УДК 681.3

Кравцов Г.А., директор ООО «НВФ «БКП-Консалтинг», г.Киев.

Задача дискретного интегрирования разностного уравнения неразрешимого в квадратурах.

В 1969 году Джеймс Месси в своей работе [1] сформулировал универсальную криптоаналитическую атаку на генераторы шифрующей последовательности, которая потенциально заменяет любой шифрогенератор его кратчайшим линейным эквивалентом.

Если с помощью регистра сдвига с линейной обратной связью порождена шифрующая последовательность (далее - гамма), то достаточно исследовать $2L$ бит гаммы с линейной сложностью L.

Под линейной сложностью (линейным размахом) шифрующей последовательности понимается длина L самого короткого регистра сдвига с линейной обратной связью (далее - РСЛОС), способного породить эту последовательность.

Результаты Джеймса Месси нашли практическое применение в алгоритме Берлекампа-Месси [1], который ставит под вопрос использование методов шифрования с наложением гаммы.

Однако, известный с 1926 года шифр Дж.С.Вернама [2], остается единственной надеждой на совершенную защиту, а изложенный выше материал приводит к необходимости использования случайного ключа.

Основным свойством случайного ключа считается его непредсказуемость, т.е. все допустимые значения на следующем шаге предсказания равновероятны и последовательность не может быть рационально аппроксимирована функцией, которая бы выражалась через рациональные функции. Дополнительно, существует необходимость противодействия алгоритму Берлекампа-Месси.

Была сформулирована четкая задача получения механизма противодействия алгоритму Берлекампа-Месси и цель исследования - изучить возможность противодействия алгоритму Берлакампа-Месси и при положительном результате предложить легко реализуемый механизм.

В ходе исследований было изучено большое множество элементарных и специальных функций, однако особый интерес вызвало уравнение Риккати.

Общеизвестно, что дифференциальное уравнение Риккати

$$\frac{dy}{dx} = P(x)y^2 + Q(x)y + R(x), \qquad (1)$$

вообще говоря, не интегрируется в квадратурах (т.е. нахождение его решения не может быть сведено к конечному числу последовательных интегрирований).

Если заменить дифференциальное уравнение (1) разностным уравнением или уравнением в конечных разностях (заменив дифференциал конечной разностью) и переписать в удобном для практического применения в криптографии виде, то получим:

$$\Delta y + P(x)y^2 + Q(x)y = R(x), \tag{2}$$

Если полагать, что функции $P(x)$ и $Q(x)$ могут быть представлены последовательностями P и Q соответственно, а функция y последовательностью Y, то легко получить значение последовательности R, заменяющей функцию $R(x)$ и очень тяжело (в принципе невозможно) по известным P,Q,R найти последовательность Y.

Уравнение (2) может быть в терминах последовательности записано в виде:

$$Y_i - Y_{i-1} + P_i Y_i^2 + Q_i Y_i = R_i. \tag{3}$$

Если известны последовательности P, Q и R, то найти последовательность Y можно, решив систему уравнений

$$\begin{cases} y_1 - y_0 + p_1 y_1^2 + q_1 y_1 = r_1 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ y_i - y_{i-1} + p_i y_i^2 + q_i y_i = r_i \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ y_n - y_{n-1} + p_n y_n^2 + q_n y_n = r_n \end{cases}.$$

В общем случае решение системы сводиться к решению уравнения двух переменных вида $f(y_n^k, y_0) = 0$, где $k = 2^n$. Рассматриваемая система уравнений имеет бесконечное число решений, так как число переменных больше, чем число уравнений.

Учитывая, что большая часть задач криптографии нацелена на практическое применение и размерность используемых чисел ограничена, то целесообразно переписать уравнение (3) в виде:

$$(Y_i - Y_{i-1} + P_i Y_i^2 + Q_i Y_i) \bmod p = R_i, \tag{4}$$

где P,Q - известные последовательности (параметры);

p - простое число;

R - конечное поле $GF(p)$,

Y - искомая последовательность.

Предполагается, что криптоаналитику известны значения P,Q,R. Если Y является ключевой последовательностью (ключом), то криптоаналитику необходимо решить задачу дискретного интегрирования разностного уравнения неразрешимого в квадратурах.

Как базовый вариант Y предлагается использовать последовательность, полученную с помощью регистра сдвига с нелинейной обратной связью размерности n с эквивалентной линейной сложностью L. Если в уравнении используются значения Y_i, такие что $\log_2 Y_i << n$, то алгоритм линейного синтеза Берлекампа-Месси «не дает» короткого неприводимого многочлена (т.е. степень неприводимого полинома близка к количеству бит в сообщении, поделенному пополам), используя который, можно «читать вслед» (по результатам двухлетних исследований).

Очевидно, что (4) может быть легко применена в условиях современного развития средств вычислительной техники. Однако в данном случае приходиться оперировать с регистрами ограниченной размерности n. В таком случае, необходимо учитывать следующее ограничение: $\log_2 p \to n$.

Проведем краткий сравнительный анализ. Известная задача Диффи-Хелмана [3] основана на использовании функции возведения в степень в мультипликативной группе простого поля: $f(x) = a^x \bmod p$, где p - простое число, a - примитивный элемент поля $GF(p)$, $1 < x < p-1$. Эта функция является кандидатом в однонаправленные функции. Действительно, она легко вычислима, так как, используя метод квадратов, значения этой функции можно вычислять с полиномиальной сложностью, оцениваемой величиной $O((\log p)^3)$, в то время как обратная задача является сложной. Однако, не следует забывать, что задача логарифмирования сама по себе сегодня является обыденной.

Библиография

1. J.L. Massey, “Shift-Register synthesis and BCH decoding”, IEEE Trans. Inform. Theory, vol.IT-15, pp.122-127, Jan.1969
2. G.S. Vernam, “Cipher printing telegraph system for wire and radio telegraphic communication”, J.Amer.Inst.Elec.Eng., vol. 45, pp. 109-115, 1926
3. Dh.W.Diffie, M.E.Hellman. “New directions in cryptography”, IEEE Trans. Inform. Theory, vol.IT-22, pp.644-654, Nov.1976