

ность «Компьютерная безопасность». Разработана система учебных пособий [3,5] и проект стандарта по специальности «Компьютерная безопасность».

С 2001 г. в БГУ открыта аспирантура и докторантуре по специальности 05.13.19 – Методы защиты информации и информационная безопасность (физико-математические и технические науки). С 2005 г. совместно с Государственным центром безопасности информации при Президенте Республики Беларусь на базе БГУ открыты постоянно действующие курсы повышения квалификации в области безопасности информационных технологий. ННИЦ ППМИ участвует в организации научных конференций и издании сборников статей по проблемам информационной безопасности.

Литература

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2002. – 480 с.
2. Пярин В.А., Кузьмин А.С., Смирнов С.Н. Безопасность электронного бизнеса. – М.: Гелиос АРВ, 2002. – 432 с.
3. Харин Ю.С., Агиевич С.В. Компьютерный практикум по математическим методам защиты информации. – Минск: БГУ, 2001. — 190 с.
4. Харин Ю.С., Агиевич С.В., Галинский В.А., Микулич Н.Д. Алгоритм блочного шифрования ВейТ. – «Управление защитой информации», 2002, т. 6, № 4, с. 407-412.
5. Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В. Математические и компьютерные основы криптологии. — Минск: Новое знание, 2003. — 320 с.
6. Menezes A.J., van Oorschot P. C., Vanstone S.A. Handbook of Applied Cryptography. — CRC Press, 1996. — 816 p.

ПОКАЗАТЕЛИ И ОЦЕНКИ СТОЙКОСТИ БЛОЧНЫХ ШИФРОВ ОТНОСИТЕЛЬНО СТАТИСТИЧЕСКИХ АТАК ПЕРВОГО ПОРЯДКА

А. Н. Алексейчук, Л. В. Скрыпник, А. С. Шевцов

Украина, г. Киев

Одной из центральных проблем современной симметричной криптографии является создание общей теории обоснования стойкости блочных шифров. Разнообразие существующих методов их криptoанализа, появление новых перспективных направлений в этой области [1] требуют систематизации, упорядочения и осмысления с единых, общих позиций накопленных фактов и отдельных теоретических результатов.

Несмотря на повышенное внимание специалистов к проблеме теоретического обоснования эффективности известных статистических методов криptoанализа блочных шифров [2, 3], эти методы, в подавляющем большинстве, остаются полуэвристическими, "работающими" на практике, но не имеющими строгого обоснования. К их числу относятся классические методы дифференциального и линейного криptoанализа, а также их многочисленные обобщения [1, 3 – 8]. Отсутствие строгости в обосновании известных оценок надежности (вероятности правильного восстановления ключа) или сложности (необходимого числа

открытых сообщений) указанных статистических методов связано, прежде всего, с использованием, в явном или неявном виде, различных эвристических или упрощающих предположений, наподобие гипотез “о стохастической эквивалентности”, “строгой различимости ключей” и др. [4, 6, 7]. Как отмечено в [9] (стр. 414), проверить эти предположения для реальных криптосхем практически невозможно; кроме того, обычно несложно построить пример криптосистемы, для которой рассматриваемое предположение не выполнено.

Безусловно строгое обоснование условий, обеспечивающих стойкость блочных шифров относительно различающих атак, предложено в [2]. Вместе с тем, модель различающей атаки является несколько ограничительной, и результаты [2] непосредственно не применимы к решению задач оценки или обоснования стойкости блочных шифров относительно практических (“вскрывающих”) атак.

В докладе представлены теоретически обоснованные верхние границы надежности статистических атак первого порядка на блочные шифры. (Согласно [2, 3], атаками первого порядка называются атаки на основе известных или подобранных открытых сообщений, при которых для получения очередной “порции” информации о ключе криптоаналитику достаточно зашифровать ровно одно сообщение. Примерами служат атаки, основанные на методах линейного [5], обобщенного линейного [6], билинейного криптоанализа [8] или методе криптоанализа на основе разбиений [10]. Дифференциальному криптоанализу соответствуют атаки второго порядка, поскольку в этом случае зашифрованию подвергаются определенные пары открытых сообщений).

Полученные оценки позволяют ввести показатели стойкости блочных шифров относительно указанных атак, не прибегая к каким-либо эвристическим или упрощающим предположениям. В случае линейной различающей атаки полученная оценка стойкости (сложности атаки) оказывается примерно на один-два порядка точнее известной оценки [2].

Обозначим S^{V_n} симметрическую группу подстановок на множестве $V_n = \{0, 1\}^n$. Рассмотрим r -раундовый блочный шифр \mathcal{R} с множеством открытых (шифрованных) сообщений V_n , множеством раундовых ключей K , семейством раундовых шифрующих преобразований ($f^{(k)} \in S^{V_n} : k \in K$) и функцией шифрования $F: V_n \times K \rightarrow V_n$. Преобразование $F^{(k)}$ открытого сообщения $x \in V_n$ в шифрованный текст $y \in V_n$ на ключе $k = (k(1), \dots, k(r)) \in K$ шифра \mathcal{R} является композицией r раундовых шифрующих преобразований:

$$y = F^{(k)}(x) = (f^{(k(r))} \circ \dots \circ f^{(k(1))})(x), x \in V_n. \quad (1)$$

Зафиксируем отличную от константы булеву функцию $\phi: V_n \times V_n \rightarrow \{0, 1\}$. Различающая атака на шифр \mathcal{R} , основанная на отображении ϕ , осуществляется при следующих вероятностных предположениях [2]. Вначале с вероятностью $\frac{1}{2}$ выбирается число $v \in \{0, 1\}$. Затем фиксируется значение случайной подстановки C , которая распределена равномерно на всей симметрической группе

S^{V_n} , если $v=0$, и совпадает с вероятностью $|K|^{-r}$ с любой из подстановок $F^{(k)}$, $k \in K'$, если $v=1$. Атака состоит в проведении t независимых испытаний, в i -м из которых криптоаналитик генерирует не зависящий от подстановки C случайный вектор X_i с равномерным распределением на множестве V_n и вычисляет значение случайной величины

$$\xi_i = I\{\phi(X_i, C(X_i)) = 0\}, \quad i \in \overline{1, t}, \quad (2)$$

где $I(A)$ – индикатор произвольного события A . Целью атаки является проверка по наблюдаемой реализации случайной последовательности (2) гипотезы $H_0: v=0$ относительно альтернативы $H_1: v=1$. Стойкость шифра \mathfrak{R} к описанной атаке характеризуется предпочтением оптимального критерия различия указанных гипотез (см. [2]).

Справедлива следующая теорема.

Теорема 1. Пусть $\phi(x, y) = g(x) \oplus h(y)$, $(x, y) \in V_n^2$, где g, h – уравновешенные булевые функции n переменных, $\pi^*(\mathfrak{R}, \phi)$ – предпочтение оптимального критерия для проверки гипотез H_0 и H_1 по реализации случайной последовательности (2). Тогда

$$\pi^*(\mathfrak{R}, \phi) \leq 2\sqrt{t}((\bar{\lambda}_\phi)^{1/2} + (2^n - 1)^{-1/2}), \quad (3)$$

где

$$\bar{\lambda}_\phi = |K|^{-r} \sum_{k \in K'} (2P\{\phi(X, F^{(k)}(X)) = 0\} - 1)^2. \quad (4)$$

Различающую атаку нетрудно модифицировать таким образом, чтобы получить "вскрывающую" статистическую атаку на блочный шифр \mathfrak{R} . Такая атака проводится на основе выбираемых открытых сообщений и использует, помимо указанной выше булевой функции ϕ , уравновешенную функцию $\psi: K' \rightarrow \{0, 1\}$.

Пусть k – неизвестный случайный ключ шифра \mathfrak{R} , выбираемый с вероятностью $|K|^{-r}$ из множества K' . При проведении атаки криптоаналитик генерирует t независимых, случайных и равновероятных открытых сообщений X_1, \dots, X_t , зашифровывает их на ключе k и вычисляет значения случайных величин (2), где C обозначает случайное и равновероятное шифрующее преобразование шифра \mathfrak{R} . Цель атаки состоит в том, чтобы восстановить значение $\psi(k)$, то есть проверить по наблюдаемой реализации случайной последовательности (2) справедливость гипотезы $\tilde{H}_0: \psi(k) = 0$ относительно альтернативы $\tilde{H}_1: \psi(k) = 1$.

Теорема 2. Пусть $\pi^*(\mathfrak{R}; \phi, \psi)$ – предпочтение оптимального критерия для проверки гипотез \tilde{H}_0 и \tilde{H}_1 по реализации случайной последовательности (2). Тогда справедливо неравенство

$$\pi^*(\mathcal{R}; \phi, \psi) \leq 4\sqrt{t} (\bar{\lambda}_\phi)^{\frac{1}{2}}, \quad (6)$$

где $\bar{\lambda}_\phi$ определяется по формуле (4).

Отметим, что доказательства сформулированных теорем не используют эвристических предположений (вроде гипотез "о стохастической эквивалентности" или "строгой различности ключей" [4, 6, 7, 10]) относительно шифра \mathcal{R} .

Соотношения (3), (6) позволяют ввести (обоснованно, не прибегая к эвристическим рассуждениям) показатели стойкости блочных шифров относительно известных методов криptoанализа (обобщенного линейного, билинейного и др.). В частном случае, когда ϕ является линейной булевой функцией, описанная выше "вскрывающая" атака на шифр \mathcal{R} близка к так называемому алгоритму 1, предложенному Матчуи [5], а параметр (4) совпадает с классическим показателем стойкости блочных шифров относительно метода линейного криptoанализа.

Приведем верхнюю оценку параметра (4) для ГОСТ-подобного шифра \mathcal{R} при $r = 2$ и ряда билинейных функций ϕ (билинейный криptoанализ [8]).

Напомним [11], что ГОСТ-подобным называется шифр Фейстеля с длиной блока $n = 2m$, шифрующие преобразования которого в каждом из раундов имеют вид

$$f^{(k)}(x) = f^{(k)}(u, v) = (v, u \oplus g(v + k)), \quad x = (u, v), \quad u, v \in V_m, \quad (7)$$

где $+$ обозначает операцию сложения двоичных чисел, соответствующих булевым векторам, по модулю 2^m , а подстановка $g \in S^{V_m}$ определяется по формуле

$$g(z) = L(s^{(p-1)}(z^{(p-1)}), \dots, s^{(0)}(z^{(0)}))^T, \quad z = (z^{(p-1)}, \dots, z^{(0)}) \in V_m, \quad (8)$$

где $p, t \in \mathbb{N}$, $m = pt$, $z^{(j)} \in V_t$, $s^{(j)} \in S^{V_t}$, $j \in \overline{0, p-1}$, L – обратимая матрица порядка t над полем GF(2).

Рассмотрим семейство билинейных функций

$$\phi_A(x, y) = u_1 A L^{-1} v_1^T \oplus u_2 A L^{-1} v_2^T, \quad x = (u_1, v_1), \quad y = (u_2, v_2) \in V_n, \quad (9)$$

параметризованное двоичными матрицами A размера $t \times t$. Для любой подстановки $s \in S^{V_t}$ обозначим

$$I^{(s)} = \max_{B \neq 0} \left\{ 2^{-t} \sum_{k \in V_t} \left(2^{-t} \sum_{x \in V_t} \chi(x B s (x+k)^T) \right)^2 \right\}, \quad (10)$$

где $\chi(u) = (-1)^u$, $u \in \{0, 1\}$, $+$ обозначает сложение t -разрядных двоичных чисел по модулю 2^t , а максимум берется по всем ненулевым двоичным матрицам B порядка t .

Теорема 3. Пусть \mathcal{R} – 2-раундовый ГОСТ-подобный блочный шифр, описываемый соотношениями (1), (7) и (8), A_0, \dots, A_{p-1} – симметрические двоичные матрицы порядка t , не равные одновременно нулю, и $A = \text{diag}(A_{p-1}, \dots, A_0)$. Тогда параметр (4), соответствующий функции (9), удовлетворяет следующему неравенству:

$$\bar{\lambda}_{\Phi, A} \leq \max \{(\lambda^{(j)})^2 : j \in \overline{0, p-1}\}. \quad (11)$$

Отметим, что неравенства (6) и (11) позволяют оценивать снизу сложность билинейных атак на шифр, удовлетворяющий условиям теоремы 3, непосредственно по таблицам его узлов замены (подстановок $s^{(j)}$, $j \in \overline{0, p-1}$).

Результаты статистического оценивания распределения параметра (10) для случайной и равновероятной подстановки π степени 2^4 показывают, что для более чем 21 тысячи (из 25 тысяч генерированных) подстановок значение указанного параметра заключено в пределах от 0,31 до 0,35.

Литература

1. Birgukov A. Block ciphers and stream ciphers: the state of the art // <http://eprint.iacr.org/2004/094>.
2. Vaudenay S. Decorrelation: a theory for block cipher security // J. of Cryptology. – 2003. – Vol. 16. – № 4. – P. 249 – 286.
3. Wagner D. Towards a unifying view of block cipher cryptanalysis // Fast Software Encryption. – FSE'04, Proceedings. – Springer Verlag, 2004. – P. 116 – 135.
4. Lai X., Massey J.L., Murphy S. Markov ciphers and differential cryptanalysis // Advances in Cryptology – EUROCRYPT'91, Proceedings. – Springer Verlag, 1991. – P. 17 – 38.
5. Matsui M. Linear cryptanalysis methods for DES cipher // Advances in Cryptology – EUROCRYPT'93, Proceedings. – Springer Verlag, 1994. – P. 386 – 397.
6. Harpes C., Kramer G.G., Massey J.L. A generalization of linear cryptanalysis and the applicability of Matsui's piling-up lemma // Advances in Cryptology – EUROCRYPT'95, Proceedings. – Springer Verlag, 1995. – P. 24 – 38.
7. Junod P. On the complexity of Matsui's attack // Fast Software Encryption. – FSE'01, Proceedings. – Springer Verlag, 2001. – P. 199 – 211.
8. Courtois N.T. Feistel schemes and bi-linear cryptanalysis // Advances in Cryptology – CRYPTO'04, Proceedings. – Springer Verlag, 2004. – P. 23 – 40.
9. Логачев О.А., Сальников А.А., Ященко В.В. Булевые функции в теории кодирования и криптологии. – М.: МЦНМО, 2004. – 470 с.
10. Harpes C., Massey J.L. Partitioning cryptanalysis // Fast Software Encryption. – FSE'97, Proceedings. – Springer Verlag, 1997. – P. 13 – 27.
11. Alekseychuk A.N., Kovalchuk L.V. Upper bounds of maximum values of average differential and linear characteristic probabilities of Feistel cipher with adder modulo 2^m // Theory of Stochastic Processes. – 2006. – Vol. 12(28). – № 1, 2. – P. 20 – 32.

УТОЧНЕННЫЕ ОЦЕНКИ ПРАКТИЧЕСКОЙ СТОЙКОСТИ ГОСТ-ПОДОБНЫХ БЛОЧНЫХ ШИФРОВ ОТНОСИТЕЛЬНО МЕТОДОВ ЛИНЕЙНОГО И РАЗНОСТНОГО КРИПТОАНАЛИЗА

А. Н. Алексейчук, Л. В. Ковалчук, Л. В. Скрыпник

Украина, г. Киев

Линейный криптоанализ [1] и разностный криптоанализ [2] относятся к числу наиболее мощных статистических методов криптографического анализа