V Заключение

В работе сформулирована и решена задача расчета и обоснования срока действия ключей поточного шифра или блочного шифра, используемого в режиме гаммирования.

Данная задача является сложной и противоречивой и включает в себя построение оценок различных параметров, характеризующих так называемое явление перекрытия отрезков последовательности, соответствующих заданным различным значениям вектора инициализации. Одной из наиболее важных для последующих исследований в этом направлении является задача оценки (в зависимости от шифрующего преобразования) допустимой суммарной длины отрезков сгенерированной последовательности, при которой эффектом их перекрытия можно пренебречь. Данная задача частично рассмотрена в [5]. Также было определено, что алгоритмы такого класса безопасны при использовании стандартных длин ключа более 128 бит.

Следует отметить, что изложенные результаты вероятностного анализа перекрытий отрезков последовательностей могут быть непосредственно применены при расчете сроков действия ключей поточных и блочных шифров, используемых в режиме счетчика.

Литература: ***1.*** *Харин Ю. С., Берник В. И., Матвеев Г. В. Математические основы криптологии. – Минск: Изд-во БГУ, 1999. – 319 с.* ***2.*** *Колчин В. Ф., Севастьянов Б. А., Чистяков В. П. Случайные размещения. – М.: Наука, 1976. – 223 с.* ***3.*** *Михайлов В. Г. О повторяемости состояний датчика псевдослучайных чисел при его многократном использовании // Теория вероятности и ее применение – 1995. – Т. 40. – Вып. 4. – С. 786 – 797.* ***4.*** *Левин Б. Р. Теоретические основы статистической радиотехники. Книга первая. Изд. 2-е, перераб. и доп., М., «Сов. Радио», 1974, 552 с.* ***5.*** *Коваленко И. Н., Левитская А. А., Савчук М. Н. Избранные задачи вероятностной комбинаторики. – К.: Наукова думка, 1986. – 224 с.* ***6.*** *Малая советская энциклопедия, под ред. Б. А. Введенского, т. 7, изд, 3-е, 1959 г.*

УДК 681.3.06:519.248.681

МЕТОД ФОРМИРОВАНИЯ ЦИКЛОВЫХ ПОДКЛЮЧЕЙ НА БАЗЕ ЛИНЕЙНЫХ РЕГИСТРОВ СДВИГА В РАСШИРЕННЫХ ПОЛЯХ GF (2^N)

Александр Лепеха
Харьковский национальный университет радиоэлектроники

Анотація: **Сформульовані вимоги до сучасних схем розгортання ключів. Розглядається метод побудови схеми розгортання на базі лінійних регістрів зсуву в розширених полях GF(2^n). Приводиться порівняльний аналіз із аналогічними конструкціями.**
Summary: **In this article are presented requirements to modern key schedules. The method of construction of the circuit of deployment is considered on the basis of linear registers of shift in the expanded fields GF(2^n). The comparative analysis with similar designs is carried out.**
Ключові слова: **Схема розгортання ключів, генератор псевдовипадкових послідовностей, лінійні регістри зсуву.**

Введение

При оценке криптографической стойкости блочного симметричного шифра (БСШ) большое внимание уделяется способности шифра противостоять наиболее мощным на сегодняшний день методам линейного и дифференциального криптоанализа. В связи с этим большинство работ посвящены совершенствованию указанных методов криптоанализа либо улучшению криптографических свойств цикловой функции шифра. Однако в последнее десятилетие получили развитие методы криптоанализа, которые используют особенности формирования цикловых подключей схемами разворачивания ключей. Проведенный автором обзор современных БСШ, представленных в проекте NESSIE [1], показал, что многие криптографические алгоритмы, обладающие цикловой функцией, способной противостоять атакам на основе линейного и дифференциального криптоанализов, оказываются уязвимыми к атакам на схемы разворачивания ключей. Примером могут служить 3-DES, IDEA, SAFER (SAFER+), Hierocrypt, Noekeon. Для других алгоритмов использование атак на схему разворачивания ключей оказалось более эффективно по сравнению с классическими методами криптоанализа. Например, для БСШ Rijndael одним из недостатков, указанных при проведении конкурса NESSIE, является низкая граница безопасности (запас 2 цикла для версии алгоритма с

длиной ключа $l_k = 128$). В ряде работ [2] отмечается, что к таким атакам предрасположены схемы разворачивания ключей, которые формируют цикловые подключи при помощи некоторого простого линейного преобразования над битами исходного ключа (например, перестановка битов секретного ключа). Для усложнения возможности проведения таких атак авторы рекомендуют избегать использования линейных законов формирования цикловых подключей. В некоторых работах [3] предлагается использовать в качестве процедуры формирования подключей генераторы псевдослучайных последовательностей (ГПСП). Таким образом, совершенствование методов формирования цикловых ключей для БСШ является актуальной задачей, особенно с учетом развития криптоанализа и вычислительных систем.

Кроме криптографической стойкости, обеспечиваемой шифром в целом, в настоящее время немаловажным является увеличение производительности и минимизация затрат на реализацию, что отображено в требованиях к конкурсантам при проведении проекта NESSIE. Так БСШ нередко используются в качестве строительных блоков при разработке хеш-функций или схем поточного шифрования. Поэтому уменьшение времени выработки цикловых ключей является важным моментом в тактико-технических характеристиках схемы разворачивания ключей.

Сформулируем критерии, которыми необходимо руководствоваться при проектирования схемы разворачивания ключей:

1. криптографическая стойкость против известных аналитических атак;
2. сложность восстановления цикловых подключей либо исходного ключа при условии, что криптоаналитику известны биты других цикловых подключей;
3. минимизация времени разворачивания ключа при соблюдении условий 1 и 2;
4. простота реализации конструкции; возможность эффективной программной, программно-аппаратной и аппаратной реализации с приблизительно одинаковой сложностью.

В настоящей статье рассматривается универсальный метод формирования цикловых ключей на базе линейных регистров сдвига (ЛРС), удовлетворяющий требованиям высокой криптографической стойкости. На основе предложенного метода разработана схема разворачивания ключей, которая прошла испытания в составе БСШ «Торнадо» [4], разработанного в АО «ИИТ». Проведен анализ основных тактико-технических характеристик предложенной конструкции со схемами разворачивания ключей, использующих аналогичный принцип формирования цикловых подключей.

I Построение схем разворачивания ключа на основе генератора ПСП

Одним из способов построения схем разворачивания ключей является использование в качестве процедуры разворачивания ключа однонаправленного генератора псевдослучайных последовательностей. Далее под генератором будем понимать следующее.

Определение 1.

Под криптографическим генератором понимается автономный шифрующий автомат (конечный) общего вида $A_\Gamma = (S, Y, K, z, g, h, f)$, который вырабатывает последовательность, обладающую определенными статистическими свойствами, где S – множество состояний шифрующего автомата, Y – множество выходов автомата, K – множество ключей автомата; z, g, h, f – соответственно функции инициализации ключа, обновления ключа, переходов между состояниями и функцией выходов ($z : K \to S$; $g : S\ x\ K \to K$; $h : S\ x\ K \to S$; $f : S\ x\ K \to Y$).

Под однонаправленностью подразумевается высокая вычислительная сложность восстановления состояния S генератора (и соответственно, неизвестных элементов последовательности) по некоторому множеству известных элементов выходной последовательности *Y*.

К достоинствам таких конструкций необходимо отнести высокую криптографическую безопасность, универсальность конструкции и простоту реализации. Чтобы минимизировать затраты на реализацию целесообразно строить такие конструкции на базе цикловой функции, используемой в БСШ. Положительной стороной такого подхода является то, что разработчик может сконцентрировать свое внимание на разработке цикловой функции с требуемыми показателями криптографической стойкости. Поэтому целесообразным является использование в качестве конструкции генератора ПСП либо БСШ в одном из стандартных режимов поточного шифрования, либо ГПСП на базе линейного рекуррентного регистра.

Качество криптографического генератора определяется свойствами его выходных последовательностей. Сформулируем эти свойства.

1. В связи с тем, что шифрующий автомат конечный, очевидно, что формируемая им последовательность имеет период. При любом исходном ключе $k \in K$ вырабатываемая гамма $y_1, y_2, y_3 \ldots y_n \in Y$ должна

иметь период, достаточный для формирования из этой последовательности всех необходимых цикловых ключей.

2. Формируемая гамма должна обладать рядом статистических свойств. В частности, равновероятностью появления различных знаков, образующих последовательность, а также *r*-грамм, то есть наборов из *r* соседних знаков, $r = 1, 2, ...r_0$ (r_0–некоторая константа, определяемая возможностями вскрытия системы с использованием неравновероятности мультиграмм гаммы).

3. Зависимость между битами формированной ПСП должна обладать экспоненциальной сложностью восстановления гаммы (фактически битов цикловых подключей) по ее некоторому отрезку (битам известного циклового подключа). Такая ситуация возможна в случае, если криптоаналитик смог осуществить некоторую успешную атаку на шифр и определить часть битов каких-либо цикловых ключей. Зная механизм формирования битов цикловых ключей он может попытаться восстановить остальные биты. Этот критерий связан с понятием линейной сложности.

4. Система уравнений, связывающая неизвестные элементы ключа $k \in K$ с известными знаками гаммы, должна иметь высокую сложность решения, исключающую возможность практической реализации алгоритма решения.

Такие требования в большинстве случаев реализации БСШ являются избыточными, однако их выполнение служит универсальным способом защиты от атак на схему разворачивания ключа и, кроме того, позволяет построить безопасную (устойчивую к коллизиям) хеш-функцию, например, в соответствии со схемой Девиса-Мейера или другими подобными схемами.

Так как предполагается, что символы выходной последовательности Y формируются как результат функции от ключа и предыдущего состояния $f : S\ x\ K \to Y$ (в соответствии с определением генератора ПСП), то может существовать некоторый ключ, имеющий регулярную структуру или состоящий только из полностью нулевых и единичных байтов, который приведет к формированию последовательности, не удовлетворяющей хотя бы одному из указанных выше свойств. Введем понятие «вырожденного» ключа.

Определение 2.

Ключ $k \in K$, при котором сформированная последовательность Y не будет удовлетворять хотя бы одному из указанных выше условий 1 – 4, будем называть вырожденным ключом.

Выделим два класса возможных конструкций выработки ПСП.

1. На базе блочного шифра в одном из возможных режимов поточного шифрования. Учитывая менее жёсткие требования к этой процедуре, чем к поточным схемам шифрования, можно рекомендовать использовать производительные схемы «счётчика» либо OFB режима с полноразрядным выходом. Для сокращения затрат на реализацию БСШ эту схему целесообразно строить на основе (возможно упрощённой) цикловой функции базового шифра.

2. На основе линейных регистров сдвига. Выходная последовательность таких генераторов имеет большой период, который можно доказуемо рассчитать, и обладает хорошими статистическими свойствами. Затраты на реализацию таких схем незначительны. Генераторы, построенные на основе ЛРС имеют высокие показатели скорости выработки гаммы [5].

В соответствии с первым подходом в качестве процедуры разворачивания ключа можно использовать «усиленную» схему поточного шифрования [6] на базе схемы счетчика с «плавающим» периодом и функции блочного шифрования с длиной блока m. Достоинствами указанной схемы является наличие нелинейной ключезависимой обратной связи (подобно OFB-режиму) и гарантированный период (режим счетчика). На базе такой конструкции была предложена процедура разворачивания ключей [4, 7], построенная по схеме циклического шифрования состояний генератора в режиме «связки шифроблоков» (CBC-режим). Указанная конструкция нашла свое практическое применение в экспериментальном БСШ «Торнадо», разработанном в АО «ИИТ» [4]. Автором статьи были проведены исследования рассматриваемой процедуры разворачивания ключей [8] в соответствии с требованиями 1 – 4, предъявляемыми к выходной последовательности генератора. Для исследований применялись статистические тесты из пакета NIST STS [9]. Полученные результаты сопоставимы с результатами для эталонной выборки, рекомендованной NIST STS. Кроме того, количество тестов, в которых тестирование прошло 99% последовательностей для предлагаемой процедуры разворачивания ключа, выше, чем для BBS генератора. Также использовались корреляционные методы анализа для выявления связей между битами сформированной ПСП: расчет степени лавинного эффекта, строго лавинного критерия и полноты. При проведении эксперимента зависимостей между битами и битами цикловых подключей исходного ключа обнаружено не было. Таким образом, конструкция удовлетворяет требованиям высокой криптографической безопасности.

Отметим достоинства и недостатки предложенной конструкции.

К достоинствам следует отнести высокую криптографическую безопасность, универсальность конструкции (возможность быстрого внедрения ее в любой блочный шифр), простоту программной реализации на 32-х и 64-х битных процессорах. Недостатком схемы является использование операций сложения по модулю 2^{32} (2^{64}), которые трудно реализуемы на платформах с разрядностью процессора, отличной от 32 (64) бит. Скоростные показатели связаны, прежде всего, со скоростью криптографических преобразований цикловой функции и, следовательно, будут варьироваться от алгоритма к алгоритму.

В качестве второго подхода формирования цикловых подключей предлагается использовать генераторы ПСП на базе ЛРС в расширенных полях. Рассмотрим особенности построения таких генераторов.

II Процедуры разворачивания цикловых ключей на базе ЛРС в полях GF (2^n)

Далее под ЛРС будем понимать внутренне автономный автомат Мура.

Определение 3.

Автомат A называется автоматом Мура или внешнеавтономным, если функция выходов $f(s,x)$ не зависит от x, то есть функция f задает следующее отображение $f: S \to Y$, где S – внутренние состояния автомата, Y – выходная последовательность.

Следовательно, мы имеем генератор вида $A = (S, Y, h, f)$, причем функции такого генератора зависят только от начального состояния.

Отметим особенности использования регистров в расширенных полях Галуа GF (2^N). К достоинствам следует отнести:

1. большой гарантированный период формируемой последовательности: $T = N \cdot n$, где N – расширение поля, n – степень характеристического полинома $F(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_1 x + a_0$, образующего линейную обратную связь; необходимо отметить, что так как ЛРС является линейным устройством, то нулевое состояние является запрещенным состоянием; по определению 2 исходный ключ, состоящий полностью из нулевых битов, будем считать вырожденным и рассматривать как «слабый» ключ;
2. доказуемые статистические свойства формируемых ПСП, близкие к идеальным [10];
3. простота реализации на процессорах любой разрядности, что определяется использованием расширенных полей; поэтому реализации программная, программно-аппаратная и аппаратная будут приблизительно одинаковой сложности;
4. универсальность использования конструкции.

Недостатками использования ЛРС является высокая зависимость между битами. Эта зависимость, в частности, позволяет по небольшому отрезку ЛРП определить начальный вектор из решения системы линейных уравнений. Таким образом, сформированные ЛРС последовательности не удовлетворяют требованию 3, предъявляемого к ПСП.

В связи с этим, формируемую линейную рекуррентную последовательность (ЛРП) необходимо усложнить при помощи нелинейной функции. Такие конструкции называются нелинейными фильтрующими генераторами (рис. 1).

Определение 4.

Пусть P – конечное поле. Тогда *нелинейным фильтрующим генератором* над полем P будем называть автономный автомат $A = (P^n, P, h, f)$, где h – преобразование ЛРС длины n над полем P. Выходную гамму фильтрующего генератора можно рассматривать как результат отображения, примененного к ЛРП порядка n, выполняемого при помощи некоторой нелинейной функции $f(x_1, x_2, ..., x_s)$, $s \le n$, сформированной ЛРС.

В качестве нелинейной функции можно использовать цикловую функцию БСШ. Однако в этом случае время разворачивания ключа будет существенно зависеть от скорости и количества криптографических преобразований, используемых в цикловой функции. Учитывая, что стоит задача разрушения межбитовых линейных связей, но не достижения нелинейной функцией предельно возможных показателей нелинейности, можно использовать значительно облегченный вариант цикловой функции. В данном случае нас также не интересуют возможные корреляционные атаки на схемы поточного шифрования, так как криптоаналитик не будет располагать достаточным количеством информации. Критерием прохождения последовательности будем считать результаты исследования корреляционными методами, которые принято использовать при статистических испытаниях БСШ.

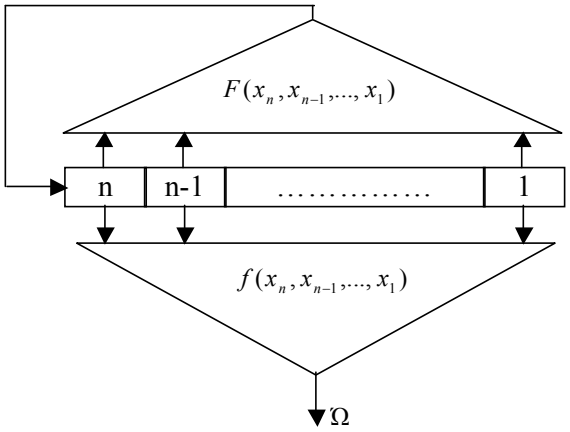

Рисунок 1 – Общая схема нелинейного фильтрующего генератора

Использование цикловой функции в качестве усложняющего выходную последовательность элемента схемы приводит к частичной потере универсальности схемы. Использование ключезависимых криптографических преобразований внутри цикловой функции приведет к необходимости использования некоторых констант для использования ее в качестве нелинейной функции генератора. Следовательно, использование такой конструкции для различных БСШ с различной длиной цикловых подключей и блоков данных будет сопряжено с проблемами подбора новых констант. Кроме того, необходимо доказать, что использование таких констант не приводит к потере криптографических свойств нелинейной функции. Поэтому необходимо построить нелинейную функцию, которая использует преобразования, не связанные с длинами ключей и блоков, используемых в конкретном БСШ.

III Особенности построения нелинейных функций

Сформулируем основные принципы построения нелинейной функции.

1. Нелинейная функция должна обеспечивать нелинейное «смешивание» всех входных разрядов (нелинейные преобразования должны обладать предельно-достижимыми показателями нелинейности).

Нелинейная функция должна обеспечивать «рассеивание активизации» (различные выходы каждого S-блока текущего «S-слоя» должны воздействовать на входы различных S-блоков следующего «S-слоя»).

3. Нелинейная функция должна обеспечивать «размножение активизации» (увеличение числа активных S-блоков при любой ограниченной активизации входов цикловой функции). В отличие от цикловой функции, которая применяется итеративно заданное количество раз, последовательность с выхода ЛРС пройдет через блок нелинейного преобразования единожды. В качестве нелинейных элементов в БСШ обычно используются S-блоки. Наша задача – достичь максимального количества активных S-блоков в пределах прохождения через нелинейную функцию. С этой целью целесообразно использовать два «S-слоя». Для обеспечения нелинейной функцией «рассеивания активизации» и «размножения активизации» возможно использование фиксированных перестановок битов между различными S-блоками, а также использование схем линейного комбинирования входов/выходов различных S-блоков, которые могут использоваться в БСШ.

В классическом варианте для нелинейного фильтрующего генератора нелинейная функция $f(x_1, x_2, ..., x_n)$ снимает аргументы с s ячеек ЛРС (рис. 1). Исследования, проведенные в проекте NESSIE [1] над поточными шифрами, показывают, что если количество точек съема s меньше половины длины ЛРС ($s \le n/2$), то такие криптосистемы подвержены ряду аналитических атак. Кроме того, существуют определенные правила выбора количества точек съема s для фильтрующей функции и множества точек обратных связей T характеристического полинома $F(\lambda)$.

Пусть Γ – множество из некоторого количества точек съема s: $\Gamma = \{s_i, 1 \le i \le n-1\}$, и пусть T – множество точек обратной связи ЛРС. Через $\Delta(\Gamma)$ обозначим далее множество положительных разностей между всеми элементами множества Γ, а через $\Delta(T)$ множество положительных разностей между элементами множества T. Введем дополнительное множество B, которое получается путем пересечения множеств $\Delta(\Gamma)$ и $\Delta(T)$, т. е. $|B| = \Delta(T) \cap \Delta(\Gamma)$.

Тогда при проектировании фильтр-генератора необходимо придерживаться следующих правил выбора точек съема и точек обратной связи [11]:

- количество точек съема s нелинейной функции должно находиться в пределах $n/2 \le s \le n-1$;

- наибольший общий делитель двух парных (соседних) элементов множества точек съёма s нелинейной функции $f(x_1, x_2, ..., x_n)$ должен быть равен 1;

- наибольший общий делитель двух парных (соседних) элементов множества точек обратных связей характеристического полинома $F(\lambda)$ должен быть равен 1;

- количество элементов множества B должно быть минимально достижимым.

Очевидно, что при заданных r (максимальная степень характеристического полинома $F(\lambda)$) стоит задача поиска такого множества положительных разностей $\Delta(I)$, чтобы минимизировать мощность множества B. Полные множества положительных разностей можно получать путем систематического поиска (разновидность целочисленного линейного поиска [12]), либо из таблиц, уже опубликованных в открытой печати.

Таким образом, при разработке нелинейной функции стоит вопрос определения входной разрядности функции, а именно, количества точек съема при заданных точках обратной связи. На рис. 2 представлена упрощенная схема нелинейной функции, особенностью которой является простота расширения входа/выхода до разрядности **64n** бит (**n**=1, 2, 3,… – коэффициент). Необходимым условием является кратность входного блока 64 битам. Далее блок разбивается на подблоки длиной 64 бита, которые проходят блоки нелинейной подстановки, реализуемые S-блоками (8 x 8). После этого выполняется «равномерная» битовая перестановка из 8 элементов P_{bit}. Перестановка имеет следующий вид:

$$\mathrm{P}_{\mathrm{bit}}: \quad \mathbf{W} \to \mathbf{W}$$
$$Y = \mathrm{P}_{\mathrm{bit}}(X); \quad X, Y \in \mathbf{W};$$
$$X = \langle b_{63} \parallel ... \parallel b_1 \parallel b_0 \rangle; \quad Y = \langle b'_{63} \parallel ... \parallel b'_1 \parallel b'_0 \rangle;$$
$$b'_{8\times j+i} = b_{8\times i+j}; \quad i, j = \overline{0, 7}; \quad b_t, b'_t \in \{0, 1\},$$

где $\mathbf{W}$ – векторное пространство 64-битных элементов (слов), $\mathbf{W} = \mathrm{GF}(2)^{64} = \{0,1\}^{64}$, b_i, b'_i – отдельные разряды.

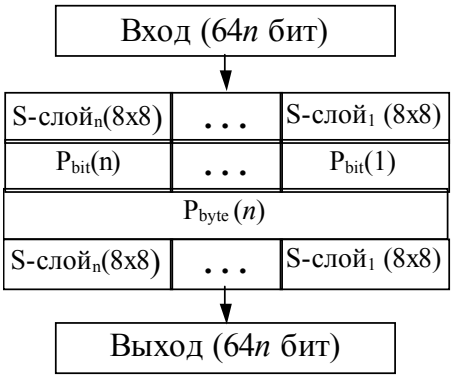

Рисунок 2 – Структура нелинейной функции

Перестановка P_{bit} на всём пространстве ключей сохраняет введенное выше свойство «равновероятности» перестановки для любой пары «бит-источник → бит-получатель», при этом обеспечивается свойство «равномерного рассеивания активизации», т. е. каждый байт слова-результата всегда содержит по одному биту из каждого байта «слова-источника».

В каждом отдельно взятом бите слова-результата криптоаналитик имеет неопределённость как относительно позиции байта-источника, так и относительно позиции бита внутри этого байта.

Следующим слоем следует фиксированная перестановка байтов $P_{byte}(n)$, которая может быть описана аналитически следующим образом:

$$\mathrm{P}_{\mathrm{byte}}(n): \quad B'_i = B_{n\times(i \bmod 8)+(i \operatorname{div} 8)}, \quad B_i \in \mathbf{B}, \quad i = \overline{0, 8n-1},$$

где B_j – байт-источник (j – позиция байта в исходном полублоке); B_i'– байт-получатель (i – позиция байта в результирующем полублоке).

Под полублоком понимается блоки по 64 бита, на которые происходит разбиение входного блока длиной **64n** (рис. 2).

Применение преобразования $P_{byte}(n)$ позволяет «связать» различные слова, составляющие полублок (для случая $n > 1$).

Перестановка $P_{byte}(n)$ построена таким образом, что после выполнения этого преобразования каждое 64-битное слово-получатель содержит одинаковое число байт из каждого слова-источника, то есть она обеспечивает «равномерное» распределение информации между словами полублока.

Далее следует второй слой нелинейной подстановки, реализуемый S-блоками (8 x 8). Использование легко реализуемых табличным способом преобразований $P_{byte}(n)$ и P_{bit} позволяет в пределах одного прохода такой функции активизировать максимально возможное количество S-блоков, реализуя тем самым сформулированные требования к нелинейной функции.

При таком подходе к проектированию нелинейного усложняющего узла мы можем сформировать нелинейную функцию необходимой разрядности с учетом рассчитанного для конкретного ЛРС количества точек съема s и точек обратной связи T.

При практической реализации нелинейной функции использовались криптографические преобразования, реализованные при проектировании цикловой функции криптографического алгоритма «Торнадо» [8], разработанного в соответствии с требованиями высокой криптографической стойкости.

IV Экспериментальная конструкция схемы разворачивания ключей

В соответствии с принципами, изложенными в предыдущих разделах, была разработана экспериментальная версия схемы разворачивания ключей на базе нелинейного фильтрующего генератора. Для испытаний использовался БСШ «Торнадо». Описание криптографического алгоритма, а также исследований его криптографических свойств подробно освещено в [8].

В качестве ЛРС был выбран регистр над расширенным полем $GF(2^{32})$, использовавшийся в поточном шифре SOBER-128 [12] для минимизации затрат, связанных с расчетом необходимых точек съема и точек обратной связи. Расширение поля не является принципиальным. В нашем случае выбрано расширение поля $GF(2^{32})$ для эффективной реализации на 32-х битных микропроцессорах.

На рис. 3 приведена структурная схема процедуры разворачивания ключей.

Регистр формирует поток $\{s[t]\}$ 32-х битных «слов», используя операции в расширенном поле $GF(2^{32})$. В основе регистра лежит характеристический полином вида $P(X) = X^{17} + X^{15} + X^4 + \alpha$ над $GF(2^{32})$, где α – это константа, которая в соответствии со спецификацией [25] равна $0x00000100$ или в виде полинома $y = 0x00 \cdot y^3 + 0x00 \cdot y^2 + 0x01 \cdot y + 0x00$. Регистр состоит из $n = 17$ ячеек памяти, называемых состояниями $s[t+i]$ ($i = \overline{1-17}$) и каждая ячейка представляет собой 32-х битное «слово».

Вектором $\sigma_t = (s[t], ..., s[t+1])$ будем обозначать далее состояние регистра в момент времени t. Начальное состояние ЛРС соответственно $\sigma_t = (s[0], ..., s[16])$. На каждом новом такте в момент времени t регистр обновляет свое состояние σ_{t+k} в соответствии со следующей формулой: $s[t+17] = s[t+15] \oplus s[t+4] \oplus \alpha \cdot s[t]$

Линейная рекурсия над полем $GF(2^{32})$ может быть эффективно заменена при помощи 32-х обычных двоичных ЛРС, работающих параллельно, каждый длиной $32 \cdot 17 = 544$. Другими словами, рассматриваемый ЛРС может быть эффективно заменен ЛРС в поле $GF(2)$, характеристический полином которого имеет следующий вид: $P'(X) = 1 + X^{17} + X^{19} + X^{21} + ... + X^{544}$. Следовательно, период рассматриваемого ЛРС будет $T = 2^{544} - 1$. Таким образом, выпоняется требование гарантии периода ПСП для формирования всех необходимых подключей.

Нелинейная фукнция была разработана в соотвествии с принципами, изложенными в предыдущем разделе. В качестве криптографических преобразований использовались эелементы цикловой фукнции БСШ «Торнадо».

Точки съема для нелинейной фукнции были выбраны аналогично тем, которые предлагались в спецификации алгоритма SOBER-128: $s[t]$, $s[t+1]$, $s[t+6]$, $s[t+13]$ и $s[t+16]$. Каждое снимаемое состояние является 32-х битным числом, и, таким образом, на вход нелинейной функции поступает 160 бит во время каждого момента времени t. В общем виде преобразование нелинейного фильтра можно выразить в следующем виде: $\nu_t = F\big(s[t], s[t+1], s[t+6], s[t+13], s[t+16]\big)$.

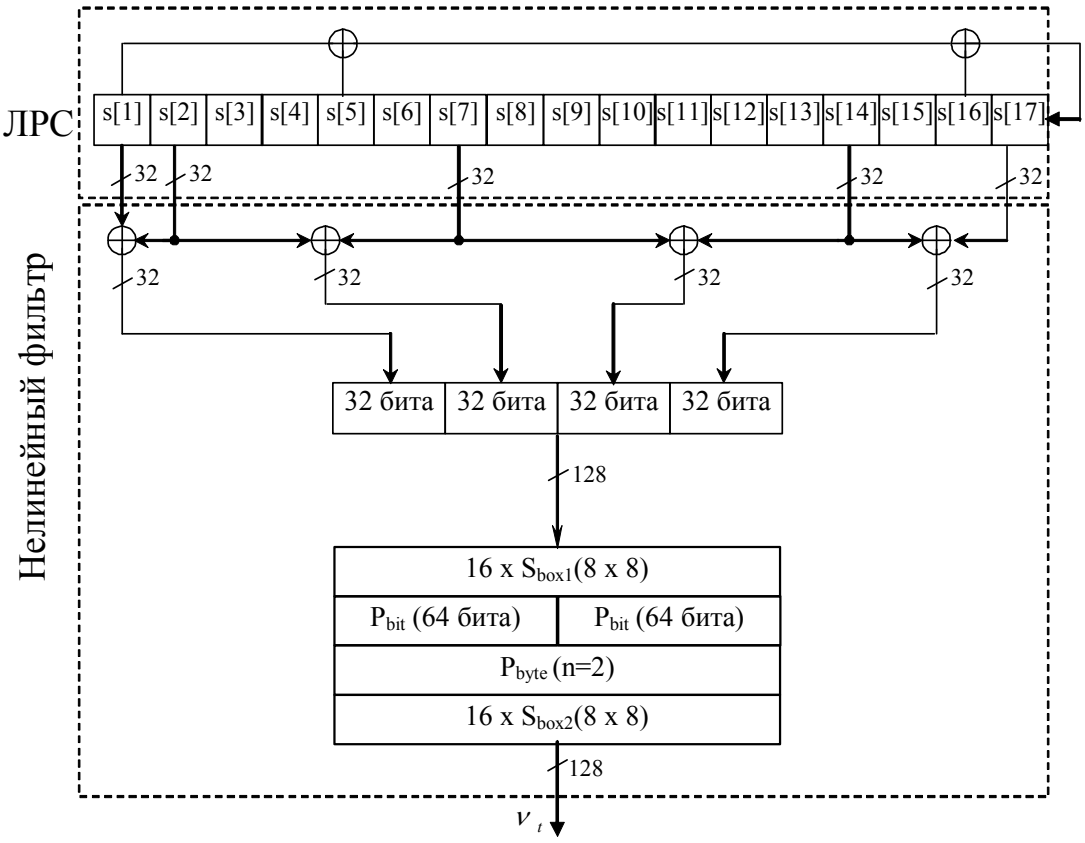

Рисунок 3 – Процедура выработки цикловых ключей на базе ЛРС в поле GF(2^{32})

Чтобы иметь возможность использовать фиксированную перестановку байтов P_{byte} при реализации нелинейной фукнции, был выбран коэффициент $n = 2$. Таким образом, длина входного двоичного вектора в цикловую функцию F равняется $l_b = 128$ бит. Перед тем как двоичные вектора с указанных точек съема поступят на вход нелинейной функции, выполняется предварительная рандомизация, целью которой является сжатие 160 битного вектора $\sigma_t = \big(s[t], s[t+1], s[t+6], s[t+13], s[t+16]\big)$ в 128 битный вектор:

$\sigma'_t = \big(s[t] \oplus s[t+1], s[t+1] \oplus s[t+6], s[t+6] \oplus s[t+13], s[t+13] \oplus s[t+16]\big)$. Для этого выполняется сложение по модулю 2 двух соседних точек съема $s[t+i]$ и $s[t-i]$ ($0 \le i \le 16$).

Структура нелинейной функции приведена на рис. 2. В качестве нелинейных преобразований используется последовательность криптографических операций P_{byte}, фиксированная перестановка байтов между байтами «слов» *W*, подстановки S_1 и S_2, задаваемые при помощи S-box, и «равномерная» битовая перестановка P_{bit} внутри каждого «слова» *W*. Аналитически формирование последовательности ν_t можно представить следующим образом $\nu_t = F(\sigma'_t)$:

1. $X_{<128>} = P_{byte}(\sigma'_t)$;
2. $X'_{<128>} = S_1(X_{<128>})$;

3. $X''_{<128>} = P_{bit}(X'_{<128>})$;

4. $\nu_t = S_2(X''_{<128>})$.

V Исследование статистических свойств схемы разворачивания ключей на базе ЛРС в поле GF(2^n)

Пакет NIST STS включает 16 различных статистических тестов, направленных на выявление различных «дефектов» случайности. При этом некоторые из тестов рассчитываются для нескольких различных «тестовых шаблонов», проверка каждого из которых фактически является отдельным тестом. В связи с этим общее количество тестов составляет 189. Описание пакета NIST STS и методики проведения исследований приводятся в [8].

Результаты экспериментальной проверки конструкции схемы разворачивания ключей в составе БСШ «Торнадо» представлены на рис. 4.

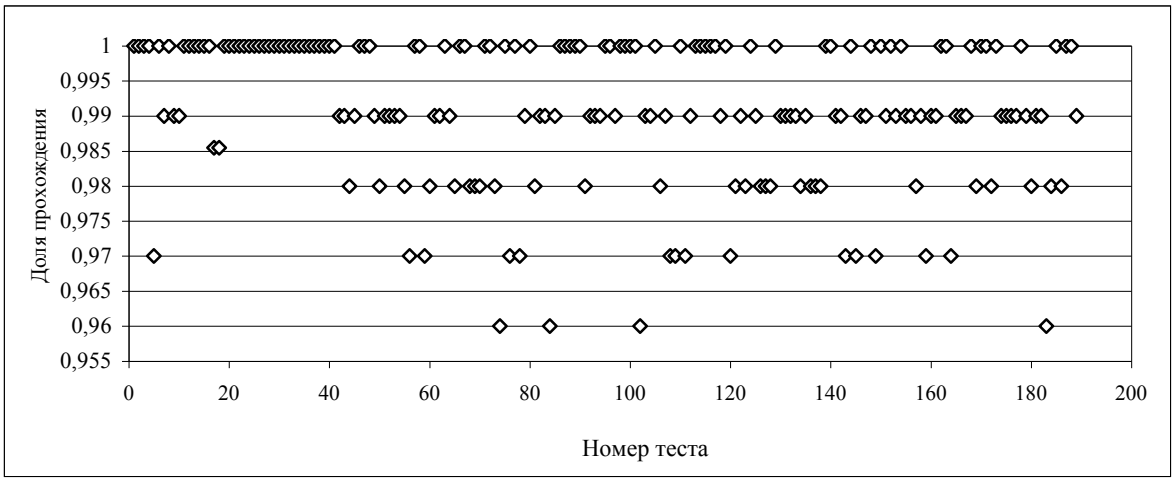

Рисунок 4 – Диаграмма прохождения тестов

По результатам проведенных испытаний можно сделать следующие частные выводы:

1. значение вероятности P_j по всем тестам для всех протестированных выборок удовлетворяет ограничению $P_j > 0{,}0001$;

2. выборок, не прошедших ограничение $r_j \geq 0{,}96015$ по некоторому тесту, зафиксировано не было;

3. выборок, не прошедших какой-либо тест в ходе тестирования, зафиксировано не было.

Полученные результаты сопоставимы с результатами для эталонной выборки, рекомендованной NIST STS. Кроме того, количество тестов, в которых тестирование прошло 99% последовательностей для предлагаемой процедуры разворачивания ключа, выше, чем для BBS генератора.

VI Исследование корреляционных свойств схемы разворачивания ключей на базе ЛРС в поле GF(2^n)

Для более адекватной оценки статистической безопасности процедуры разворачивания ключей с целью выявления статистических связей между битами сформированной последовательности и между битами исходного ключа и цикловых подключей были проведены исследования ее корреляционных свойств. Методика проведения исследований и описание самих тестов рассматривалось ранее в [8] и здесь не приводится.

Для исследования корреляционных свойств алгоритма использовалось три теста, позволяющие выявить «простые» статистические зависимости:

1) количества бит (N), которые изменились в развернутом ключе при изменении одного (любого) бита в исходном ключе;

2) степени «лавинного эффекта» (d_a);

3) степени «строгого лавинного критерия» (d_{sa});

4) степени «полноты» (d_c).

Для всех перечисленных выше тестов были рассчитаны математическое ожидание M и дисперсия D. Математическое ожидание отражает количество изменившихся бит в блоке (длина блока 128 бит), а дисперсия показывает разброс значений.

Процедура разворачивания ключа рассматривается как блочное преобразование: вход – 7 полублоков исходного пользовательского ключа (7 x 64 = 448 бит), выход – 4 x 5 + 4 полублоков «сырого» рабочего (развернутого) ключа ((4 x 5 + 4) x 64 = 1536 бит), в соответствии со спецификацией алгоритма «Торнадо». Результаты представлены в табл. 1.

Таблица 1 – Результаты корреляционного анализа

Наименование теста	Зависимость между отдельными битами	
	M	D
N, количество изменившихся бит	799,99367	400,24293
Степень лавинного эффекта, d_a	0,998758	
Степень строгого лавинного критерия, d_s	0,991720	
Степень полноты, d_c	1,000000	

По результатам (табл. 1) можно отметить, что между битами исходного ключа и развернутого линейных связей не анализируется.

VII Оценка времени разворачивания исходного ключа

Как уже говорилось минимизация времени разворачивания ключа является важной тактико-технической характеристикой для схем разворачивания ключей при условии обеспечения высокой криптографической безопасности.

Был проведен сравнительный анализ предлагаемой конструкции схемы разворачивания ключей и конструкции на базе БСШ в режиме усиленной схемы поточного шифрования, которая уже прошла испытания в составе криптоалгоритма «Торнадо» [8]. Оценивалось количество исходных ключей (длина ключа l_k =128 бит), которые схема развоарчивания развернет в выходную «сырую» последовательность длиной 1536 бит за секунду. Испытания проводились на ПК Celeron-600, Windows'2000. Результаты приводятся в табл. 2.

Таблица 2 – Оценка времени разворачивания ключей

Тип схемы разворачивания ключей	**Длина развернутого ключа, бит**	**Количество ключей/сек**
на базе ЛРС в поле GF(2^{32})	1536	10000
на базе усиленной схемы поточного шифрования	1536	3000

По полученным результатам (табл. 2) видно, что предлагаемая конструкция обладает преимуществом более, чем в три раза при использовании в качестве нелинейной функции одинаковых криптографичсеких преобразований.

Выводы

Показано, что для построения процедур «разворачивания ключа» могут использоваться простые криптографические схемы формирования ПСП, которые удовлетворяют высоким требованиям криптографической безопасности. В качестве таких схем возможно использование поточного шифра, построенного на основе базовой цикловой функции БСШ. Сформулированы требования, которым должны удовлетворять такие конструкции.

Предложен универсальный метод формирования цикловых подключей, использующий ЛРС в расширенном поле с нелинейной фильтрующей функцией на выходе. Исследования экспериментальной схемы разворачивания ключей показали высокие криптографические свойства. В отличие от аналогичных методов формирования развернутых ключей, она обладает большей гибкостью при использовании в составе различных БСШ без конструктивных изменений, не использует ключезависимых преобразований в нелинейной функции, в отличие от конструкций на базе БСШ в поточных режимах, обладает высокими

показателями производительности формирования развернутого ключа и большой гибкостью при реализации на платформах с различной разрядностью.

Литература: ***1.*** *NESSIE Call for Cryptographic Primitives, Version 2.2, 8 March 2000: http://cryptonessie.org.* ***2.*** *L. R. Knudsen. Practically secure Feistel ciphers. In R. Anderson, editor, Fast Software Encryption 1993, Cambridge Security Workshop (FSE1), Volume 809 of Lecture Notes in Computer Science, pp. 211, 1994. Springer-Verlag.* ***3.*** *J. Kelsey, B.Schneier, D. Wgner "Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER and 3-DES" //CRYPTO'96, Springer-Verlag, 1996, pp. 237 – 251.* ***4.*** *Гловашич С. А., Горбенко И. Д. Алгоритм блочного симметричного шифрования «Торнадо». Спецификация преобразования. //Радиотехника: Всеукр межвед. науч.-техн. сб.– 2003. Вып. 134. С.155–190.* ***5.*** *Иванов М. А. «Криптографические методы защиты информации в компьютерных системах и сетях». Москва «Кудиц-образ», 2001.– 363 с.* ***6.*** *Головашич С. А. Безопасность режимов блочного шифрования //Радиотехника: Всеукр межвед. науч.-техн. сб.– 2001. Вып. 119. С.135–145.* ***7.*** *Лепеха А. Н. Алгоритм формирования псевдослучайной последовательности. //конференция «Актуальные проблемы и перспективы развития финансово-кредитной системы Украины», Харьков.– 2002.– с. 339.* ***8.*** *Лепеха А. Н., Головашич С. А. Статистический анализ БСШ «Торнадо» //Радиотехника: Всеукр межвед. науч.-техн. сб.– 2003. Вып. 134. С. 89 – 96.* ***9.*** *Потий А. В., Орлова С. Ю. и др. Статистическое тестирование генераторов случайных и псевдослучайных чисел с использованием набора статистических тестов NIST STS. //Радиотехника: Всеукр межвед. науч.-техн. сб. 2000. Вып. 114. С. 14.* ***10.*** *Фомичев В. М. «Дискретная математика и криптология». М.: «Диалог МИФИ», 2003.– 397 с.* ***11.*** *Philip Hawkes, Gregory Rose "Primitive Specification For SOBER-128" Qualcomm, Australia, 2003.* ***12.*** *R. Lorentzen, R. Nilsen "Application of linear programming to the optimal difference triangle set problem". IEEE Trans. Inform. Theory, vol IT-37, 1991, pp 1486-1488.*

УДК 681.3.06: 519.248.681

МЕТОДИКА ОЦЕНКИ ЭФЕКТИВНОСТИ ПОТОЧНЫХ ШИФРОВ

Светлана Орлова

Харьковский национальный университет радиоэлектроники

Анотація: **Наводиться удосконалена система критеріїв і показників ефективності функціонування схем потокового шифрування, яка дозволяє відібрати допустимі параметри шифру таким чином, щоб відповідати вимогам криптографічної стійкості, оптимальності та адаптивності. На основі цієї системи пропонується методика дослідження ефективності потокових шифрів, призначена безпосередньо для оцінювання нових та відомих шифрів і проведення їх порівняльного аналізу.**

Summary: **In this paper the improved system of criteria and metrics of operation efficiency of the stream encryption schemes, that allow to select valid parameters of the cipher so that to satisfy the requirement of cryptographic security, optimality and adaptivity is proposed. On the basis of this system the technique of research of efficiency of the stream ciphers intended directly for estimation of the new and known ciphers and for making the comparative analysis of their is offered.**

Ключові слова: **Потоковий шифр, оцінка ефективності, криптографічна стійкість.**

Введение

Стремительное развитие информационных технологий обуславливает необходимость применения систем защиты информации, обеспечивающих высокий уровень информационной безопасности наравне с высокой скоростью передачи данных по каналам связи. В основе таких систем используются поточные шифры (ПШ). Однако на сегодняшний день в этой области не существует стандартов, удовлетворяющих требованиям надёжности, ни в Украине, ни за рубежом. Это объясняется тем фактом, что большинство используемых на практике схем поточного шифрования либо запатентованы, либо конфиденциальны [1]. Однако опыт показывает, что засекречивание применяемых в системе алгоритмов не обеспечивает их практической стойкости. Так, например, согласно политике безопасности системы мобильной связи GSM [2], используемые алгоритмы долгое время были засекречены, однако это не помешало осуществлению многочисленных случаев её компрометации [3 – 5]. Единственная гарантия надёжности криптографических алгоритмов – это их открытость, которая позволяет широкой общественности изучать алгоритмы и находить в них слабые места. Согласно этому принципу с 2000 по 2003 год проходил масштабный Европейский проект NESSIE [6], основной задачей которого было создание набора криптографических примитивов с последующим внедрением его в международные органы стандартизации. Среди претендентов на стандарт впервые рассматривались и схемы поточного шифрования. И хотя для поточных шифров проект закончился