

ДЕТЕРМИНИРОВАННЫЕ ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ ПОТОКОВОГО ШИФРОВАНИЯ НА ОСНОВЕ ДЛРР

А.А. ТОРБА, В.А. БОБУХ, М.О. ТОРБА, А.О. ТОРБА

В работе проанализированы алгоритмы потокового шифрования на основе динамических линейных рекуррентных регистров (ДЛРР) и методы повышения их криптостойкости. Эти алгоритмы используют рандомизированный подход, основанный на создании объёмной задачи; криптограф тем самым пытается сделать решение задачи дешифрования физически невозможным.

Ключевые слова: потоковый шифр, динамический линейный рекуррентный регистр, гаммирующая последовательность, рандомизированный подход.

ВВЕДЕНИЕ

Максимальная скорость передачи информации в каналах связи с ограниченным доступом определяется быстродействием аппаратных (или программно-аппаратных) алгоритмов шифрования и расшифрования сообщений.

Наибольшим быстродействием среди известных симметричных алгоритмов криптографических преобразований обладают потоковые алгоритмы, которые позволяют формировать каждый очередной бит псевдослучайной гаммы за один такт синхронизации.

Потоковые шифры, которые шифруют и дешифруют данные по одному биту, не очень подходят для программных реализаций. А блочные шифры легче реализовывать программно, т. к. 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 подход основан на создании для криптоаналитика сложной, ранее неисследованной проблемы.
- Сложностно-теоретический подход основан на сложной, но известной проблеме (например, факторизация чисел или дискретное логарифмирование).
- Информационно-технический подход основан на попытке утаить открытый текст от криптоаналитика – вне зависимости от того сколько времени потрачено на дешифрование, криптоаналитик не найдёт однозначного решения.
- Рандомизированный подход основан на создании объёмной задачи; криптограф тем самым пытается сделать решение задачи дешифрования физически невозможным.

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 рекуррентны (номера отводов m_k обратной связи) и хранятся в секрете, то они могут быть определены по $2n$ выходным битам генератора с помощью алгоритма Берлекэмп-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).

ОСНОВНАЯ ЧАСТЬ

Простейший детерминированный генератор псевдослучайных последовательностей для потокового шифрования на основе ДЛРР «AUGUST-1», описанный в патенте Украины [1,2], позволяет динамически изменять параметры рекурренты в процессе формирования псевдослучайной гаммы.

Скорость формирования псевдослучайной последовательности определяется быстродействием программируемых логических интегральных схем (ПЛИС) и может составлять от 10 МГц до 1 ГГц.

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

Выходная псевдослучайная последовательность гаммы является детерминированной (т.е. может быть полностью восстановлена на приемной стороне канала связи) и зависит от секретного значения кратковременного сеансового ключа K_s , от случайного значения инициализации IV и долговременных секретных параметров (ключей):

- длины секретного ключа « n »,
 - таблицы коммутации мультиплексора MS и
 - коэффициента деления первого счетчика CT1.
- Секретное значение длины « n » кратковременного

сеансового ключа K_s делает бесполезной лобовую атаку по перебору всех значений ключа.

В алгоритме потокового шифрования «AUGUST-2» [3,4] для увеличения криптостойкости генератора гаммирующей последовательности на основе ДЛРР предложено изменять величины интервалов времени между сменами параметров рекурренты в псевдослучайном порядке.

Эти временные интервалы задаются счетчиком с программируемым коэффициентом деления, информационные входы которого подключены в произвольном порядке к выходам сдвигающего регистра. Поэтому величины временных интервалов будут зависеть от начального значения сеансового ключа K_s , 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».

Также преимуществом алгоритма «AUGUST-2» является введение второго выходного элемента «ИСКЛЮЧАЮЩЕЕ ИЛИ» (элемента «XOR»), входы которого подключены в произвольном порядке к выходам ДЛРР. С выхода этого элемента «ИСКЛЮЧАЮЩЕЕ ИЛИ» снимается псевдослучайная гаммирующая последовательность. Это улучшает статистические свойства формируемой гаммы, а именно: уменьшает разность вероятностей «нулей» и «единиц» выходной последовательности, а также уменьшает нормированные коэффициенты автокорреляционной функции [5].

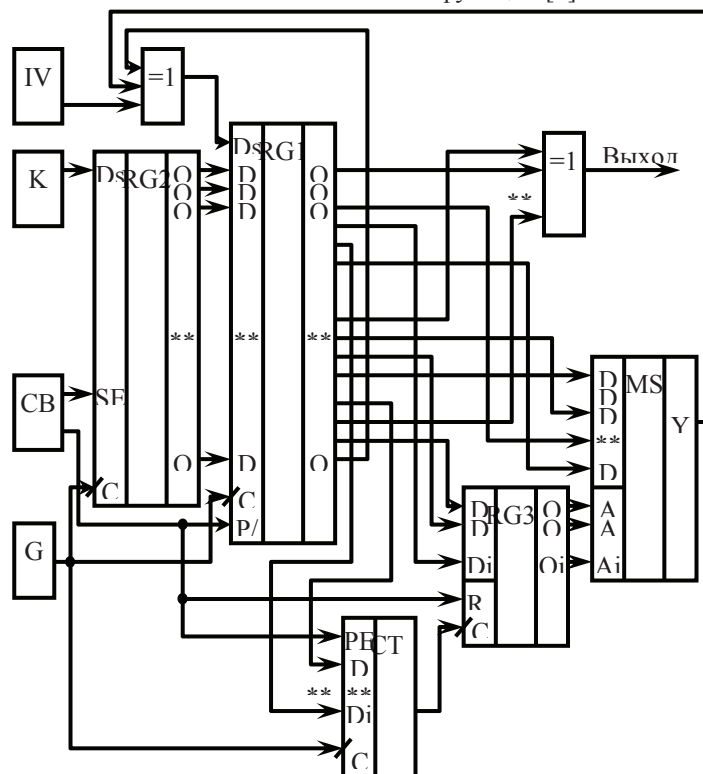


Рис. 1. Алгоритм потокового шифрования «AUGUST-4»

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.

В алгоритме потокового шифрования «AUGUST-3» [4,6] для увеличения криптостойкости генератора гаммирующей последовательности на основе ДЛРП предложено изменять параметры рекурренты в псевдослучайном порядке.

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

В алгоритме потокового шифрования «AUGUST-4» [7] (рис.1) для увеличения криптостойкости генератора гаммирующей последовательности на основе ДЛРР объединены преимущества алгоритмов «AUGUST-2» и «AUGUST-3».

Параметры рекурренты (номера отводов «п») ДЛРР на основе сдвигающего регистра RG1 изменяются в псевдослучайном порядке.

Для этого на адресные входы мультиплексора MS подаются логические уровни с выходов параллельного регистра RG3, который запоминает псевдослучайные сигналы с произвольных выходов сдвигающего регистра RG1.

Псевдослучайные временные интервалы смены параметров рекурренты задаются делителем с про-

граммируемым коэффициентом деления СТ.

Такое техническое решение с нелинейным характером изменения параметров рекурренты еще более усложняет криптоанализ, осуществить который в разумные сроки – физически невозможно.

В алгоритме потокового шифрования «AUGUST-5» [8] (рис.2) для увеличения криптостойкости генератора гаммирующей последовательности на основе ДЛРП введено несколько мультиплексоров, изменяющих параметры рекурренты. Например, один мультиплексор коммутирует отводы рекуррентного регистра RG1, которые определяют длину ДЛРП, а остальные мультиплексоры изменяют номера отводов рекуррентного регистра.

Возможна также ситуация, при которой, отвод регистра RG1, определяющий длину ДЛРР, в следующем такте может стать промежуточным отводом, а длина ДЛРР формируется другим мультиплексором.

На рис. 2 приведен случай, когда номера отводов ДЛРР коммутируются в постоянном порядке и через фиксированные временные интервалы. Возможно также изменить порядок коммутации отводов на псевдослучайный (как в алгоритме «**AUGUST-3**»), или через псевдослучайные временные интервалы (как в алгоритме «**AUGUST-2**»), или одновременно использовать псевдослучайное управление (как в алгоритме «**AUGUST-4**»).

ЗАКЛЮЧЕНИЕ

Предложенные и запатентованные алгоритмы потокового шифрования «AUGUST-1», «AUGUST-2», «AUGUST-3», «AUGUST-4» и «AUGUST-5» разрушают линейные свойства ЛПП и тем самым делают

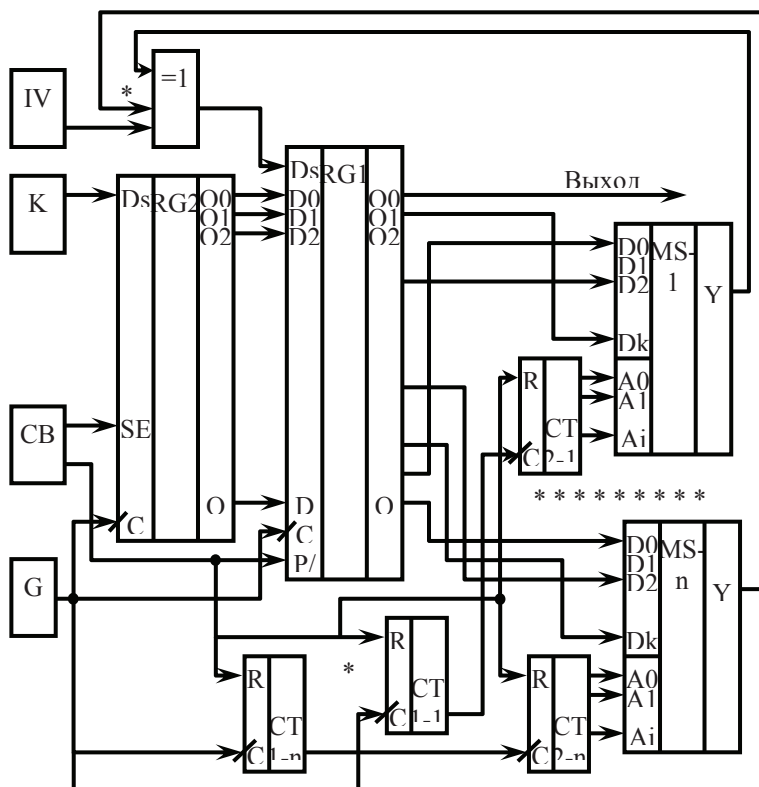


Рис. 2. Алгоритм потокового шифрования «AUGUST-5»

такие системы криптографически более стойкими за счет динамического изменения параметров рекуррентности в процессе формирования псевдослучайной гаммирующей последовательности.

Криптостойкость предложенных алгоритмов потокового шифрования определяется разрядностью кратковременного секретного ключа K_s , которая может составлять от 100 до нескольких тысяч бит. Причем секретным является не только значение ключа K_s , но и его длина.

Скорость формирования псевдослучайной гаммирующей последовательности ограничивается быстродействием используемых логических микросхем и может достигать 1000 МГц

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.

Литература.

- [1] Патент Украины на полезную модель № 85039, опубл. Бюл. № 21, 2013 г.
- [2] Торба А.А. Быстродействующий детерминированный генератор псевдослучайных последовательностей для потокового шифрования // [Текст]. А.А. Торба, В.А. Бобух, А.А. Бобкова. – Прикладная радиоэлектроника: научн.-техн. журнал. – 2014. – Том 13. – №3. – С. 316 – 318.
- [3] Патент Украины на полезную модель № 93477, опубл. Бюл. № 19, 2014 г.
- [4] Торба А.А. Методы повышения криптостойкости алгоритмов потокового шифрования // [Текст]. А.А. Торба, В.А. Бобух, М.О.Торба, А.О.Торба. – // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2016. – Вып. 184. – С. 178 – 183.
- [5] Торба А.А. Методы и средства генерации случайных битовых последовательностей // [Текст]. А.А. Торба, А.А. Бобкова, Ю.И. Горбенко, В.А. Бобух. – Под ред. д.т.н., профессора Горбенко И.Д. – Харьков: Изд-во «Форт», 2012. – 232 с.
- [6] Патент Украины на полезную модель № 93117, опубл. Бюл. № 18, 2014 г.
- [7] Патент Украины на полезную модель № 99194, опубл. Бюл. № 10, 2015 г.
- [8] Патент Украины на полезную модель № 97734, опубл. Бюл. № 7, 2015 г.



Торба Александр Алексеевич, кандидат технических наук, профессор кафедры ЭВМ, ХНУРЭ. Область научных интересов: аппаратные средства криптографических систем.



Бобух Всеволод Анатольевич, кандидат технических наук, начальник отдела аппаратных средств. Область научных интересов: аппаратные средства криптографических систем.



Торба Максим Олегович, студент ХНУРЭ. Область научных интересов: программирование баз данных, аппаратные средства криптографических систем.



Торба Александр Олегович, студент, ХНУРЭ. Область научных интересов: компьютерная анимация, аппаратные средства криптографических систем.

УДК 681.324.067

Детерміновані генератори псевдовипадкових послідовностей для потокового шифрування на основі ДЛРР / О.О. Торба, В.А. Бобух, М.О. Торба, О.О. Торба // Прикладна радіоелектроніка: наук.-техн. журнал. – 2016. – Том 15, № 3. – С. 191 – 194.

В роботі проаналізовано алгоритми потокового шифрування на основі динамічних лінійних рекурентних регістрів (ДЛРР) і методи підвищення їх криптостійкості. Ці алгоритми використовують рандомізований підхід, заснований на створенні об'ємної задачі; криптограф тим самим намагається зробити розв'язання завдання дешифрування фізично неможливим.

Ключові слова: потоковий шифр, динамічний лінійний рекурентний регістр, гамуюча послідовність, рандомізований підхід.

Іл.: 02. Бібліогр.: 08 найм.

UDC 681.324.067

Deterministic pseudorandom sequence generators for stream-based encryption D L R R / A.A. Torba, V.A. Bobuch, M.O. Torba, A.O. Torba // Applied Radio Electronics: Sci. Journ. – 2016. – Vol. 15, № 3. – P. 191 – 194.

The algorithms of streaming encryption based on dynamic linear recurrent registers (DLRR) and methods to improve their reliability are analyzed in the paper. These algorithms use a randomized approach based on a voluminous task; thus, the cryptographer tries to make the solution of a decrypting problem physically impossible.

Keywords: stream cipher, linear dynamic recurrent register, gamma sequence, randomized approach.

Fig.: 02. Ref.: 08 items.