УДК 681.3.06

А.А. Кузнецов, Ю.А. Избенко, А.А. Юкальчук

Харьковский университет Воздушных Сил им. И. Кожедуба

РАЗРАБОТКА СХЕМЫ ПОТОЧНОГО ШИФРОВАНИЯ ИНФОРМАЦИИ В АСУВ С ИСПОЛЬЗОВАНИЕМ ВЫСОКОНЕЛИНЕЙНЫХ ПРЕОБРАЗУЮЩИХ ФУНКЦИЙ

Рассматриваются процедуры поточного преобразования данных в АСУВ для повышения информационной скрытности. Предлагаются высоконелинейные преобразующие функции для перспективных средств поточной защиты информации в АСУВ.

поточное преобразование данных, высоконелинейные преобразующие функции

Введение

Постановка проблемы в общем виде и анализ литературы. Важным показателем эффективности современной АСУВ является информационная скрытность [1]. Основным механизмом ее обеспечения являются методы засекречивания (шифрования) информации [2 – 4], которые составляют основной объект исследований в теории секретных систем [5].

Наибольшее развитие в настоящее время получили симметричные методы криптографической обработки информации, которые основаны на выполнении процедур замешивания и рассеивания [2 – 4]. Перспективным направлением в этом смысле является построение криптографически стойких булевых функций, позволяющих аналитически описать основные этапы криптографического преобразования информации и конструировать аппаратуру шифрования с требуемыми для практики свойствами. **Целью статьи** является разработка схемы поточного шифрования информации в АСУВ с использованием высоконелинейных преобразующих функций.

Результаты исследований

В настоящее время существует несколько стандартизированных схем поточного шифрования информации [2 – 4], в том числе один из режимов отечественного алгоритма криптографического преобразования данных [2]. Одной из наиболее перспективных является схема LILI-II, прообраз которой, схема LILI-128, был представлен на международном криптографическом конкурсе NESSIE в качестве претендента на европейский стандарт поточного преобразования информации [6]. Схема LILI-128 была отвергнута на первой фазе конкурса в связи с обнаруженными уязвимостями. В частности, нелинейное преобразование схемы было представлено как потенциально уязвимое преобразование. Схема LILI-II является усиленной версией схемы LILI-128 и, согласно заявлениям разработчиков, не содержит в себе прежних уязвимостей. Схема поточного преобразования информации LILI- II является бит-ориентированной схемой и принадлежит к классу схем с неравномерным движением регистра. Схема использует 128 битный ключ и является примером классической схемы поточного шифрования на основе управляющего регистра с неравномерным движением. Компоненты схемы (рис.1) сгруппированы в две подсистемы: подсистему управления движением и подсистему генерации данных.

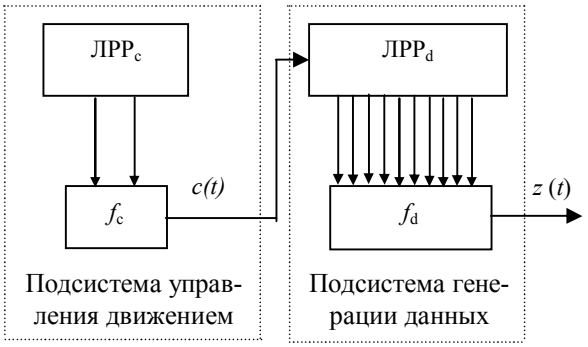

Рис. 1. Схема поточного криптографического преобразования LILI-II

Подсистема управления движением основана на линейном рекуррентном регистре длиной 128 бит, подсистема генерации данных - на линейном рекуррентном регистре длиной 127 бит. Каждая подсистема использует собственную нелинейную функцию. Оба регистра основаны на примитивном полиноме, что гарантирует генерацию последовательности с максимальным периодом и хорошими статистическими свойствами.

Подсистема управления движением использует псевдослучайную двоичную последовательность, сгенерированную двоичным регистром управления ЛРР$_c$ длиной L_c=128 бит с равномерным движением, и функцию f_c, оперирующую содержимым $k = 2$ ячеек ЛРР$_c$ для генерации псевдослучайной целочисленной последовательности, $c = \{c(t)\}_{t=1}^{\infty}$.

Полином обратной связи ЛРР$_c$ имеет вид:

$$h_1(x) = x^{128} + x^{126} + x^{125} + x^{124} + x^{123} + x^{122} + x^{119} + x^{117} + x^{115} + x^{111} + x^{108} + x^{106} + x^{105} + x^{104} + x^{103} + x^{102} + x^{96} + x^{94} + x^{90} + x^{87} + x^{82} + x^{81} + x^{80} + x^{79} + x^{77} + x^{74} + x^{73} + x^{72} + x^{71} + x^{70} + x^{67} + x^{66} + x^{65} + x^{61} + x^{60} + x^{58} + x^{57} + x^{56} + x^{55} + x^{53} + x^{52} + x^{51} + x^{50} + x^{49} + x^{47} + x^{44} + x^{43} + x^{40} + x^{39} + x^{36} + x^{35} + x^{30} + x^{29} + x^{25} + x^{23} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{11} + x^{9} + x^{8} + x^{7} + x^{6} + x^{1} + 1. \quad (1)$$

Начальное нулевое заполнение ЛРР$_c$ исключается процедурой инициализации ключа. В момент времени t содержимое 0 и 126 ячеек ЛРР$_c$ является входными данными функции f_c, выходом которой является целочисленное $c(t)$, такое что $c(t) \in \{1, 2, 3, 4\}$. Функция f_c определена как

$$f_c(x_0, x_{126}) = 2(x_0) + x_{126} + 1. \quad (2)$$

Подсистема генерации данных использует целочисленную последовательность $c(t)$ для управления двоичным ЛРР$_d$ длиной $L_d = 127$ бит: каждый раз регистр сдвигается c раз.

Полином обратной связи ЛРР$_d$ имеет вид:

$$h_2(x) = x^{127} + x^{121} + x^{120} + x^{114} + x^{107} + x^{106} + x^{103} + x^{101} + x^{97} + x^{96} + x^{94} + x^{92} + x^{89} + x^{87} + x^{84} + x^{83} + x^{81} + x^{76} + x^{75} + x^{74} + x^{72} + x^{69} + x^{68} + x^{65} + x^{64} + x^{62} + x^{59} + x^{57} + x^{56} + x^{54} + x^{52} + x^{50} + x^{48} + x^{46} + x^{45} + x^{43} + x^{40} + x^{39} + x^{37} + x^{36} + x^{35} + x^{30} + x^{29} + x^{28} + x^{27} + x^{25} + x^{23} + x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + x^{14} + x^{10} + x^{8} + x^{7} + x^{6} + x^{4} + x^{3} + x^{2} + x + 1. \quad (3)$$

Начальное нулевое заполнение ЛРР$_d$ исключается процедурой инициализации ключа.

Ячейки, значения которых являются входными данными для нелинейной функции, удовлетворяют полному множеству положительных разностей. Значения десяти фиксированных ячеек (0, 1, 3, 7, 12, 20, 30, 44, 65, 80, 96, 122) ЛРР$_d$ являются входными данными для специально выбранной булевой функции f_d. Вид булевой функции не приводится, известно лишь, что функция является сбалансированной, обладает корреляционным иммунитетом первого порядка, алгебраическая степень функции равна 10, функция не имеет линейных структур и достигает нелинейности 1992.

Двоичный выход f_d – поток бит $z(t)$. После того, как $z(t)$ вычислен, два ЛРР сдвигаются и процесс повторяется для формирования потока $z = \{z(t)\}_{t=1}^{\infty}$. Алгоритм ключевой инициализации и реинициализации детально рассмотрен в [6]. По предварительным оценкам, период последовательности, генерируемой схемой, составляет $(2^{128} - 1)(2^{127} - 1) \approx 2^{255}$, что значительно больше, чем требуемые 2^{128} бит для проведения атаки грубой силой. Введение схемы управления обеспечивает высокую линейную сложность генерируемой последовательности и устойчивость к атаке Берлекемпа-Месси [6].

Схема поточного шифрования с высоконелинейной булевой функцией. Для усиления криптографических свойств схемы поточного шифрова-

ния информации LILI – II предлагается использовать высоконелинейные булевы функции. В соответствии с [7] сформирована высоконелинейная булевая функция f_d над V_{12} (от двенадцати переменных) как аналог функции схемы LILI – II. Полиномиальная форма сформированной функции состоит из 1857 одночлена (терма) и имеет максимально достижимую алгебраическую степень, равную 11.

Основные криптографические свойства сформированной функции приведены в табл. 1. Для сравнения приведены так же свойства функции, используемой в алгоритме поточного шифрования информации LILI – II.

Таблица 1

Показатели стойкости булевых функций

	Показатель нелинейности функции, N_f	Алгебраическая степень функции, $deg(f)$	Алгебраическая степень каждой переменной, $deg(f, x_i)$	Число термов функции, $term$ (f_i)	Значение функции автокорреляции, $AC(f)$	Абсолютное значение корреляции функции, C_f
f_{lili}	1992	10	9, 10	280	336	0,027344
$f_{раз.}$	2010	11	11	1857	24	0,018555

Как показывает анализ данных табл. 1, булева функция $f_{раз.}$ сформированная в соответствии с методом [7] имеет лучшие значения по сравнению с булевой функцией f_{lili}, используемой в алгоритме поточного шифрования LILI – II. Действительно, по алгебраической степени функции, алгебраической степени каждой переменной, числу термов, значению функции автокорреляции и абсолютному значению корреляции сформированная булева функция имеет лучшие показатели. Кроме того, сформированная булева функция имеет высокий показатель нелинейности, приближающийся к теоретической верхней границе нелинейности ($N_{верх.} = 2014$) и удовлетворяет строгому лавинному критерию.

На основе использования сформированной высоконелинейной булевой функции предлагается схема поточного шифрования информации в АСУВ. В качестве прототипа использовалась схема LILI – II.

Разработанная схема содержит (рис. 2): линейный рекуррентный регистр $ЛРР_C$, для управления движением с многочленом обратной связи (1); блок функционального преобразования f_C, для реализации функционального преобразования (2); линейный рекуррентный регистр $ЛРР_d$, для генерации данных с многочленом обратной связи (3); блок функционального преобразования f_d, для реализации функционального преобразования сгенерированных данных с использованием высоконелинейной булевой функции над V_{12}.

Криптографическое преобразование выполняется аналогично рассмотренной выше схеме, представленной на рис. 1. Основное отличие состоит в выполнении функционального преобразования в блоке функционального преобразования f_d. В предлагаемой схеме используется высоконелинейная булева функция над V_{12}, сформированная в соответствии с разработанным в [7] методом. Основные криптографические свойства поточного криптографического преобразования соответствуют данным, приведенным в табл. 1.

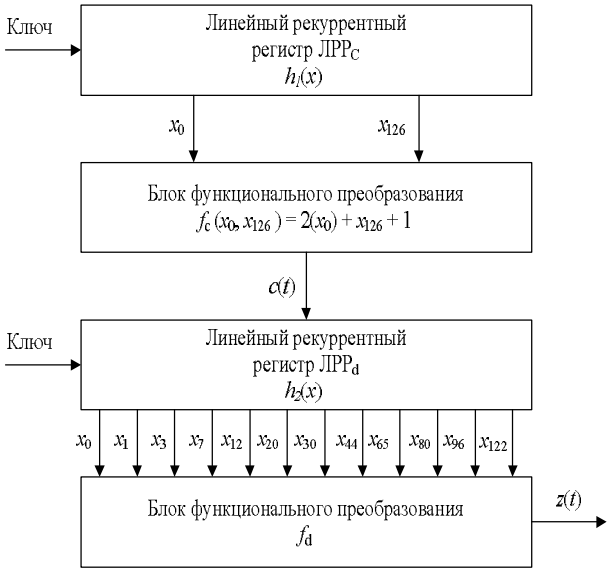

Рис. 2, Схема поточного криптографического преобразования с использованием сформированной высоконелинейной булевой функции

Выводы

Применение высоконелинейных булевых функций для схем поточного шифрования информации в АСУВ позволяет эффективно реализовать поточную криптографическую обработку информации. Наряду с простотой реализации этот подход позволяет обеспечить высокую устойчивость схем поточного шифрования к известным атакам противника.

Исследования эффективности поточного криптопреобразования информации в АСУВ с использованием сформированной высоконелинейной булевой функции показали, что по большинству показателей и критериев предлагаемая схема превосходит ближайший аналог – схему поточного шифрования LILI – II. Сформированная криптографическая функция над V_{12} обладает высоким показателем нелинейности, имеет максимально достижимую алгебраическую степени, удовлетворяет строгому лавинному критерию, имеет удовлетворительные корреляционные свойства. Кроме того, по показателю автокорреляции и абсолютному значению корреляции сформированная булева функция существенно превосходит лучшие известные аналоги.

Перспективным направлением дальнейших исследований является исследование устойчивости предлагаемой схемы поточного преобразования информации к известным методам криптоанализа.

Список литературы

1. ДСТУ В 3265 – 95. Зв'язок військовий. – К.: Укр-НДІССІ, 1995. – 23 с.

2. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М.: Изд-во стандартов. – 1989. – 18 с.

3. National Institute of Standards and Technology, "FIPS-46-3: Data Encryption Standard." Oct. 1999. Available at http://csrc.nist.gov/publications/fips.

4. National Institute of Standards and Technology, "FIPS-197: Advanced Encryption Standard." Nov. 2001. Available at http://csrc.nist.gov/publications/fips.

5. Шеннон К. Теория связи в секретных системах. – М.: Изд-во иностранной литературы. – 1963. – 604 с.

6. Final report of European project number IST-1999-12324 // New European Schemes for Signatures, Integrity and Encryption. – April 19, 2004 – 836 с.

7. Стасев Ю.В., Кузнецов О.О., Юкальчук А.А. Метод построения высоконелинейных булевых функций // Матеріали 2 НТК ХУ ПС. – Х.: ХУ ПС, 2006. – С. 86.

Поступила в редколлегию 21.09.2006

Рецензент: д-р техн. наук, проф. Ю.В. Стасев, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.