УДК 004.056.55

АНАЛИЗ СХЕМ ГОМОМОРФНОГО ШИФРОВАНИЯ НА ТЕОРИИ РЕШЁТОК

Кустов Е.Ф. (Университет ИТМО)
Научный руководитель – д.т.н, профессор Беззатеев С.В.
(Университет ИТМО)

Введение. Схемы гомоморфного шифрования применяются в случаях, когда необходимо для данного шифротекста любому человеку получить шифротекст от любой желаемой функции до тех пор, пока данная функция может быть эффективно вычислена. Однако большинство схем основаны на задаче факторизации и дискретного логарифмирования. После изобретения Питером Шором квантового алгоритма возник вопрос о создании новых систем устойчивых к атаке с использованием квантового компьютера. Одним из возможных решений описанной проблемы может являться схема, основанная на теории решёток.

Основная часть. Был проведён сравнительный анализ схем гомоморфного шифрования на основе трёх критериев: размеры ключей, вычислительная сложность алгоритма и устойчивость к современным атакам. Большинство современных схем, хоть и удовлетворяют поставленным критериям, однако не являются постквантовыми.
Возможным решением могут являться схемы на теории решёток. Исследований схем, основанных на теории решёток, не так много. Основная суть данных схем заключается в использование модифицированной схемы NTRU. Безопасность схем базируется на проблемах M-LWE и M-SIS, которые являются np сложными и устойчивы к атакам с использованием квантового компьютера.
Однако постквантовые схемы гомоморфного шифрования не отвечают современным требованиям, так как обладают достаточно большими размерами ключей. Для практического применения необходимо уменьшить размеры ключей, это задача для будущих исследований.

Выводы. В результате исследований был получен сравнительный анализ схем гомоморфного шифрования на основе трёх критериев. Исходя из анализа, ясно, что схемы, применимые на практике, не являются постквантовыми, а постквантовые схемы не удовлетворяют современным требованиям.

Список использованных источников:

1. Gentry C. Fully homomorphic encryption using ideal lattices //Proceedings of the forty-first annual ACM symposium on Theory of computing. – 2009. – С. 169-178.
2. Brakerski Z., Vaikuntanathan V. Fully homomorphic encryption from ring-LWE and security for key dependent messages //Advances in Cryptology–CRYPTO 2011: 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings 31. – Springer Berlin Heidelberg, 2011. – С. 505-524.
3. Li Y., Ng K. S., Purcell M. A Tutorial Introduction to Lattice-based Cryptography and Homomorphic Encryption //arXiv preprint arXiv:2208.08125. – 2022.
4. Chaudhary P. et al. Analysis and comparison of various fully homomorphic encryption techniques //2019 International Conference on Computing, Power and Communication Technologies (GUCON). – IEEE, 2019. – С. 58-62.
5. Zheng Z., Liu F., Tian K. An Unbounded Fully Homomorphic Encryption Scheme Based on Ideal Lattices and Chinese Remainder Theorem //arXiv preprint arXiv:2301.12060. – 2023.

Кустов Е.Ф. (автор) Подпись

Беззатеев С.В. (научный руководитель) Подпись