М. А. Иванов, В. Е. Рябков, И. В. Чугунков, И. М. Ядыкин

СПОСОБ ФОРМИРОВАНИЯ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ГАРАНТИРОВАННЫМ ПЕРИОДОМ НА ОСНОВЕ *R*-БЛОКОВ

Введение

Информационная безопасность давно стала самостоятельным направлением исследований и разработок. Однако, несмотря на это, проблем не становится меньше, что объясняется появлением все новых компьютерных технологий, которые не только создают новые проблемы информационной безопасности, но и представляют, казалось бы, уже решенные вопросы совершенно в новом ракурсе. Кроме того, появление новых компьютерных технологий, новых математических методов дает в руки нарушителей и создателей разрушающих программных воздействий все новые и новые возможности.

Можно долго перечислять причины трудоемкости решения задачи обеспечения безопасности информации (ОБИ) в современных условиях, но следует выделить главную из них:

- все большее отстранение пользователей от процессов управления и обработки информации и передача его полномочий ПО, обладающему некоторой свободой в своих действиях и поэтому очень часто работающему вовсе не так, как предполагает пользователь.

Цель создания систем ОБИ — предотвращение или оперативное устранение последствий умышленных или случайных деструктивных воздействий.

Эффективная система ОБИ должна обеспечивать:

- секретность всей информации или наиболее важной ее части;
- аутентичность субъектов и объектов информационного взаимодействия;
- правильность функционирования компонентов системы в любой момент времени, в том числе отсутствие недокументированных возможностей;
- своевременный доступ пользователей к необходимой им информации или компонентам системы;
- защиту авторских прав собственников информации, возможность разрешения конфликтов;
- разграничение ответственности за нарушение правил информационных взаимоотношений;
- непрерывный анализ защищенности процессов управления, обработки и передачи информации.

Стохастические методы защиты информации

Стохастическими методами защиты принято называть методы защиты информации, прямо или косвенно основанные на использовании генераторов псевдослучайных чисел (ПСЧ) и производных от них хеш-генераторов. При этом эффективность защиты в значительной степени определяется качеством используемых алгоритмов генерации ПСЧ. Средства генерации

ПСЧ успешно решают большинство упомянутых выше задач, стоящих перед разработчиками систем ОБИ. Средства генерации ПСЧ используются при реализации большинства методов защиты; более того, один из самых перспективных методов защиты, а именно метод внесения неопределенности в работу программных систем (реализация которого в принципе невозможна без использования генераторов ПСЧ), является универсальным. Он может использоваться совместно с любым другим методом защиты, автоматически повышая его качество. Итак, роль средств генерации ПСЧ является решающей. Именно от качества формируемых последовательностей зависит эффективность механизмов защиты программных систем.

Среди многочисленных работ по теории и применению генераторов ПСЧ следует выделить работы В. Н. Ярмолика [1, 2] и С. А. Осмоловского [3, 4], связанные с исчерпывающим исследованием вопросов применения генераторов ПСЧ соответственно в задачах тестового диагностирования и помехоустойчивого кодирования.

Стохастические методы универсальны, широко распространены и бурно развивающиеся в последние годы криптографические и стеганографические методы являются лишь их частными случаями. В работах отечественных и зарубежных авторов, посвященных решению задач защиты компьютерных систем от умышленных деструктивных воздействий, генератор ПСЧ рассматривается только как один из ряда не менее важных криптографических примитивов. На самом деле роль качественных генераторов ПСЧ — ведущая, при их наличии можно эффективно строить все другие криптографические примитивы.

Постановка задачи

Таким образом, возникает актуальная научная задача, суть которой заключается в развитии теории стохастических методов защиты информации, в том числе в разработке новых, более эффективных, учитывающих тенденции развития компьютерных технологий стохастических методов и программных средств защиты компьютерных систем от случайных и умышленных деструктивных воздействий.

Качественный генератор ПСЧ должен удовлетворять следующим требованиям [5, 6]:

1) он должен быть непредсказуемым (непредикативным влево); иначе говоря, для противника, перехватившего фрагмент выходной псевдослучайной последовательности (ПСП) конечной длины, задача определения предшествующего элемента последовательности должна быть вычислительно неразрешима;

2) формируемая им ПСП должна быть статистически безопасна; иначе говоря, ни один статистический тест не должен выявлять в ней никаких закономерностей;

3) формируемая им ПСП должна иметь большой период;

4) он должен допускать эффективную программную и/или аппаратную реализации.

В работе [6] проведена классификация генераторов ПСЧ по следующим параметрам:

- тип используемой нелинейной функции;
- структура генератора;
- использование внешних источников случайности;
- принцип управления синхронизацией;
- принцип получения выходной последовательности;
- принцип использования блоков замены и блоков стохастического преобразования (S- и R-блоков);
- наличие каскадов.

Можно выделить следующие наиболее перспективные семейства алгоритмов генерации ПСЧ.

1) Эллиптические алгоритмы генерации ПСЧ. Согласно классификации, предложенной в [6], они относятся к наиболее математически обоснованным генераторам ПСЧ, а именно к генераторам, нелинейное преобразование которых строится с использованием односторонних функций. Непредсказуемость генераторов этого типа базируется на сложности решения задачи дискретного логарифмирования над группой точек эллиптической кривой.

Существенным недостатком генераторов этого типа, значительно ограничивающим область их использования, является чрезвычайно низкое быстродействие, которое в сотни раз ниже быстродействия генераторов ПСЧ блочного типа, специфицированных в государственных стандартах России и США (соответственно ГОСТ 28147-89 и AES). При этом следует учитывать, что криптографические блочные генераторы сами считаются медленными, так как строятся по итерационному принципу, предполагающему при реализации нелинейных функций обратной связи (или выхода) многократное использование одних и тех же преобразований замены и перестановки.

2) Генераторы ПСЧ на регистрах сдвига с нелинейными обратными связями на основе так называемых стохастических сумматоров или R-блоков [6, 7]. На рис. 1 показаны принцип функционирования, условное графическое обозначение R-блока и схема генератора ПСЧ, названного RFSR (Random Feedback Register), где Q_i — регистр разрядности n, $i = \overline{0, (N-1)}$.

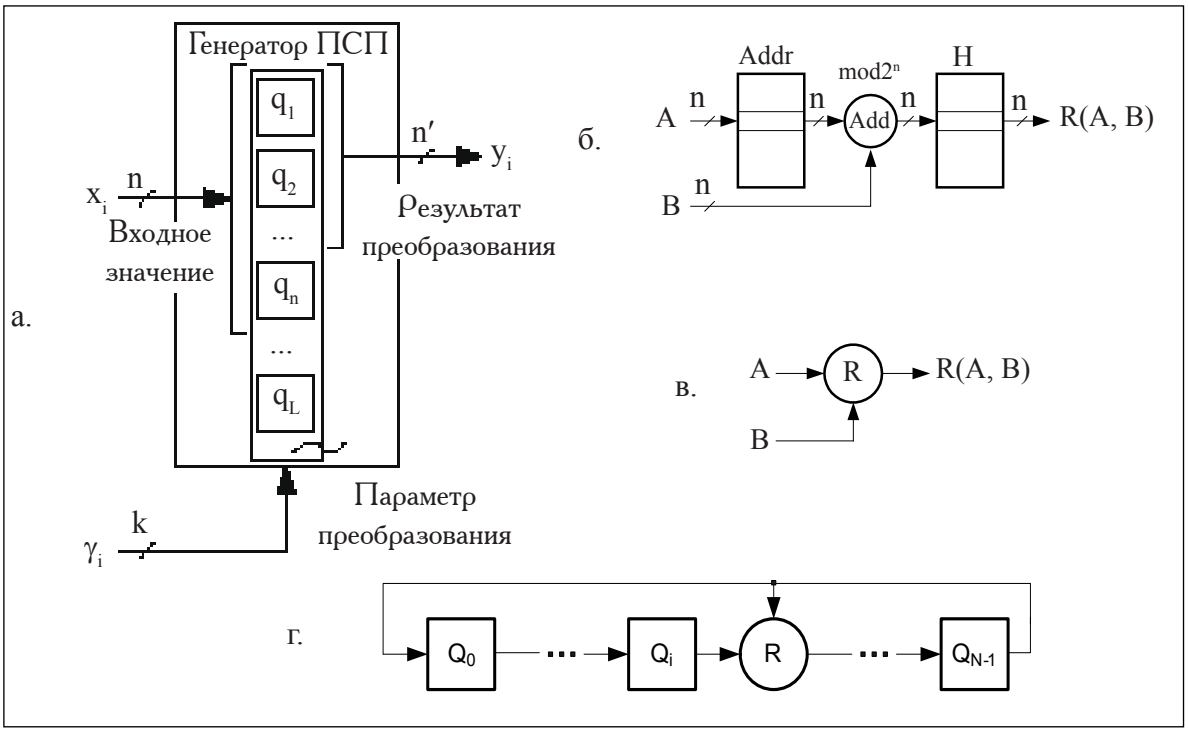

Рис. 1. Стохастическое преобразование: а — принцип стохастического преобразования, б — логика работы R-блока, в — условное графическое обозначение R-блока, г — схема RFSR

Технические характеристики генераторов ПСЧ на основе стохастических сумматоров (R-блоков):

- эффективная программная реализация: от 6 до 20 инструкций Ассемблера на реализацию любой базовой операции; $N + 2^{n+1}$ ячеек памяти, где N — число регистров генератора ПСЧ, n — разрядность R-блока;
- возможность получения любого значения предпериода и периода ПСЧ, в том числе максимально возможного при заданном числе элементов памяти;
- возможность получения нелинейных М-последовательностей;
- число различных таблиц стохастического преобразования при заданной разрядности R-блока равно $2^{n-1}!$;
- длина ключа — от 1 до 2^n n-разрядных слов.

На рис. 2 показан пример нелинейного генератора последовательности максимальной длины.

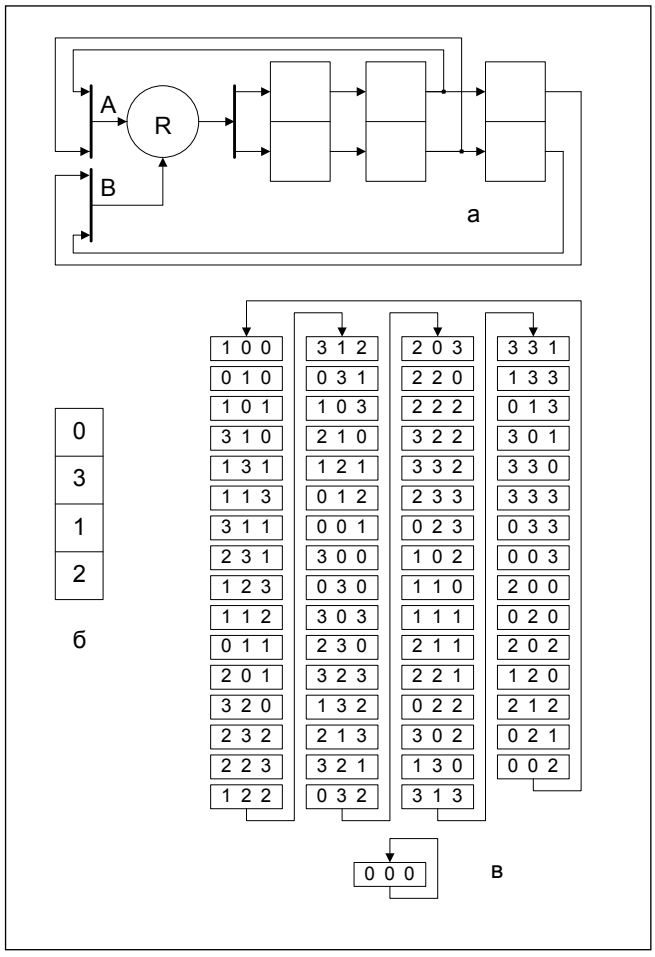

Рис. 2. RFSR: а — схема генератора нелинейной M-последовательности; б — таблица стохастического преобразования; в — диаграмма переключений генератора

В работе ставится задача получения на основе RFSR ПСП с гарантированной длиной периода не менее 2^N, где N — число регистров генератора.

Генератор ПСЧ с гарантированной длиной периода

При некоторых таблицах стохастического преобразования генератор ПСЧ вырождается, иначе говоря, формируемая последовательность имеет период значительно меньше максимально возможного. Это является недопустимым в тех случаях, когда заполнение таблицы H — ключевая информация. Кроме того, часто требуется обеспечить период ПСП не меньше некоей заранее заданной величины. Предлагается двухступенчатая структура генератора ПСЧ на основе R-блоков, при этом первая ступень — NLFSR (регистр сдвига с нелинейной обратной связью) с произвольным значением периода [6], а вторая ступень собственно RFSR. Если значения периодов M и N последовательностей, формируемых соответственно NLFSR и RFSR, являются взаимно простыми, результирующий период оказывается равным NM. На рис. 3 показан принцип построения $(n + 1)$-разрядного генератора ПСЧ с гарантированной длиной периода не менее 2^N, где N — число регистров генератора. На рис. 3 рассмотрен случай, когда период последовательности, формируемой NLFSR, равен 2^N. Введены следующие обозначения:

q_i — разряды NLFSR, где $i = 0, ..., (N - 1)$,

Q_i — регистры RFSR, где $i = 0, ..., (N - 1)$,

RSM — стохастический сумматор разрядности n,

SM — одноразрядный сумматор,
cri — вход переноса,
БПС — блок пространственного сжатия $(n + 1) \rightarrow n$.

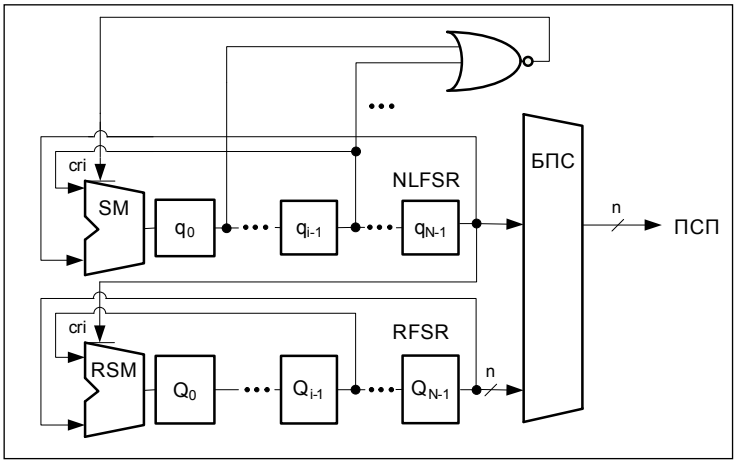

Рис. 3. Принцип построения генератора ПСЧ с гарантированной длиной периода

Другой способ формирования n-разрядных ПСЧ заключается в использовании $(n + 1)$-разрядного R-блока, ключевая таблица H которого содержит младший столбец с чередующимися 0 и 1. В результате эквивалентная схема генератора будет содержать N-разрядный генератор М-последовательности. Таким образом, n-разрядная ПСП, снимаемая с выхода БПС $n + 1 \rightarrow n$, будет иметь период не менее $2^N - 1$. Таблица H формируется на основе двух n-разрядных ключевых таблиц H_1 и H_2. Для формирования H_1 и H_2 может быть использован алгоритм формирования таблицы замен поточного шифра RC4 [7].

Заключение

Выделена роль качественных генераторов ПСЧ при построении систем ОБИ компьютерных систем. Рассмотрены основные направления совершенствования алгоритмов генерации ПСЧ.

Приведены технические характеристики нового класса быстродействующих генераторов ПСЧ. Предложен способ получения ПСП с гарантированной длиной периода, основанного на использовании в цепи обратной связи генератора ПСЧ стохастических сумматоров или R-блоков.

СПИСОК ЛИТЕРАТУРЫ:

1. *Ярмолик В. Н., Демиденко С. Н.* Генерирование и применение псевдослучайных сигналов в системах испытаний и контроля / Под ред. П. М. Чеголина. Минск: Наука и техника, 1986. — 200 с.
2. *Ярмолик В. Н.* Контроль и диагностика цифровых узлов ЭВМ. Минск: Наука и техника, 1988. — 240 с.
3. *Осмоловский С. А.* Стохастические методы передачи данных. М.: Радио и связь, 1991. — 240 с.
4. *Осмоловский С. А.* Стохастические методы защиты информации. М.: Радио и связь, 2003. — 320 с.
5. *Иванов М. А., Чугунков И. В.* Теория, применение и оценка качества генераторов псевдослучайных последовательностей (Серия СКБ (специалисту по компьютерной безопасности). Книга 2). М.: КУДИЦ-ОБРАЗ, 2003. — 240 с.
6. *Иванов М. А., Мацук Н. А., Чугунков И. В. и др.* Стохастические методы защиты информации в компьютерных системах и сетях. М.: КУДИЦ-ПРЕСС, 2009. — 512 с.
7. *Асосков А. А., Иванов М. А., Тютвин А. Н. и др.* Поточные шифры (Серия СКБ (специалисту по компьютерной безопасности). Книга 3). М.: КУДИЦ-ОБРАЗ, 2003. — 336 с.