УДК 681.324.067

БЫСТРОДЕЙСТВУЮЩИЙ ДЕТЕРМИНИРОВАННЫЙ ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ ПОТОКОВОГО ШИФРОВАНИЯ

А.А. ТОРБА, В.А. БОБУХ, А.А. БОБКОВА

В работе проанализированы некоторые недостатки известного аппаратного алгоритма потокового шифрования А5 и предложен аппаратный быстродействующий генератор псевдослучайных последовательностей, в значительной мере устраняющий недостатки известного алгоритма.

Ключевые слова: алгоритм А5, генератор псевдослучайных последовательностей.

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.

Согласно Райнеру Рюппелю можно выделить четыре основных подхода к проектированию поточных шифров:

- 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 расшифрования физически невозможной.

Теоретические критерии Райнера Рюппеля для проектирования поточных систем:

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

1. АЛГОРИТМ ПОТОКОВОГО ШИФРОВАНИЯ А5

Известный **потоковый алгоритм шифрования А5** используется для обеспечения конфиденциальности передаваемых данных между телефоном и базовой станцией в европейской системе мобильной цифровой связи GSM (Group Special Mobile).

Шифр основан на побитовом сложении по модулю два (булева операция XOR) генерируемой псевдослучайной последовательности и шифруемой информации [1].

В А5 псевдослучайная последовательность гаммы реализуется на основе трёх линейных рекуррентных регистров (ЛРР) сдвига с обратной связью. Регистры имеют длины: L(R1) = 19, L(R2) = 22 и L(R3) = 23 бита (рис. 1). Сдвигами управляет специальная схема. В каждом регистре есть биты синхронизации: R1(8), R2(10) и R3(10), над которыми вычисляется мажоритарная функция:

$$F = (x \,\&\, y) \vee (x \,\&\, z) \vee (y \,\&\, z),$$

где x, y, z – биты синхронизации.

В каждом такте сдвигается только тот регистр, у которого бит синхронизации равен функции F, т.е. на каждом шаге смещается два или три регистра, что приводит к их неравномерному движению. Результирующая псевдослучайная последовательность формируется путём операции XOR над выходными битами трех регистров (рис. 1).

Недостатком алгоритма А5 является недопустимо малая криптостойкость, которая определяется длиной сеансового ключа – 64 бита (определяемой суммарной длиной всех ЛРР), поэтому сложность атаки, основанной на прямом переборе, не превышает 2^{64}.

Учитывая, что в алгоритме А5 принудительно обнулены 10 бит ключа [1], – криптостойкость этого алгоритма даже ниже, чем у алгоритма DES (с длиной ключа – 56 бит).

Практика показывает, что свыше 40 % сеансовых ключей в алгоритме А5 приводят к минимальной длине периода генерируемой псевдослучайной последовательности, а именно: $T = 2^{23} - 1$.

Известна также атака Андерсона на открытом тексте, основанная на предположении о содержании первых двух ЛРР и попытке определения самого длинного третьего ЛРР по ключевой последовательности.

2. АЛГОРИТМ ПОТОКОВОГО ШИФРОВАНИЯ AUGUST-1

Детерминированный генератор псевдослучайных последовательностей для потокового

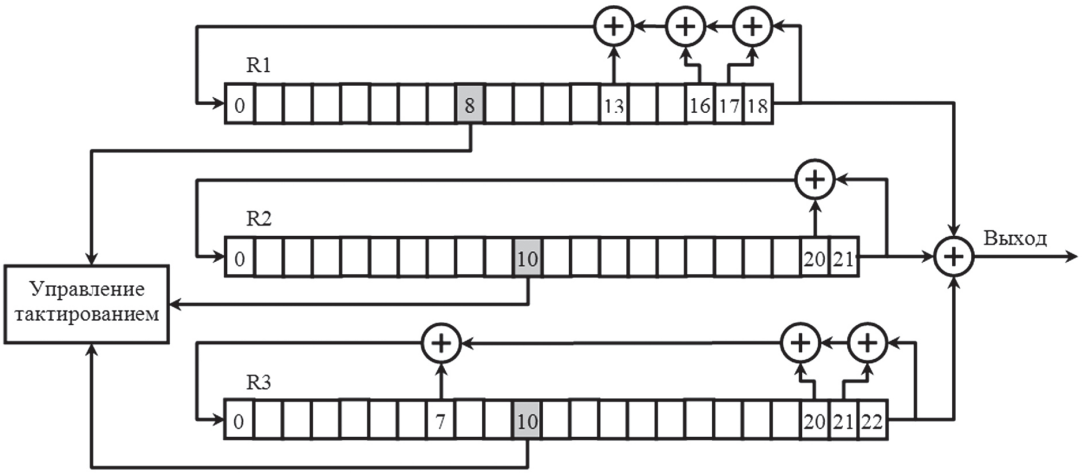

Рис. 1

шифрования AUGUST-1, описанный в патенте Украины [2], позволяет в значительной мере устранить указанные недостатки алгоритма A5. Упрощенная структурная схема этого генератора приведена на рис. 2.

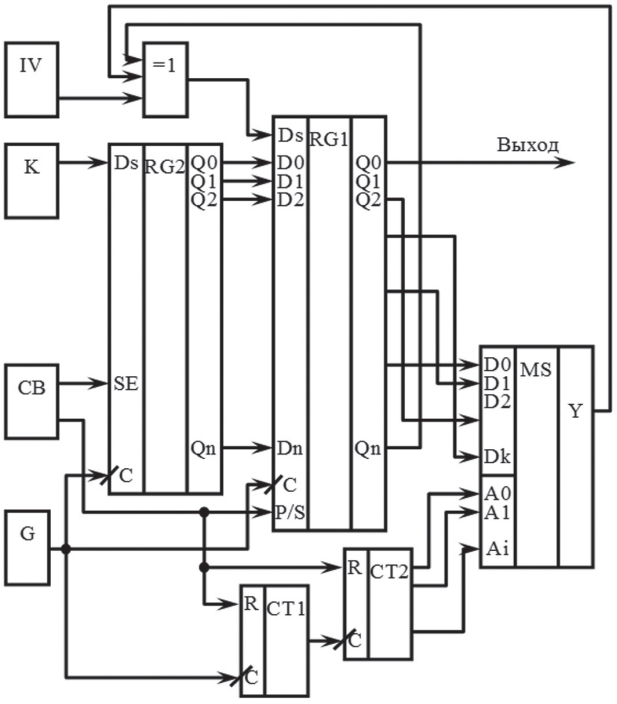

Рис. 2

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.

На информационные входы (D1...Dk) мультиплексора (MS) подаются сигналы с отводов 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.

На адресные входы мультиплексора MS (A0...Ai) подаются выходные сигналы двоичного счетчика CT2. Коэффициент деления счетчика CT1 определяет периодичность смены параметров рекурренты (обычно эта периодичность во много раз меньше разрядности сдвигающего регистра «*n*»). Желательно выбирать коэффициент деления счетчика CT1 и длину ЛРР (т.е. разрядность «*n*» сдвигающего регистра RG1) как взаимно простые числа.

Известные математические алгоритмы, которые позволяют вычислить параметры рекурренты псевдослучайных генераторов на основе ЛЛР (т.е. рассчитать основные параметры – «*m*» и «*n*») по результатам наблюдения выходной битовой последовательности, длительность которой в несколько раз превышает разрядность сдвигающего регистра, – в данном случае являются бесполезными, – потому что параметр «*m*» за время наблюдения многократно изменится.

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 Kc. Алгоритм Диффи-Хеллмана (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 Kc 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 Kc) может составлять от 100 до нескольких тысяч бит.

До начала шифрования сформированный секретный ключ Kc вводится в параллельный регистр RG2. Для этого блок управления (CB) вырабатывает сигнал разрешения последовательного ввода (SE), который поступает на вход управления параллельного 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 значение инициализации IV (Initialisation Value или синхропосылка). Это значение инициализации не является секретным и передается по открытому каналу связи перед каждым сеансом шифрования. Использование для всех сообщений отдельных случайных значений инициализации IV позволяет формировать различные значения псевдослучайной гаммы для каждого нового сообщения. При этом даже одинаковые начальные тексты сообщений будут зашифрованы по-разному.

Одновременно с передачей в канал связи значение 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 секретного ключа «*n*», таблицы коммутации мультиплексора MS и коэффициента деления первого счетчика СТ1.

Секретное значение длины «*n*» кратковременного сеансового ключа Кс делает бессмысленной лобовую атаку по перебору всех значений ключа.

ВЫВОДЫ

Предложенный и запатентованный быстродействующий детерминированный генератор псевдослучайных последовательностей для потокового шифрования AUGUST-1 позволяет устранить большинство недостатков известного алгоритма А5. Криптостойкость предложенной системы потокового шифрования определяется разрядностью кратковременного секретного ключа Кс, которая может составлять от 100 до нескольких тысяч бит. Причем секретным является не только значение ключа Кс, но и его длина.

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

Литература

[1] http://ru.wikipedia.org/wiki/A5.

[2] Патент Украины на полезную модель № 85039, опубл. Бюл. № 21, 2013 г.

Поступила в редколлегию 28.05.2014

Торба Александр Алексеевич, кандидат технических наук, доцент кафедры ЭВМ ХНУРЭ. Научные интересы: аппаратные средства криптографических систем.

Бобух Всеволод Анатольевич, кандидат технических наук, начальник отдела аппаратных средств АО «ИИТ». Научные интересы: аппаратные средства криптографических систем.

Бобкова Анна Александровна, кандидат технических наук, доцент кафедры ПИ ХНУРЭ. Научные интересы: аппаратно-программные средства криптографических систем.

УДК 681.324.067

Швидкодіючий детермінований генератор псевдовипадкових послідовностей для потокового шифрування / А.А. Торба, В.А. Бобух, А.А. Бобкова // Прикладна радіоелектроніка: наук.-техн. журнал. — 2014. — Том 13. — № 3. — С. 316–318.

У роботі проаналізовано деякі недоліки відомого апаратного алгоритму потокового шифрування А5 та запропоновано апаратний швидкодіючий генератор псевдовипадкових послідовностей, який значною мірою усуває недоліки відомого алгоритму.

Ключові слова: алгоритм А5, генератор псевдо-випадкових послідовностей.

Іл.: 2. Бібліогр.: 2 найм.

UDC 681.324.067

The high-speed determined generator of pseudo-random sequences for flow encryption / A.A. Torba, V.A. Bobukh, A.A. Bobkova // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 316–318.

Some imperfections of known hardware flow encryption algorithm A5 are analyzed and a hardware high-speed generator of pseudo-random sequences to a great extent eliminating imperfections of the known algorithm is offered in the paper.

Keywords: algorithm A5, generator of pseudo-random sequences.

Fig.: 2. Ref.: 2 items.