КРИПТОГРАФИЧЕСКАЯ СХЕМА ОБУЧЕНИЯ С ОШИБКАМИ НА РЕШЕТКАХ С ДОПОЛНИТЕЛЬНЫМ КОДИРОВАНИЕМ ПОЛЯРНЫМ КОДОМ

В.В. Панькова, С.Б. Саломатин

[1]*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь*

Гомоморфное шифрование обеспечивает безопасную обработку данных непосредственно над шифротекстом, результаты вычислений которого также шифруются. Известны схемы асимметричного шифрования для побитового шифрования потока данных. Схемы обучения с ошибками (RLWE), полностью гомоморфны и имеют два подпроцесса: один связан с целочисленными векторами, принятия решений, а другой связан с целочисленными полиномами [1].

Существует компромисс в схемах шифрования с открытым ключом (PKE), основанных на кольцевом обучении с ошибками (RLWE), а именно: требование более широкого распределения ошибок для повышения безопасности.

Прямым решением этой проблемы является код исправления ошибок [2]. Однако применение корректирующих кодов к криптографическим схемам имеет свои особенности. Во-первых, остаточный компонент ошибки, полученный при расшифровании, имеет коррелированные коэффициенты. Наиболее распространенные коды с исправлением ошибок предполагают, что шум канала является независимым и не имеет памяти. Это объясняет, почему в существующих схемах PKE на основе RLWE используются только простые методы исправления ошибок. Во-вторых, компонент остаточной ошибки имеет коррелированные коэффициенты, что затрудняет точную оценку частоты отказов расшифрования. В-третьих, большинство кодов, исправляющих ошибки, плохо спроектированы с точки зрения безопасности, например, декодирование синдрома носит непостоянный характер во времени.

Одним из путей решения задачи является применение схемы полярного кодирования [3] систем PKE на основе RLWE. Биноминальное распределение весов и предположение о «независимости» используется для получения некоррелированного остатка шумовой компоненты, а стратегия беспроводной связи, отказ, применяется для построения полярных кодов.

Моделирование схемы показало, что предлагаемая структура повышает запас по частоте отказов расшифрования. Полярное кодирование и декодирование имеют квазилинейный характер сложности и обладает внутренней поддержкой реализаций с постоянным временем.

Список литературы

1. Гаража А.А., Герасимов И.Ю., Николаев М.В. Об использовании библиотек полностью гомоморфного шифрования // International Journal of Open Information Technologies. 2021. Vol. 9, no. 3. С. 11–20.

2. Fritzmann T., Poppelmann T., Sepulveda J. Analysis of error correcting codes for lattice-based key exchange // International Conference on Selected Areas in Cryptography. 2018. P. 369–390.

3. Гладких А.А., Климов Р.В., Чилихин Н.Ю. Методы эффективного декодирования избыточных кодов и их современные приложения. Ульяновск : УлГТУ, 2016. 258 с.