УДК 681.325.36.049.2

Н.Е. Сапожников, проф., д-р техн. наук
Севастопольский национальный институт ядерной энергии и промышленности
ул. Курчатова 33, г. Севастополь, Украина
E-mail: nesapoghnikov@pisem.net

ПРЕИМУЩЕСТВА ВЕРОЯТНОСТНОЙ ФОРМЫ ПРЕДСТАВЛЕНИЯ ИНФОРМАЦИИ

Рассмотрен вопрос защиты информации, представленной в дискретной вероятностной форме. Показано, что нелинейное преобразование информации в форму вероятностного отображения с произвольным законом распределения вспомогательного случайного сигнала автоматически приводит к её криптографической защите.

Известно, что представление дискретного сигнала в вероятностной форме позволяет получить ряд преимуществ для вероятностных процессоров сравнительно с цифровыми в затратах оборудования и скорости обработки информации [1-3]. Однако до сих пор неисследованным оставался вопрос использования преимуществ вероятностного представления дискретного сигнала. Дело в том, что возможность нелинейного вероятностного преобразования с переменным количеством независимых статистических испытаний каждого значения исходного сигнала позволяет параллельно с обработкой сигнала проводить его криптографическую защиту. Действительно, при нелинейном вероятностном преобразовании информации, предварительно представленной в аналоговой либо цифровой формах, и выполнении над вероятностными отображениями арифметических и логических операций значение математического ожидания от вероятностного отображения оказывается равным значению ординаты интегрального закона распределения вспомогательного сигнала $F(R)$ [2]:

$$M[Y_i(t)] = \sum_{l=1}^{2} y_{ijl} P_l = P(y_{ij} = 1) = P[R(t) < (x_i = r)] = F_{x_i}(R);$$

$$M[\&_{q=1}^{Q} Y_{qij}(t)] = \prod_{q=1}^{Q} F_{x_q}(R_q);$$

$$M[S(t)] = M[Y_1(t)] + M[Y_2(t)] + \ldots + M[Y_Q(t)] =$$

$$= \sum_{q=1}^{Q} \sum_{l=1}^{2} y_{qjl} P_{ql} = \sum_{q=1}^{Q} P(y_{qj} = 1) = \sum_{q=1}^{Q} P[R_q(t) < (r = x_q)] = \sum_{q=1}^{Q} F_{x_q}(R_q);$$

$$M[S(t)] = M[Y_1(t)] - M[Y_2(t)] = F_{x_1}(R_1) - F_{x_2}(R_2).$$

Это позволяет на этапе шифрования получать кодированный сигнал в виде нелинейного вероятностного отображения, а на этапе дешифрования,

зная параметры закона распределения вспомогательной функции и количество независимых статистических испытаний каждого преобразуемого значения исходного сигнала, легко осуществлять обратное преобразование, получая отсчёты в виде двоичных машинных слов.

Покажем это для случая, когда вспомогательный случайный сигнал $R(t)$ подчиняется нормальному закону распределения, а вероятностное отображение получено путём однолинейного однополярного преобразования [3]. Используя функцию Лапласа, запишем выражение для интегрального нормального закона распределения в виде

$$F(R) = \frac{1}{2}\left[1 + \Phi\left(\frac{r - m_r}{\sigma_r}\right)\right],$$

где m_r и σ_r – математическое ожидание и среднее квадратическое отклонение вспомогательной случайной функции $R(t)$. Учитывая следствие из теоремы Чебышева, примем в качестве оценки для математического ожидания вероятностного отображения величины $a = x_i$, подлежащей кодированию (нелинейному вероятностному преобразованию), среднее арифметическое суммы его членов, т.е.

$$\{M[Y_i(t)]\}^* = [F_{x_i}(R)]^* = \frac{1}{K}\sum_{j=1}^{K} y_{ij} .$$

В работе [3] показано, что данная оценка является состоятельной, эффективной и несмещенной.

Теперь, преобразовывая предыдущее выражение с учетом последнего, получаем

$$\Phi(\xi) = \frac{2}{K}\sum_{j=1}^{K} y_{aj} - 1,$$

где $\xi = (a^* - m_r)/\sigma_r$.

На втором этапе, используя таблицы для интеграла вероятности, определим ξ и далее, путём функционального преобразования произведём декодирование сигнала в соответствии с выражением

$$a^* = \xi\sigma_r + m_r.$$

Ключами для дешифровки являются знание параметров закона распределения $F_a(R)$ и количество независимых статистических испытаний K. В соответствии с вышеизложенным алгоритм защиты информации при её вероятностном преобразовании представляется следующим. Информация, подлежащая криптографической защите, поступает на нелинейный однополярный вероятностный преобразователь, вероятностное отображение с выхода которого через канал связи подаётся в счётчик-интегратор, где суммируется за K

тактов, после чего полученная оценка $[F_a(R)]^*$ переписывается в функциональный преобразователь, где по $\Phi(\xi)$ определяется ξ и затем a^*.

Перехват вероятностного отображения в канале связи и перебор всех возможных значений K с соответствующим анализом позволяет дешифровать сообщение за конечное время только при известном равномерном законе распределения вспомогательного случайного сигнала $R(t)$. При любом ином непрерывном законе распределения $R(t)$ задача становится практически неразрешимой, так как неизвестна форма кривой закона распределения. Можно представить ситуацию, когда анализ количества поступлений одинаковых чисел в канал связи (при уже определённом K) и соотнесение их с вероятностями появления тех или иных символов в произвольном языке позволит с помощью достаточно мощной ЭВМ за конечное время определить форму кривой закона распределения. Учитывая, что корреляция между ключом шифрования, обусловленным числом испытаний K и вторым ключом, задающим закон распределения вспомогательного случайного сигнала $R(t)$, отсутствует, приходим к выводу, что рассмотренная гипотетическая ситуация маловероятна. Тем не менее, для большего повышения криптостойкости может быть рассмотрен вариант введения в алгоритм защиты ещё одного ключа. При однолинейном однополярном представлении сомножителей a и b выражение для их произведения, представленных в форме вероятностных отображений, запишется в виде [2]:

$$M[Y_a(t)Y_b(t)] = F_a(R)F_b(R) \cong \frac{1}{K}\sum_{j=1}^{K}(y_{aj} \,\&\, y_{bj}).$$

Если криптографической защите подлежит только символ a, а нелинейному вероятностному преобразованию (для простоты и наглядности примем распределения $R_1(t)$ и $R_2(t)$ по-прежнему нормальными с различными значениями математических ожиданий и дисперсий) подвергаются и a и b, то аналогично предыдущему случаю получаем

$$\Phi(\xi_1) + \Phi(\xi_2) + \Phi(\xi_1)\Phi(\xi_2) = 0{,}25K\sum_{j=1}^{K}(y_{aj} \,\&\, y_{bj}) - 1.$$

Полученное уравнение решения не имеет. Иная ситуация возникает, если сомножитель, не подлежащий криптографической защите, представляется в виде линейного вероятностного отображения путём применения в качестве вспомогательного, случайного сигнала с равномерным распределением мгновенных значений

$$F_b(R) = \begin{cases} 0 & \text{при } r < 0 \\ r & \text{при } 0 \le r \le 1 \\ 1 & \text{при } r > 1 \end{cases}.$$

Выполняя простые преобразования, для этого случая получаем

$$\Phi(\xi_a) = \frac{\sum_{j=1}^{K}(y_{aj} \,\&\, y_{bj}) - 0{,}5\sum_{j=1}^{K} y_{bj}}{\sum_{j=1}^{K} y_{bj}}.$$

Откуда по ранее рассмотренной методике определим a^*. Предусмотреть при несанкционированной дешифрации выполнение операций в соответствии с последним выражением или ему подобными при иных законах распределения практически невозможно.

В соответствии с полученными выражениями, рассмотрим алгоритм защиты информации при её вероятностном преобразовании с одновременным применением трёх ключей. Каждый из сомножителей, представленный либо в виде квантованного по времени аналогового сигнала, либо в виде двоичного позиционного кода, подаётся на собственный вероятностный преобразователь – сомножитель b на линейный, сомножитель a – на нелинейный. Количество статистических испытаний для каждого сомножителя выбирается одинаковым, что позволяет получить вероятностное отображение произведения с помощью операции логического умножения. Для получения вероятностного отображения разности в числителе последней формулы может быть использован реверсивный счётчик, на суммирующий вход которого подается вероятностное отображение произведения, а на вычитающий – деленное пополам с помощью счётного триггера вероятностное отображение b. Операция деления выполняется вероятностным делителем. Выигрыш в затратах оборудования по сравнению с цифровым криптомодемом, ключ которого состоит из 64 бит, составляет [4]

$$\mu = \frac{4833}{1254 + 12h},$$

где h – число разрядов двоичных машинных слов. Число в числителе получено в предположении, что в качестве шифратора используется микропроцессор с двухбайтной шиной данных. Тогда при $h = 16$ $\mu = 3{,}3$.

Аналогичным образом можно решить проблему третьего ключа, используя операцию вероятностного сложения для двух слагаемых.

Быстродействие вероятностного криптомодема зависит от верхней граничной частоты работы дискретных комплектующих элементов f и количества статистических испытаний K и составляет

$$F_t = f / K.$$

Быстродействие может быть повышено в K/h раз за счёт передачи по каналу связи не вероятностных отображений, а соответствующих им двоичных позиционных кодов.

Проанализируем точность восстановления передаваемых сообщений. Полученное в результате обратного преобразования значение оценки a^* бу-

дет отличаться от истинного значения a на величину погрешности, которую назовём абсолютной погрешностью дешифрации

$$\Delta_a = \left| a^* - a \right|.$$

Её величина определяется значениями погрешностей, возникающих при кодировании исходной информации (при преобразовании в дискретную вероятностную форму) и при её преобразовании в исходную форму. Первую из них принято называть погрешностью вероятностного преобразования. В соответствии с [3] выражение для неё имеет следующий вид

$$\Delta_{ВП} = \frac{\sqrt{2}\Phi^{-1}(P)}{\sqrt{K}} \sqrt{F_a(R) - F_a^2(R)},$$

где P – вероятность того, что истинное значение $F_a(R)$ находится внутри интервала с границами:

$$I_P = \left\{ F_a^*(R) - \Delta_{ВП};\ F_a^*(R) + \Delta_{ВП} \right\}.$$

Величина второй составляющей погрешности, назовём её погрешностью восстановления, для нормального закона распределения может быть найдена аналогично тому, как было выполнено определение величины $\Phi(\xi)$

$$\Phi(\xi_\Delta) = \frac{2}{K} \sum_{j=1}^{K} y_{aj} - \Delta_{ВП} - 1,$$

где $\xi_\Delta = \dfrac{a^* - \Delta_a - m_r}{\sigma_r}$.

Откуда $\Delta_a = a^* - m_r - \xi_\Delta \sigma_r$.

Выбирая математическое ожидание вспомогательного сигнала равным $m_r = 0{,}5$, вероятность попадания оценки в доверительный интервал $P = 0{,}9973$ и количество статистических испытаний $K = 144$, получаем, что минимальная погрешность дешифрования при кодировании с помощью вспомогательного случайного сигнала с нормальным законом распределения может быть получена путём правильного выбора величины дисперсии этого сигнала. Действительно, при $1/3 \geq \sigma_r \geq 1/6$ значение погрешности не превысит 0,08 от величины единичного динамического диапазона, причём её дальнейшее уменьшение может быть достигнуто путём увеличения количества статистических испытаний K. Очевидно, что близкие результаты будут получены и при использовании случайных сигналов с законами распределения, отличными от нормального. Важным при этом является выполнение требования отсутствия резко выраженных эксцесса и асимметрии.

Итак, представление информации в дискретной вероятностной форме и выполнение арифметических и логических операций над вероятностно представленными операндами может быть практически без дополнительных аппаратурных затрат совмещено с криптографической защитой обра-

батываемой информации, причём степень защиты может варьироваться путём применения разного количества ключей.

Дальнейшими перспективными исследованиями в данной области могут быть признаны исследования степени защиты информации в зависимости от вида закона распределения вспомогательного случайного сигнала.

Библиографический список

1. Гладкий В.С. Процессор для обработки гидрофизической информации / В.С. Гладкий, Н.Е. Сапожников // Морские гидрофизические исследования. — 1970. — № 3. — С. 149–156.

2. Сапожников Н.Е. Сравнительная оценка эффективности дискретных форм представления информации / Н.Е. Сапожников // Сборник трудов СИЯЭиП. — Севастополь, 2000. — Вып. 1. — С. 64–70.

3. Сапожников Н.Е. О вероятностном преобразовании информации / Н.Е. Сапожников // Приборостроение. — К., 1983. — Вып. 34. — С. 31–38.

4. Мартин Дж. Вычислительные сети и распределенная обработка данных / Дж. Мартин. — М.: Финансы и статистика, 1986. — 269 с.

Поступила в редакцию 10.01.2003 г.