AMC bonus task

Работу выполнили: Петрушина Ксения и Моложавенко Александр, Б05-906

Данная криптосистема устроена следующим образом:

i) Задаётся целочисленное значение $module$, далее случайным образом генерируются ключи: приватный (A, S, E, ASE) и публичный (A, ASE). у A каждый элемент в диапазоне от 1 до $module$, у E, S в диапазоне от $-module/2 + 1$ до $module/2$. ASE вычисляется по формуле:

$$A \cdot S + E \mod module$$

ii) Сообщение msg подписывается по алгоритму, который сначала генерирует векторы y_1, y_2 в том же диапазоне, что и E, S, затем вычисляется новый вектор w следующим образом:

$$w = y_1 \cdot A + y_2 \mod module$$

Затем вычисляется ещё один вектор c по формуле:

$$c = w + hash(msg) \mod module$$

Далее подсчитываются очень важные векторы z_1, z_2:

$$z_1 = S \cdot c + y_1 \mod module$$

$$z_2 = E \cdot c + y_2 \mod module$$

Кортеж из трёх значений $\{c, z_1, z_2\}$ — наша подпись.

iii) Проверка подписи составляет вычисление следующего предиката:

$$A \cdot z_1 + z_2 - ASE \cdot c + hash(msg) \equiv c \mod module \tag{0.1}$$

При этом z_1, z_2 не равны нулевому вектору.

Наша задача по публичному ключу $\{A, AES\}$ подобрать подходящие S^*, E^* так, чтобы предикат возвращал на них единицу. Вычислить их можно напимер из тождества на ASE ($ASE = A \cdot S + E \mod module$). Наши решения отличаются лишь тем, что в решении Александра вектор S^* берётся тождественно равным вектору, каждая координата которого равна 1, а в решении Ксении S^* генерируется случайно в диапазоне от 1 до $module$. Затем отличий нет и E^* вычисляется по формуле $E^* = ASE - A \cdot S^* \mod module$.

Алгоритм очевидно полиномиальный от $module$ (всю сложность составляет вычисление $\mod module$, принимая остальные арифметические вычисления за константу).

Взлом происходит корректно, поскольку при таких S^*, E^* тождество (0.1) выполняется:

$$A \cdot (S^* \cdot c + y_1) + (E^* \cdot c + y_2) - (A \cdot S^* + E^*) \cdot c + hash(msg) \equiv$$

$$\equiv A \cdot y_1 + y_2 + hash(msg) \equiv w + hash(msg) \equiv c$$