УДК 004.056.55

УЛУЧШЕНИЕ КРИПТОСТОЙКОСТИ И ПРОИЗВОДИТЕЛЬНОСТИ ПОСТКВАНТОВОГО АЛГОРИТМА NTRUENCRYPT

Ляшенко Н.Г.(ДГТУ),
Научный руководитель – д.ф.-м.н., профессор кафедры «Кибербезопасность информационных систем » Черкесова Л.В. (ДГТУ)

Введение. NTRUEncrypt – постквантовый алгоритм ассиметричного шифрования, который был впервые предложен в 1996 году, а в 2011 году был включён в стандарт IEEE P1361.1 [1]. В отличие от алгоритма RSA и схемы Эль-Гамаля, алгоритм NTRUEncrypt является устойчивым к атакам с применением квантового компьютера. В 2016 году этот алгоритм был заявлен на конкурс NIST, целью которого является стандартизация алгоритмов постквантовой криптографии [2]. Известной уязвимостью алгоритма NTRUEncrypt является возможность осуществления атаки на основе подобранного шифротекста, которая позволяет злоумышленнику вычислить открытый ключ, использовав ограниченное количество пар открытых тектов и соответствующих им шифротекстов [3].

Основная часть. В работе предложена модификация постквантового алгоритма ассиметричного шифрования NTRUEncrypt. Преимуществами модификации являются более высокая производительность и защита от атаки на основе подобранного шифротектса. Повышение производительности алгоритмов генерации ключей, шифрования и расшифрования. Наиболее вычислительно затратной операцией алгоритма NTRUEncrypt является операция умножения полиномов. При использовании стандартного алгоритма, умножение полиномов имеет квадратичную сложность относительно количества разрядов числа. Для повышения производительности алгоритма предложено применить алгоритм Карацубы, который обладает меньшей вычислительной сложностью. Для противодействия атаке на основе подобранного шифротекста, используется хэш-функция, входным значением которой является конкатенация открытого текста и случайной последовательности. Таким образом, вычисление закрытого ключа невозможно для злоумышленника, осуществляющего атаку на основе подобранного шфиротектса.

Выводы. Построена математическая модель модифицированного алгоритма. Выполнена программная реализация системы шифрования с графическим интерфейсом на основе модифицированного алгоритма NTRUEncrypt.

Список использованных источников:

1. Azizi A., Laaji H. A Boosted Performances of NTRUEncrypt Post-Quantum Cryptosystem. Journal of Cyber Security and Mobility. – 2021. – pp. 725–744. https://doi.org/10.13052/jcsm2245-1439.1045
2. Hülsing, A.; Rijneveld, J.; Schanck, J.; Schwabe, P. High-Speed Key Encapsulation from NTRU. In Cryptographic Hardware and Embedded Systems—CHES 2017; Springer International Publishing: Cham, Switzerlamd, 2017; pp. 232–252, https://doi.org/10.1007/978-3-319-66787-4_12
3. Jonghwan K., Jong-Hwan P. NTRU++: Compact Construction of NTRU Using Simple Encoding Method, IEEE Transactions on Information Forensics and Security, 2023, vol 18, pp.4760-4774, https://doi.org/10.1109/TIFS.2023.3299172

Автор _____ Ляшенко Н. Г.

Научный руководитель_____Черкесова Л.В.