4. Инфокоммуникационная технология в управлении системами водоснабжения позволяют повысить надежность работы оборудования и элементов водоснабжения, оперативную передачу сообщений о возникновении аварийных ситуациях, состоянии насосных систем и уровне потребления электроэнергии.

5. Повсеместное распространение и развитие мобильных технологий, высокая скорость передачи информации в системах связи и многие другие факторы стали основой для появления цифровой экономики, которая также включает мониторинг и управление объектами водоснабжения с помощью инфокоммуникационных технологий.

1. Алымов Н.Л. Анализ сфер применения средств беспроводного доступа в системе муниципального коммунального хозяйства/ Н.Л. Алымов, А.А. Горшков, В.А. Кочетков, И.В. Солдатов// Известия ТулГУ. Технические науки. 2018. № 9.
2. Гришин А.П. GSM в технологиях водоснабжения/ Сантехника, отопление, кондиционирование. 2010. № 10 (106). С. 22-25.
3. Гришин А.П. Оценка инновационного эффекта сотовой информационной технологии в водоснабжении. Инновации. 2007. № 9. С. 85-90.
4. Ефимушкин В. А. Инфокоммуникационное технологическое пространство цифровой экономики/ Т.В. Ледовский, Е.Н. Щербакова // Т-Сomm: Телекоммуникации и транспорт. 2017. Т. 11. № 5. С. 15-20.
5. Юшкевич И. SCADA и мобильники. Оценка безопасности приложений, превращающих смартфон в пульт управления заводом [Электронный ресурс] – Режим доступа: <https://xakep.ru/2015/08/03/scada-and-mobile-security/> (дата обращения 16.04.2019).

Иванов С.В., Давыдов С.А., Никулин Н.П.
Модификация генератора случайных чисел

*Краснодарское высшее военное училище
им. генерала армии С. М. Штеменко
(Россия, Краснодар)*

doi: 10.18411/lj-04-2019-258

idsp: ljjournal-04-2019-258

Аннотация

В работе рассматриваются основные свойства псевдослучайных последовательностей (ПСП) линейных рекуррентных регистров сдвига (ЛРРС), а также аналитическая оценка криптостойкости псевдослучайных последовательностей (ПСП), сформированная с использованием нелинейных узлов усложнения. Формулируются необходимые и достаточные условия обеспечения необходимой стойкости к раскрытию ее структуры. Указываются модификации генератора псевдослучайной последовательности (ПСП), с помощью которых обеспечивается необходимая стойкость.

Ключевые слова: псевдослучайная последовательность, генератор случайных чисел, генератор псевдослучайной последовательности, линейный рекуррентный регистр сдвига.

Введение

В современной информационной обстановке создание защищенных информационных технологий, которые могут противостоять атакам злоумышленника является приоритетом для ведущих стран мира. Поэтому для защиты информации в различных программных и программно-аппаратных средствах защиты применяются псевдослучайные последовательности (ПСП), полученные с использованием линейных рекуррентных регистров сдвига (ЛРРС). На данный момент псевдослучайные последовательности, могут быть вскрыты с использованием алгоритмов криптоанализа с различными методами перебора. Поэтому необходимо вводить модификации генератора псевдослучайной последовательности (ПСП), которые смогли бы обеспечить необходимую стойкость и противостоять атакам злоумышленника.

Постановка задачи

В области защиты информации широкое применение находят, генераторы случайных чисел (ГСЧ), образованные на основе псевдослучайных последовательностей с использованием линейных рекуррентных регистров сдвига. Рассмотрим линейный рекуррентный регистр на рисунке 1.

Рисунок 1 – Линейный рекуррентный регистр

ЛРРС работает следующим образом: в ячейки памяти заносятся значения, далее при каждом такте происходит сдвиг значения в правую ячейку, а сумматор осуществляет сложение. По окончании выходит бесконечная последовательность.

Для нахождения свойств выходных последовательностей необходимо ввести некоторые понятия:

Определение 1: Если любой многочлен $f(x)$ с коэффициентами 0 и 1 нельзя представить, как произведение двух или более других многочленов с коэффициентами 0 и 1 кроме тривиальных $1 \times f(x)$, то $f(x)$ называется неприводимым многочленом.

Определение 2: Если неприводимый многочлен делит без остатка многочлен $x^{2^n} - 1$ и не делит никакой многочлен $x^n - 1$, $n < 2^n - 1$, то он называется примитивным многочленом.

Определение 3: Поле F , это множество элементов, в котором определены операции сложения, вычитания, умножения и деления. Для любых α, β, γ принадлежащих полю F должны выполняться следующие условия: $\alpha + \beta = \beta + \alpha$; $\alpha\beta = \beta\alpha$; $\alpha + (\beta + \gamma) = (\beta + \alpha) + \gamma$; $\alpha(\beta\gamma) = (\alpha\beta)\gamma$. Кроме того, в поле должны существовать такие элементы как: 0; 1; $-\alpha$; α^{-1} (для $\alpha \neq 0$) и выполняться следующие соотношения: $0 + \alpha = \alpha$; $(-\alpha) + \alpha = 0$; $0 \times \alpha = 0$; $1 \times \alpha = \alpha$; $(\alpha - 1) = \alpha$. Таким полем называется поле Галуа.

Далее необходимо ввести свойства выходных последовательностей ЛРРС:

1. Период выходной последовательности ЛРРС. Число состояний регистра равно 2^n , из них одно нулевое состояние, то период не может быть больше $2^n - 1$. Когда период равен $2^n - 1$, то полином регистра примитивный.

2. Свойство «окна». Если «окно» шириной n перемещать вдоль выходной последовательности на примитивном многочлене, то каждый из $2^n - 1$ ненулевых наборов будет виден точно один раз.

3. Свойство сложения. Если фиксирован примитивный многочлен, то число возможных числовых последовательностей равно числу начальных состояний, то есть $2^n - 1$. Почленная сумма 2-х выходных последовательностей по mod2 снова даст выходную последовательность ЛРРС.

4. Свойство сдвига. Любой циклический сдвиг выходной последовательности, также есть выходная последовательность ЛРРС.

5. Свойство баланса. Любая выходная последовательность содержит 2^n единиц и $2^n - 1$ нулей. Между 1 и $2^n - 1$ имеем $2^m - 1$ нечетных чисел, двоичное представление которых оканчивается на 1, и $2^m - 1$ четных чисел, которые оканчиваются на 0.

6. Свойство серий. Любая выходная последовательность имеет половину серий длины 1, четверть серий длины 2, 1/8 серий длины 3 и т.д. В каждом случае число серий из 0 равно числу серий из 1.

Данные свойства показывают и дают основания называть выходные последовательности ЛПРС, псевдослучайными.

Решение задачи.

Рассмотрим ЛПП, построенный на произвольном полиноме

Рисунок 3 – Схема усложнения выходной последовательности рекуррентного регистра при помощи операции умножения

Полином $h(x) = 1 + x + x^3$, содержащий три ячейки ($n=3$) памяти и один узел перемножения показан на рисунке 3. То есть состояния ячеек памяти регистра можно представить через примитивные элементы поля следующим образом:

$$\begin{aligned} a_i &= a^i + a^{2i} + (a^2 + a)^i \\ a_{i+1} &= a^{i+1} + a^{2(i+1)} + (a^2 + a)^{i+1} \end{aligned}$$

Окончательно имеем:

$$\begin{aligned} h(x) &= h_1(x) \times h_2(x) = (x^3 + x + 1) \times (x^3 + x + 1) = \\ &= x^6 + x^5 + x^3 + x^4 + x^3 + x + x^3 + x^2 + 1 = \\ &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1. \end{aligned}$$

Тогда эквивалентный ЛПП путем преобразования, принимает вид, изображенный на рисунке 4.

Рисунок 4 – Модифицированная схема эквивалентного регистра для усложненной последовательности

Период выходной последовательности здесь сохранился прежним, то есть он равен $2^3 - 1 = 7$. Можно и далее усложнять схему выполняя многократное перемножение от элементов одного и того же регистра, как показано на рисунке 4. Можно построить регистр с нелинейностью m -го порядка (на рисунок 4, $m=2$) и произведя аналогичные расчеты обнаружить новые корни и в конечном итоге построить эквивалентный ЛПП.

Число корней будет равно $\sum_{i=1}^m C_n^i$

Как раз, так и будет, если эквивалентный регистр, вместо того, чтобы иметь длину $C_4^1 + C_4^2 + C_4^3 = 4 + 4 + 6 = 16$, имеет длину 10 и вид, показанный на рисунок 5. Если $m \rightarrow n$, где n -длина ЛПП, то длина эквивалентного регистра $n' \rightarrow 2n - 1$ и большего

усложнения получить невозможно. Чтобы еще больше увеличить эквивалентную сложность мы должны иметь большее расширение поля.

Рисунок 5 – Эквивалентный регистр для усложненной последовательности

Рассмотрим нелинейное преобразование «узел Джеффи», показанный на рисунке 6.

Рисунок 6 – Узел Джеффи

Узел Джеффи, показанный на рисунке 6, состоит из трех регистров: ЛРР1, ЛРР2, ЛРР3. ЛРР2 управляет поочередным подключением на сумматор по mod2 выходных последовательностей от ЛРР1 или от ЛРР3. При этом одновременное подключение выходов ЛРР1 и ЛРР2 исключено. Если с выхода ЛРР2 поступает 1, то к сумматору подключается выход ЛРР1, а если 0 – выход ЛРР3, так как второй умножитель имеет инверсный вход.

Из таких элементов можно образовывать каскадные соединения, сложность которых будет весьма велика.

Рисунок 7 – Каскадное соединение из 3-х элементов Джеффи

На рисунке 7 показан пример такого каскадного соединения. Над кругами указаны длины ЛРР, а рядом с линиями - эквивалентная сложность для каждой подпоследовательности. Видно, что эквивалентная сложность оказывается свыше миллиона. Число исходных ЛРР равна 9, с общей длиной каскадов 159. Если все ЛРР

реализованы на примитивных полиномах, то период выходной последовательности будет практически бесконечным и баланс между нулями и единицами будет очень хорошим. Из рисунка 7 видно, что достаточно объединить три криптографических примитива еще одним устройством и эквивалентная сложность возрастает до $10^6 \cong 2 \cdot 10^{12}$.

Вывод

Таким образом, для того, чтобы повысить стойкость выходной последовательности к раскрытию необходимо разорвать рекуррентную зависимость элементов этой последовательности. Для этого используют нелинейные преобразователи (различные комбинации из логических элементов И, ИЛИ, НЕ и др.), которые позволяют за счет усложнения структуры выходной последовательности ЛРРС увеличить ее эквивалентную сложность. То есть в системах защиты информации недостаточно увеличивать только степень порождающего полинома ЛРРС, необходимо также применять нелинейные преобразования над элементами псевдослучайной последовательности.

1. Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата).
2. Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 09.03.01 Информатика и вычислительная техника (уровень бакалавриата).
3. Исаков В.Н. Элементы численных методов / В.Н. Исаков // М.: Издательский центр «Академия», 2003. – 118 с.
4. Шнайер Б. Прикладная криптография Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф, 2013. — 816 с.
5. Golomb, S. Shift Register Sequences, San Francisco, Holden-Day, 1967. KEY E.L. An Analysis of the Structure and Complexity of Nonlinear Binary Sequence Generators. - IEEE Trans. on Inform. Theory. 1976, v. IT-22, No.6.
6. Головина Л.И. Линейная алгебра и некоторые ее приложения. - М.: Наука, 1985
7. Kerckhoffs, A. La Cryptographie militaire /A. Kerckhoffs // Journales Scientices Militaires, 9th Series. – 1983. February. – P. 161 – 191. Andelman, D. On the Cryptanalysis of Rotor Machines and Substitution – Permutation Networks / D. Andelman, J.Reeds // IEEE Trans. On IT. – 1981. – Vol IT-28, №4/
8. Коржик В.И., Яковлев В.А. Основы криптографии: учебное пособие / В.И.Коржик, В.А.Яковлев. – СПб., ИЦ Интермедия, 2016. – 312 с. : илл.

Костюкова Т. П., Хвойнова Э.Д.

Защита персональной информации в локальной сети предприятия

*Уфимский государственный авиационный технический университет
(Россия, Уфа)*

doi: 10.18411/lj-04-2019-259

idsp: ljjournal-04-2019-259

Аннотация

Расчетные листки выдаваемые бухгалтерией являются персональной информацией сотрудников, поэтому вопросы защищенности и своевременности передачи их сотрудникам является актуальной задачей, связанной с защитой конфиденциальных данных сотрудников. Для решения задачи использованы методы экономического анализа, анализ бизнес-процессов и способы обеспечения защиты информации.

Ключевые слова: расчетный листок, бухгалтерия, сотрудник, конфиденциальность, защита информации, межсетевые экраны.

Abstract

Payments issued by the accounting department are personal information of employees, so the issues of security and timeliness of their transfer to employees is an important task related to the protection of confidential data of employees. To solve the problem, the methods