УДК 681.3

ПОСТРОЕНИЕ ЛИНЕЙНОГО ВЕРОЯТНОСТНОГО ПОТОЧНОГО ШИФРАТОРА

Сапожников Н. Е., Столярчук Ю. Ю., Моисеев Д. В.
(Севастопольский нац. унив-т ядерной энергии и промышленности)

В работе рассматривается принципиальная возможность применения вероятностной формы представления информации для создания приёмо-передающих устройств обладающих криптографической стойкостью.

Введение. Известно, что представление дискретного сигнала в вероятностной форме позволяет получить ряд преимуществ в виде уменьшения аппаратного объема и повышения скорости обработки [1-3].

Группы численных методов, основанных на получении большого числа реализаций стохастического (случайного) процесса, который формируется таким образом, чтобы его вероятностные характеристики совпадали с аналогичными величинами решаемой задачи, достаточно давно известны.

Постановка задачи. В существующие устройства для защиты информации внутри корпоративной сети (поточные шифраторы) положены принципы детерминированных шифросистем, или детерминированный шифр, такой как ГОСТ 28147-89. Структурная схема поточных шифраторов рассмотрена в [4].

Основной недостаток рассмотренных схем – это детерминированная шифросистема кодирования, которая составляет основу вычислителя.

Цель данной работы, является анализ возможности построения поточных шифраторов, за счет использования вероятностной формы представления данных.

Решение задачи. В общем виде суть стохастического или вероятностного преобразования заключается в том, что любому значению параметра преобразуемой величины можно привести в соответствие некоторую вероятность. Сам процесс преобразования выполняется в соответствии с правилом:

$$\begin{cases} param > rand_i(); & \text{vector[i]} = 1 \\ param \le rand_i(); & \text{vector[i]} = 0 \end{cases}$$

где $param$ – значение параметра преобразуемого сигнала; $rand_i()$ – значение вспомогательного случайного сигнала на i-ом такте; $vect[i]$ – вероятностное отображение значения сигнала $param$; i – количество статистических испытаний.

Следует отметить, что вероятностное отображение информации обладает рядом преимуществ, одно из которых – криптостойкость**,** а также принципиальная возможность линейного вероятностного преобразования с переменным количеством независимых статистических испытаний каждого значения исходного сигнала, представленного в аналоговой, либо цифровой форме позволяет параллельно с обработкой сигнала проводить его криптографическую защиту.

Определим математическое ожидание вероятностного отображения информации (МО): $M[vector] = P(vector[i] = 1) = P[rand_i() < param] = F_{param}(rand_i())$.

Таким образом, вероятность появления «1» в вероятностном отображении есть МО от отображения и численно равняется значению интегрального закона распределения [2] вспомогательного сигнала $rand_i()$ при уровне сравнения $param$.

Особый интерес представляет случай, когда вспомогательный случайный сигнал $rand_i()$ подчиняется равномерному закону распределения [3] в соответствии с правилом:

$$F_{param}(rand_i()) = \begin{cases} 0, & \text{при } rand_i() < 0 \\ rand_i(), & \text{при } 0 \le rand_i() \le 1 \\ 1, & \text{при } rand_i() > 1 \end{cases}.$$

В данном случае последнее выражение для МО преобразуется в вид:

$$M[vector] = P(vector[i] = 1) = param.,$$

т.е. имеем случай линейного вероятностного преобразования [3].

Важнейшим следствием из выражений для МО является тот факт, что значение параметра *param* поддаётся восстановлению из вероятностного отображения, то есть, возможно обратное преобразование «вероятность -– значение параметра» (числа, амплитуды, частоты, фазы и т.д.). Действительно, априори зная закон распределения вспомогательного случайного сигнала $rand_i()$ и определяя математическое ожидание от вероятностного отображения, то есть ординату интегрального закона распределения $F_{param}(rand_i())$, путём функционального преобразования можно определить величину $param^*$, являющуюся оценкой *param* [3]. В качестве такой оценки, удовлетворяющей требованиям несмещенности, состоятельности и эффективности, в соответствии с теоремой Чебышева, принимается: $\{M[vector]\}^* = \{F_{param}(rand_i())\}^* = \frac{1}{i}\sum_1^i vector$.

Таким образом, для защиты информации от несанкционированного доступа следует произвести линейное однополярное вероятностное преобразование исходной информации представленной либо в аналоговой, либо цифровой форме, чтобы злоумышленник не был допущен к количеству статистических испытаний каждого преобразуемого значения исходной информации. Над преобразованным сигналом можно производить арифметико-логические операции, а также приемопередачу по средствам телекоммуникаций. Для обратного преобразования в цифровой код либо в аналоговый сигнал, в соответствии с выражением для МО, необходимо, произвести оценку МО вероятностного отображения $param^*$ и путем функционального преобразования перейти к искомому значению *param*.

Тогда структурно-функциональная схема простейшего приёмо-передатчика примет вид, показанный на рис. 1.

Информация, подлежащая криптографической защите поступает на линейный вероятностный преобразователь, с выхода которого вероятностное отображение, представляющее в данном случае кодированный сигнал, через канал связи подается в счетчик, где суммируется за *i* тактов. После этого полученная оценка $\{F_{param}(rand_i())\}^*$ переписывается в функциональный преобразователь, где, зная величину *i* и закон распределения вспомогательного случайного сигнала, осуществляется дешифрация.

Перехват вероятностного отображения в канале связи и перебор всех возможных значений *i* с соответствующим анализом позволяет дешифровать сообщения за конечное время только при известном равномерном законе распределения вспомогательного случайного сигнала $rand_i()$. При любом ином непрерывном законе распределения $rand_i()$ задача криптоанализа становится практически не разрешимой, так как неизвестна форма кривой закона распределения.

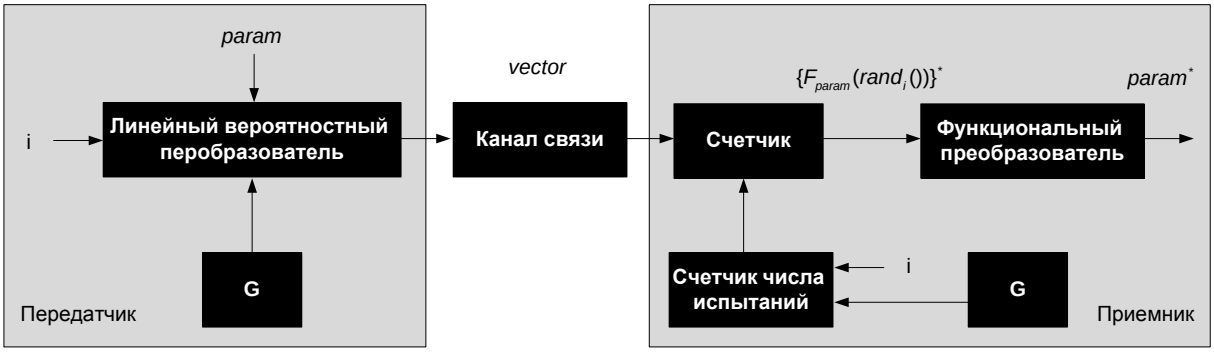

Рис. 1. Структура простейшего вероятностного приемо-передатчика

Выводы. Применение вероятностной формы представления информации, позволяет воспользоваться не только известными преимуществами: малый аппаратный объем, возможность функционирования в масштабе реального времени, повышенной помехозащищенностью, но и дополнительным преимуществом, выраженным в виде криптографической защиты данных, представленных вероятностными отображениями.

Предложенная структурная схема линейного вероятностного поточного шифратора позволяет:

- увеличить сложность проведения атак на основе статистических закономерностей функций шифрования;
- поскольку одному и тому же тексту с одинаковым ключом соответствует абсолютно разное вероятностное представление, атака по словарю стает не эффективной;
- увеличить сложность проведения атак с открытым текстом, поскольку криптоаналитик может быть ограничен в количестве текста (закодированном на этом ключе) для успешной реализации атаки;
- внести дополнительный параметр безопасности, управляя законом распределения случайных чисел, для формирования вероятностного отображения, появляется возможность увеличить время жизни ключа.

Литература

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. – 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. Панасенко С. П. Аппаратные шифраторы / С.П. Панасенко // Мир ПК 2002. – С. 77-83