UDC 003.26:621.39 **DOI:10.30837/rt.2026.2.225.08**

Ye.V. KOTUKH, Cand. Sc. (Eng.), M.V. KOROBCHYNSKYI, Dr. Sc. (Eng.), V.V. KOZLOVSKYI, Dr. Sc. (Eng.), H.Z. KHALIMOV, Dr. Sc. (Eng.), S.O. KUDRENKO, Cand. Sc. (Eng.), D.V. KOZLOVSKA

PROBLEMS AND PROSPECTS OF BUILDING AUTHENTICATION METHODS IN QUANTUM KEY DISTRIBUTION CHANNELS

Statement of the problem in general and its connection with important scientific and practical tasks

Quantum Key Distribution (QKD) is a technology that provides information-theoretic security of key-material distribution based on the fundamental laws of quantum mechanics rather than on hypothetical computational hardness [1, 2]. It is precisely this property that drives interest in QKD as a component of prospective secure telecommunication infrastructures, in particular under the threat posed by quantum computing. However, the security of QKD protocols is conditional: the security proofs of the BB84 [1], E91 [3] protocols and their practical derivatives rely on the assumption of an authenticated classical channel through which the parties exchange service messages during post-processing (basis sifting, parameter estimation, information reconciliation and privacy amplification) [4, 5, 21].

The quantum resistance of the key-distribution process itself does not eliminate the need to authenticate the participants [22]. QKD establishes a shared secret between the two ends of the channel but provides no means of confirming who exactly is located at those ends. As a result, an unauthenticated quantum channel remains vulnerable to the man-in-the-middle attack: an active adversary interposes itself between the legitimate parties, runs independent instances of the protocol with each of them and reconciles two keys that it fully controls. The information-theoretic security of the quantum layer in this case protects a channel that terminates at the attacker. Authentication is therefore not an auxiliary but a constitutive condition of QKD security, and the practical construction of its methods constitutes a relevant scientific and technical task directly connected with the deployment of secure quantum networks [23–26].

The relevance of the task is reinforced by the transition of QKD from point-to-point links to network architectures – metropolitan, national, satellite and prospective quantum-internet architectures [6, 7, 27]. In such networks the task shifts from authenticating individual messages to authenticating a large number of mutually distrustful nodes, possibly in different administrative domains [28]. This makes the issues of scalability, key management and trust distribution central to the construction of authentication methods.

Analysis of recent research and publications and identification of previously unresolved parts of the general problem

It is expedient to classify existing methods of authenticating the classical QKD channel by the cryptographic primitive employed.

Symmetric methods based on universal hashing. The canonical approach is that of Wegman–Carter [8], which performs message authentication based on ε-almost-strongly-universal families of hash functions with one-time-pad masking of the tag. The approach is information-theoretically secure. In [9] it is extended to variable-length messages using polynomial hashing, which reduces key-material consumption. A fundamental limitation is the need for a pre-shared secret even before the first quantum exchange. QKD is therefore more correctly interpreted as a key-growing primitive. At the network level this approach requires pairwise secrets whose number grows quadratically with the number of nodes.

Pre-shared secrets and fixed keys. In [10] it is shown that even the reuse of a fixed secret authentication key has a fundamental limit: since privacy amplification does not reduce the adversary's information to zero, partial knowledge of the masking information leaks information about the fixed hash function, and this information accumulates linearly with the number of rounds. This limits the safe lifetime of the key and aggravates the key-management task in long-term operation [11].

Public-key infrastructure (PKI) and survey works. In the survey [4], PKI is considered as a candidate for authenticating the classical channel, while its inherent trade-offs are noted: classical signatures are vulnerable to quantum cryptanalysis, and trust is concentrated in certification authorities. The same survey systematizes open problems: the trade-off between information-theoretic authentication and resistance to denial of service, the handling of partially weak keys, and network scaling.

Two-way authentication. In [12] a scheme is proposed. Here is a mutual identity authentication that is performed simultaneously with key distribution. The approach removes the asymmetry of one-sided authentication but relies on a centralized authority and symmetric pre-shared material, which reproduces the problems of key management and centralized trust.

Entity authentication at the quantum layer. In [13] mutual authentication of QKD network nodes is implemented using authentication qubits over a deployed fibre network; the approach is bound to the physical layer and a star topology and requires pre-shared information. In [14] quantum identity authentication based on counterfactual QKD is proposed, while in [15] a mediated authenticated protocol based on differential phase shift with an untrusted mediator is proposed. The common features of these solutions are dependence on a pre-shared secret, binding to quantum hardware and limited scalability.

Authentication based on zero-knowledge proofs. Zero-knowledge proofs (ZKP) make it possible to confirm possession of a secret without revealing it [16]. In [17] the first practical implementation of a quantum ZKP for user authentication on existing QKD hardware is presented: the protocol is interactive, and the acceptance decision is made by the level of quantum error. In [18] a quantum ZKP with a designated verifier based on conjugate coding is proposed. These works target individual user-authentication scenarios, are quantum (they require a quantum channel and resources on the prover side) and do not consider scalable networks. Conceptually close is the work [19], where classical ZKPs are applied over the control channel to hide topology and confirm connectivity of a QKD network; however, the proven property is connectivity, not entity identity. The impact of real authentication mechanisms on formal QKD security proofs is studied in [20], where a reduction between honest and practical authentication models is established [29].

Thus, existing methods cover only individual fragments of the requirements space (Table 1). The task of building a scalable method for authenticating *entities* that would combine non-disclosure of the secret, quantum resistance, sub-quadratic scaling and minimisation of trust assumptions remains unresolved [30–33].

The aim of the article is a systematic analysis of the problems of building authentication methods in quantum key distribution channels and the substantiation of a prospective direction for their development. To achieve this aim, the following tasks are set:

– to formalize the role of authentication as a condition of QKD security and the threat model;

– to perform a comparative analysis of existing authentication methods by the criteria of key management, scalability and trust distribution;

– to identify the unresolved scientific and technical gap;

– to substantiate the requirements for a prospective entity-authentication method for scalable QKD networks.

Table 1

Comparative analysis of authentication methods in QKD

Method	Primitive / basis	No pre-shared secret	Scalability	Post-quantum resistance
Universal hashing [8, 9]	symmetric key	no	low, O(n²)	yes (ITS), requires PSK
Fixed key [10]	symmetric key	no	low	limited key resource
PKI [4]	asymmetric signatures	yes	medium, single CA	no / only PQC
Two-way [12]	symmetric + authority	no	low	depends on primitive
Authentication qubits [13]	quantum layer	no	limited (star)	physical
Quantum ID auth. [14, 15]	quantum layer	no	low	physical
Quantum ZKP [17, 18]	quantum ZKP	no	low (physical layer)	physical
Classical ZKP (topology) [19]	classical ZKP	yes	high	yes (post-quantum)

Presentation of the main research material.

Threat model and problem formalization. Consider a QKD network as a set of entities E = {e₁ , …, e□} that interact through the quantum layer (physical transmission), the classical control layer (post-processing and management service messages) and the key-management layer. The adversary is assumed to be active at the quantum and classical layers and quantum-capable. The entity-authentication task is to ensure, for any pair (e□, e□), mutual confirmation of identity with a probability of successful forgery that does not exceed a negligible value.

Let λ be the security parameter. An authentication method is considered secure if the advantage of an adversary A in the game of impersonating a legitimate entity satisfies the condition

$$Adv_{IMP}(A) \le negl\ \ \lambda\ \ , \qquad (1)$$

where) is a negligible function. For methods based on pre-shared secrets, security is achieved at the cost of pairwise key material whose volume in a network of n nodes is

$$N_{key} = n\ \ n-1\ \ /2 = O\ \ n^2\ \ , \qquad (2)$$

which is precisely what causes the fundamental scalability limitation of symmetric methods. By contrast, methods based on identity registration potentially yield a linear initial-state volume and a constant online verifier state, which is a quantitative advantage when building large networks.

The scalability and key-management problem. The analysis (Table 1) shows that symmetric methods [8–10, 12] and quantum-layer methods [13–15] require a pre-shared secret and, accordingly, inherit the quadratic growth. This complicates the onboarding of new nodes and the re-registration of participants, since adding a node requires the prior distribution of secrets to all potential partners. Public-key infrastructure [4] removes the quadratic dependence but introduces a single point of trust concentration (the certification authority) and, in its classical form, quantum-vulnerable primitives.

The problem of disclosing identification information. Methods that transmit a verifiable token (signature) or directly use identification information in every session [4, 12–15] increase the leakage surface of service data. By contrast, the zero-knowledge proof paradigm [16] makes it possible to confirm possession of an identification secret without revealing it, which structurally reduces this surface.

The problem of binding to the physical layer. Quantum authentication methods [13–15, 17, 18] require a quantum channel and quantum resources on the side of the prover, which binds them

to a specific physical line and impairs applicability in multi-domain networks. Classical ZKPs over the control channel [19] do not have this limitation, but the existing work solves the topology-hiding task rather than entity authentication.

The problem of trust distribution and compatibility with security proofs. Centralized methods [4, 12] contradict the multi-domain nature of prospective networks. At the same time, any method must be consistent with formal QKD security proofs: in [20] it is shown that practical authentication mechanisms (in particular, asymmetric abort) differ from the idealized assumptions of the proofs, but under moderate conditions security is preserved. This defines the formal contract that a prospective method must satisfy.

Substantiation of the prospective direction. The juxtaposition of the identified problems makes it possible to formulate the requirements for a prospective entity-authentication method in scalable QKD networks, namely:

1) the requirement of identity confirmation without revealing the secret (the zero-knowledge property);
2) the requirement of quantum (post-quantum) resistance of the underlying primitive;
3) the requirement of sub-quadratic scaling with minimisation of pairwise key material;
4) the requirement of abandoning a single trust centre;
5) the requirement of operating over the classical control plane without binding to the physical layer;
6) the requirement of compatibility with formal QKD security proofs.

None of the analysed methods satisfies this set of requirements simultaneously: symmetric and quantum methods do not provide (3)–(4), PKI does not provide (1), (4) and, in its classical form, (2), while existing classical ZKPs for QKD networks [19] do not solve the entity-authentication task. The prospective direction is therefore the construction of entity-authentication methods based on post-quantum zero-knowledge proofs over the classical control plane of scalable QKD networks.

Conclusions and prospects for further research.

1. Authentication is a constitutive condition of quantum key distribution security: the security of the BB84, E91 protocols and their derivatives formally presupposes an authenticated classical channel, while the man-in-the-middle attack constitutes a fundamental threat to unauthenticated systems.

2. The comparative analysis of authentication methods has shown that symmetric and quantum-layer methods provide security at the cost of pre-shared secrets with a quadratic growth of key material, public-key infrastructure introduces centralized trust and quantum-vulnerable primitives, and existing zero-knowledge-proof-based methods are quantum and bound to the physical layer.

3. An unresolved scientific and technical gap has been identified – the absence of a scalable entity-authentication method that combines non-disclosure of the secret, quantum resistance, sub-quadratic scaling and minimisation of trust assumptions.

4. A prospective direction has been substantiated – the construction of entity-authentication methods based on post-quantum zero-knowledge proofs over the classical control plane of scalable QKD networks. Further research should be directed towards formalizing the corresponding model and protocol, analysing their completeness, soundness and zero-knowledge properties, and evaluating scalability in multi-domain networks.

References

1. Bennett C. H. and Brassard G. Quantum cryptography: Public key distribution and coin tossing // Proc. IEEE Int. Conf. Computers, Systems and Signal Processing, Bangalore, India. 1984. P. 175–179.

2. F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan. Secure quantum key distribution with realistic devices // Rev. Mod. Phys. 2020. Vol. 92, no. 2, art. 025002. DOI: https://doi.org/10.1103/RevModPhys.92.025002

3. Ekert A. K. Quantum cryptography based on Bell's theorem // Phys. Rev. Lett. 1991. Vol. 67, no. 6. P. 661–663. DOI: https://doi.org/ 10.1103/PhysRevLett.67.661

4. Fregona M. et al. Authentication methods for quantum key distribution: Challenges and perspectives // Toward a Quantum-Safe Communication Infrastructure, NATO Sci. Peace Secur. Ser. D. 2024. Vol. 64, Amsterdam: IOS Press, 2024. P. 54–66. DOI: https://doi.org/10.3233/NICSP240007

5. Portmann C. and Renner R. Security in quantum cryptography // Rev. Mod. Phys. 2022. Vol. 94, no. 2, art. 025008. DOI: https://doi.org/10.1103/RevModPhys.94.025008

6. Wehner S., Elkouss D., and Hanson R. Quantum internet: A vision for the road ahead // Science. 2018. Vol. 362, no. 6412, art. eaam9288, 2018. DOI: https://doi.org/10.1126/science.aam9288

7. Cao Y., Zhao Y., Wang Q., Zhang J., S. X. Ng, and Hanzo L. The evolution of quantum key distribution networks: On the road to the Qinternet // IEEE Commun. Surv. Tutorials. 2022. Vol. 24, no. 2. P. 839–894. DOI: https://doi.org/10.1109/COMST.2022.3144219

8. Wegman M. N. and Carter J. L. New hash functions and their use in authentication and set equality // J. Comput. Syst. Sci. 1981. Vol. 22, no. 3. P. 265–279. DOI: https://doi.org/10.1016/0022-0000(81)90033-7

9. Bibak K., Kapron B. M., and Srinivasan V. Authentication of variable length messages in quantum key distribution // EPJ Quantum Technol. 2022. Vol. 9, art. 8. DOI: https://doi.org/10.1140/epjqt/s40507-022-00127-0

10. Abidin A. and Larsson J.-Å. Security of authentication with a fixed key in quantum key distribution // arXiv:1109.5168, 2011.

11. Pacher C., Abidin A., Lorünser T., Peev M., Ursin R., Zeilinger A., and Larsson J.-Å. Attacks on quantum key distribution protocols that employ non-ITS authentication // Quantum Inf. Process. 2016. Vol. 15, no. 1. P. 327–362. DOI: https://doi.org/10.1007/s11128-015-1160-4

12. Zheng Z. and Zhao S. Quantum key distribution with two-way authentication // Opt. Quantum Electron. 2021. Vol. 53, art. 304. DOI: https://doi.org/10.1007/s11082-021-02845-8

13. Park H., Park J., Woo B., Kang M.-S., Choi J., Kang S.-W., Yeom S., and Han S.-W. Mutual entity authentication of quantum key distribution network system using authentication qubits // EPJ Quantum Technol. 2023. Vol. 10, art. 48, 2023. DOI: https://doi.org/10.1140/epjqt/s40507-023-00205-x

14. Liu B., Gao Z., Xiao D., Huang W., Zhang Z., and Xu B. Quantum identity authentication in the counterfactual quantum key distribution protocol // Entropy. 2019. Vol. 21, no. 5, art. 518. DOI: https://doi.org/10.3390/e21050518

15. Tsai C.-W. et al. Mediated authenticated differential phase shift quantum key distribution // Optik, 2023. DOI: https://doi.org/10.1016/j.ijleo.2022.170417

16. Goldwasser S., Micali S., and Rackoff C. The knowledge complexity of interactive proof systems // SIAM J. Comput. 1989. Vol. 18, no. 1. P. 186–208. DOI: https://doi.org/10.1137/0218012

17. García-Cid M. I. et al. Experimental implementation of a quantum zero-knowledge proof for user authentication // Opt. Express. 2024. Vol. 32, no. 9. P. 15955–15966. DOI: https://doi.org/10.1364/OE.517754

18. Garcia-Diaz V., Escanez-Exposito D., Caballero-Gil P., and Molina-Gil J. Conjugate coding based designated verifier quantum zero knowledge proof for user authentication // Cryptogr. Commun. 2026. DOI: https://doi.org/10.1007/s12095-026-00878-y

19. Cozzolino D., Krenn S., and Lorünser T. Topology-hiding connectivity assurance for QKD inter-networking // arXiv:2604.01876, 2026.

20. Tupkary D., Nahar S., and Tan E. Y.-Z. Authentication in security proofs for quantum key distribution // arXiv:2601.17960, 2026.

21. Kotukh Y. (2026). Sub-cubic quantum gate synthesis via stochastic commutator decomposition // arXiv. https://arxiv.org/abs/2605.02051

22. Kotukh Y. Methods of implementing post-quantum cryptography standards based on an OCaml-oriented modular architecture // Radiotekhnika. 2026. No 224. P. 72–80.

23. Khalimov G., & Kotukh Y. (2026). LINEture: Novel signature cryptosystem // arXiv. https://arxiv.org/abs/2601.07071

24. Kotukh Y., Khalimov G. (2026). Security parameter analysis of the LINEture post-quantum digital signature scheme // arXiv. https://arxiv.org/abs/2601.03465

25. Khalimov G., Sun X., Kotukh Y., Dzhura I., Wyglinski A., Khivrenko H. New Key Encapsulation Method for Authentication in 5G Network in the Post-quantum Era // Bradford, P.G., Koul, S.K., Gadsden, S.A., Ghatak, K.P. (eds) Proceedings of IEMTRONICS 2025. IEMTRONICS 2025. Lecture Notes in Electrical Engineering. 2026. Vol 1468. Springer, Singapore. DOI: https://doi.org/10.1007/978-981-95-0433-6_4

26. Kotukh Y. V. On a unified cryptographic coprocessor architecture for post-quantum cryptography in 6G // Radiotekhnika. 2025. No 223. P. 121–125. DOI: https://doi.org/10.30837/rt.2025.4.223.13

27. Khalimov G., Kotukh Y., Khalimova S., Korobchynskyi M., Podlipaiev V. and Zaitsev O. Cryptanalysis of a LINE cryptosystem // 2025 5th International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Zanzibar, Tanzania, United Republic of. 2025. P. 1–7. DOI: https://doi.org/10.1109/ICECCME64568.2025.11277439

28. Kotukh Y. Quantum-resistant cryptography for protecting critical infrastructure from cyber threats // Proceedings of the 3rd Scientific and Practical Conference “Resilience of Dynamic Systems”. 2025. Vol. 1, no. 1. P. 85–88.

29. Kotukh Y. V., Khalimov G. Z., & Dzhura I. Y. Cryptographic competitiveness of cryptosystems based on non-commutative groups // Radiotekhnika. 2025. No 221. P. 72–82. DOI: https://doi.org/10.30837/rt.2025.2.221.10

30. Kotukh Y. Quantum computing criteria in cryptoanalysis problems // Theoretical and Applied Cybersecurity. 2025. 123.

31. Khalimov G., & Kotukh Y. (2025). LINE: Public-key encryption // arXiv. https://arxiv.org/abs/2507.04501

32. Kotukh Y. V., Khalimov G. Z., Korobchynskyi M. V., & Dzhura I. Y. Analysis of the limitations of quantum computing in cryptanalysis problems // Radiotekhnika. 2025. No 220. P. 92–101.
DOI: https://doi.org/10.30837/rt.2025.1.220.08
33. Kotukh Y. Current problems and prospects for the development of applied quantum informatics // Proceedings of the V All-Ukrainian Scientific and Practical Conference “Current Problems and Prospects for the Development of Fundamental, Applied, General-Technical and Security Sciences”. 2025. Vol. 1, no. 1. P. 42–47.

Надійшла до редколегії 07.03.2026
Прийняття до друку після рецензування 25.06.2026
Публікація (оприлюднення) 25.07.2026

Відомості про авторів:
Котух Євген Володимирович – канд. техн. наук, доцент, професор кафедри кібербезпеки; Національний технічний університет «Дніпровська політехніка»; Дніпро, Україна; e-mail: yevgenkotukh@gmail.com; ORCID: https://orcid.org/0000-0003-4997-620X
Коробчинський Максим Володимирович – д-р техн. наук, професор, начальник другої кафедри Другого Навчально-наукового інституту Воєнної Академії ім. Євгена Березняка; Київ, Україна; e-mail:maks_kor@ukr.net; ORCID: https://orcid.org/0000-0001-8049-4730
Козловський Валерій Валерійович – завідувач кафедри технічного захисту інформації Державного університету «Київський авіаційний інститут»; Київ, Україна; e-mail: valerii.kozlovskyi@npp.kai.edu.ua; ORCID: https://orcid.org/0000-0002-8301-5501
Халімов Геннадій Зайдулович – д-р техн. наук, професор, завідувач кафедри безпеки інформаційних технологій; Харківський національний університет радіоелектроніки; Харків, Україна; e-mail: hennadii.khalimov@nure.ua; ORCID: https://orcid.org/0000-0002-2054-9186
Кудренко Станіслава Олексіївна – доцент кафедри технічного захисту інформації, Державний університет «Київський авіаційний інститут»; Київ, Україна; e-mail: stanislava.kudrenko@npp.nau.edu.ua; ORCID: https://orcid.org/0000-0002-0759-3908
Козловська Діана Валеріївна – студентка факультету комп'ютерних наук і технологій Державного університету «Київський авіаційний інститут»; Київ, Україна; e-mail: vvkzeos@gmail.com. ORCID: https://orcid.org/0009-0004-6223-0319