А. Г. Ростовцев

Большие подстановки для программных шифров

1. Симметричные шифры

В последние годы наблюдается отход от подстановочно-перестановочных шифров, типичными представителями которых являются DES, ГОСТ 28147-89. С одной стороны, это обусловлено публикацией в открытой печати новых методов криптоанализа, в первую очередь, дифференциального и линейного. С другой стороны, такие шифры имеют малую нелинейность и диффузию, что компенсируется увеличением количества циклов шифрования (например, 32 цикла в ГОСТ 28147–89). Кроме того, эти шифры ориентированы на аппаратное построение, поэтому шифраторы получаются дорогими, а большое число циклов шифрования и короткая подстановка приводит к низкой производительности.

Зарубежные популярные шифры последних лет [1] (IDEA, SAFER, RC5, Blowfish и т. п.) имеют другую, процессорно-ориентированную, структуру. Особенностью этих шифров является работа не с битами, а со словами, длина которых равна разрядности процессора. Для получения высокой нелинейности используются операции умножения. Например, шифр IDEA использует умножение в группе $\mathbf{F}^*_{2^{16}+1}$. Другим примером является шифр SAFER, в котором нелинейная операция выполняется возведением образующей в степень или логарифмированием в группе $\mathbf{F}^*_{2^8+1}$. Подстановки SAFER и IDEA невелики (8 или 16 бит), поскольку они используют поля вычетов по модулю простых чисел Ферма — $2^8 + 1$ и $2^{16} + 1$, тогда как более удобные числа $2^{32} + 1$, $2^{64} + 1$ — составные.

Приведенные примеры показывают, что проблема создания широкого класса больших процессорно-ориентированных нелинейных подстановок с хорошей диффузией является актуальной при разработке шифров.

2. Операция подстановки

Предлагаемая подстановка задается многочленом над кольцом $R = \mathbf{Z}/(2^m)$. Разрядность подстановки целесообразно выбирать в соответствии с разрядностью процессора (m = 16, 32, 64, 128). Уравнение подстановки над R имеет вид

$$x \leftarrow \sum_{0 \le i < \log_2 m} a_i x^{2^i} \pmod{2^m}, \tag{1}$$

«Проблемы информационной безопасности. Компьютерные системы»,
СПб., 2000. № 3. С. 31–35

где число ненулевых слагаемых в сумме (1) нечетно и не менее 3, и все ненулевые коэффициенты a_i обратимы, $a_0 \neq 0$. Наиболее простое уравнение неаффинной подстановки имеет вид

$$x \leftarrow a_2x^4 + a_1x^2 + a_0x \pmod{2^m}, \tag{2}$$

где a_0, a_1, a_2 — обратимые элементы в R, которые могут являться частью ключа.

Теорема 1. Уравнение (2) описывает подстановку в R.

Доказательство. Очевидно, что (2) отображает кольцо R в себя. Функция (2) не является подстановкой тогда и только тогда, когда она принимает какое-нибудь значение дважды. Если предположить, что при переборе x функция (2) принимает дважды некоторое значение b, то сравнение

$$a_2x^4 + a_1x^2 + a_0x - b \equiv 0 \pmod{2^m} \tag{3}$$

должно иметь двойной корень. Кратные корни можно определить вычислением наибольшего общего делителя (3) и производной. Поскольку в R каждый неделитель нуля обратим, нужно рассматривать наибольший общий делитель над каждым главным идеалом, который является делителем нуля в кольце R. Достаточно рассмотреть случаи колец $\mathbf{Z}/(2)$, $\mathbf{Z}/(2^2)$, …, $\mathbf{Z}/(2^m)$.

Производная левой части (3) равна $4a_2x^3 + 2a_1x + a_0$. Нетрудно видеть, что левая часть (3) не делится на производную ни над одним из указанных колец. Кроме того, производная не имеет корней ни в одном из этих колец, так как коэффициент a_0 нечетный, а коэффициенты при степенях x четные. Многочлен, задающий производную, имеет степень три, поэтому он может раскладываться на множители лишь тогда, когда хоть один из делителей имеет степень 1, то есть когда производная имеет корень в указанных кольцах. Поскольку корней нет, то производная от (2) не раскладывается на множители ни над одним из указанных колец. Следовательно, наибольший общий делитель функции (3) и ее производной над каждым из указанных колец равен обратимой константе, и (2) задает подстановку в R. ■

Основной операцией при вычислении (2) является возведение в квадрат, эта операция может быть несколько упрощена, если m вдвое превышает разрядность процессора. Пусть $x = x_0 + x_1 2^{m/2}$. Тогда $x^2 \equiv x_0^2 + 2x_0x_1 2^{m/2} \pmod{2^m}$. Однако второе слагаемое можно не умножать на 2, так как использование выражения $y \leftarrow x_0^2 + x_0x_1 2^{m/2} \pmod{2^m}$ вместо возведения в квадрат в (2) тоже задает подстановку.

Подстановка (2) может быть использована непосредственно как одна из операций шифрования над словами длины m бит, так и над более короткими словами. Подстановка (2) переводит нечетные числа в нечетные. Выберем (m – 1)-битное слово, дополним его единицей в младшем разряде и применим подстановку (2). Из результата подстановки удалим младший единичный разряд. Поскольку этот разряд всегда содержит единицу, то (2) действует указанным образом как подстановка и в $\mathbf{Z}/(2^{m-1})$.

Вместо одного бита можно присоединять произвольное число l младших битов, выполнять вычисление согласно (2) и затем удалять l младших битов. В этом случае (2) задает подстановку, которая действует на кольце $\mathbf{Z}/(2^{m-l})$. Добавляемые младшие биты, как и коэффициенты a_0, a_1, a_2 являются параметрами подстановки и могут быть частью ключа.

Рассмотренная подстановка задает одновременно и диффузию, и перемешивание. Если шифратор выполнять по фейстелевой схеме [2], то вычисление подстановки, обратной к (2), не понадобится.

3. Нелинейность, диффузия и дифференциалы подстановки

Семейство подстановок (2) задается алгебраическими функциями над кольцом $\mathbf{Z}/(2^m)$ с делителями нуля. Наличие делителей нуля приводит к тому, что у этих подстановок появляются специфические свойства, которые могут быть использованы в криптоанализе. Однако эти свойства можно скомпенсировать за счет мощной диффузии и нелинейных перемешивающих свойств, присущих данным подстановкам.

Нелинейность подстановки обычно определяется через нелинейность над $\mathbf{F}_2$ булевых функций, задающих подстановку. *Нелинейность булевой функции* как многочлена из $\mathbf{F}_2[X_1, .., X_n]/(X_1(1 + X_1), .., X_n(1 + X_n))$ определим как кодовое расстояние между таблично заданной функцией и наилучшей ее аффинной аппроксимацией. Максимально достижимая нелинейность сбалансированной k-разрядной булевой функции равна $2^{k-1} - 2^{[k/2]}$. Нелинейность такой функции всегда четная.

Младший двоичный разряд подстановки $y = f(x) = x^4 + x^2 + x$, рассматриваемой как вектор $\mathbf{y} = f(X_0 + 2X_1 + 4X_2 + \ldots + 2^{31}X_{31})$, описывается аффинной над $\mathbf{F}_2$ функцией и равен X_0. Второй разряд также описывается аффинной булевой функцией и равен $X_0 + X_1$. Третий разряд описывается булевой функцией $X_0X_1 + X_2$ с нелинейностью 2. Четвертый разряд описывается булевой функцией $X_0X_2 + X_3$ с нелинейностью 4. Пятый разряд описывается булевой функцией $X_0X_3 + X_1X_2 + X_4$ с нелинейностью 12 и т. д. Видно, что нелинейность булевых функций быстро возрастает. Кроме того, перечисленные булевы функции являются “самыми нелинейными” среди сбалансированных функций соответственно от 3, 4, 5 переменных.

Определим *нелинейность подстановки* (над $\mathbf{F}_2$) как среднее арифметическое нелинейностей булевых функций. Нелинейность булевых функций быстро растет с ростом старшинства разрядов. Максимальную нелинейность имеют старшие разряды подстановки. Экстраполируя на старшие разряды то свойство, что нелинейность булевых функций, описывающих младшие разряды подстановки, максимальна, можно получить оценку для нелинейности подстановки. Для 32-разрядной подстановки (2) эта нелинейность равна 10^8, для 16-разрядной подстановки (2) нелинейность составляет $2{\cdot}10^3$. Таким образом, данная подстановка имеет высокую нелинейность. Есть основания предполагать, что линейный криптоанализ шифра, основанный на использовании булевых функций над $\mathbf{F}_2$, будет неэффективным.

Подстановка обладает значительной диффузией, поэтому остальные операции, используемые при шифровании, должны обеспечивать диффузию разностей для m-разрядных слов внутри шифруемого блока. Такой операцией может служить преобразование вида

$$x_i \leftarrow \sum_{j=1}^{n} x_j - x_i (\operatorname{mod} 2^m)$$

(n — число m-разрядных слов в блоке) в сочетании с циклическими сдвигами слов или умножение шифруемого блока как n-мерного вектора над $\mathbf{Z}/(2^m)$ на неособую матрицу в сочетании с циклическими сдвигами слов.

Подстановка действует на кольце $R = \mathbf{Z}/(2^m)$ и задается многочленом над этим кольцом. Кольцо $\mathbf{Z}/(2^m)$ имеет гомоморфизмы с кольцами $\mathbf{Z}/(2^{m-k})$ для натуральных k, которые сохраняются под действием подстановки. Поэтому шифр, построенный на основе указанной подстановки, может быть уязвим по отношению к анализу на основе гомоморфизмов. Указанная операция диффузии должна обеспечивать неэффективность криптоанализа на основе гомоморфизмов.

Оценим стойкость шифра, построенного с использованием подстановки (2), к дифференциальному методу анализа (точнее, к его усиленному варианту — методу на пучках дифференциалов). Для этого найдем наиболее вероятный дифференциал (НВД) подстановки (2) над R из максимального числа решений уравнения $f(x + a) - f(x) \equiv b \pmod{2^m}$, где f — подстановка (2), при всевозможных a, b. После раскрытия скобок последнее уравнение в R примет вид

$$4aa_2x^3 + 6a^2a_2x^2 + 4a^3a_2x + 2aa_1x + f(a) - b = 0. \tag{4}$$

Максимальное число решений уравнения (4) в R равно 2^m. Это соответствует случаю $a = b = 2^{m-1}$. Следовательно, НВД вида $(2^{m-1}, 2^{m-1})$ для подстановки (2) имеет вероятность 1. Аналогично можно показать, что каждый из четырех дифференциалов вида $(c{\cdot}2^{m-2}, d{\cdot}2^{m-2})$ при нечетных c, d для этой же подстановки имеет вероятность 1/2 и т. д.

Предположим, что другие операторы шифрования реализуют циклические сдвиги m-разрядных слов и операции сложения и что анализ проводится на основе подобранных открытых текстов. Тогда после второго цикла шифрования НВД будет иметь вероятность $2^{-m/2}$. После трех циклов НВД будет иметь вероятность 2^{-m} и т. д.

Пусть шифратор с неизвестным ключом работает непрерывно в течение 10 лет со скоростью 10^8 бит/с и нарушитель знает открытые и соответствующие зашифрованные тексты. За это время нарушитель сможет получить $3 \cdot 10^{14}$ 128-разрядных блоков текста. Для успешного дифференциального анализа необходимо, чтобы произведение объема статистики на вероятность НВД было близко к 1. Тогда вероятность появления НВД после предпоследнего цикла шифрования, меньшая 2^{-63}, представляется безопасной.

Предположим, что распределение дифференциалов на различных циклах шифрования независимо и использование пучков дифференциалов для криптоанализа невозможно (подстановка обладает сильным перемешиванием, поэтому предположение допустимо при условии, что остальные операторы шифрования обеспечивают необходимую диффузию на уровне слов). Тогда для $m = 32$ вероятность НВД после двух циклов шифрования не будет превышать 2^{-16}. После трех циклов получаем вероятность наиболее вероятного дифференциала не более 2^{-32} и т. д. Отсюда следует, что для успешного противостояния дифференциальному методу криптоанализа достаточно 6 циклов шифрования. Для $m = 16$ достаточно 10 циклов, а для $m = 64$ — только 4 или 5 циклов. Из этих оценок следует, что возможна реализация программного шифратора со скоростью десятки мегабит в секунду на 32-разрядном процессоре со встроенным умножителем.

Отметим, что данная оценка является приблизительной и получена в предположении, что НВД не зависит от входных текстов и алгоритм шифрования обеспечивает необходимый уровень диффузии на уровне m-разрядных слов, исключающий возможность использования пучков дифференциалов. Для повышения стойкости к линейному над R методу анализа необходимо тщательно выбирать оператор диффузии.

Литература

1. Menezes A., van Oorchot P., Vanstone S. Handbook of applied cryptography. — CRC Press, 1997.
2. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. — J. Wiley & Sons, New York, 1996.