УДК 003.26

ПОСТ-КВАНТОВЫЕ ПРОТОКОЛЫ ВЫРАБОТКИ ОБЩЕГО СЕКРЕТНОГО КЛЮЧА

Ниткин И.С., Кирьянова А.П.
Научный руководитель – Давыдов В.В.
Университет ИТМО

Введение.

Протокол Диффи – Хеллмана представляет собой способ выработки общего секретного ключа участниками защищенного обмена информацией [1]. Данный протокол является востребованным аналогом асимметричных протоколов PKE (public key encapsulation), которые предполагают выработку секретного ключа одним из участников обмена информацией с последующей передачей выработанного ключа другим участникам в зашифрованном виде.

Криптографическая стойкость протокола Диффи – Хеллмана основана на сложности решения задачи дискретного логарифмирования в конечном поле [2]. Однако указанная задача может быть решена за полиномиальное время на квантовом компьютере при помощи алгоритма Шора [3]. В этой связи востребованными являются исследования в области разработок пост-квантовых аналогов протокола Диффи – Хеллмана, стойкость которых должна быть основана на вычислительных задачах, которые не могут быть решены за полиномиальное время на квантовом компьютере.

Основная часть.

В рамках представляемого исследования проведен сравнительный анализ протоколов, аналогичных протоколу Диффи – Хеллмана, построенных на основе различных пост-квантовых примитивов. Рассмотрены протоколы на основе изогений суперсингулярных эллиптических кривых (в том числе CSIDH [4]), решеток (в т.ч. New Hope [5]), корректирующих кодов (протокол на основе квазициклических MDPC кодов [6]). Приводится сравнительная характеристика быстродействия и теоретической стойкости протоколов на основе вычислительной сложности задач, лежащих в их основе.

На основе анализа рассмотренных протоколов сделаны выводы о проблемах построения протоколов выработки общего секретного ключа на основе других общеизвестных пост-квантовых примитивов: хэш-функций и систем многомерных уравнений.

Заключение.

Таким образом, в рамках проведенного исследования изучены наиболее распространенные протоколы выработки общего секретного ключа на основе пост-квантовых примитивов, определены их достоинства и недостатки.

На основе результатов проведенного исследования могут быть выполнены исследования по разработке оптимального пост-квантового протокола выработки общего секретного ключа, в том числе выбору базового криптографического примитива.

Список использованных источников:

1. Diffie W. New Directions in Cryptography / W. Diffie, M. E. Hellman // IEEE Trans. Inf. Theory : электронный журнал. – URL: https://dx.doi.org/10.1109/TIT.1976.1055638. – Дата публикации: 1976.
2. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography / Menezes A.J. – Boca Raton : CRC Press, 2001. – 816 с.
3. Shor P. W. Algorithms for quantum computation: discrete logarithms and factoring / P. W. Shor // Proceedings of the 35th Annual Symposium on Foundations of Computer Science : электронный журнал. – URL: https://doi.org/10.1109/SFCS.1994.365700.

4. Castryck W. CSIDH: An Efficient Post-Quantum Commutative Group Action / W. Castryck, T. Lange, C. Martindale, L. Panny, J. Renes// Cryptology ePrint Archive, Paper 2018/383 : электронный журнал. – URL: https://eprint.iacr.org/2018/383. – Дата публикации: 2018.

5. Alkim E. Post-quantum key exchange - a new hope / E. Alkim, L. Ducas, T. Pöppelmann, P. Schwabe // Cryptology ePrint Archive, Paper 2015/1092 : электронный журнал. – URL: https://eprint.iacr.org/2015/1092. – Дата публикации: 2015.

6. Sendrier N. Code-Based Cryptography: State of the Art and Perspectives / N. Sendrier // IEEE Security & Privacy, vol. 15, no. 4 : электронный журнал. – URL: https://ieeexplore.ieee.org/document/8012331/authors#authors. – Дата публикации: 2017.

Ниткин И.С. (автор) _____

Кирьянова А.П. (соавтор) _____

Давыдов В.В. (научный руководитель) _____