УДК 519.72

НОВЫЙ СИММЕТРИЧНЫЙ АЛГОРИТМ ШИФРОВАНИЯ

Вишневский К.П., Чижиков В.И., Барышенский Д.С., Жучкова В.В.

Предложен новый симметричный способ шифрования большого объема данных в реальном времени. Он является наиболее быстрым среди уже известных симметричных методов. Важное преимущество данного подхода состоит в возможности изменения длины ключа без изменения алгоритма шифрования. Ключ может быть любой длины.

Введение

При шифровании большого объема данных в реальном времени требуются быстрые алгоритмы. Для этих целей подходят поточные шифры. Они, как правило, похожи на одноразовый шифр-блокнот. Его суть заключается в сложении по модулю 2 битов потока ключей с битами сообщения. Однако вместо фиксированного потока ключей, который в ранних поточных шифрах и являлся секретным ключом, в современных системах поток ключей генерируется из короткого основного ключа с помощью однозначно определенных детерминированных алгоритмов. Над развитием разных способов их комбинирования с целью создания быстрых поточных шифров работают многие лаборатории.

Используемые на практике симметричные и несимметричные криптосистемы должны удовлетворять определенным требованиям:

1) знание использованного алгоритма не должно снижать надежность шифрования;

2) зашифрованный текст не может быть прочитан без знания ключа;

3) каждый ключ из многообразия ключей должен обеспечивать достаточную надежность;

4) изменение длины ключа не должно приводить к изменению алгоритма шифрования;

5) если известны зашифрованный и открытый тексты, то число операций, необходимых для определения ключа, не должно быть меньше полного числа возможных ключей;

6) дешифрование текста путем перебора всех возможных ключей должно выходить далеко за пределы возможностей компьютеров, используемых на практике;

7) не должно быть легко устанавливаемой зависимости между последовательно используемыми ключами;

8) исходный и зашифрованный тексты должны быть одинакового размера;

9) алгоритм может быть реализован аппаратно.

Следует подчеркнуть, что для обратного преобразования зашифрованного текста часто используются два термина: расшифровывание и дешифрование. При расшифровывании ключ считается известным, а при дешифровании ключ неизвестен. Однако мы не будем делать различия между ними.

Согласно теореме К. Шеннона [1] совершенной секретностью обладает традиционная система шифрования Г. Вернама или одноразовый шифр-блокнот. В ней для пересылки битов необходим ключ, содержащий тоже количество двоичных знаков, что и сообщение. Каждый бит посылаемого текста складывается по модулю 2 с соответствующим битом ключа и получается криптограмма. Любой ключ разрешается использовать только один раз. Следовательно, распределение ключей в этой системе является основной проблемой [2].

В принципе любой способ шифрования сообщения, использующего битовое представление информации, можно формально рассматривать как систему Г. Вернама. Действительно, пусть M – сообщение, C – криптограмма и K – ключ. Тогда $C = M \oplus K$, $K = C \oplus M$, $M = C \oplus K$, т.е. знание C и M позволяет рассматривать любой способ шифрования как одноразовый шифр-блокнот.

В данной статье мы предлагаем измененный способ реализации этой системы шифрования. Основной элемент – ключ генерируется случайным образом. Причем его длина меньше длины сообщения ($K \le M$). Само сообщение перед шифрованием зашумляется. Это способствует уменьшению длины ключа. Кроме того, на основе операции сложения по модулю 2 образуется информационная свертка. Она играет основную роль в предлагаемом способе шифрования, который мы назвали SEA (симметричный алгоритм шифрования).

Концепция нового способа шифрования

Принцип работы симметричного алгоритма шифрования (SEA) основан на применении информационной свертки – специальным образом организованной процедуры поглощения битов.

Для ее демонстрации рассмотрим процедуру информационного свертывания на примере произвольной битовой строки. Свертка данных происходит следующим образом: берутся два смежных входных бита и на основе их значений устанавливается значение выходного бита. Далее процесс повторяется, т.е. рассматриваются следующие два смежных бита. Важной особенностью информационной свертки является возможность обратного преобразования при условии применения симметричного правила преобразования. В данном случае (битовая строка) используется следующая таблица преобразований (табл. 1). Очевидно, что эта процедура для двух битов является сложением по модулю два ($A \oplus B$).

Таблица 1.

Таблица преобразований значений для 2 битов

Входные значения	*Выходное значение*
0 0	0
0 1	1
1 0	1
1 1	0

Как видно из таблицы, преобразование является симметричным. На рис. 1 показан принцип работы информационной свертки: после каждого этапа свертывания размер данных уменьшается на 1 бит.

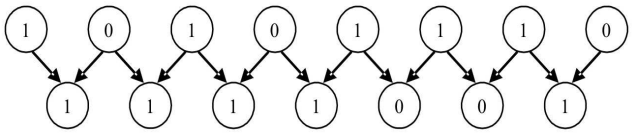

Рис. 1. Информационная свертка

При обратном процессе получения информационной развертки размер данных увеличивается на 1 бит. Однако в результате развертки образуются две битовых строки, свертка которых даст исходную строку (рис. 2). Данное свойство информационной свертки можно использовать для шифрования данных. Рассмотрим два вида шифрования с фиксированным ключом и с генерируемым ключом в процессе свертки.

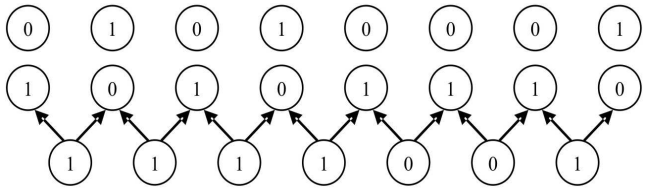

Рис. 2. Информационная развертка

Шифрование данных с созданием ключа производиться путем циклической свертки данных (рис. 3), в результате чего зашифрованные данные имеют уменьшенный размер. Дешифрование происходит во время циклической развертки с выбором выходного варианта таким образом, что бы он совпадал с ключом.

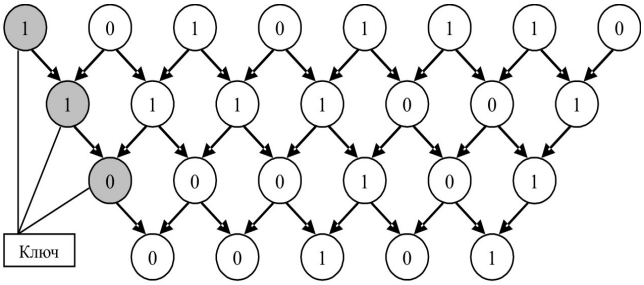

Рис. 3. Шифрование с генерацией ключа

Шифрование данных с фиксированным ключом, несколько отличается от рассмотренного выше метода. Данные так же шифруются с применением циклической свертки, однако на каждом этапе к строке прибавляется очередной бит ключа. В результате такого шифрования размер данных остается неизменным. Дешифрование происходит во время циклической развертки с выбором выходного варианта таким образом, что бы он совпадал с ключом. При этом после каждого шага развертки происходит отбрасывание ключевого бита.

Иногда в процессе шифрования/дешифрования выгоднее использовать не битовые строки, а байтовые строки. В этом случае преобразование байтов A и B проводится по формуле: $C = A$ XOR B.

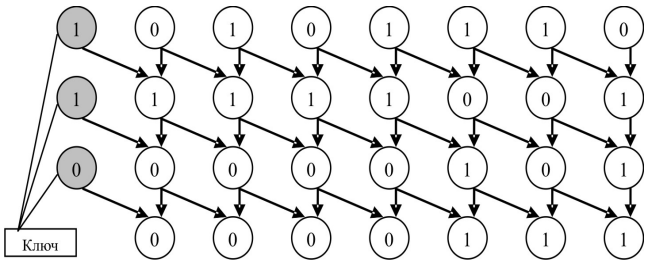

Рис. 4. Шифрование с фиксированным ключом

Для повышения криптостойкости метода, можно использовать простой алгоритм зашумления: $M_0 =$ Key, $N_i = N_i$ XOR M_i, $M_i = M_i \; Z_i^3$, $Z_i = i*k$, где N_i – текущий байт информации, M_i и Z_i – рекурсивные параметры зашумления, k – произвольный коэффициент.

Сравнение различных способов шифрования

Для сравнения различных способов шифрования возьмем следующий рисунок 5: черный круг на белом фоне. При шифровании размер рисунка сохраняется.

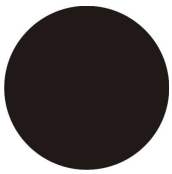

Рис. 5. Исходный объект для шифрования

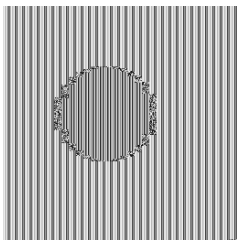

Рис. 6. Метод 3DES

Зашифрованный методом 3DES текст посредством формата raw показан на рис. 6.

Аналогично зашифрованные методами DES, BLOWFISH, RIJNDAEL и SEA тексты показаны на рис. 7, 8, 9 и 10 соответственно.

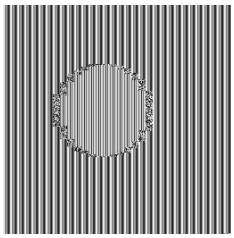

Рис. 7. Метод DES

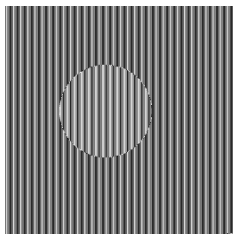

Рис. 8. Метод BLOWFISH

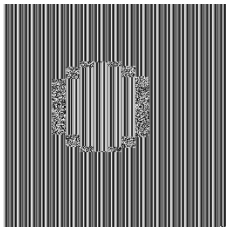

Рис. 9. Метод RIJNDAEL

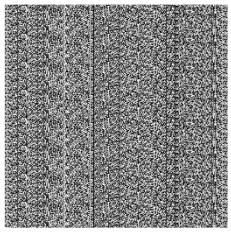

Рис. 10. Метод SEA

Скорости шифрования при использовании различных методов приведены в таблице 2. При сравнении в предлагаемом алгоритме SEA длина ключа составляла 128 байтов.

Таблица 2.

Сравнение скорости работы различных алгоритмов

Алгоритм	Скорость на P4 2.6 ГГц
SEA	247 Мбит/сек
Blowfish	128 Мбит/сек
Rijndael	54 Мбит/сек
3DES	24 Мбит/сек
DES	21 Мбит/сек

Заключение

Предложенный способ шифрования SEA (Symmetric Encryption Algorithm) является наиболее быстрым среди уже известных симметричных методов. При аппаратной реализации шифрование может происходить со скоростью *N* тактов на блок, где *N* длина ключа. Блок же может достигать больших размеров (мегабайт и более). Самым важным преимуществом SEA перед другими симметричными способами является возможность изменять длину ключа без изменения алгоритма шифрования. Она может быть любой. Естественно, что скорость шифрования зависит от длины ключа. Поскольку длина ключей не велика, то для их распространения можно использовать известные методы.

Литература

1. Введение в криптографию. Под общей редакцией Ященко В. В. –М.: МЦНМО: “Черо”, 1999. –272 с.
2. Насыпный В. В. Одноразовое шифрование с открытым распределением ключей // Открытые системы. 2004, №1. С. 66–69.

НОВЫЕ КНИГИ

Цифровая обработка сигналов. Практическое руководство для инженеров и научных работников (+CD) / Стивен Смит; пер. с англ. А. Ю. Линовича, С.В. Витязева., И.С. Гусинского. – М. : Додэка-XXI, 2008. — 720 с. : ил. — (Серия «Схемотехника»).
ISBN 978-5-94120-145-7
Заказ: www.dokabooks.ru

В книге изложены основы теории цифровой обработки сигналов. Акцент сделан на доступности изложения материала и объяснении методов и алгоритмов так, как они понимаются при практическом использовании. Цель книги — практический подход к цифровой обработке сигналов, позволяющий преодолеть барьер сложной математики и абстрактной теории, характерных для традиционных учебников. Изложение материала сопровождается большим количеством примеров, иллюстраций и текстов программ (которые вы также можете найти на прилагаемом CD). Книга предназначена научным работникам и инженерам, желающим применять методы цифровой обработки в различных технических сферах. Рекомендуется аспирантам и студентам, изучающим цифровую обработку сигналов.

ЦОС В УНИВЕРСИТЕТАХ

В течение ряда лет, начиная с первого выпуска в 1999 году, редакция журнала систематически отслеживает появление на мировом и российском рынках новых перспективных DSP-технологий и знакомит читателей с тенденциями и направлениями развития цифровых сигнальных процессоров и инструментальных средств проектирования систем ЦОС на их основе. За прошедшие годы неоднократно публиковались статьи, отражающие развитие DSP-технологий таких мировых лидеров в этой области, как компании Texas Instruments Inc. и Analog Devices Inc. Что особенно приятно отметить – редакция журнала всегда откликалась одной из первых на новые разработки в области DSP-технологий отечественных фирм: НТЦ «Модуль», ГУП НПЦ «ЭЛВИС», ЗАО «Инструментальные системы», ЗАО «АВТЭКС», ЗАО «СКАН Инжиниринг-телеком» и др.

Отвечая целям и задачам укрепления и расширения сотрудничества с ведущими мировыми и отечественными производителями современной элементной базы DSP-технологий и средств проектирования систем ЦОС, с одной стороны, и российскими вузами, с другой стороны, редакция журнала открыла новую рубрику: «ЦОС в университетах». В рамках новой рубрики найдут отражение вопросы организации учебного процесса и учебно-методического обеспечения по широкому спектру дисциплин, связанных с применением ЦОС и DSP-технологий, текущая информация об университетских программах, семинарах и конкурсах фирм-производителей, новых разработках научных лабораторий российских вузов.

Приглашаем к сотрудничеству все заинтересованные организации и творческие коллективы преподавателей и сотрудников российских вузов и стран СНГ, работающих в области ЦОС и DSP-технологий.

Зам. Главного редактора, профессор В. В. Витязев