УДК 681.3.06: 519.248.681

АНАЛИЗ ВЕРОЯТНОСТИ ПЕРЕКРЫТИЯ БЛОКОВ БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ

М.С. МИХАЙЛЕНКО

Рассматриваются блочные симметричные шифры с точки зрения стойкости против атак типа создание коллизии и определение необходимой длины блока шифрования.

The paper considers sectional symmetric codes from the point of view of security against attacks of the type of creating a collision and determining the necessary length of ciphering block.

ВВЕДЕНИЕ

На наш взгляд, при построении БСШ, необходимо определить требования к допустимым значениям перекрытия шифра или, другими словами, совпадения отрезков зашифрованных текстов, при использовании разных ключей и открытых текстов. Анализ ряда источников, которые относятся к проектам AES и NESSIE [1, 2], показал, что в явном виде эти требования не задавались. Можно согласиться, что вероятность перекрытия шифра в значительной степени зависит от длины блока, которая используется в БСШ. Ни соответствующей теории оценки перекрытия шифра, ни практических рекомендаций и ограничений не установлено. Другим важным моментом является учёт режимов работы БСШ. В этом плане на наш взгляд все режимы можно разделить на два класса: непосредственно блочного симметричного шифрования и выработки имитовставки; и различные поточные режимы, включая выработку псевдослучайных последовательностей.

1. АНАЛИЗ ВЕРОЯТНОСТИ ПЕРЕКРЫТИЯ БЛОКОВ

По сути, рассматривается некоторое шифрообразующее устройство (ШОУ) рис. 1, на вход которого подаётся некоторая синхропоследовательность $СП_i$ и ключевые данные K_j, а на выходе получаем некоторую гамму шифрующую длины $СП_i$.

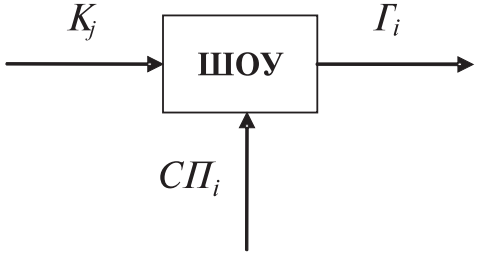

Рис. 1. Шифрообразующее устройство

Множество

$$(СП_i,\ K_j) \qquad (1)$$

определяет начальное состояние ШОУ, при этом также на начальное состояние может влиять выход $Г_i$, например за счет обратной связи по шифротексту. При указанных условиях, начальное состояние ШОУ каждый раз можно считать случайным. Если длина блока БСШ будет N_b, то число возможных выходов (блоков)

$$N_k = 2^{N_b}. \qquad (2)$$

Согласно введенной выше модели, нас будут интересовать двукратные коллизии, когда за промежуток времени ΔT, или выполнения числа тактов ΔS возникает коллизия, т.е. при разных $СП$ и $СП'$, и одном и том же ключе K, мы получаем одинаковые гаммы шифрующие $Г = Г'$ некоторой длины L_n.

При данных условиях возможны два варианта:

1. Произошло перекрытие (коллизия)

$$P(L_n, N_b) = P_п,$$

где $P_п$ – вероятность перекрытия. Т.е. выходные блоки совпадают на длине L_n при случайном состоянии ШОУ.

2. Не произошло перекрытие

$$P_о = 1 - P_п,$$

где $P_о$ – вероятность отсутствия перекрытия.

Для указанных условий найдём в наиболее обобщенном виде вероятность того, что перекрытие отсутствует. Для этого воспользуемся уже известным математическим аппаратом обобщенного парадокса дня рождения [3], но учитывая специфику постановки нашей задачи, например $N_b = L_n$. При этом будем считать $P(1) = P(0) = 0{,}5$, т.е. появление 1 и 0 на выходе ШОУ является равновероятным. Учитывая наложенные условия, вероятность появления блоков длиной L_n подчиняется биномиальному закону распределения выходов $Г_i$ длиной L_n [4].

Рассмотрим вероятность того, что перекрытие не произошло.

$$P_о = \frac{N_i}{N_\Sigma}, \qquad (3)$$

где N_i – число сформированных отрезков $Г_i$ длиной L_n, т.е. N_i – количество событий, которые произошли и не произошла коллизия, N_Σ – полное множество возможных отрезков $Г_i$. $N_\Sigma \neq N_K$ в общем случае, сейчас мы рассмотрим вариант, когда $N_\Sigma = N_K$.

При первом обращении существует N_K вариантов выбора гаммы. При втором обращении и следующих выбирается N_K–1, N_K–2... и т.д. вариан-

тов выбора отрезков. Таким образом число сформированных отрезков принимает вид

$$N_i = N_K(N_K-1)(N_K-2)...(N_K-i+1), \quad (4)$$

а общее число событий с вероятностью перекрытия соответствует

$$N_\Sigma = {N_K}^i. \quad (5)$$

Тогда вероятность отсутствия коллизии в общем случае выглядит так

$$P_o = \frac{N_K(N_K-1)(N_K-2)...(N_K-i+1)}{{N_K}^i}, \quad (6)$$

а вероятность перекрытия гамм

$$P_\text{п} = 1-\frac{N_K(N_K-1)(N_K-2)...(N_K-i+1)}{{N_K}^i}. \quad (7)$$

Формула (7) может быть использована для вычисления возникновения коллизий. Оценим возможность проведения вычислений по этой формуле на ПК. Коллизии могут возникать в этой системе при больший значениях i, пусть длина блока задана формулой (2), тогда сложность вычисления можно будет найти по следующей формуле

$$I = \sqrt{N_K} = 2^{\frac{Nb}{2}}, \quad (8)$$

при $N_b = 128$, $I = 2^{64}$, при $N_b = 256$, $I = 2^{128}$. Найдем время решения задачи для общего случая

$$t = \frac{a}{\gamma K}P_\text{в}, \quad (9)$$

где a – число событий; γ – число операций в секунду, например операций умножения, для нашего примера $\gamma = 10^{12}\ {}^{\text{опер}}/_{\text{с}}$; K – количество секунд в году, $3{,}15 \cdot 10^7\ {}^{\text{с}}/_{\text{год}}$; $P_\text{в}$ – вероятность вычисления, $P_\text{в} = 1$.

Тогда сложность вычислений для длины блока 256 бит равняется

$$t_j^{256} = \frac{2^{128}}{10^{12}\cdot 3{,}15\cdot 10^7}\cdot 1 \approx 11\cdot 10^{18}\ \text{лет}.$$

Аналогичные вычисления для длины блока 128 бит, $t_j^{128} = \frac{2^{64}}{10^{12}\cdot 3{,}15\cdot 10^7}\cdot 1 \approx 0{,}6$ года.

Таким образом, формула (7) является прозрачной, но с точки зрения применения на практике она не реализуема. Поэтому рекомендуется перейти к ряду аппроксимаций. Представим ее в другом виде

$$P_\text{п} = 1-1(1-\frac{1}{N_K})(1-\frac{2}{N_K})...(1-\frac{i-1}{N_K}) \quad (10)$$

Воспользуемся разложением экспоненты в виде ряда Тейлора

$$e^x = \sum_{n=0}^{\infty}\frac{x^n}{n!}. \quad (11)$$

Известно, что если $x < 0{,}1$, то $e^{-x} \approx 1\text{-}x$, тогда, если $\frac{1}{N}$ представить в виде x, вероятность перекрытия можно аппроксимировать в следующем виде

$$P_\text{п} = 1-e^{-\frac{1}{N_K}}e^{-\frac{2}{N_K}}...e^{-\frac{i-1}{N_K}} = 1-e^{-\left(\frac{1}{N_K}+\frac{2}{N_K}+...+\frac{i-1}{N_K}\right)}, \quad (12)$$

где $\left(\frac{1}{N_K}+\frac{2}{N_K}+...+\frac{i-1}{N_K}\right)$ является арифметической прогрессией, результат которой можно записать, как $\frac{1+i-1}{2N_K}(i-1) = \frac{i(i-1)}{2N_K}$. Тогда конечная формула расчета вероятности перекрытия представляется в таком виде

$$P_\text{п} = 1-e^{\frac{i(1-i)}{2N_K}} \quad (13)$$

Таким образом мы получили связь между вероятностью перекрытия $P_\text{п}$ и числом возможных выходов гамм Γ_i. С точки зрения криптоанализа нас интересует объем реализаций по схеме рис. 1, сколько гамм сформировано в системе на одних и тех же ключах с заданной вероятностью.

Получив формулу (13), мы можем привести обоснование длины блока БСШ с точки зрения коллизионной стойкости для режима работы зашифрования синхропоследовательностей. Согласно формуле (2), количество возможных формируемых блоков (гамм) зависит от длины блока ШОУ, в данном случае блока БСШ, тогда формула (13) может быть записана как

$$e^{\frac{i(1-i)}{2^{N_b+1}}} = 1-P_\text{п}. \quad (14)$$

Прологарифмируем формулу (14) по натуральному основанию,

$$\frac{i(1-i)}{2^{N_b+1}} = \ln(1-P_\text{п}) \quad (15)$$

умножим левую и правую часть на знаменатель левой части

$$i(1-i) = 2^{N_b+1}\ln(1-P_\text{п}), \quad (16)$$

прологарифмируем формулу (16) по основанию 2

$$\log_2 i(1-i) = \log_2(2^{N_b+1}\ln(1-P_\text{п})), \quad (17)$$

$$\log_2 i(1-i) = \log_2(2^{N_b+1}) + \log_2\ln(1-P_\text{п}), \quad (18)$$

$$\log_2 i(1-i) = N_b + 1 + \log_2\ln(1-P_\text{п}). \quad (19)$$

В конечном виде длина блока N_b примет такой вид

$$N_b = \log_2 i(1-i) - \log_2\ln(1-P_\text{п}) - 1 \quad (20)$$

$$N_b = \log_2\frac{i(1-i)}{2\ln(1-P_\text{п})}. \quad (21)$$

Таким образом в формуле (21) мы получили связь между количеством полученных гамм i, ве-

роятностью перекрытия $P_п$, и длиной блока N_b, что позволяет сделать нам оценку и обоснование длины блока БСШ для режима зашифрования синхропоследовательностей, при заданном количестве гамм и вероятностью их перекрытия. Предварительные результаты расчета представлены в табл. 1.

Таблица 1

Результаты расчета длины блока

I	$P_п$	N_b	i	$P_п$	N_b	i	$P_п$	N_b	i	$P_п$	N_b
10	10^{-02}	13	10^{02}	10^{-02}	19	10^{03}	10^{-02}	26	10^{04}	10^{-02}	33
	10^{-03}	16		10^{-03}	23		10^{-03}	29		10^{-03}	36
	10^{-04}	19		10^{-04}	26		10^{-04}	33		10^{-04}	39
	10^{-05}	23		10^{-05}	29		10^{-05}	36		10^{-05}	43
	10^{-06}	26		10^{-06}	33		10^{-06}	39		10^{-06}	46
	10^{-09}	36		10^{-09}	43		10^{-09}	49		10^{-09}	56
	10^{-12}	46		10^{-12}	53		10^{-12}	59		10^{-12}	66
	10^{-16}	59		10^{-16}	66		10^{-16}	73		10^{-16}	79
	10^{-24}	86		10^{-24}	92		10^{-24}	99		10^{-24}	106
	10^{-32}	112		10^{-32}	119		10^{-32}	126		10^{-32}	132
10^{05}	10^{-02}	39	10^{06}	10^{-02}	46	10^{07}	10^{-02}	53	10^{08}	10^{-02}	59
	10^{-03}	43		10^{-03}	49		10^{-03}	56		10^{-03}	63
	10^{-04}	46		10^{-04}	53		10^{-04}	59		10^{-04}	66
	10^{-05}	49		10^{-05}	56		10^{-05}	63		10^{-05}	69
	10^{-06}	53		10^{-06}	59		10^{-06}	66		10^{-06}	73
	10^{-09}	63		10^{-09}	69		10^{-09}	76		10^{-09}	83
	10^{-12}	73		10^{-12}	79		10^{-12}	86		10^{-12}	93
	10^{-16}	86		10^{-16}	93		10^{-16}	99		10^{-16}	106
	10^{-24}	112		10^{-24}	119		10^{-24}	126		10^{-24}	132
	10^{-32}	139		10^{-32}	146		10^{-32}	152		10^{-32}	159
10^{09}	10^{-02}	66	10^{10}	10^{-02}	73	10^{11}	10^{-02}	79	10^{12}	10^{-02}	86
	10^{-03}	69		10^{-03}	76		10^{-03}	83		10^{-03}	89
	10^{-04}	73		10^{-04}	79		10^{-04}	86		10^{-04}	93
	10^{-05}	76		10^{-05}	83		10^{-05}	89		10^{-05}	96
	10^{-06}	79		10^{-06}	86		10^{-06}	93		10^{-06}	99
	10^{-09}	89		10^{-09}	96		10^{-09}	102		10^{-09}	109
	10^{-12}	99		10^{-12}	106		10^{-12}	112		10^{-12}	119
	10^{-16}	112		10^{-16}	119		10^{-16}	126		10^{-16}	132
	10^{-24}	139		10^{-24}	146		10^{-24}	152		10^{-24}	159
	10^{-32}	166		10^{-32}	172		10^{-32}	179		10^{-32}	186

ВЫВОДЫ

Основываясь на данных, представленных в табл. 1, можно сделать вывод, что наиболее распространенной длины блока БСШ 128 для режима шифрования синхропоследовательностей достаточно для всех количеств гаммы шифрующей вплоть до 10^{12} и вероятность их перекрытия 10^{-12}, однако при количестве гамм 10^{12} и вероятности коллизии 10^{-16} необходимо переходить к более длинным блокам.

Литература

[1] NESSIE public report D10. Description of Methodology for Security Evaluation. http://cryptonessie.org.

[2] *J. Daemen, V.Rijmen*. Rijndael for AES. 3rd AES conference. http://www.nist.gov/aes.

[3] *В. Столлингс*. Криптография и защита сетей: Принципы и практика. 2-е изд. – Киев: Изд. дом «Вильямс», 2001. – 669 с.

[4] *Попович Е.В., Горбенко Ю.И.* Критерии оценки требований к генераторам случайных последовательностей в криптографических системах // Радиотехника. – №141, 2005.

Поступила в редколлегию 23.09.2008

Михайленко Матвей Сергеевич, аспирант кафедры безопасности информационных технологий ХНУРЭ. Область научных интересов: криптография и криптоанализ блочных симметричных шифров.