ВОССТАНОВЛЕНИЕ КЛЮЧЕЙ ШИФРА ГОСТ 28147 НА ОСНОВЕ СЛАЙД АТАКИ

Казимиров А.В.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, 14, каф. безопасности информационных технологий, тел. 7021425,
Email: okazymyrov@gmail.com; факс (057) 702-14-25

In given work a method for recovering long-term key and special session key of cipher GOST 28147 is described.

Шифр ГОСТ 28147 широко применяется в Украине и других странах СНГ [1]. Алгоритм основан на цепи Фейстеля с количеством раундов *r* равным 32 и функцией усложнения *F*, представленной на рисунке 1. Ключ шифрования представляется в виде долговременного (512 бит) и сеансового (256 бит) ключей. На сегодняшний день в открытой публикации не представлены работы, которые позволяют получить сеансовый ключ со сложностью меньшей, чем полный перебор. Тем не менее, получение долговременного ключа не такая сложная задача. В работе [2] были представлены некоторые идеи восстановления S-блоков со сложностью 2^{32}, однако изложенный алгоритм не позволяет получить практический результат и оценить эффективность применения на практике данной методики.

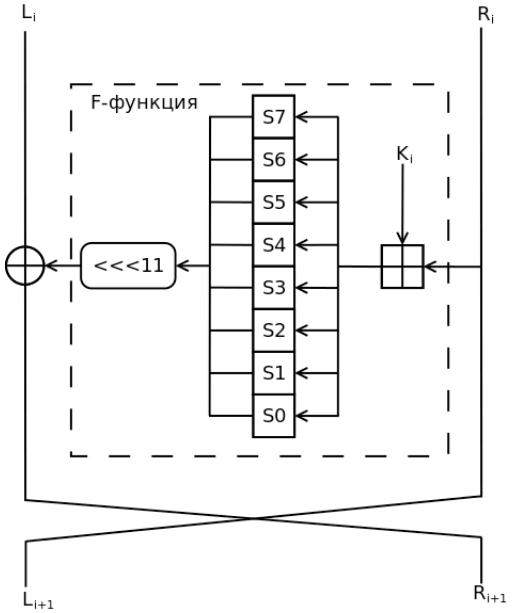

Рисунок 1 – Раундовая функция шифра ГОСТ 28147

Предлагаемая в данной работе методика восстановления долговременных ключей основана на слайд атаке [3], а также на атаке выбранных ключей. На рисунке 2 представлена схема атаки на шифр ГОСТ 28147, при идентичной цикловой функции. Это возможно, когда сеансовый ключ имеет вид $K_i = k$, где $0 \le k \le 2^{32} - 1$.

Восстановления долговременных ключей проходит в два этапа. На первом этапе необходимо установить значение сеансового ключа в 0, зашифровать сообщение $P' = (x,0), x = 0$ и получить шифротекст $C' = (c,a)$. Далее, перебирая все значения y от 0 до $2^{32} - 1$, необходимо найти такое значение $P = (y,x)$, при зашифровании которого получим сообщение $C = (a,b)$. Если нашли такую пару, значит можно вычислить значения всех восьми подстановок в точке ноль, используя уравнение $y = F(0)$.

Для нахождения остальных значений подстановок применяется метод полного перебора. Пусть $S_i(u) = v$ *i*-ая подстановка шифра ГОСТ. Из предыдущего шага известны *v* для всех подстановок в точке ноль ($S_i(0)$). Перебирая все возможные *i*, *v*, *u*, необходимо найти равные значения левой ($C_L = a$) и правой половины ($C'_R = a$) шифротекстов для открытых сообщений $P = (F(u \lll 4i), u \lll 4i)$ и $P' = (u \lll 4i, 0)$ соответственно, чтобы получить верное значение *v*

для *i*-ой подстановки в *u*-й точке. Применяя данную методику можно получить все подстановки шифра ГОСТ 28147, при этом сложность первого этапа будет не более 2^{32}, второго $2^3(2^4\text{-}1)2^4 2 \approx 2^{12}$. Общая сложность равна $2^{12}+2^{32} \approx 2^{32}$.

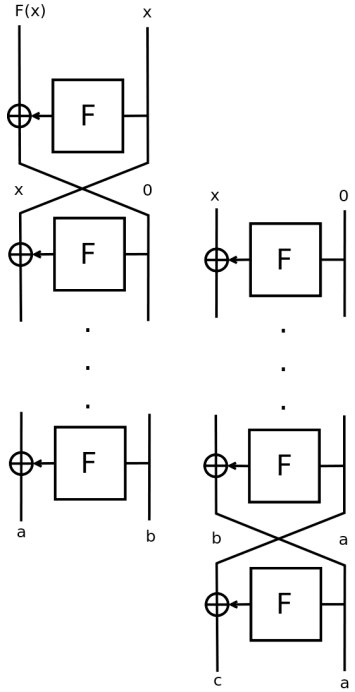

Рисунок 2 – Слайд атака на шифр ГОСТ 28147

В статье [4] приводится зависимость ключей вида $K_1 = K_8,\ K_2 = K_7,\ K_3 = K_6,\ K_4 = K_5$, которая позволяет получить открытое сообщение из шифротекста путём повторного зашифрования. Однако в такой ситуации невозможно создать новое сообщение с соответствующим правильным шифротекстом. Представленная выше методика позволяет получить не только долговременные ключи, но и сеансовые ключ вида $K_i = k$, при известных подстановках.

Для получения сеансового ключа необходимо зашифровать сообщение $P' = (x,0), x = 0$ и получить шифротекст $C' = (c,a)$. Далее найти такое значение $P = (y,x)$, при зашифровании которого получим сообщение $C = (a,b)$. Если нашли такую пару, значит можно вычислить ключ, используя уравнение $y = F(0)$. Сложность поиска не превышает 2^{32}.

Практические результаты показали, что максимальное время восстановления долговременного ключа шифра ГОСТ не превышает 2-х минут. Проведение 100 опытов по получению S-блоков показало, что в среднем время получения подстановок занимает около 1 минуты, при программной реализации алгоритма шифрования на компьютере с процессором Intel Core i7 870.

Приведённая методика позволяет восстановить все долговременные ключи шифра ГОСТ на практике со сложностью 2^{32}, которая гораздо меньше, чем полный перебор 2^{512}.

1. GOST 28147-89. Information Processing Systems. Cryptographic Protection. Algorithm for Cryptographic Transformation [in Russian], Gosstandart SSSR, Moscow (1989).
2. Saarinen M. J. A chosen key attack against the secret S-boxes of GOST. – 1998. – P. 1-3.
3. Biryukov A., Wagner D. Slide Attacks. Proceedings of FSE'99, LNCS 1636, Springer Verlag. – 1999. – P. 245-259.
4. Marcel Zanechal. An algebraic approach to fix points of GOST-algorithm. Mathematica Slovaca, Vol. 51 (2001), No. 5, P. 583 – 591.