СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

УДК 681.324.067

А.А. ТОРБА, канд. техн. наук, В.А. БОБУХ, канд. техн. наук, М.О. ТОРБА, А.О. ТОРБА

МЕТОДЫ ПОВЫШЕНИЯ КРИПТОСТОЙКОСТИ АЛГОРИТМОВ ПОТОКОВОГО ШИФРОВАНИЯ

Введение

Большинство существующих симметричных шифров однозначно могут быть отнесены либо к потоковым (ПШ), либо к блочным шифрам (БШ). Но теоретическая граница между ними является довольно размытой. Например, алгоритмы блочного шифрования часто используются в режиме потокового шифрования (режиме гаммирования).

Важнейшим достоинством потоковых шифров перед блочными является высокая скорость шифрования, соизмеримая со скоростью поступления входной информации, что позволяет шифровать аудио- или видеопотоки в реальном масштабе времени.

Потоковые шифры, которые шифруют и дешифруют данные по одному биту, не очень подходят для программных реализаций. А блочные шифры легче реализовывать программно, так как они позволяют избежать трудоемких манипуляций с битами и оперируют удобными для компьютера блоками данных, соизмеримыми с разрядностью регистров общего назначения (РОН). С другой стороны, потоковые шифры на регистрах сдвига больше подходят для аппаратной реализации.

Согласно Райнеру Рюппелю можно выделить четыре основных подхода к проектированию потоковых шифров (ПШ):

- *системно-теоретический* – основан на создании для криптоаналитика сложной, ранее неисследованной проблемы;
- *сложностно-теоретический* – основан на сложной, но известной проблеме (например, факторизация чисел или дискретное логарифмирование);
- *информационно-технический* – основан на попытке утаить открытый текст от криптоаналитика – независимо от того, сколько времени потрачено на дешифрование, криптоаналитик не найдет однозначного решения;
- *рандомизированный* – основан на создании объемной задачи; криптограф тем самым пытается сделать решение задачи дешифрования физически невозможным.

Известны теоретические критерии Райнера Рюппеля для проектирования ПШ (хотя до сих пор не доказано, что эти критерии необходимы или достаточны для безопасности потоковой системы шифрования):

- длинные периоды выходных гаммирующих псевдослучайных последовательностей;
- большая линейная сложность;
- диффузия – рассеивание избыточности в подструктурах, «размазывание» статистики по всему гаммирующему потоку;
- каждый бит гаммирующей последовательности должен быть сложным преобразованием большинства битов ключа;
- критерий нелинейности для логических функций.

Большое количество реальных потоковых шифров основано на регистрах сдвига с линейной обратной связью – линейных рекуррентных регистрах (ЛРР). Основные преимущества ЛРР:

- высокое быстродействие криптографических алгоритмов;
- применение только простейших операций сложения и умножения, аппаратно реализованных практически во всех вычислительных устройствах;
- хорошие криптографические свойства (генерируемые последовательности имеют большой период и хорошие статистические свойства);

- легкость анализа с использованием алгебраических методов за счет линейной структуры.

Сами по себе ЛРР являются хорошими генераторами псевдослучайных последовательностей, но они обладают некоторыми нежелательными неслучайными свойствами. Для ЛРР с количеством разрядов «*n*» внутреннее состояние представляет собой предыдущие «*n*» выходных битов генератора. Даже если параметры рекурренты (номера отводов m_k обратной связи) хранятся в секрете, они могут быть определены по *2n* выходным битам генератора с помощью алгоритма Берлекэмпа – Мэсси.

Существует несколько методов проектирования генераторов псевдослучайного ключевого потока, которые разрушают линейные свойства ЛРР и тем самым делают такие системы криптографически более стойкими:

- использование нелинейной функции, объединяющей выходы нескольких ЛРР (генератор Геффа и др.);
- использование нелинейной фильтрующей функции для содержимого каждой ячейки единственного ЛРР;
- использование выхода одного ЛРР для управления синхросигналом одного (или нескольких) ЛРР (алгоритм А5 и др.);
- динамическое изменение параметров рекурренты (длины регистра «*n*» и номеров отводов m_k) в процессе формирования псевдослучайной гаммирующей последовательности – так называемые динамические линейные рекуррентные регистры (ДЛРР).

Алгоритм потокового шифрования «AUGUST-1»

Простейший алгоритм потокового шифрования на основе ДЛРР «AUGUST-1» описан в патенте Украины [1, 2]. Упрощенная структурная схема генератора псевдослучайной гаммирующей последовательности приведена на рис. 1.

Основу генератора составляет линейный рекуррентный регистр (ЛРР), реализованный на сдвигающем регистре (RG1). На информационный вход последовательного сдвига (Ds) этого регистра подается сигнал с выхода элемента «ИСКЛЮЧАЮЩЕЕ ИЛИ» (элемента «XOR»), а к входам этого элемента подключены: последний выход сдвигающего регистра «Qn» и выход мультиплексора MS.

Информационные входы (D0…Dk) мультиплексора (MS) подключены в произвольном порядке к отводам сдвигающего регистра (RG1). Номера всех отводов m_k должны удовлетворять известному условию для ЛЛР: полином, вычисленный на коэффициентах $-1 + x^m + x^n$ – должен быть примитивным и неприводимым над полем Галуа.

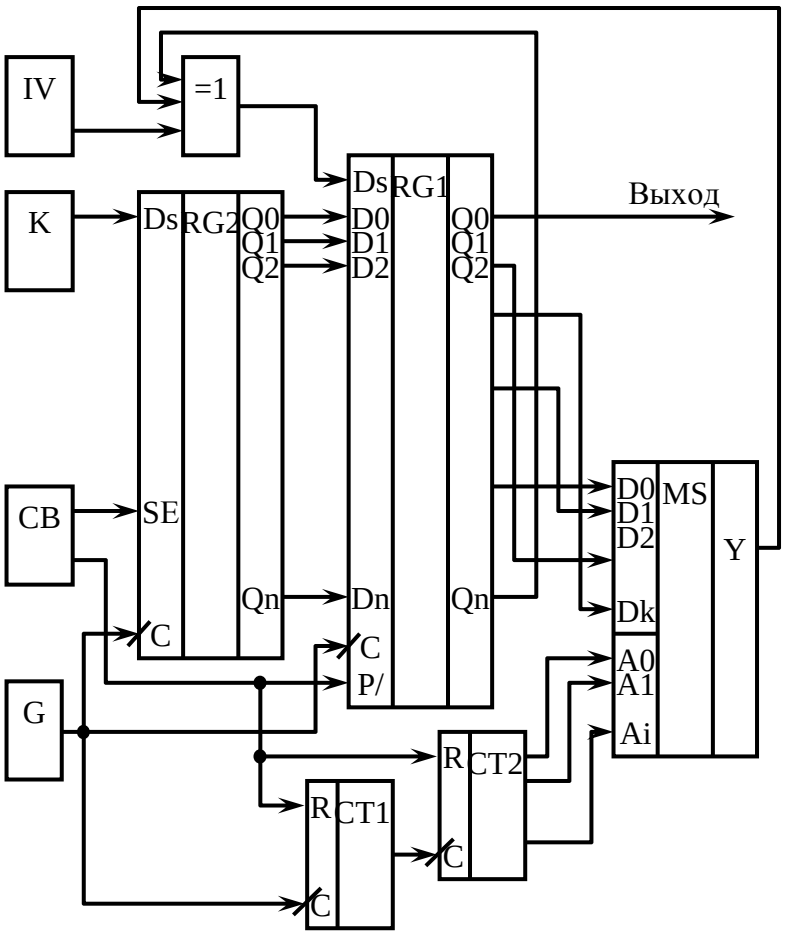

Рис. 1

На адресные входы мультиплексора MS (A0…Ai) подаются последовательные двоичные коды с выходов счетчика СТ2. Коэффициент деления счетчика СТ1 определяет периодичность смены параметров рекурренты (обычно периодичность в несколько раз меньше разрядности сдвигающего регистра «*n*»). Желательно выбирать коэффициент деления счетчика СТ1 и длину ДЛРР (т.е. разрядность «*n*» сдвигающего регистра RG1) как взаимно простые числа.

Скорость формирования псевдослучайной последовательности определяется частотой тактового генератора (G) и может составлять от 10 МГц до 1 ГГц.

До начала шифрования абоненты обмениваются секретными кратковременными (или сеансовыми) ключами Кс. Алгори́тм Ди́ффи-Хе́ллмана (англ. Diffie-Hellman, D-H) позволяет двум или более пользователям обменяться без посредников секретным ключом, который будет использован затем для симметричного шифрования.

Длина секретного ключа Кс в битах определяет криптостойкость алгоритма потокового шифрования и равняется разрядности «*n*» сдвигающего регистра RG1. При использовании современных программируемых логических интегральных схем (ПЛИС) разрядность регистра RG1 (и секретного ключа Кс) может составлять от 100 до нескольких тысяч бит.

До начала шифрования сформированный секретный ключ Кс вводится в регистр RG2. Для этого блок управления (СВ) вырабатывает сигнал разрешения последовательного ввода (SE), который поступает на вход управления регистра RG2.

После ввода секретного ключа в регистр RG2 – этот ключ в параллельном формате записывается в регистр сдвига RG1. Для этого блок управления (СВ) формирует логический сигнал, который переводит первый регистр RG1 в режим параллельной загрузки, а также удерживает в нулевом состоянии первый и второй счетчики СТ1, СТ2.

Перед шифрованием в канал связи передается случайное (чаще всего – псевдослучайное) значение инициализации IV (Initialisation Value или синхропосылка). Это значение инициализации не является секретным и передается по открытому каналу связи перед каждым сеансом шифрования. Обычно длина IV в битах не превышает разрядность рекуррентного регистра RG1.

Использование для всех сообщений отдельных случайных значений инициализации IV позволяет формировать различные значения псевдослучайной гаммирующей последовательности для каждого нового сообщения. При этом даже одинаковые начальные тексты сообщений будут зашифрованы по-разному.

Одновременно с передачей в канал связи значения инициализации IV в последовательном формате вводится в сдвигающий регистр RG1 через третий вход элемента «ИСКЛЮЧАЮЩЕЕ ИЛИ» (элемента «XOR»). На первый и второй входы этого элемента «XOR» подаются сигналы с последнего выхода последовательного регистра RG1 и выхода мультиплексора MS для формирования рекуррентной псевдослучайной последовательности гаммы.

Для смены параметров рекурренты первого регистра сдвига RG1 его логические уровни с промежуточных выходов m_k подаются на информационные входы мультиплексора MS, а адресные входы этого мультиплексора подключены к выходам второго счетчика СТ2.

Выходная псевдослучайная последовательность гаммы, которая может сниматься с любого выхода первого регистра сдвига RG1, является детерминированной (т.е. может быть полностью восстановлена на приемной стороне канала связи) и зависит от секретного значения кратковременного сеансового ключа Кс, от случайного значения инициализации IV и долговременных секретных параметров (ключей):

- длины кратковременного (сеансового) секретного ключа «*n*»,
- размера и содержимого матрицы коммутации мультиплексора MS,
- коэффициента деления первого счетчика СТ1.

Работа генератора гаммирующей последовательности при динамическом изменении параметров рекурренты не может быть описана системой линейных уравнений. Это соответствует критерию Райнера Рюппеля – нелинейности логических функций.

Поэтому криптоаналитику необходимо будет произвести полный перебор всех значений секретных долговременных параметров и для каждого значения этих параметров провести лобовую атаку по перебору всех кратковременных (сеансовых) ключей Кс, что делает процесс дешифрования в разумные сроки физически невозможным.

Алгоритм потокового шифрования «AUGUST-2»

В алгоритме потокового шифрования «AUGUST-2» [3] для увеличения криптостойкости генератора гаммирующей последовательности на основе ДЛРР предложено изменять величины интервалов времени между сменами параметров рекурренты в псевдослучайном порядке (рис 2).

Эти временные интервалы задаются счетчиком с программируемым коэффициентом деления СТ1, информационные входы которого подключены в произвольном порядке к выходам сдвигающего регистра RG1 (рис 2). Поэтому величины временных интервалов будут зависеть от начального значения сеансового ключа Кс, значения инициализации IV и текущего состояния сдвигающего регистра.

Это позволяет реализовать один из критериев Райнера Рюппеля: «Каждый бит гаммирующей последовательности должен быть сложным преобразованием большинства битов ключа».

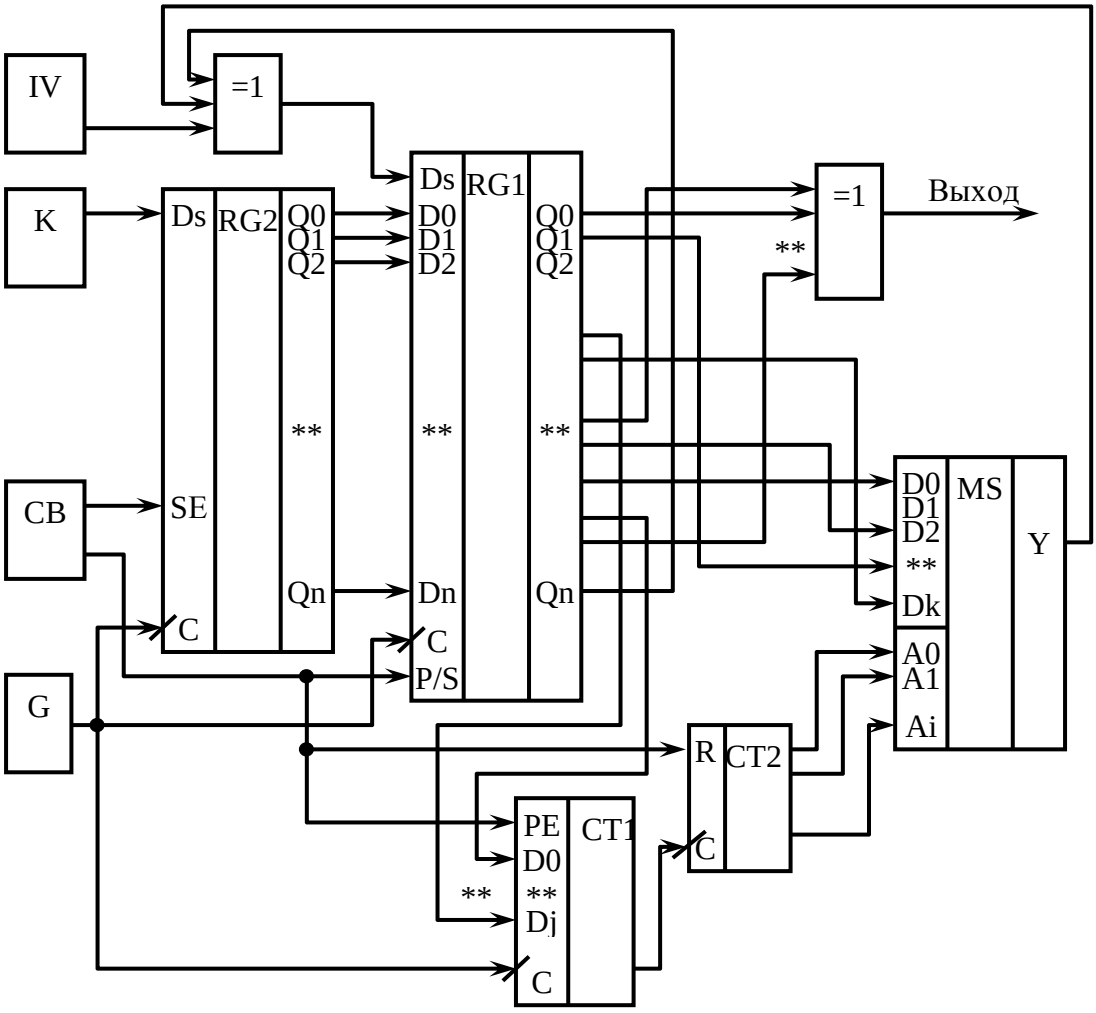

Рис. 2

Кроме перечисленных долговременных секретных параметров (ключей) алгоритма «AUGUST-1» в этом алгоритме добавлены новые секретные долговременные параметры:

- диапазон изменения коэффициента деления счетчика CT1,
- номера выходов регистра RG1, которые подключены к информационным входам счетчика CT1.

Еще одним преимуществом алгоритма «AUGUST-2» является введение второго выходного элемента «ИСКЛЮЧАЮЩЕЕ ИЛИ» (элемента «XOR»), входы которого подключены в произвольном порядке к выходам ДЛРР (рис. 2). С выхода этого элемента «ИСКЛЮЧАЮЩЕЕ ИЛИ» снимается псевдослучайная гаммирующая последовательность. Это позволяет улучшить статистические свойства формируемой гаммы: уменьшить разность вероятностей «нулей» и «единиц» выходной последовательности, а также уменьшить нормированные коэффициенты автокорреляционной функции [4].

Алгоритм потокового шифрования «AUGUST-3»

В алгоритме потокового шифрования «AUGUST-3» [5] для увеличения криптостойкости генератора гаммирующей последовательности на основе ДЛРР предложено изменять параметры рекурренты в псевдослучайном порядке (рис. 3).

Для этого на адресные входы мультиплексора подаются двоичные коды с выходов дополнительного параллельного регистра RG3, в котором через фиксированные интервалы времени сохраняются коды с произвольных выходов RG1.

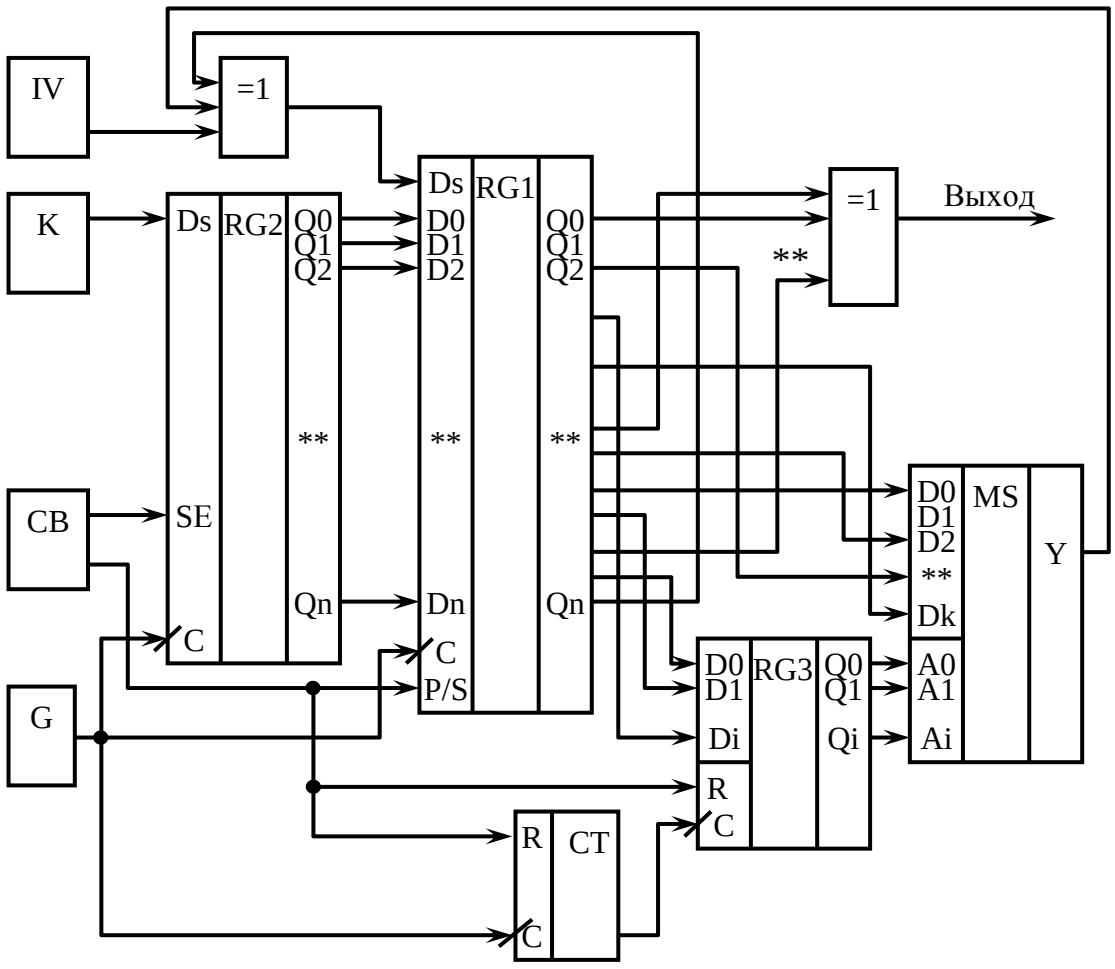

Рис. 3

Такое техническое решение с нелинейным характером изменения параметров рекурренты еще более усложняет критоанализ, осуществить который (даже без этих нововведений) в разумные сроки физически невозможно.

Выводы

Предложенные и запатентованные алгоритмы потокового шифрования «AUGUST-1», «AUGUST-2» и «AUGUST-3» разрушают линейные свойства ЛРР и тем самым делают такие системы криптографически более стойкими за счет динамического изменения параметров рекурренты в процессе формирования псевдослучайной гаммирующей последовательности.

В отличие от известных криптоалгоритмов (DES, AES и др.), в которых полностью известен математический аппарат криптопреобразований, а неизвестным является только единственный секретный параметр – кратковременный ключ, – в предложенных алгоритмах на основе ДЛРР присутствует очень большое количество долговременных секретных параметров (полный перебор которых может занять миллиарды лет).

Поэтому криптоанализ таких алгоритмов с перебором всех долговременных секретных параметров и для каждого такого параметра перебор всех значений секретного кратковременного (сеансового) ключа является физически невозможным в разумные сроки.

Список литературы: 1. *Патент* Украины на полезную модель № 85039. Опубл. Бюл. № 21, 2013 г. 2. *Торба А.А.* Быстродействующий детерминированный генератор псевдослучайных последовательностей для потокового шифрования / А.А. Торба, В.А. Бобух, А.А. Бобкова // Прикладная радиоэлектроника. – 2014. – Т. 13, №3. – С. 316-318. 3. Патент Украины на полезную модель № 93477.Опубл. Бюл. № 19, 2014 г. 4. *Торба А.А.* Методы и средства генерации случайных битовых последовательностей / А.А. Торба, А.А. Бобкова, Ю.И. Горбенко, В.А. Бобух ; под ред. И.Д. Горбенко. – Харьков : Форт, 2012. – 232 с. 5. *Патент* Украины на полезную модель № 93117. Опубл. Бюл. № 18, 2014 г.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 11.03.2016