39 AddRot

Задача. Боб разрабатывает алгоритм шифрования, в котором к n-битовым машинным словам применяются преобразования двух типов: Add_c — сложение слова-как-числа с числом c по модулю 2^n, Rot_r — циклический сдвиг слова на r битов влево, $c = 1, 2, \ldots, 2^n - 1$, $r = 1, 2, \ldots, n-1$. Доказать, что с помощью сложений Add_c и сдвигов Rot_r можно реализовать любое биективное преобразование машинных слов.

Решение. Задача решена теоретико-групповыми методами в работе [Zieschang T. Combinatorial Properties of Basic Encryption Operations // Advances in Cryptology — EUROCRYPT'97 Proceedings, 1997]. Ниже приводится элементарное решение, полученное участниками олимпиады NSUCrypto-2014.

Будем отождествлять n-битовые слова с числами от 0 до $2^n - 1$. Интересующие нас преобразования Add_c, Rot_r являются подстановками на множестве $\{0, 1, \ldots, 2^n - 1\}$.

Рассмотрим подстановку-комопозицию $\tau = \mathrm{Rot}_1\mathrm{Add}_1\mathrm{Rot}_{n-1}\mathrm{Add}_{2^n-2}$ (действие τ состоит в применении сначала Add_{2^n-2}, затем Rot_{n-1}, Add_1 и наконец Rot_1). Подстановка τ оставляет на месте числа $x \geq 2$: для этих чисел

$$\begin{aligned}\tau(x) &= \mathrm{Rot}_1\mathrm{Add}_1\mathrm{Rot}_{n-1}(x-2) = \\ &= \mathrm{Rot}_1\mathrm{Add}_1\left(2^{n-1}((x-2) \bmod 2) + [(x-2)/2]\right) = \\ &= \mathrm{Rot}_1(2^{n-1}(x \bmod 2) + [x/2]) = x.\end{aligned}$$

Кроме этого,

$$\tau(1) = \mathrm{Rot}_1\mathrm{Add}_1\mathrm{Rot}_{n-1}(2^n - 1) = \mathrm{Rot}_1\mathrm{Add}_1(2^n - 1) = \mathrm{Rot}_1(0) = 0$$

и, следовательно, $\tau(0) = 1$.

Таким образом, подстановка τ является транспозицией чисел 0 и 1: $\tau = (0\ 1)$. С помощью τ и Add_c можно построить другие транспозиции соседних чисел:

$$\mathrm{Add}_1\tau\mathrm{Add}_{2^n-1} = (1\ 2), \quad \mathrm{Add}_2\tau\mathrm{Add}_{2^n-2} = (2\ 3), \ldots.$$

С помощью этих транспозиций можно реализовать любую подстановку на множестве $\{0, 1, \ldots, 2^n - 1\}$, т. е. любое биективное преобразование машинных слов. □