ОСОБЕННОСТИ ФОРМИРОВАНИЯ КЛЮЧЕВЫХ ДАННЫХ ДЛЯ ЭЦП CRYSTALS-DILITHIUM

Мельникова О.А., Смирнов Е.В.
Харьковский национальный университет радиоэлектроники, г. Харьков

В рамках конкурса NIST-Post-Quantum Cryptography проводится отбор перспективных асимметричных криптосистем. Из ЭЦП, основанных на преобразованиях в алгебраических решетках, во второй раунд отбора вышли следующие алгоритмы: FALCON, CRYSTALS-DILITHIUM, qTESLA. В данной работе рассматриваются особенности формирования ключевых данных для электронной цифровой подписи (ЭЦП) CRYSTALS-DILITHIUM [1].

В большинстве алгоритмов подписи на алгебраических решетках, формирование секретных случайных значений основывается на использовании дискретного распределения Гаусса. Разработка алгоритмов генерации подобных случайных значений, которые были бы защищены от, так называемых, атак со сторонних каналов, является сложной задачей. То есть, высока вероятность снижения как степени безопасности, так и вычислительной эффективности криптосистемы именно на этапе реализации. Поэтому разработчики алгоритма предлагают, в качестве упрощенного варианта, ограничиться использованием равномерно распределенных случайных значений. Данный алгоритм может применятся в методе [2].

Основные параметры для формирования ключевой пары алгоритма:

(k, l) – размерность матрицы A, определяющей стойкость ключей; может принимать значения (3,2); (4,3); (5,4); (6,5);

q – простое число, равное 8380417 ($q = 2^{23} – 2^{13} + 1$);

η – предельное значение коэффициентов формируемых векторов s_1 и s_2.

Алгоритм генерации ключевой пары $\{pk, sk\}$ формирует матрицу A размера $k \times l$, элементы которой интерпретируются как полиномы кольца $R_q = Z_q[X] / (X^n + 1)$, где $n = 256$. Далее создаются случайные ключевые вектора s_1 и s_2. Каждый коэффициент этих векторов является элементом кольца R_q с коэффициентами $\eta < 8$. Вторая часть t открытого ключа pk вычисляется с использованием матрицы A и случайных ключевых векторов: $t = A \cdot s_1 + s_2$. При этом все алгебраические операции выполняются над элементами кольца R_q. Сформированная несимметричная ключевая пара состоит из следующих значений: $pk = (A, t)$ – открытый ключ проверки ЭЦП, $sk = (A, t, s_1, s_2))$ – личный конфиденциальный ключ формирования ЭЦП.

Литература:

1. Ducas L., Kiltz E., Lepoint T., Lyubashevsky V., Schwabe P., Seiler G., Stehlé D. (2018), CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme: [Электронный ресурс]. – Режим доступа: https://eprint.iacr.org/2017/633.pdf. **2.** Белей О.І. Гомоморфное шифрование данных в облачном хранилище методом матричных полиномов / О.І. Белей // Современное состояние научных исследований и технологий в промышленности. – 2018. – № 4 (6). – С. 5-14.