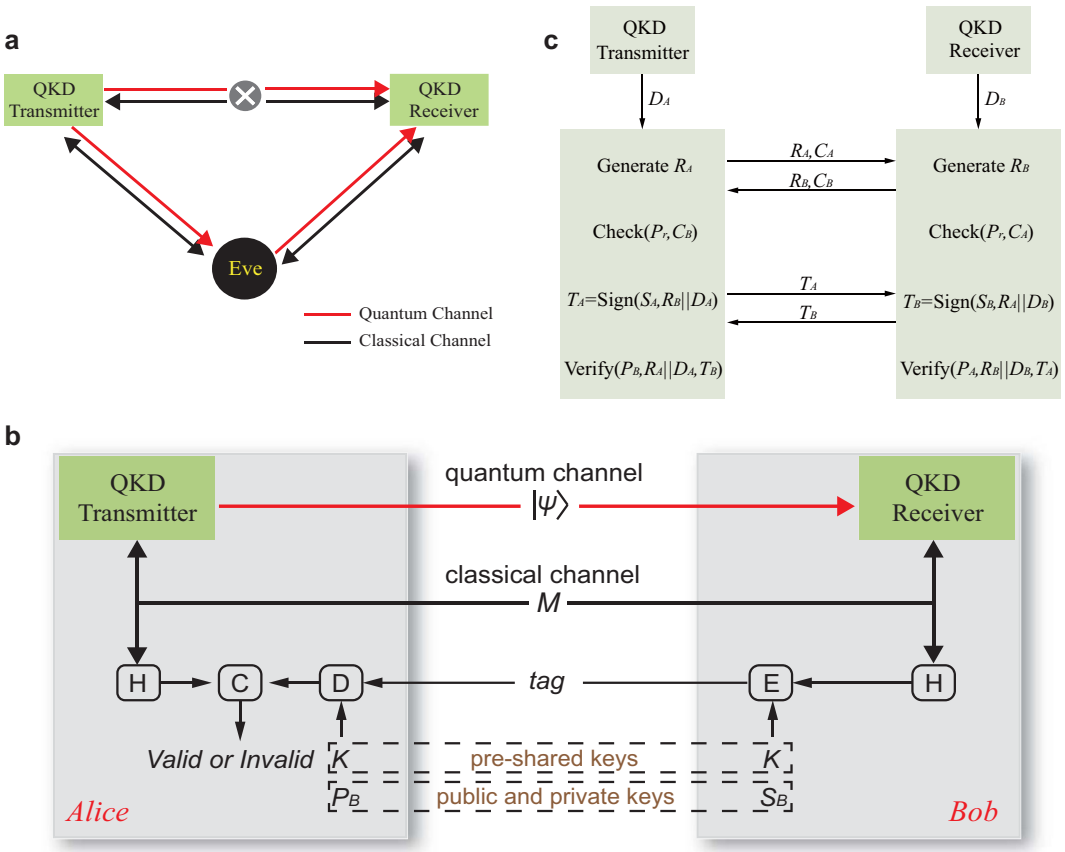

Fig. 1 Schematic of man-in-the-middle attack and flow diagram of post-quantum cryptography authentication. a As a middleman, Eve pretends to be a legitimate party. He cuts off the quantum channel, reconnects the legitimate parties, and carries out the man-in-the-middle attack. **b** The QKD transmitter sends quantum signals ($|\psi\rangle$) through a quantum channel to the QKD receiver, and they carry out data processing via a classical channel by exchanging classical messages (M). To authenticate the classical messages, Alice and Bob each generate a digest using a hash function (H), which is the SM3 hash algorithm in our experiment. Then, Bob encrypts (E) his digest with a pre-shared key (K) or Bob's private key (S_B) and subsequently sends the tag to Alice. After receiving the tag, Alice decrypts (D) it with the same pre-shared key (K) or Bob's public key (P_B) and compares (C) the result with her own digest. If the two are the same, the authentication is successful; otherwise, the authentication fails. The figure shows that Alice authenticates Bob's identity. In the experiment, we implemented two-way authentication, that is, Bob also authenticates Alice's identity. **c** Alice and Bob exchange their own certificates (C_A, C_B) and random nonce (R_A, R_B) with each other. Then, they use the public key of certificate authority (P_r) to verify that the other public key belongs to its identity, and use the PQC algorithm to sign the message digest (D_A, D_B) and the nonce under their own private keys (S_A, S_B) to generate signatures (T_A, T_B). Afterwards, they use the confirmed public keys of the other to verify the correctness of the received signatures. Because only the legitimate party has the corresponding private key, it can be confirmed that the message is signed legally. || denotes concatenating two bit strings.

reduces the interconnection between users. Moreover, when new users join a QKD network, they need to pre-share symmetric keys with the trusted relay or the original users on demand. If the new user's QKD task is urgent, it may be too late to distribute the authentication key pairs.

Another type of secure authentication method is to use the post-quantum public key algorithm and public key infrastructure (PKI)[23], as shown in Fig. 1b, c. Each user receives a digital certificate signed by a trusted certification center, which contains his/her identity, public key and other items required by the PKI standard. For a network of n users, the number of digital certificates issued is n. If a new user joins the QKD network, he/she needs to obtain only a digital certificate. Therefore, the authentication based on the public key algorithm can solve the problems of pre-sharing symmetric keys. As long as the PQC algorithm is secure during the authentication process, the security of this round of authentication and the key generated by QKD can be guaranteed. Even if the PQC algorithm is cracked in the future, the security of the previous authentication and keys will not be affected; thus, we need to assume only the short-term security of PQC. This is different from using the PQC algorithm for confidentiality or key distribution, which requires long-term security of the PQC algorithm. Here, we verify the application of PQC in QKD authentication, which greatly improves the operability and efficiency of the QKD authentication process.

PQC algorithm and authentication protocol

The PQC algorithm we used is Aigis-Sig[24], an efficient lattice-based digital signature scheme from variants of the learning with errors (LWE)[25] and small integer solutions (SIS)[26] problems. It has been shown that these two problems are at least as hard as some worst-case lattice problems (e.g., Gap-SIVP) for certain parameter choices[27–29]. Therefore, the post-quantum security of Aigis-Sig algorithm is based on the conjectured quantum resistance of the underlying lattice problems. Furthermore, it has not been found that quantum algorithms have substantial advantages (beyond polynomial speedup) over classical ones in solving lattice problems.

Our authentication protocol adopts a PKI enhanced with post-quantum secure Aigis-Sig as shown in Fig. 1c. The transmitter and the receiver exchange their certificates with each other, and they sign the message digest with private keys and verify the signatures with public keys. To prevent the replay attack, we introduce the nonce in our authentication protocol, which is a random number generated by Intel chips. We exchange the nonces together with the certificates and concatenate the nonce with the message digest together as our signing message. Note that we implemented two-way authentication in the QKD data processing.

QKD network authentication

We realized the application of PQC in the QKD point-to-point link, with fiber distances from 10 to 100 km. Figure 2 shows the key rates as a function of the fiber length. It can be seen that the key rates decrease exponentially with the fiber length, which is consistent with the theoretical expectation. We compared the key rates at the same fiber length using the pre-shared key authentication and the post-quantum algorithm authentication, and the difference between the average key rates of the two cases is <1 standard deviation. This is because the execution time of post-quantum algorithm authentication is <1 ms (see the "Methods" section), far less than one authentication cycle of the QKD system, which is ≥1 s. In the experiment, we also deliberately set the PQC algorithm to feed back that the authentication failed, and as a result, the QKD system discards the keys for these periods. This indicates that the PQC authentication is working properly.

QKD networks can generally be divided into two types: all-pass network and trusted relay network. For the all-pass network, users are connected by optical switches (OSs). To achieve an arbitrary

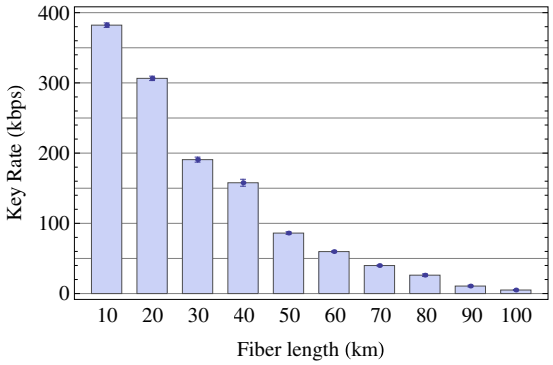

Fig. 2 The secure key rate as a function of the fiber length when QKD is authenticated by the PQC algorithm. The values shown are the average values over 5 min. The error bar represents a standard deviation of 10 key rate values for each fiber length.

connection between users, each user must have a QKD transmitter and a receiver. We built an all-pass network for four users, connected by an optical switch, as shown in Fig. 3a. The network can realize two typical topological relationships, i.e., a ring connection and a cross connection, as shown in Fig. 3b and c, respectively. We verified the application of PQC authentication in these two kinds of all-pass networks. The experimental results are shown in Table 1. We note that because the performances of different QKD devices are not exactly the same, their key rates and QBERs are different under the same fiber lengths. Using PQC authentication, we also demonstrated the QKD relay network (see Supplementary Note 1, Supplementary Fig. 1 and Supplementary Table 1).

The above results verify the feasibility of the PQC algorithm for QKD network authentication. To demonstrate the efficiency of PQC authentication, we built two trusted relay networks and connected them to simulate the QKD metropolitan area network. They can be located on both sides of a city. Each relay network contains five user nodes, with a total of 10 users in the entire network, as shown in Fig. 3d.

When using pre-shared key authentication, a trusted relay is usually needed to manage pre-shared keys at the cost of reducing the interconnection. With PQC authentication, the trusted relay can be replaced with an optical switch to realize arbitrary interconnection. Each user needs only one digital certificate for authentication, instead of pre-sharing $C_{10}^2 = 45$ pairs of symmetric keys, as shown in Fig. 3e. The interconnectivity of the QKD network has been greatly improved. To illustrate this point, in the experiment, we compared the QKD results of three pairs of users U1–U3, U5–U6, and U8–U10 in two cases, as shown in Table 2. Moreover, with the PQC authentication, users need to trust only the CA, reducing the security dependence on multiple trusted relays, which can improve the actual security of the entire network.

In the experiment, two new users U11 and U12 join the QKD network, as shown in Fig. 3e. If pre-shared key authentication is used, for the relay network, new users need to pre-share keys with the relay, and can perform QKD only with the relay, and not with other users. For the all-pass network, each new user needs to pre-share 10 pairs of symmetric keys with 10 original users and 1 pair of keys between the two new users. A total of 21 pairs of keys need to be pre-shared to achieve a connection between any two users. In contrast, if PQC authentication is adopted, trusted relays can be replaced with OSs. Each new user needs to apply for only one digital certificate, and a total of two digital certificates is sufficient to realize the connection of any two users. This greatly increases the accessibility of the network and the interconnection for new users. After U11 and U12 receive digital certificates, we demonstrate the QKD between U11–U2, U11–U7, U12–U4, U12–U9, and U11–U12. The results are shown in Table 3.

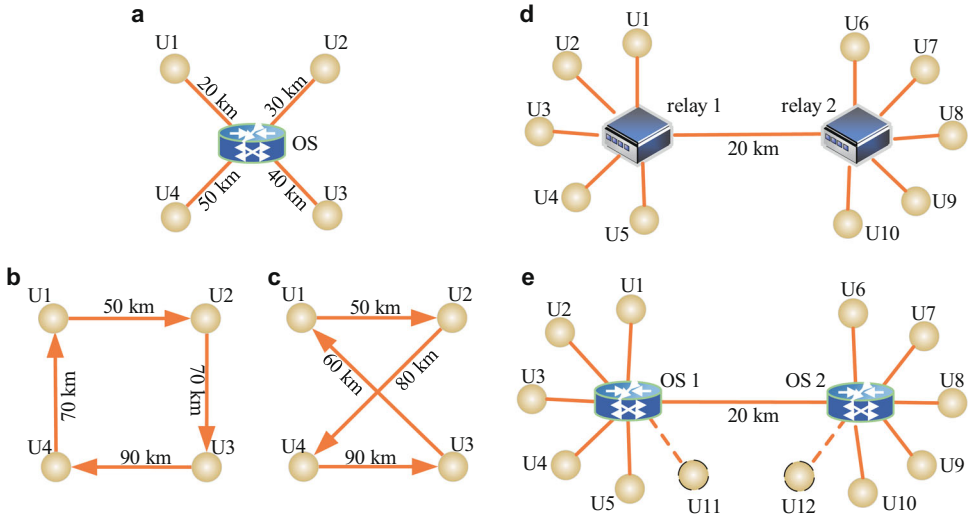

Fig. 3 PQC authentication in QKD networks. a All-pass QKD network. Four users are connected to each other through an optical switch. **b** Ring network. **c** Cross network. The actual distance between any two users is the sum of their respective distances from the optical switch. **d** A 10-node QKD metropolitan area network composed of two relay networks. **e** Trusted relays are replaced with optical switches to form an all-pass network. U11 and U12 are new users. See the text for the distance from each user to the trusted relay (optical switch).

Table 1. Key rates and QBERs of the QKD all-pass network authenticated by the PQC algorithm.

Connection	Length (km)	Loss (dB)	Key rate (kbps)	QBER (%)
(a) *Ring network*				
U1–U2	50	11.26	72.16	0.751
U2–U3	70	15.35	20.17	1.140
U3–U4	90	18.81	10.52	0.883
U4–U1	70	15.4	30.58	0.647
(b) *Cross network*				
U1–U2	50	11.21	68.65	0.779
U2–U4	80	16.31	19.45	1.014
U4–U3	90	18.46	9.71	0.786
U3–U1	60	12.15	76.82	0.517

Finally, we tested the stability of PQC authentication with a pair of QKD devices. The fiber length is 40 km, and it has been running continuously for 30 h. The PQC program keeps running normally, and the QKD systems continuously generate keys (see Supplementary Note 2, Supplementary Figs. 2 and 3).

Table 2. Comparison of key rates and QBERs between the relay network and all-pass network.

	Connection	Length (km)	Loss (dB)	Key rate (kbps)	QBER (%)
(a) *Relay network*					
U1–U3	U1–R1	10	2.69	363.59	0.648
	R1–U3	30	6.70	194.32	0.761
U5–U6	U5–R1	20	3.99	293.53	0.752
	R1–R2	20	4.08	288.16	0.475
	R2–U6	20	4.11	288.74	0.364
U8–U10	U8–R2	10	2.62	287.47	0.511
	R2–U10	10	2.66	333.06	0.529
(b) *All-pass network*					
	U1–U3	40	9.02	90.83	0.630
	U5–U6	60	12.12	48.00	0.978
	U8–U10	20	5.23	200.87	0.514

R1 and R2 stand for relay 1 and relay 2 in Fig. 3d, respectively. The fiber length between two users in the all-pass network is the sum of the fiber lengths of the links between the two users in the relay network.

DISCUSSION

In summary, we used the lattice-based post-quantum digital signature algorithm Aigis-Sig, combined with the PKI, to achieve efficient and quantum secure authentication of QKD. Since the Aigis-Sig algorithm is highly computationally efficient, it does not affect the performance of QKD, such as the key rate. We experimentally verified the feasibility of its application in a metropolitan QKD relay network and an all-pass network. With PQC authentication, the trusted relay in the QKD network can be replaced with an optical switch. Each user needs to apply for only one digital certificate through the PKI to realize a direct connection between any two users. We note that when the distance between the two parties of QKD exceeds the point-to-point tolerable distance, the trusted relay cannot be replaced with an optical switch. Moreover, when a new user joins the network, he/she needs only to obtain a digital certificate, instead of distributing symmetric keys with all other users, and can immediately establish a QKD connection. Compared with the pre-shared key authentication, PQC authentication has obvious operability and efficiency advantages. Furthermore, if the number of trusted relays is fewer, the security dependence on trusted relays in the network can be reduced, thus improving the security of the entire QKD network. We also verified the long-term stability of PQC authentication.

METHODS

QKD setup

In the experiment, we used the BB84 protocol combined with the decoy state method[30], with polarization encoding. The system operating frequency was 625 MHz, and the source was weak coherent states of an attenuated laser. We used polarization beam splitters (PBSs) to generate four polarization states: horizontal and vertical states and 45° and −45°

aligned states, which are encoded as 0, 1, 0, and 1, respectively. Alice launches the signal states, weak decoy states, and vacuum decoy states with a probability ratio of 6:1:1, and the average photon numbers of signal and weak decoy states are 0.6 and 0.2, respectively. We used a mechanical optical switch. Its switching time is <10 ms, and the insertion loss is ~1.0 dB. In the experiment, single-photon detectors based on InP/InGaAsP avalanche photodiodes were used, and they worked in gated mode with a detection efficiency of 12% and a dark count rate of 1×10^{-6} per clock cycle. To reduce the probability of afterpulsing, we set the dead time of the detectors to 500 ns. The QKD transmitter and the QKD receiver were synchronized by periodic pulsed light. The synchronous light was transmitted with the quantum signal light via a single optical fiber through wavelength-division multiplexing. The QKD systems used the SM3 hash algorithm to generate digest values of 256 bits for the messages to be authenticated and then output them to the PQC program. The finite-key effect was considered in the data processing.

The PQC algorithm: Aigis.Sig

In general, a lattice-based PQC signature is slightly more complicated than its classic counterparts such as RSA and ECDSA. We briefly introduce our PQC digital signature algorithm Aigis.Sig, which is based on the "Fiat-Shamir with Aborts" technique and can be seen as a variant of the NIST PQC round-3 finalist CRYSTALS-DILITHIUM.

Preliminary. Let $R_q = \mathbb{Z}[X]/(X^n + 1)$ denote the quotient ring containing all polynomials over the $\mathbb{Z}_q$ in which X^n is identified with -1. Let Hash$(\cdot)$ denote a hash function. Let $||\cdot||_\infty$ denote the maximum norm. Let HighBits$(r, a) = \lfloor r/a \rfloor$ and LowBits$(r, a) = r \bmod a$ denote the higher-order and lower-order bits of r with respect to the divisor a, respectively. S_η denotes the set of ring elements of R, where each coefficient is taken from the set $\{-\eta, -\eta + 1, \ldots, \eta\}$ for some positive integer $\eta \ll q$. Let $n, q, k, l, \eta, \gamma_1, \gamma_2, \beta$ denote other parameters. We can now describe the key generation, signature signing and verification algorithms by Algorithms 1, 2, and 3, respectively. The procedure has at least 128-bit quantum security (against any quantum algorithms who attempt to forge a valid signature) based on the underlying quantum hardness of the lattice problems, and the correctness is ensured in the sense that any legitimate signature can be correctly verified by the verification algorithm. Finally, we remark that the "repeat until" subroutine in the signature algorithm represents the "rejection sampling" technique, which is necessary to sample from the desired distribution for security purposes and takes only up to a handful of trials.

The PQC authentication algorithm, which includes the key generation, signature, and verification algorithms, is as follows:

We implement the PQC algorithm in Windows 10 64-bit, Intel(R) Core (TM) i7-9750H CPU @2.60 GHz, 8 GB RAM. The average CPU cycle of signature generation is 459,903. The average CPU cycle of signature

Table 3. QKD key rates and QBERs between new users U11 and U12 and original users in the network and between U11 and U12.

Connection	Length (km)	Loss (dB)	Key rate (kbps)	QBER (%)
U11–U2	40	8.11	139.79	0.846
U11–U7	50	11.26	90.18	0.573
U12–U4	40	8.11	113.42	0.792
U12–U9	40	8.16	101.78	0.873
U11–U12	50	11.07	83.05	0.858

Algorithm 1: Key Generation Algorithm

Function KeyGen

$A \leftarrow R_q^{k \times l}$;
$s_1, s_2 \leftarrow S_\eta^l \times S_\eta^l$;
$t = As_1 + s_2$;
$pk = (A, t), sk = (s_1, s_2, pk)$;
return (pk, sk)

Algorithm 2: Signature Algorithm

Function Sign $sk{=}(s_1, s_2, pk), \mu$

repeat
  $y \leftarrow S_{\gamma_1 - 1}^{l+k}$;
  $w = Ay$;
  $c = \text{Hash}(\text{HighBits}(w, 2\gamma_2)||\mu)$;
  $z = y + cs_1$;
until $||z||_\infty < \gamma_1 - \beta$ *and* $\text{LowBits}(Ay - cs_2, 2\gamma_2) < \gamma_2 - \beta$;
return $\sigma = (z, c)$

Algorithm 3: Verification Algorithm

Function Verify $pk{=}(A,t), \sigma = (z, c), \mu$

if $||z||_\infty < \gamma_1 - \beta$ *and* $c = \text{Hash}(\text{HighBits}(Az - ct, 2\gamma_2)||\mu)$ **then**
  return *true* ;
return *false* ;

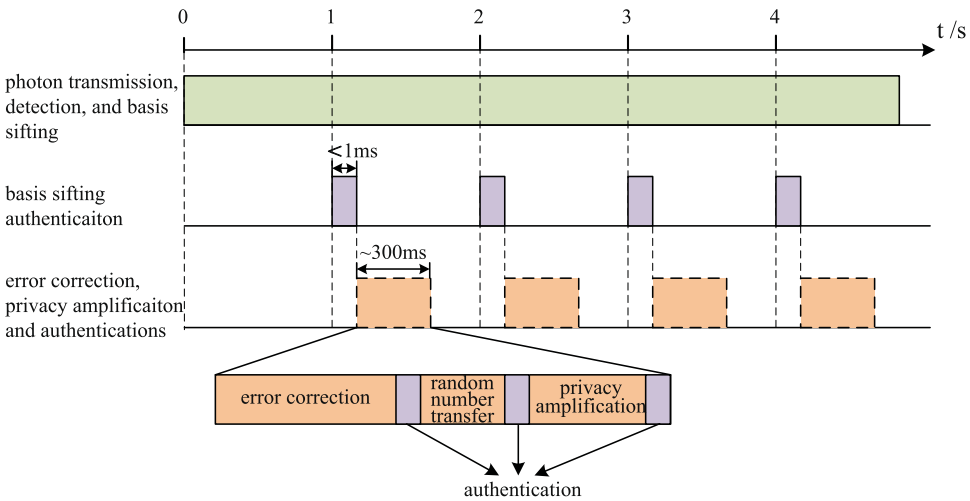

Fig. 4 Timing diagram of the sequence and durations of the authentication and QKD processes. The basis sifting authentication was performed once per second after basis sifting, followed by error correction, privacy amplification and the corresponding authentication processes. Each authentication process was executed within 1 ms.

verification is 104,337. The signature size is 2445 bytes. The real execution time is <1 ms.

Timing diagram

The timing diagram of the sequence and durations of the authentication and QKD processes is shown in Fig. 4. In our experiment, the photon transmission and detection and the basis sifting were performed continuously, while the basis sifting authentication was executed once per second for the basis sifting messages of the previous second. Then, error correction, privacy amplification and the corresponding authentication processes were carried out within 300 ms. However, they were not necessarily executed every second but were determined by the amount of data after base sifting, which is related to the distance of the fiber and the link loss. After error correction, there are three authentication processes: error correction verification, authentication of random number transfer, and final key verification.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request.

CODE AVAILABILITY

The code that support the findings of this study are available from the corresponding author upon reasonable request.

Received: 13 October 2020; Accepted: 12 March 2021;
Published online: 06 May 2021

REFERENCES

1. Arute, F. et al. Quantum supremacy using a programmable superconducting processor. *Nature* **574**, 505–510 (2019).
2. Shor, P. W. Algorithms for quantum computation: discrete logarithms and factoring. In *Proc. 35th Annual Symposium on Foundations of Computer Science* (ed. Goldwasser, S.) 124–134 (IEEE, 1994).
3. Grover, L. K. A fast quantum mechanical algorithm for database search. In *Proc. 28th Annual ACM Symposium on Theory of Computing*, 212–219 (1996).
4. Boudot, F. et al. Comparing the difficulty of factorization and discrete logarithm: a 240-digit experiment. In *The 40th Annual International Cryptology Conference (Crypto 2020), Advances in Cryptology—CRYPTO* (eds Micciancio, D. & Thomas, R.) (Springer, 2020).
5. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145 (2002).
6. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. In *Proc IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, 175–179 (IEEE, 1984).
7. Ekert, A. K. Quantum cryptography based on Bell theorem. *Phys. Rev. Lett.* **67**, 661 (1991).
8. Scarani, V. et al. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301 (2009).
9. Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **92**, 025002 (2020).
10. Islam, N. T., Lim, C. C. W., Cahall, C., Kim, J. & Gauthier, D. J. Provably secure and high-rate quantum key distribution with time-bin qudits. *Sci. Adv.* **3**, e1701491 (2017).
11. Chen, J.-P. et al. Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km. *Phys. Rev. Lett.* **124**, 070501 (2020).
12. Fang, X.-T. et al. Implementation of quantum key distribution surpassing the linear rate-transmittance bound. *Nat. Photonics* **14**, 422–425 (2020).
13. Yin, J. et al. Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature* **582**, 501–505 (2020).
14. Peev, M. et al. The SECOQC quantum key distribution network in Vienna. *N. J. Phys.* **11**, 075001 (2009).
15. Chen, T. Y. et al. Metropolitan all-pass and inter-city quantum communication network. *Opt. Express* **18**, 27217 (2010).
16. Sasaki, M. et al. Field test of quantum key distribution in the Tokyo QKD network. *Opt. Express* **19**, 10387 (2011).
17. Fröhlich, B. et al. A quantum access network. *Nature* **501**, 69 (2013).
18. Wang, S. et al. Field and long-term demonstration of a wide area quantum key distribution network. *Opt. Express* **22**, 21739–21756 (2014).
19. Liao, S.-K. et al. Satellite-relayed intercontinental quantum network. *Phys. Rev. Lett.* **120**, 030501 (2018).
20. Chen, L. et al. *Report on Post-quantum Cryptography*. Technical Report NISTIR 8105 (National Institute of Standards and Technology, 2016).
21. Fung, C.-H. F., Ma, X. & Chau, H. F. Practical issues in quantum-key-distribution postprocessing. *Phys. Rev. A* **81**, 012318 (2010).
22. Hughes, R. J. et al. Network-centric quantum communications with application to critical infrastructure protection. Preprint at http://arxiv.org/abs/quant-ph/1305.0305 (2013).
23. Mosca, M., Stebila, D. & Ustaoğlu, B. Quantum key distribution in the classical authenticated key exchange framework. In *Post-Quantum Cryptography* (ed. Gaborit, P.) 136–154 (Springer, 2013).
24. Zhang, J., Yu, Y., Fan, S., Zhang, Z. & Yang, K. Tweaking the asymmetry of asymmetric-key cryptography on lattices: kems and signatures of smaller sizes. In *IACR International Conference on Public-Key Cryptography*, 37–65 (Springer, 2020).
25. Regev, O. On lattices, learning with errors, random linear codes, and cryptography. In *Proc. 37th Annual ACM Symposium on Theory of Computing*, Baltimore, MD, USA, May 22–24, 2005 (eds Gabow, H. N. & Fagin, R.) 84–93 (ACM, 2005).
26. Ajtai, M. Generating hard instances of lattice problems (extended abstract). In *Proc. 28th Annual ACM Symposium on the Theory of Computing*, Philadelphia, Pennsylvania, USA, May 22–24, 1996 (ed. Miller, G. L.) 99–108 (ACM, 1996).
27. Regev, O. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM* **56**, 34:1–34:40 (2009).
28. Peikert, C. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In *Proc. 41st Annual ACM Symposium on Theory of Computing, STOC 2009*, Bethesda, MD, USA, May 31–June 2, 2009 (ed. Mitzenmacher, M.) 333–342 (ACM, 2009).
29. Gentry, C., Peikert, C. & Vaikuntanathan, V. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*, Victoria, British Columbia, Canada, May 17–20, 2008 (ed. Dwork, C.) 197–206 (ACM, 2008).
30. Ma, X. F., Qi, B., Zhao, Y. & Lo, H. K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **72**, 012326 (2005).

ACKNOWLEDGEMENTS

This work was supported by the National Key R&D Program of China (Grant No. 2017YFA0304000), the National Natural Science Foundation of China (Grant No. 62001414), the Chinese Academy of Sciences (CAS), the Shanghai Municipal Science and Technology Major Project (Grant No. 2019SHZDZX01), the Anhui Initiative in Quantum Information Technologies, and the Yunnan Fundamental Research Project (Grant No. 202001BB050028) and the Major Science and Technology Project (Grant No. 2018ZI002).

AUTHOR CONTRIBUTIONS

Q.Z., Y.Y. and J.-W.P. conceived the research and designed the experiments. L.-J.W., K.-Y.Z., J.-Y.W., J.C., Y.-H.Y., S.-B.T., Y.-L.T., Y.Y. and Q.Z. prepared the setup and implemented the experiments. K.-Y.Z., Y.Y., D.Y., and Z.L. designed the PQC algorithm and developed the software. L.-J.W., K.-Y.Z., D.Y., Y.Y., Q.Z. and J.-W.P. analyzed the data and wrote the manuscript. L.-J.W. and K.-Y.Z. contributed equally to this work. All authors discussed the results and reviewed the manuscript.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41534-021-00400-7.

Correspondence and requests for materials should be addressed to Y.Y., Q.Z. or J.-W.P.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.