УДК 003.26:621.39:530.145

С.О. Гнатюк, Т.О. Охріменко, С.А. Дорожинський
(Національний авіаційний університет, Україна)

Підходи до побудови квантово-безпечної критичної інформаційної інфраструктури

Робота присвячена розв'язанню актуальної наукової задачі дослідження підходів до побудови квантово-безпечної критичної інформаційної інфраструктури держави на базі квантових детерміністичних протоколів, які мають низку принципових переваг у порівнянні з неквантовими криптографічними протоколами

Новітні ІКТ відкривають широкі можливості щодо створення та використання сучасних мережевих та Інтернет сервісів, проте з іншого боку вони породжують цілу низку нових уразливостей та загроз безпеці даних. Як зазначалось, загрози можна диференціювати за тріадою CIA відповідно до характеристик безпеки – загрози конфіденційності, загрози цілісності і загрози доступності даних (інформаційної інфраструктури). Перші дві характеристики, як правило, забезпечуються криптографічними методами і засобами, а останню можна забезпечити резервуванням елементів інфраструктури і каналів зв'язку, фільтруванням і корегуючим кодуванням. Використовувані криптографічні алгоритми не завжди дозволяють забезпечити релевантний рівень захисту від відомих атак, зокрема до атак на основі квантових алгоритмів (Шора, Гровера, Ксіонга-Ванга, Дойча-Йожі тощо). Сучасні методи симетричної й асиметричної криптографії ґрунтуються на принциповій неможливості зловмисником розв'язати складну математичну задачу (пошук по повністю невпорядкованій базі даних, факторизація та логарифмування в дискретних полях великого розміру тощо) за поліноміальний час. Потенційна поява стабільно-працюючого квантового комп'ютера спонукає до пошуку альтернативних безпекових методів, що залишатимуться стійкими у пост-квантовий період. Все це спонукає до пошуку альтернативних безпекових методів, що залишатимуться стійкими у пост-квантовий період. Такими підходами можуть бути методи квантової і пост-квантової криптографії. З огляду на це, актуальною науково-прикладною проблемою є розробка і дослідження методів квантової та пост-квантової криптографії, які не залежать від обчислювальних та інших можливостей зловмисників і дозволяють забезпечити захист інформаційної інфраструктури в пост-квантовий період.

Як показав проведений аналіз, є два взаємодоповнюючі підходи до побудови квантово-стійкої інформаційної інфраструктури (стійкої у пост-квантовий період):

1) розробкою і дослідженням квантово-криптографічних методів та засобів займаються такі вітчизняні та закордонні вчені [1-5, 11-12]: Ч. Беннет, Ж. Брассар, Є. Васіліу, Н. Гісін, І. Джорджевіч, А. Еккерт, П. Завадскі, У. Збінден, С. Кілін, Н. Люткенхаус, М. Нільсен, В. Скарані, А. Цайлінгер та інші. Більшість з цих досліджень орієнтовані на так звані методи квантового

розподілу ключів (BB84, SARG, COW, B92, E91 та ін.) [1-3, 5], які дозволяють вирішити проблему розподілу ключів шифрування в умовах секретності і, як правило, використовуються разом із симетричними криптографічними алгоритмами. Іншим напрямком квантової криптографії є використання методів квантового прямого безпечного зв'язку (КПБЗ) [1,4], які дозволяють передавати інформацію відкритим каналом напряму без попереднього шифрування. Проте, в оригінальному вигляді зазначені квантово-криптографічні протоколи, не завжди забезпечують теоретико-інформаційну стійкість, вони є уразливими до спеціалізованих атак і потребують удосконалення.

2) розробкою і дослідженням методів пост-квантової криптографії займаються такі вітчизняні та закордонні вчені [6-10, 13-14]: Д. Бернштейн, Д. Бонех, І. Горбенко, В. Кінзерявий, Н. Кучинська, О. Кузнецов, А. Олексійчук, Р. Олійников, Р. Райвест, Т. Фернандез-Карамес, М. Явіч, С. Яковлєв та багато інших. Дослідження орієнтовані на розробку блокових симетричних пост-квантових криптоалгоритмів [6-8], потокових симетричних пост-квантових криптоалгоритмів [9], асиметричних криптоалгоритмів [10], що як правило, ґрунтуються на геш-функціях, коригуючих кодах, решітках, багатовимірних квадратичних системах, ізогеній суперсингулярних еліптичних кривих тощо. Наразі триває становлення пост-квантових алгоритмів як в Україні (прийняті стандарти криптографічного захисту даних «Калина», «Купина», «Струмок», «Скеля»), так і у світі, а тому великий спектр завдань залишається невирішеним.

Крім того, важливим на сьогодні є комплексний підхід до захисту інформаційної інфраструктури у пост-квантовий період, тобто одночасне забезпечення конфіденційності, цілісності та доступності (так звана, тріада CIA).

Основними перевагами методів квантового розподілу ключів є можливість точного виявлення порушника і забезпечення теоретико-інформаційної стійкості. Пост-квантова ж криптографія забезпечує стійкість в умовах реалізації відомих квантових алгоритмів. На цей час вже відомо багато алгоритмів і протоколів як квантового-розподілу ключів, так і пост-квантової криптографії, проте залишається ціла низка задач, розв'язання яких має важливе наукове значення в галузі кібербезпеки.

Список літератури

1. G. Brassard, "Quantum communication complexity: a survey," Proceedings. 34th International Symposium on Multiple-Valued Logic, 2004, pp. 56-, doi: 10.1109/ISMVL.2004.1319920.

2. P. Chaiwongkhot, Y. Zhang, J.-Ph. Bourgoin, N. Lütkenhaus et al, Eavesdropper's ability to attack a free-space quantum-key-distribution receiver in atmospheric turbulence, Physical Review A, 2019, vol.99, issue 6, 062315.

3. B. Djordjevic, "Hybrid QKD Protocol Outperforming Both DV- and CV-QKD Protocols," in IEEE Photonics Journal, vol. 12, no. 1, pp. 1-8, Feb. 2020, Art no. 7600108, doi: 10.1109/JPHOT.2019.2946910.

4. Y. Vasiliu, I. Limar, T. Gancarczyk and M. Karpinski, "New Quantum Secret Sharing Protocol Using Entangled Qutrits," 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems:

Technology and Applications (IDAACS), 2019, pp. 324-329, doi: 10.1109/IDAACS.2019.8924256.

5. Boaron, G. Boso, D. Rusca, H. Zbinden et al, Secure Quantum Key Distribution over 421 km of Optical Fiber, Phys. Rev. Lett., vol. 121, No. 190502, 2018.

6. Cohen, R. G. L. D'Oliveira, S. Salamatian and M. Médard, "Network Coding-Based Post-Quantum Cryptography," in IEEE Journal on Selected Areas in Information Theory, vol. 2, no. 1, pp. 49-64, March 2021, doi: 10.1109/JSAIT.2021.3054598.

7. T. M. Fernández-Caramés, "From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things," in IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6457-6480, July 2020, doi: 10.1109/JIOT.2019.2958788.

8. Daniel J. Bernstein, Tanja Lange, Post-quantum cryptography, 2017, Nature, vol. 549, issue 7671, pp. 188-194.

9. Gorbenko, O. Kuznetsov, Y. Gorbenko, A. Alekseychuk and V. Tymchenko, "Strumok keystream generator," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), 2018, pp. 294-299, doi: 10.1109/DESSERT.2018.8409147.

10. Mustafa et al., "A Lightweight Post-Quantum Lattice-Based RSA for Secure Communications," in IEEE Access, vol. 8, pp. 99273-99285, 2020, doi: 10.1109/ACCESS.2020.2995801.

11. Hu Z., Gnatyuk S., Okhrimenko T., Tynymbayev S., Iavich M. High-speed and secure PRNG for cryptographic applications, International Journal of Computer Network and Information Security, Volume 12, Issue 3, pp. 1-10, 2020.

12. Iavich M., Kuchukhidze T., Iashvili G., Gnatyuk S. Hybrid quantum random number generator for cryptographic algorithms, Radioelectronic and Computer Systems, 2021, Issue 4, pp. 103-118.

13. Iavich M., Iashvili G., Gnatyuk S., Tolbatov A., Mirtskhulava L. Efficient and Secure Digital Signature Scheme for Post Quantum Epoch, Communications in Computer and Information Science, Vol. 1486, pp. 185-193, 2021.

14. Labadze G., Iavich M., Iashvili G., Gagnidze A., Gnatyuk S. Post-quantum digital signature scheme with BB84 protocol, CEUR Workshop Proceedings, Vol. 2915, pp. 35-44, 2021.