МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2017 Т. 8 № 2 С. 77 – 86

УДК 519.719.2

New methods of error correction in quantum cryptography using low-density parity-check codes

D. A. Kronberg

Lomonosov Moscow State University, Moscow

Получено 18.III.2016

Abstract. The problem of error correction in quantum cryptography is considered, including the estimation of error rate. We show that low-density parity-check (LDPC) codes are appropriate for this problem, and propose some modifications to achieve better code performance, taking into account the special properties of quantum cryptography.

Keywords: quantum cryptography, error correction, coding theory, LPDC-code

Новые методы исправления ошибок в квантовой криптографии с использованием LDPC-кодов

Д. А. Кронберг

Московский государственный университет им. М. В. Ломоносова, Москва

Аннотация. В работе рассматривается задача коррекции ошибок в квантовой криптографии совместно с оценкой уровня ошибок. Показано, что для решения такой задачи подходят коды с малой плотностью проверок на четность (LDPC-коды). С учетом особенностей квантовой криптографии предлагаются некоторые модификации применения этих кодов, повышающие их эффективность.

Ключевые слова: квантовая криптография, коррекция ошибок, теория кодирования, LDPC-код

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 2, pp. 77–86 (Russian)

References

[1] Gallager R., “Low-density parity-check codes”, *IRE Trans. Inf. Theory*, **IT-8** (1962), 21–28.

[2] MacWilliams F. J., Sloane N. J. A., *The Theory of Error-Correcting Codes*, Amsterdam : North Holland, 1977, xx+762 pp.

[3] MacKay D. J. C., *Information Theory, Inference and Learning Algorithms*, Cambridge : Cambridge Univ. Press, 2003, xii+628 pp.

[4] Johnson S. J., *Iterative Error Correction: Turbo, Low-Density Parity-Check and Repeat-Accumulate Codes*, Cambridge : Cambridge Univ. Press, 2009, 356 pp.

[5] Molotkov S. N., “Cryptographic robustness of a quantum cryptography system using phase-time coding”, *Z. Eksper. Teor. Fisiki*, **133** :1 (2008), 5–24 (in Russian); англ. пер. , *J. Exper. Theor. Physics*, **106** :1 (2008), 1–16.

[6] Kronberg D. A., Molotkov S. N., “Security of a two-parameter quantum cryptography system using time-shifted states against photon-number splitting attacks”, *Z. Eksper. Teor. Fisiki*, **136** :4 (2009), 650–683 (in Russian); англ. пер. , *J. Exper. Theor. Physics*, **109** :4 (2009), 557–584.

[7] Elliott C., Colvin A., Pearson D., Pikalo O., Schlafer J., Yeh H., “Current status of the DARPA quantum network”. In: “*Defense and Security*”: Int. Society for Optics and Photonics, 2005, 138–149.

[8] Elkouss D., Leverrier A., Alleaume R., Boutros J. J., “Efficient reconciliation protocol for discrete-variable quantum key distribution”. In: “*IEEE Int. Symp. Inf. Theory*”, 2009, 1879–1883.

[9] Dixon A. R., Sato H., “High speed and adaptable error correction for megabit/s rate quantum key distribution”, *Scientific reports*, **4** :7275 (2014), https://www.nature.com/articles/srep07275.

[10] Brassard G., Salvail L., “Secret-key reconciliation by public discussion”. In: “*EUROCRYPT’93*”, Lect. Notes Comput. Sci., **765**, 1993, 410–423.

[11] Pedersen T. B., Toyran M., “High performance information reconciliation for QKD with CASCADE”, *Quant. Inf. and Comput.*, **15** :5-6 (2015), 419–434.

[12] Martinez-Mateo J., Pacher C., Peev M., Ciurana A., Martin V., “Demystifying the information reconciliation protocol cascade”, *Quant. Inf. and Comput.*, **15** :5-6 (2015), 453–477.