О СОЗДАНИИ ОТКАЗОУСТОЙЧИВЫХ КРИПТОГРАФИЧЕСКИХ СИСТЕМ

П.П.Урбанович, Н.В.Пацей

Белорусский государственный технологический университет, г. Минск, РБ

Аннотация: В статье рассматривается один из методов повышения отказоустойчивости криптографических систем защиты информации, путем их дополнения линейными корректирующими кодами. Подобные корректо-криптграфические системы разрабатываются для защищенных сетей телекоммуникаций. Рассчитана условная оценка эффективности предлагаемой системы.

Ключевые слова: корректирующий код, криптография, оценка, эффективность, передача, система, безопасность.

1. Введение

Телефонные каналы, используемые для передачи данных, не отличаются надежностью доставки информации и высоким качеством передачи. Практика использования и тестирования [1] коммутированных телефонных каналов подтверждает вышесказанное. Кроме того, аппаратно реализуемая криптосхема, содержащая накопители, сумматоры, регистры циклического сдвига, блоки подстановки, сама может вносить битовые ошибки в шифротекст. В связи с этим возникает задача надежного преобразования, хранения и передачи информации в системах криптографической защиты. Одним из путей решения является введение в криптографическую систему защиты механизмов помехоустойчивого кодирования.

2. Корректо-криптографичкские системы

Рассмотрим симметричные блочные криптографические шифры с фиксированной длиной входного/выходного блока равной L. В общем виде шифротекст Ic, получаемый в результате шифрования/кодирования (EC) открытого текста Ip секретным ключом k:

$$Ic = EC\ (Ip,\ k) \qquad (1).$$

Аналогично выполняется операция дешифрования/декодирования:

$$Ip = DC\ (Ic^*,\ k) \qquad (2).$$

При коррекции всех возникающих при передаче информации ошибок Ip в (1) и (2) не отличается даже при $Ic \neq Ic^*$.

Для различных сред и условий передачи информации требуются различные корректирующие коды. Согласно характеру распределения ошибок в телефонных каналах в большинстве случаев появляются одиночные ошибки и пакеты ошибок длины t, в большинстве случаев равные 2 - 4 бит[1].

Для создания гибкой криптосистемы удобно использовать механизмы предвычисления и возможность изменения корректирующего кода в зависимости от типа передающей среды, а также самого криптоалгоритма.

Для решения поставленной задачи необходимо найти корректирующий код $C\ (n,k)$, где число информационных символов k равно L. В качестве такого кода могут быть использованы преобразования кода Хэмминга $(2^m-1, 2^m-1-m)$, исправляющие одиночные и обнаруживающие двойные ошибки (m -любое целое), коды-перемежения, исправляющие пакеты длины t или коды Файра $((2^m-1)(2t-1), (2^m-1)(2t-1)- m -2t + 1)$. Код C может быть построен на основе квадратично-вычетных кодов (n_1n_2, k_1k_2, d_1d_2), исправляющих $(2t_1t_2+t_2+t_1)$ ошибок, или код БЧХ [2]. Достаточно эффективные конструкции корректо-криптографических систем получаются при использовании параллельной конкатенации двух кодов, известной как турбо-коды [3].

3. Оценка эффективности систем защиты

Понятие эффективности системы строго не определено. Это может быть главная, определяющая характеристика или сочетание наиболее важных технических или экономических показателей. В настоящей работе будем рассматривать сравнительную характеристику, которая учитывает все представляющие, с нашей точки зрения, интерес параметры. Тогда общий коэффициент качества или «эффективность системы» определяется соотношением [4]:

$$\gamma = \sum_{i=1}^{N} \beta_i \eta_i \qquad (3),$$

где β_i - относительный весовой коэффициент (вес), а η_i - «коэффициент успеха».

Очевидно, что $0 \le \gamma \le 1$.

На практике всегда существуют «важные» параметры и «менее важные». Поэтому все параметры разбиваются на группы, в которых параметры равносущественны, для расчета парциальных коэффициентов K. Тогда:

$$\beta_i = K / D_i \qquad (4),$$

где D_i - общий относительный вес группы.

Введем в рассмотрение следующие группы характеристик:

1 группа - пропускная способность системы, удельная помехоустойчивость, относительная теоретическая стойкость криптосистемы;

2 группа - время, необходимое на реинициализацию криптосхемы, надежность системы и др.;

3 группа - стоимость эксплуатации системы, компактность и др.

Приводимая ниже оценка эффективности является условной из-за варьируемости приоритета тех или иных параметров.

В расчетах вес для первой группы параметров 0.1. По данной методике вычисления эффективность корректо-криптографической системы примерно на 20% (по расчетам на 19.3%) эффективнее обычной криптографической системы.

Таким образом, условие целесообразности создания корректирующих криптосистем подкреплено достигаемым при этом эффектом.

4. Заключение

Отказоустойчивые криптографические системы защиты информации позволяют создавать на их основе безопасную инфраструктуру внутренних коммуникаций, обеспечивающую надежную защиту, в частности, наиболее критичной, подсистемы управления сети предприятия

Литература

1. Урабанович П.П., Пацей Н.В., Спиридонов В.В. Распределение ошибок в телефонных каналах передачи дискретной информации// Известия Белорусской инженерной академии. Спец. выпуск.- Мн., 1997.-№1(3)\.-С.24-26.

2. Error-Control Tech. for Digital Comm., A.Michelson, A. Levesque. John Wiley & Son: Inc. 1985, pp.45.

3. S. Benedetto, G. Montorsi «Design of parallel concatenated convolutional codes» // IEEE Transaction on Communication, May, 1996, vol.44, no.5,P.591-600.

4. А. Чанас, У.Купер Модели условной экстремизации и их использование для оценки качества систем. Общая теория систем. Сборник. М., «Мир»,1986.