УДК 681.3.06

А.А. Кузнецов[1], И.В. Московченко[2]

[1]*Харьковский университет Воздушных Сил им. И. Кожедуба*
[2]*Харьковский институт танковых войск НТУ «ХПИ»*

ВЕРОЯТНОСТНАЯ МОДЕЛЬ СИНТЕЗА НЕЛИНЕЙНЫХ УЗЛОВ ЗАМЕН БЛОЧНЫХ СИММЕТРИЧНЫХ КРИПТОГРАФИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Исследуются модели и вычислительные методы формирования нелинейных узлов замен для симметричных криптографических средств защиты информации. Разрабатывается вероятностная модель формирования нелинейных узлов замен, в основе которой лежит вероятностный отбор криптографических функций с требуемыми показателями стойкости. Исследуется эффективность предложенного метода, показано, что его использование позволяет строить функции с наилучшими известными на сегодняшний день криптографическими профилями.

Ключевые слова: *защита информации, симметричные криптографические средства.*

Введение

Постановка проблемы в общем виде, анализ литературы. Наибольшее применение в комплексных системах защиты информации нашли симметричные криптографические средства, которые, в соответствии с классическими положениями теории секретных систем [1, 2], строятся на основе последовательного выполнения простых и вычислительно эффективных блоков преобразований (криптопримитивов): блоков нелинейных замен (блоков подстановок), блоков линейного рассеивания (блоков перестановок) и некоторых функциональных преобразований, например, сдвиг, сложение по модулю и пр.

Проведенный анализ показал, что на сегодняшний день в Украине нет отечественного стандарта симметричного криптографического преобразования информации, используемый советский стандарт ГОСТ 28147-89 устарел и не удовлетворяет современным требованиям [3 – 5].

Проводимый в настоящее время открытый конкурс симметричных криптографических алгоритмов [6] направлен на обоснование моделей и методов построения отдельных узлов симметричных криптографических средств защиты информации, обоснование принципов построения и отбор перспективных алгоритмов-кандидатов, на основе которых в дальнейшем может быть разработан национальный стандарт Украины.

Целью статьи является разработка вероятностной модели синтеза нелинейных узлов замен, основанной на вероятностном отборе формируемых криптографических булевых функций, удовлетворяющих накладываемой системе ограничений, что позволяет синтезировать нелинейные узлы замен с улучшенными свойствами для повышения эффективности симметричных криптографических средств защиты информации.

Разработка вероятностной модели формирования нелинейных узлов замен симметричных криптоалгоритмов

В соответствии с формальным аналитическим описанием и математической моделью [7] задача синтеза нелинейных блоков подстановок с улучшенными свойствами состоит в поиске совокупности компонентных криптографических булевых функций

$$F = \left(f_1\left(x_1,...,x_m\right), f_2\left(x_1,...,x_m\right),...,\right.$$
$$\left. f_u\left(x_1,...,x_m\right),...,f_n\left(x_1,...,x_m\right)\right\}:$$

$$\begin{cases} f_1(x_1,...,x_m) = c_{1,0} \oplus \bigoplus_{i=1}^{m} c_{1,i}x_i \oplus \bigoplus_{1\le i<j\le m} c_{1,ij}x_ix_j \oplus ... \oplus \\ \oplus c_{1,12...m}x_1x_2...x_m; \\ f_2(x_1,...,x_m) = c_{2,0} \oplus \bigoplus_{i=1}^{m} c_{2,i}x_i \oplus \bigoplus_{1\le i<j\le m} c_{2,ij}x_ix_j \oplus ... \oplus \\ \oplus c_{2,12...m}x_1x_2...x_m; \\ ... \\ f_u(x_1,...,x_m) = c_{u,0} \oplus \bigoplus_{i=1}^{m} c_{u,i}x_i \oplus \bigoplus_{1\le i<j\le m} c_{u,ij}x_ix_j \oplus ... \oplus \\ \oplus c_{u,12...m}x_1x_2...x_m; \\ ... \\ f_n(x_1,...,x_m) = c_{n,0} \oplus \bigoplus_{i=1}^{m} c_{n,i}x_i \oplus \bigoplus_{1\le i<j\le m} c_{n,ij}x_ix_j \oplus ... \oplus \\ \oplus c_{n,12...m}x_1x_2...x_m; \end{cases}$$

задающих функциональное соответствие множества входных векторов $A = \left\{A_1, A_2, ..., A_i, ..., A_{2^m}\right\}$, $A_i = \left(a_1^{(i)}, a_2^{(i)}, ..., a_m^{(i)}\right) \in A$, $a_j^{(i)} \in GF(2)$ и множества выходных векторов $B = \left\{B_1, B_2, ..., B_i, ..., B_{2^n}\right\}$, $B_i = \left(B_1^{(i)}, B_2^{(i)}, ..., B_n^{(i)}\right) \in B$, $B_j^{(i)} \in GF(2)$ и удовлетворяющих системе ограничений на отдельные криптографические показатели: $\left\{Сб_f, N_f \ge N_{тр}, КИ(k_1), КР(k_2), AC_f \le AC_{тр}\right\}$, где $Сб_f$ – требование сбалансированности; N_f – значение нелинейности, $КИ_f(k_1)$ – степень корреляционного иммунитета, $КР_f(k_2)$ – степень критерия распространения, AC_f – значение автокорреляция, $N_{тр}$ – требуемое значение нелинейности, k_1 – требуемая степень корреляционного иммунитета, k_2 – требуемая степень критерия распространения, $AC_{тр}$ – требуемое значение автокорреляции. Кроме того, соответствующей системе ограничений должны так же удовлетворять и компонентные булевы функции $\bar{f}_i(x_1,...,x_m)$ из множества $\bar{F} = \left\{\bar{f}_1(x_1,...,x_m), \bar{f}_2(x_1,...,x_m), ..., \bar{f}_u(x_1,...,x_m), ..., \bar{f}_{2^n-1}(x_1,...,x_m)\right\}$, полученные линейной комбинацией функций $f_i(x_1,...,x_m)$ из множества F.

Критерии и показатели стойкости криптографических функций определяются следующими положениями [8 – 10].

Функция f над $GF(2^n)$ является сбалансированной ($Сб_f$), если ее выходные значения являются равновероятными:

$$| \{x \mid f(x) = 0\} | = | \{x \mid f(x) = 1\} | = 2^{n-1}.$$

Нелинейность функции N_f - минимальное расстояние Хэмминга N_f между функцией f и всеми аффинными функциями над $GF(2^n)$:

$$N_f = \min \{d(f,\varphi)\},$$

где φ – множество аффинных функций.

Функция f над полем $GF(2^n)$ имеет корреляционный иммунитет порядка k, КИ(k), если ее преобразование Уолша удовлетворяет равенству $F(\omega) = 0$ для всех $\omega \in V_n$ таких, что $1 \le W(\omega) \le k$:

$$\forall \omega \in V_n; \quad F(\omega) = 0; \quad КИ(f) = k.$$

Функция f над полем $GF(2^n)$ удовлетворяет:

– критерию распространения относительно вектора α, КР(α), если функция $f(x) \oplus f(x \oplus \alpha)$ является сбалансированной, $x \in V_n$, где $x = (x_1, x_2, \ldots, x_n)$:

$$P(f(x) = f(x \oplus \alpha)) = 1/2;$$

– критерию распространения степени k, КР(k), если удовлетворяется критерий распространения относительно всех векторов $\alpha \in V_n$ при $1 \le W(\alpha) \le k$:

$$P(f(x) = f(x \oplus \alpha)) = 1/2 \ \forall \alpha : 1 \le W(\alpha) \le k;$$

– строгому лавинному критерию, СЛК, если f удовлетворяет критерию распространения степени 1:

$$P(f(x) = f(x \oplus \alpha)) = 1/2 \ \forall \alpha : W(\alpha) = 1.$$

Алгебраическая степень deg(f) является степенью самого длинного слагаемого функции, представленной в алгебраической нормальной форме.

Синтез нелинейного узла замен предлагается реализовать итеративной процедурой поэлементного вероятностного формирования множества F с последовательной проверкой криптографических свойств функций на соответствие установленной системе ограничений. Соответствующая вероятностная модель формирования нелинейного узла замен описывается следующими структурными элементами (рис. 1):

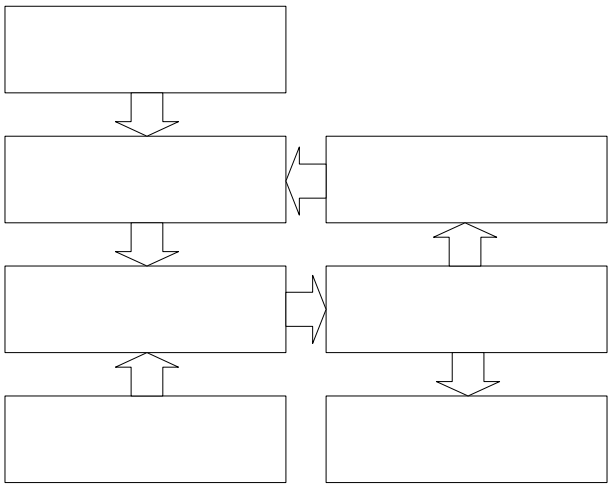

Рис. 1. Основные элементы вероятностной модели формирования нелинейных узлов замен с улучшенными свойствами

1. *Система ограничений по нелинейности и автокорреляции криптографических булевых функций*. Используется как исходная информация, задающая основные параметры вычислительного метода формирования криптографических булевых функций посредством градиентного поиска.

2. *Процедуры вычислительного поиска криптографической булевой функции методом градиентного спуска*. По введенным ограничениям с ис-

пользованием метода градиентного спуска осуществляется вероятностный поиск булевой функции. Результатом является случайно сформированная булева функция, удовлетворяющая требуемым значениям нелинейности и автокорреляции.

3. *Система ограничений на компонентные криптографические булевы функции и их линейные комбинации*. Используется как исходная информация, задающая основные параметры отбора случайно формируемых булевых функций, удовлетворяющих требуемым значениям нелинейности и автокорреляции.

4. *Процедуры проверки выполнения системы ограничений на компонентные функции и их линейные комбинации*. Формируемые булевы функции с требуемыми значениями нелинейности и автокорреляции подвергаются проверке на соответствие системным требованиям, т.е. на пригодность использования в совокупности с другими булевыми функциями.

5. *Процедуры отбора функций, удовлетворяющих заданным требованиям*. Функции, прошедшие проверку на соответствие системным требованиям отбираются для дальнейшего использования в нелинейном узле замен.

6. *Процедуры отбраковки функций, не удовлетворяющих заданным требованиям и формирование запроса на следующую функцию*. Функции, не прошедшие проверку на соответствие системным требованиям отбраковываются (не используются). Формируется запрос на вероятностный поиск следующей булевой функции с помощью метода градиентного спуска.

7. *Формирование множества компонентных криптографических булевых функций и соответствующей таблицы замен*. Из отобранных по критерию соответствия системным требованиям булевых функций формируется множество F, соответствующая таблица замен и синтезируется устройство, реализующее заложенную в него логику преобразований.

В основе вычислительного поиска криптографических булевых функций лежит итеративная процедура комплементации позиций бент-последовательностей для градиентного спуска по критерию максимизации минимального расстояния по Хеммингу между формируемыми последовательностями и последовательностями всех линейных функций, что позволяет с меньшими вычислительными затратами реализовать поиск булевых функций с требуемыми криптографическими свойствами. Графическая интерпретация предлагаемой итеративной процедуры представлена на рис. 2.

На рисунке жирными точками и символами «$L_i(x)$» схематично представлены последовательности линейных функций (как элементы векторного пространства V_{2^n}). Несбалансированная последовательность бент-функции, обладающая максимально достижимой нелинейностью (что эквивалентно максимальному расстоянию по Хеммингу к последовательностям линейных функций) представлена на рисунке под номером 1. После расчета необходимого числа комплементаций бент-последовательности на первом шаге выполняется преобразование Уолша-Адамара и определяется максимальное расстояние по Хеммингу к одной или нескольким последовательностям линейных функций $L_i(x)$. Эта операция соответствует выбору нулевых значений коэффициентов преобразования Уолша-Адамара. В данном случае на первом шаге максимальное расстояние к функции $L_2(x)$. Далее производится инвертирование элементов последовательности бент-функции, совпадающих с элементами выбранных последовательностей линейных функций. Графически это можно представить в виде градиентного смещения последовательности из точки 1 в точку 2 (по направлению к функции $L_2(x)$). В результате выполнения последней операции несбалансированность функции снижается, но снижается также и нелинейность, т.е. последовательность функции не является уже максимально отдаленной от последовательностей линейных функций $L_i(x)$.

На следующей итерации все операции повторяются. Сначала выполняется преобразование Уолша-Адамара и определяется максимальное расстояние по Хеммингу к одной или нескольким последовательностям линейных функций $L_i(x)$, производится инвертирование элементов последовательности, совпадающих с элементами выбранных последовательностей линейных функций. На этом шаге максимальное расстояние по Хеммингу к последовательности функции $L_{16}(x)$, а снижение несбалансированности приводит к смещению последовательности по направлению к $L_{16}(x)$ в точку 3. После итеративного выполнения операций вычислительного поиска формируется сбалансированная функция с незначительно сниженной нелинейностью (точка 4). Таким образом, в качестве критерия градиентного поиска криптографических функций является максимизация минимального расстояния по Хеммингу формируемой последовательности и последовательностей линейных функций.

Проведем оценку среднего числа попыток K_{cp}, необходимых для формирования криптографических булевых функций с требуемыми значениями нелинейности и автокорреляции последовательностей. На рис. 3 представлены зависимости: метод случайной генерации с 1) АС = 80 и 2) АС = 120; известный метод градиентного поиска [8-10] с 3) АС = 24 и 4) АС = 32; предложенный метод градиентного спуска [11] с 5) АС = 24 и 6) АС = 32.

Анализ приведенных зависимостей показывает, что предложенный подход обладает улучшенными свойствами – существенно меньшей вычислительной сложностью. Практически это означает, что предлагаемый метод позволяет формировать булевы функции с высокими криптографическими показателями (нелинейностью и автокорреляцией) за меньшее число попыток (в среднем).

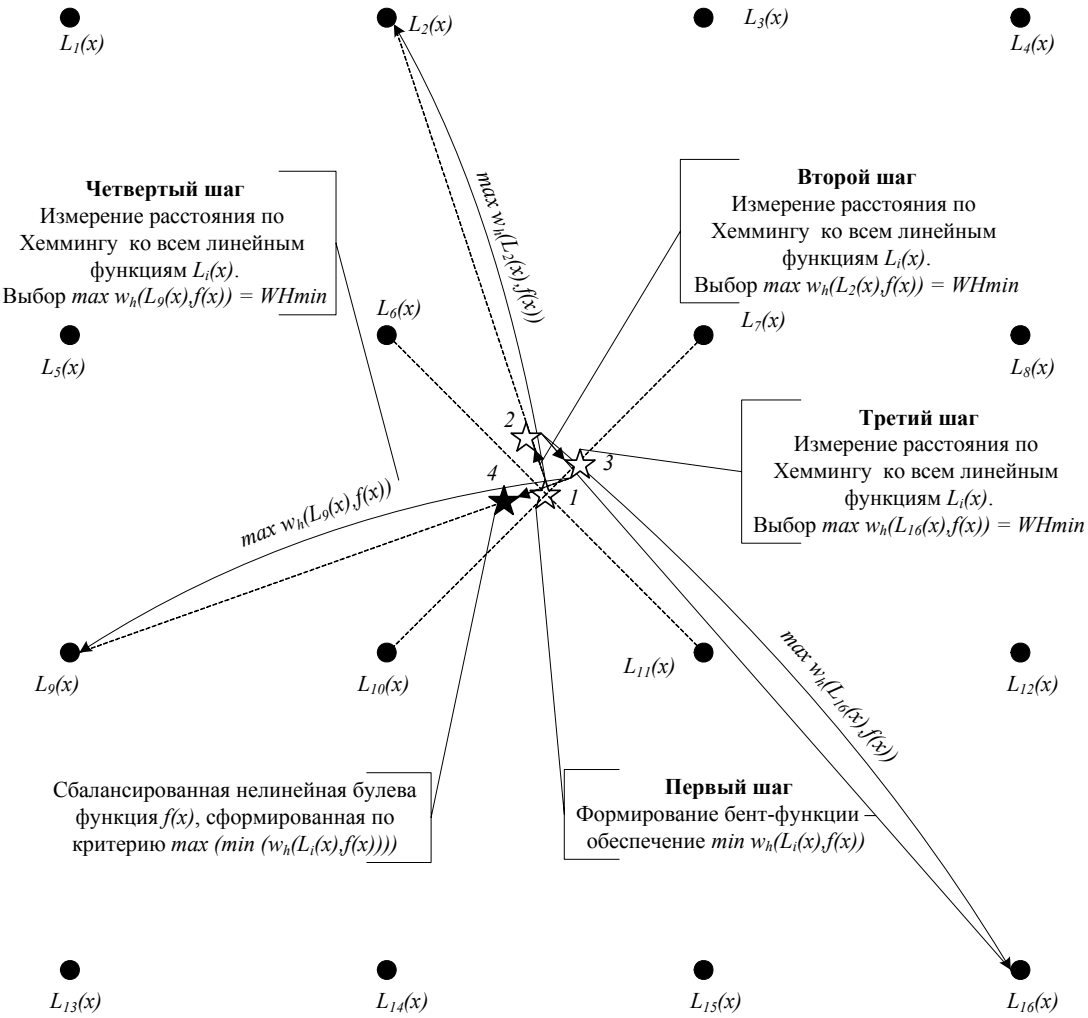

Рис. 2. Графическая интерпретация вычислительного поиска

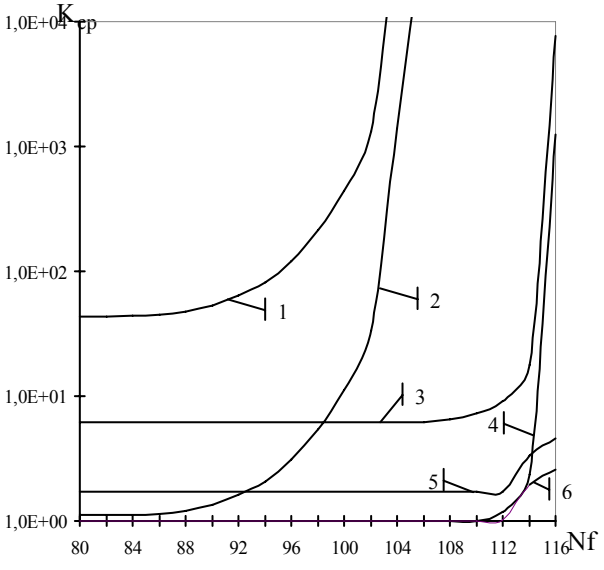

Рис. 3. Зависимости среднего числа попыток формирования криптографической функции с требуемыми свойствами

Так, например, формирование криптографической функции с АС = 24 и N = 116 для метода случайной генерации вычислительно недостижимо по причине чрезвычайно высокого среднего числа попыток. Для тех же параметров метод-прототип (метод градиентного поиска) потребует в среднем около 8000 попыток. Предложенный метод при тех же показателях потребует в среднем 4 попытки, т.е. среднее число попыток снизилось в 2000 раз. При требованиях к криптографическим свойствам АС = 24 и N=114 метод-прототип потребует в среднем около 15 попыток, а предложенный метод – около 3.

В табл. 1 приведены сравнительные характеристики основных показателей стойкости функций, полученных с использованием разработанного и наилучших известных эвристических методов.

Как видно из приведенной таблицы, разработанный метод позволяет строить функции с наилучшими известными на сегодняшний день профилями. Функции, построенные над V_6, V_8 имеют сопоставимые показатели стойкости с известными ранее; функции, построенные ранее над V_{10}, имели наилучший профиль (10, 9, 484, 56), теперь данный профиль имеет вид (10, 9, 488, 40) (увеличена нелинейность, уменьшена автокорреляция в 1,4 раза); функции, построенные над V_{12}, имели наилучший профиль (12, 10, 1992, 156), теперь данный профиль имеет вид (12, 11, 2002, 72) (значительно увеличена нелинейность, значение автокорреляции уменьшено в 2,2 раза).

Таблица 1

Наилучшие известные профили (n, deg(f), N_f, AC)

NLT	(5,3,12,8) (5,4,12,16)	(6,5,26,16)	(7,6,56,16)	(8,7,116,24) (8,5,112,16)
	(9,8,238,40)	(10,9,486,72) (10,9,484,64)	(11,9,984,96) (11,10,982,96)	(12,10,1992,156) (12,10,1990,144)
ACT	(5,3,12,8) (5,4,12,16)	(6,5,26,16)	(7,6,56,16)	(8,7,116,24) (8,5,112,16)
	(9,8,238,40)	(10,9,484,56)	(11,10,982,88)	(12,11,1986,128)
Разработанный метод	–	(6,5,26,16)	–	(8,7,116,24)
	–	**(10,9,488,40)**		**(12,11,2002,72)**

Выводы

В результате проведенных исследований показано, что использование предложенной вероятностной модели построения нелинейных узлов замен позволяет формировать блоки нелинейной подстановки для симметричных криптографических средств защиты информации. Установлено, что формируемые таким образом нелинейные узлы замен обладают улучшенными свойствами, их применение в симметричных криптографических средствах защиты информации позволяет улучшить показатели статистической безопасности.

Список литературы

1. Шеннон К. Теория связи в секретных системах / К. Шеннон // Работы по теории информации и кибернетике. – М.: Изд-во иностр. литер., 1963. – С. 333-402.

2. Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption, April 19, 2004 – Version 0.15 (beta), Springer-Verlag.

3. National Institute of Standards and Technology, "FIPS-197: Advanced Encryption Standard." Nov. 2001. – [Електронний ресурс]. – Режим доступу к документу: http://csrc.nist.gov/publications/fips/ fips197/fips-197.pdf.

4. Винокуров А. Сравнение российского стандарта шифрования, алгоритма ГОСТ 28147-89, и алгоритма Rijndael, выбранного в качестве нового стандарта шифрования США / А. Винокуров, Э. Применко // Системы безопасности. – М.: Гротэк, 2001.– №№ 1, 2. – С. 37-41.

5. Сергиенко Р.В. Исследование криптографических свойств нелинейных узлов замен алгоритма симметричного шифрования ГОСТ 28147-89 / Р.В. Сергиенко, И.В. Московченко // Системи обробки інформації: зб. наук. пр. – Х.в: ХУ ПС, 2007. – Вип. 8 (66). – С. 91-95.

6. Повідомлення організаційного комітету по проведенню відкритого конкурсу криптоалгоритмів про припинення прийому заявок на участь у конкурсі. – [Електронний ресурс]. – Режим доступу до сайту: http://dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=49027&cat_id=38710.

7. Кузнецов А.А. Разработка предложений по совершенствованию симметричных средств защиты информации перспективной системы критического применения / А.А. Кузнецов, И.В. Московченко // Радіоелектронні і комп'ютерні системи. Науково-технічний журнал – Х.: НАКУ «ХАИ», 2008. – № 2 (29). – С. 94-100.

8. Maier W. Nonlinearity criteria for cryptographic functions. In Advances in Cryptology / W. Maier, O. Staffelbach // In Proceedings of EUROCRYPT'89. – 1990. – Vol. 434, Lecture Notes in Computer Science, Springer-Verlag. – P.549-562.

9. Millan, W. Heuristic Design of Cryptographically Strong Balanced Boolean Functions, Advances in Cryptology / W. Millan, A. Clark, E. Dawson // In Proceedings of EUROCRYPT'98. – 1998. – LNCS Vol. 1403. Springer Berlin Heidelberg New York. – P. 489.

10. Pasalic E. Further results on the relation between nonlinearity and resiliency of Boolean functions / E. Pasalic, T. Johansson // In Proc. IMA Conf. Cryptography and Coding (Lecture Notes in Computer Science). – New York: Springer-Verlag, 1999. – Vol. 1746. – P. 35-45.

11. Кузнецов А.А. Метод построения криптографически стойких булевых функций на основе градиентного спуска / А.А. Кузнецов, Ю.А. Избенко, И.В. Московченко // Зб. наук. пр. ХУ ПС. – Х., 2007. – Вип. 1 (13). – С. 63-66.

Поступила в редколлегию 18.12.2008

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

ІМОВІРНІСНА МОДЕЛЬ СИНТЕЗУ НЕЛІНІЙНИХ ВУЗЛІВ ЗАМІН БЛОКОВИХ СИМЕТРИЧНИХ КРИПТОГРАФІЧНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

О.О. Кузнєцов, І.В. Московченко

Досліджуються моделі і обчислювальні методи формування нелінійних вузлів замін для симетричних криптографічних засобів захисту інформації. Розроблено імовірнісну модель формування нелінійних вузлів замін, в основі якої лежить імовірнісний відбір криптографічних функцій з необхідними показниками стійкості. Досліджується ефективність запропонованого методу, показано, що його використання дозволяє будувати функції з якнайкращими відомими на сьогоднішній день криптографічними профілями.

Ключові слова: *захист інформації, симетричні криптографічні засоби.*

PROBABILISTIC MODEL OF SYNTHESIS OF NONLINEAR KNOTS OF REPLACEMENTS OF SECTIONAL SYMMETRIC CRYPTOGRAPHIC FACILITIES OF DEFENCE OF INFORMATION

A.A. Kuznetsov, I.V. Moskovchenko

Models and calculable methods of forming of nonlinear knots of replacements are explored for symmetric cryptographic facilities of defence of information. The probabilistic model of forming of nonlinear knots of replacements is developed, in basis of which the probabilistic selection of cryptographic functions lies with the required indexes of firmness. Efficiency of the offered method is explored, it is shown that his use allows to build functions with the best cryptographic types known for today.

Keywords: *defence of information, symmetric cryptographic facilities.*