УДК 004.056.53

О ПОСТРОЕНИИ И ПРИМЕНЕНИИ КРИПТОГРАФИЧЕСКИХ ХЭШ-ФУНКЦИЙ, ОСНОВАННЫХ НА ГРАФАХ

Кирьянова А. П., **Давыдов В. В.** (Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Научный руководитель – преподаватель Давыдов В. В.

(Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Введение. На сегодняшний день, в связи с угрозой появления полноценного квантового компьютера, важным направлением исследований являются алгоритмы постквантовой криптографии. Алгоритм Шора [1], решающий задачи факторизации и дискретного логарифмирования на квантовом компьютере, бесполезен по отношению к традиционным хэш-функциям, построенных на основе функций сжатия, а также к хэшам, основанным на иных математических задачах. Хэш-функции, основанные на графах, открывают новые направления развития постквантовой криптографии.

Основная часть. В работе проанализированы хэш-функции, основанные на графах. Рассмотрены расширяющие графы, их свойства, а также математические задачи, на которых строятся хэш-функции на таких графах. Рассмотрены хэш-функции Zemor-Tillich [2], CGL [3], LPS [4] и Morgenstern [5]. Проанализирована стойкость к коллизиям и атакам нахождения первого и второго прообраза рассмотренных хэш-функций, сделаны выводы о целесообразности использования таких хэш-функций в современных криптографических алгоритмах и протоколах. Изучается связь между такими хэш-функциями и дистанционно-ограниченными протоколами, построенными на графах [6,7], для недорогих устройств, таких как RFID.

Выводы. Проанализированы хэш-функции на расширяющих графах, обсуждается их применение в реальных системах. Рассмотренные хэш-функции могут быть использованы для увеличения уровня безопасности в дистанционно-ограниченных протоколах.

Список использованных источников:

1. Shor P. W. Algorithms for quantum computation: discrete logarithms and factoring // Proceedings 35th annual symposium on foundations of computer science. – Ieee, 1994. – С. 124-134.
2. Tillich J. P., Zémor G. Hashing with SL_2 // Advances in Cryptology – CRYPTO'94: 14th Annual International Cryptology Conference Santa Barbara, California, USA August 21–25, 1994 Proceedings 14. – Springer Berlin Heidelberg, 1994. – С. 40-49.
3. Charles D., Goren E., Lauter K. Cryptographic hash functions from expander graphs // Cryptology ePrint Archive. – 2006.
4. Lubotzky A., Phillips R., Sarnak P. Ramanujan graphs // Combinatorica. – 1988. – Т. 8. – №. 3. – С. 261-277.
5. Morgenstern M. Existence and explicit constructions of q+1 regular Ramanujan graphs for every prime power q // Journal of Combinatorial Theory, Series B. – 1994. – Т. 62. – №. 1. – С. 44-62.
6. Hancke G. P., Kuhn M. G. An RFID distance bounding protocol // First international conference on security and privacy for emerging areas in communications networks (SECURECOMM'05). – IEEE, 2005. – С. 67-73.

7. Trujillo-Rasua R., Martin B., Avoine G. The Poulidor Distance-Bounding Protocol // RFIDSec. – 2010. – Т. 10. – С. 239-257.

Кирьянова А. П. (автор)

Давыдов В. В. (автор, научный руководитель)