УДК 681.324.067

НЕДЕТЕРМИНИРОВАННЫЕ ГЕНЕРАТОРЫ СЛУЧАЙНЫХ БИТОВ

А.А. ТОРБА, В.А. БОБУХ, А.А. БОБКОВА

В работе проанализированы требования международного стандарта ISO/IEC 18031:2005 к недерминированным генераторам случайных битовых последовательностей и приведены схемы генераторов, удовлетворяющие требованиям этого международного стандарта.

Ключевые слова: недетерминированный генератор случайных битов, линейный рекуррентный регистр, источник энтропии.

ВВЕДЕНИЕ

Международный стандарт ISO/IEC 18031:2005 был подготовлен совместным техническим комитетом ISO/IEC JTCI, Информационные технологии, подкомитетом SC27 Методы защиты ИТ.

Этот стандарт устанавливает обязательные требования, которых необходимо придерживаться при разработке генераторов случайных битов для криптографических применений.

Стандарт ISO/IEC 18031:2005 определяет два типа генераторов: недерминированные и детерминированные генераторы случайных битов.

Недетерминированный генератор случайных битов – НГСБ (non-deterministic random bit generator – NRBG) – это механизм генерации случайных битов, который использует источник энтропии (источник неопределенности) для генерации случайного потока битов (случайных последовательностей).

Детерминированный генератор случайных битов – ДГСБ (deterministic random bit generator – DRBG) – это механизм генерации битов, который использует детерминированные алгоритмы, такие как криптографические алгоритмы, на источнике энтропии для генерации случайного потока битов (случайных последовательностей). В этом типе генерации битов используется особенные входные данные (начальные значения) и, возможно, некоторые необязательные входные данные, которые могут (или не могут) быть общедоступными.

Обязательным требованием при проектировании НГСБ является наличие источника (или источников) энтропии в виде физического генератора шума. С учетом конечной надежности (т.е. вероятности безотказной работы менее единицы) аналоговых физических генераторов шума (источников энтропии) в стандарте ISO/IEC 18031:2005 введено требование продолжения работы недетерминированного генератора случайных битов (НГСБ) способом, не менее защищенным, чем детерминированный генератор случайных битов (ДГСБ), в случае полного сбоя источника (или всех источников) энтропии.

В стандарт включены также требования обеспечения прямой и обратной секретности, т.е. невозможности просчитать по результатам длительных наблюдений выходной случайной битовой последовательности предыдущие или последующие биты с вероятностью, значительно превышающей 0,5.

РЕАЛИЗАЦИЯ НГСБ

В значительной степени требованиям стандарта ISO/IEC 18031:2005 удовлетворяет генератор равномерно распределенных случайных битовых последовательностей, описанный в декларационном патенте Украины [1]. Упрощенная схема этого генератора приведена на рис. 1.

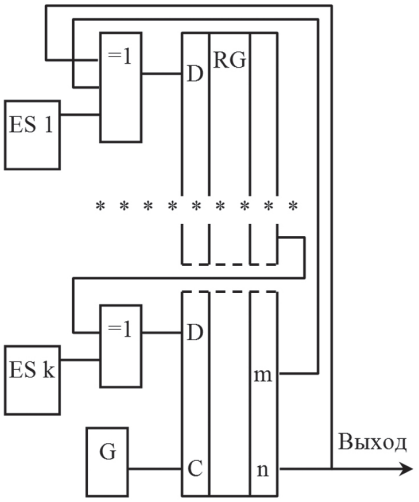

Рис. 1. Недетерминированный генератор случайных битов

Основу генератора составляет линейный рекуррентный регистр (ЛРР), реализованный на основе сдвигающего регистра (RG). На информационный вход (D) этого регистра подается сигнал с выхода первого элемента «ИСКЛЮЧАЮЩЕЕ ИЛИ» (элемента «XOR»), а на входы этого элемента подключены: последний выход сдвигающего регистра «n» и промежуточный выход этого регистра «m».

Скорость формирования случайных битов определяется частотой тактового генератора (G).

Для того, чтобы генерируемые биты были истинно случайными (непредсказуемыми, недетерминированными) к дополнительному входу первого элемента «XOR» подключен первый источник энтропии (entropy source – ES 1).

Стандарт ISO/IEC 18031:2005 не накладывает жесткие ограничения на параметры источника энтропии. Этот источник может быть смещенным (т.е. вероятности появления «логических нулей» и «логических единиц» на выходе не обязательно должны быть равными) и выходные биты могут даже зависеть один от другого. Единственное обя-

зательное требование – источник энтропии должен генерировать биты с ненулевой энтропией.

Первый элемент «ИСКЛЮЧАЮЩЕЕ ИЛИ» передает сигнал обратной связи на вход D регистра RG с инверсией (при единичном сигнале на выходе источника энтропии) или без инверсии (при нулевом выходном сигнале источника энтропии). Таким образом, в случайные моменты времени нарушается порядок следования нулевых и единичных битов, определяемый параметрами рекурренты ЛРР. Выходная случайная битовая последовательность, которую можно снимать с любого выхода сдвигающего регистра, – становится непредсказуемой.

Для повышения надежности в генератор случайных битовых последовательностей введено несколько источников энтропии (см. рис. 1). Для этого сдвигающий регистр разбит на k частей (необязательно равных) и на входы каждой части сдвигающего регистра подаются сигналы с выходов предыдущих частей этого регистра через элементы «ИСКЛЮЧАЮЩЕЕ ИЛИ». Другие входы этих элементов «XOR» подключены к выходам дополнительных источников энтропии (ES 2...ES k).

Такое решение позволяет реализовать «горячее резервирование» источников энтропии, т.е. их параллельную работу. Выходные биты НГСБ остаются случайными (непредсказуемыми) при исправной работе хотя бы одного источника энтропии (на выходах остальных неисправных источников может быть «логический нуль» или «логическая единица»). Вероятность сбоя всех источников энтропии в этой схеме ничтожно мала и равняется произведению вероятностей сбоя каждого отдельного источника энтропии.

В случае полного сбоя всех источников энтропии такой генератор продолжает работать как линейный рекуррентный регистр, т.е. недетерминированный генератор псевдослучайных последовательностей.

Известные математические алгоритмы 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. Поэтому криптостойкость такого генератора (т.е. устойчивость против хакерских атак) при полном сбое всех источников энтропии является недостаточной.

УЛУЧШЕНИЕ ПАРАМЕТРОВ НГСБ

Для того, чтобы повысить криптостойкость НГСБ и сделать невозможным вычисление параметров рекурренты – необходимо периодически изменять эти параметры. Такое техническое решение предложено в патенте [2]. На рис. 2 приведена структурная схема этого устройства.

На информационные входы (D1...Di) мультиплексора (MX) подаются сигналы с отводов (p, q ... m) сдвигающего регистра (RG). Номера всех отводов должны удовлетворять известному условию для ЛЛР: полиномы, вычисленные на коэффициентах –

$$1 + x^p + x^n;$$
$$1 + x^q + x^n \ ...$$
$$1 + x^m + x^n$$

– должны быть примитивными и неприводимыми над полем Галуа.

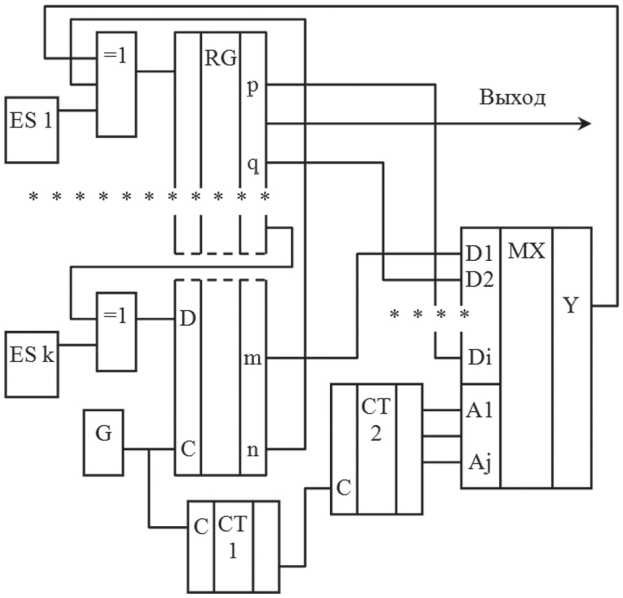

Рис. 2. Недетерминированный генератор случайных битов с изменением параметров рекурренты

Например, для сдвигающего регистра (RG) с количеством разрядов $n = 71$ этому условию удовлетворяют номера отводов (p, q ... m): 6, 9, 18, 20, 35, 36, 51, 53, 62, 65.

Для такого ЛРР с количеством разрядов $n = 71$ период повторения битовой последовательности равен:

$$T = 2^{71} - 1 = 2\ 361\ 183\ 241\ 434\ 822\ 606\ 847 \text{ (бит)}.$$

При частоте формирования псевдослучайных битов 10–20 Мит/с период повторения будет более миллиона лет, т.е. периодичность такого ЛРР – практически бесконечная.

На адресные входы мультиплексора (A1...Aj) подаются выходные сигналы двоичного счетчика СТ2. Коэффициент деления счетчика СТ1 определяет периодичность смены параметров рекурренты (обычно эта периодичность в несколько раз меньше разрядности сдвигающего регистра).

Количество адресных входов мультиплексора (A1...Aj) равняется двоичному логарифму от количества информационных входов (D1...Di).

При полном сбое всех источников энтропии за время наблюдения выходной случайной битовой последовательности (в несколько раз превышающей разрядность сдвигающего регистра), мультиплексор многократно поменяет номера отводов линейного рекуррентного регистра. Поэтому криптоаналитик не сможет вычислить параметры

рекурренты даже при сбое всех источников энтропии. Это обеспечивает одно из главных требований стандарта ISO/IEC 18031:2005 – прямую и обратную секретность генерируемых случайных битов.

В патенте Украины [3] предложена схема генерации случайных битовых последовательностей на основе ЛРР со случайными изменениями параметров рекурренты (рис. 3).

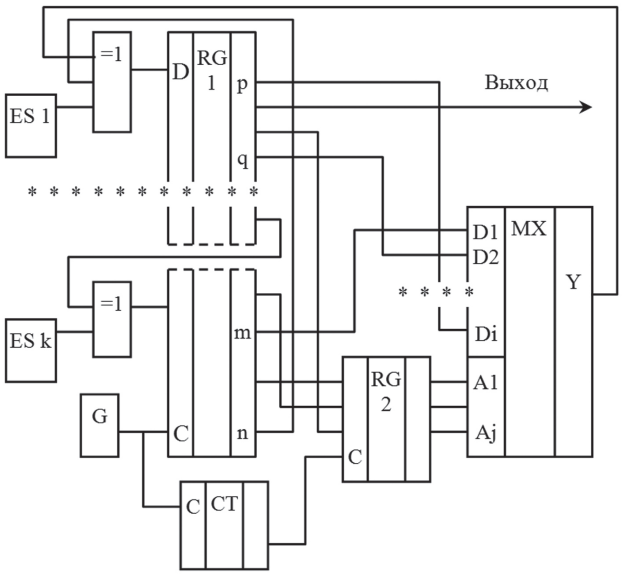

Рис. 3. Недетерминированный генератор случайных битов со случайным изменением параметров рекурренты

На адресные входы (A1...Aj) мультиплексора MX подаются случайные битовые комбинации, которые снимаются с произвольных отводов сдвигающего регистра RG1 и запоминаются в дополнительном параллельном регистре RG2. Периодичность смены случайных кодовых комбинаций в параллельном регистре определяется коэффициентом деления счетчика CT.

Случайный характер изменения параметров рекурренты исключает возможность расчета параметров ЛРР на основе криптоанализа выходной случайной битовой последовательности сколь угодно большой длительности.

ВЫВОДЫ

В соответствии с международным стандартом ISO/IEC 18031:2005 недетерминированный генератор случайных битов (НГСБ) обязательно включает один или несколько источников энтропии и детерминированный механизм псевдослучайного преобразования сигналов с выходов источников энтропии в выходные случайные биты. Это необходимо для выполнения требования стандарта ISO/IEC 18031:2005 – продолжения работы недетерминированного генератора случайных битов (НГСБ) способом, не менее защищенным, чем детерминированный генератор случайных битов (ДГСБ), в случае полного сбоя источника (или всех источников) энтропии.

Для уменьшения вероятности одновременного сбоя всех источников энтропии необходимо применять горячее резервирования нескольких источников энтропии.

Приведенные технические решения недетерминированных генераторов случайных битовых последовательностей, удовлетворяют требованиям стандарта ISO/IEC 18031:2005 и защищены патентами Украины.

Литература:

[1] Декларационный патент Украины № 50386 А, опубл. Бюл. № 10, 2002 г.;

[2] Патент Украины на полезную модель № 52380, опубл. Бюл. № 16, 2010 г.;

[3] Патент Украины на полезную модель № 52410, опубл. Бюл. № 16, 2010 г.

Поступила в редколлегию 30.05.2011

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

Бобух Всеволод Анатольевич, кандидат технических наук, начальник отдела аппаратных средств защиты информации ЗАО «ИИТ», старший научный сотрудник кафедры БИТ ХНУРЭ. Область научных интересов: апаратные средства систем защиты информации.

Бобкова Анна Александровна, ассистент кафедры ПО ЭВМ ХНУРЭ. Область научных интересов: аппаратно-программные средства криптографических систем.

УДК 681.324.067

Недетерміновані генератори випадкових бітів / А.А. Торба, В.А. Бобух, А.А. Бобкова // Прикладна радіоелектроніка: наук.-техн. журнал. – 2011. Том 10. № 2. – С. 271–273.

В роботі проаналізовані вимоги міжнародного стандарту ISO/IEC 18031:2005 до недетермінованим генераторам випадкових бітових послідовностей і приведені схеми генераторів, які задовольняють вимоги цього міжнародного стандарту.

Ключові слова: недетермінований генератор випадкових бітів, лінійний рекурентний регістр, джерело ентропії.

Іл. 3. Бібліогр.: 3 найм.

UDC 681.324.067

Nondeterministic random bit generators / A.A. Torba, V.A. Bobukh, A.A. Bobkova // Applied Radio Electronics: Sci. Journ. – 2011. Vol. 10. № 2. – P. 271–273.

The paper analyzes requirements of the international standard ISO/IEC 18031:2005 to nondeterministic random bit sequences generators and provides circuits of generators meeting the requirements of this international standard.

Keywords: nondeterministic random bit generator, linear recurrent register, entropy source.

Fig. 3. Ref.: 3 items.