УДК 004.056

НЕКОТОРЫЕ АСПЕКТЫ ПРАКТИЧЕСКОЙ РЕАЛИЗАЦИИ АБСОЛЮТНО СТОЙКИХ ШИФРОВ

Л.И. Галабурда, Д.М. Романенко
(БГТУ, г. Минск)

Криптографические методы позволяют решать важнейшие проблемы защищенной автоматизированной обработки и передачи данных. Наибольший интерес с точки зрения надежной защиты информации от несанкционированного доступа представляют абсолютно стойкие шифры. Вся их секретность сосредоточена в ключе K. Размер ключа шифрования не должен быть меньше размера шифруемого сообщения: $|K| \geq |T|$. Для зашифрования сообщение T необходимо скомбинировать с ключом K с помощью некоторой бинарной операции $\circ$ таким образом, чтобы полученный шифротекст зависел и от исходного текста T, и от ключа K. При этом уравнение зашифрования будет иметь следующий вид [1]:

$$T = E_K(T) = T \circ K. \qquad (1)$$

Все биты ключа должны быть случайны с равновероятными значениями и статистически независимы. Такой ключ может быть получен только аппаратным способом, алгоритмически его выработать нельзя.

Обсудим теперь требования, которым должна удовлетворять операция $\circ$. Во-первых, чтобы шифрование было обратимым, уравнение $T \circ K = T'$ должно быть однозначно разрешимо относительно T при любых значениях T' и K. Это означает, что у бинарной операции $\circ$ должна существовать обратная, которую мы обозначим через $\bullet$, и каковы бы ни были N-битовые блоки данных T и K, всегда должно выполняться равенство $(T \circ K) \bullet K = T$. Во вторых, для обеспечения полной секретности шифра необходимо, чтобы разные ключи давали для одинаковых исходных текстов разные шифротексты. Операции $\circ$ и $\bullet$ могут выбираться из соображений удобства. В качестве таких операций может использоваться сложение и вычитание по модулю 2^N [1]:

$$T \circ K = (T + K) \bmod 2^N,\ T \bullet K = (T - K) \bmod 2^N. \qquad (2)$$

Осуществить вычисления над сообщением как единым целым

может оказаться затруднительным по причине его значительного размера, поэтому целесообразно разбить сообщение и ключ на блоки меньшего размера и применить указанные операции к этим блокам.

Если довести этот процесс дробления до логического конца, мы придем к операции побитового сложения по модулю 2, называемой также побитовым исключающим или [1]:

$$T^{\circ} K = T \bullet K = T \oplus K. \qquad (3)$$

Последняя операция оказалась обратной к самой себе и по этой причине, а также в силу своей простоты и легкости реализации (отдельные биты сообщения в ней обрабатываются независимо друг от друга), получила наибольшее распространение.

Итак, данный шифр, который мы сейчас получили, называется одноразовой гаммой Вернама. Этот шифр обладает абсолютной стойкостью, которая, однако, оплачивается достаточно дорогой ценой – для шифрования сообщения нужен ключ такого же размера, предварительно доставленный отправителю и получателю. К устройству хранения ключа предъявляются следующие требования: большая информационная емкость, надежность хранения информации, высокое быстродействие. Данным требованиям удовлетворяют устройства хранения информации на основе полупроводниковой памяти сверхбольшой емкости (до десятков Гбайт).

Для обеспечения надежного хранения информации предлагается использовать трехмерные итеративные коды.

Трехмерный итеративный код позволяет корректировать до трех (четырех – в случае использование кода с диагональными проверками) ошибок включительно (минимальное кодовое расстояние d = 8 либо d = 10)[2].

При разработке памяти на основе данного кода огромное значение имеет корректная реализация основных преимуществ данного кода.

Данная память имеет некоторые особенности:

– корректирующий код защищает не отдельные информационные слова, а целое кодовое пространство, представляющее собой совокупность кристаллов разных пластин;

– при накоплении в кодовом пространстве трех (четырех) ошибок, они должны исправляться, т.к. появление четвертой (пятой) ошибки может привести к потере информации;

– процессы записи и чтения информации изменений не

претерпевают.

Вышеотмеченные особенности позволяют:

– более эффективно использовать информационное пространство (величина относительной избыточности составляет несколько процентов);

– реализовать основное достоинство трехмерных итеративных кодов – схожесть со структурой памяти, что должно существенно упростить алгоритмы формирования проверочных символов.

Время накопления в кодовом пространстве четырех ошибок зависит от интенсивности сбоев и от количества кристаллов на пластине. Следовательно, необходимо увеличивать последний параметр. Но это приведет к уменьшению информационной емкости одного кристалла, а, следовательно, к увеличению избыточности итеративного кода в плоскости. Из теории трехмерных итеративных кодов известно, что оптимальной является кубическая проверочная матрица. В качестве основного направления совершенствования памяти в случае использования трехмерного итеративного кода можно принять увеличение количества кристаллов на пластине (даже за счет уменьшения емкости одного кристалла), а также увеличение количества пластин, из которых будет набираться память. Все это позволит достигнуть максимального времени наработки на отказ при уменьшении избыточности, необходимой для реализации данного метода кодирования.

ЛИТЕРАТУРА

1. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. – СПб.: Лань, 2001. – 224с.

2. Урбанович П.П., Романенко Д.М. Свойства и алгоритмы аппаратной реализации нового вида итеративных кодов для систем памяти // Новые информационные технологии: третья международная конференция NITE'2000, т. 2 – Мн.: БГЭУ,2000.– с. 159–164.