УДК 681.3.06

С. А. ГОЛОВАШИЧ

МЕТОД ПОСТРОЕНИЯ УПРАВЛЯЕМЫХ S-БЛОКОВ С ПРЕДЕЛЬНЫМИ ПОКАЗАТЕЛЯМИ НЕЛИНЕЙНОСТИ

Опыт эксплуатации открытых информационно–телекоммуникационных систем свидетельствует о необходимости обеспечения в таких системах функций целостности и конфиденциальности передаваемой информации. Указанные функции могут быть обеспечены применением средств криптографической защиты информации. Задача разработки современных криптоалгоритмов может быть разбита на ряд подзадач проектирования отдельных компонентов криптопреобразования. Рассмотрим один из вариантов решения подзадачи построения криптографически стойких элементарных нелинейных преобразований (S-блоков).

В настоящее время известно четыре критерия [1] оценки стойкости алгоритмов блочного симметричного шифра (БСШ) к атакам криптоанализа цикловой функции.

1) точный критерий;
2) теоретический критерий;
3) практический критерий;
4) эвристический критерий.

На практике наиболее применимым является практический критерий [1]. Он заключается в оценке нижней границы сложности криптоанализа алгоритма на основе отдельной криптоаналитической характеристики.

1. Практический критерий оценки стойкости БСШ

Устойчивость БСШ к большинству атак криптоанализа цикловой функции определяется соответствующими показателями нелинейности отдельного S-блока, а также минимальным количеством «активных» S-блоков, задействованных в «лучшей характеристике».

Если предположить, что цикловая функция состоит из однотипных S-блоков, тогда оценка устойчивости БСШ к различным атакам криптоанализа цикловой функции может быть сведена к оценке параметров нелинейности отдельного S-блока. Так, нижняя граница сложности выполнения некоторой атаки криптоанализа БСШ может быть оценена как

$$h_f = h_s^a, \quad h_e = h_f^{c\times(r-q)} \quad \Rightarrow \quad h_e = h_s^{c\times(r-q)\times a},$$

где h_s, h_f, h_e – показатели, определяющие верхнюю границу устойчивости к некоторому методу криптоанализа соответственно для отдельного S-блока, цикловой функции и полного алгоритма БСШ; a – минимальное количество «активных» S-блоков в составе одной цикловой функции (в контексте некоторой атаки); r – общее количество циклов шифрования; c – коэффициент «активизации» циклов, определяющий отношение минимального числа «активных» циклов к общему числу циклов; q – количество циклов «отбрасываемых» в результате применения *NR*-атаки.

Отметим, что для случая наиболее эффективных атак дифференциального и линейного криптоанализа в качестве показателей стойкости выступают, соответственно, вероятности «фиксированного трансформирования» разности и линейной аппроксимации.

Алгоритм может считаться практически стойким к некоторой криптоатаке, если справедливо $h_e > p_e$, где p_e – предельная сложность «силовой атаки» (обычно $p_e = 2^{\pm n}$ либо $p_e = 2^{\pm k}$, где n – разрядность блока данных, k – разрядность ключа). Таким образом, если максимально достижимое, для выбранной разрядности S-блока, значение показателя устойчивости к некоторой атаке обозначить p_S, то минимальное число циклов шифрования, необходимых для достижения безопасности по практическому критерию, можно определить из соотношения:

$$r = \left\lceil \left(\log_{p_S} p_e\right) \Big/ (c \times a) \right\rceil + q .$$

Для построения шифра, достигающего границы устойчивости к аналитическим атакам (по практическому критерию) за минимальное число циклов, необходимо, чтобы значения показателей стойкости отдельного S-блока были максимальными (при условии фиксированной структуры циклового преобразования).

2. Показатели нелинейности S-блоков

Рассмотрим качественные и количественные показатели S-блоков, определяющие устойчивость алгоритма к известным атакам криптоанализа цикловой функции. При этом будем предполагать, что наиболее эффективные линейные и дифференциальные характеристики могут быть построены в контексте групповой операции сложения по модулю 2 (XOR).

1. Биективность.

Для защиты от простых статистических атак, S-блоки должны удовлетворять требованию *эластичности* [2], т.е. пространство выходов S-блока не должно содержать запрещённых значений, и все выходные значения должны быть равновероятны. В случае равенства разрядности входа и выхода, это требование означает биективность.

Кроме того, для шифра на базе биективной f-функции, сложность дифференциального и линейного криптоанализа как по теоретическому, так и по практическому критериям, будет меньше, чем для случая небиективной f-функции [1,3]. Задача построения биективной f-функции на основе SPN- либо SLTN- структуры имеет тривиальное решение в случае применения биективных S-блоков, поэтому дальше мы сосредоточим своё внимание исключительно на биективных S-блоках ($\mathrm{F}_2^n \to \mathrm{F}_2^n : x \mapsto S(x)$).

2. Максимальная вероятность дифференциальной характеристики S-блока $P_S^{<dc>}$.

Данный показатель определяется по таблице распределения дифференциальных разностей S-блока [4]. Индексы по строкам и столбцам этой таблицы соответствуют входной Δx и выходной Δy разностям, а элементы $\delta(\Delta x, \Delta y)$ в ячейках таблицы соответствуют количеству случаев выполнения перехода $\Delta x \to \Delta y$ на полном пространстве аргументов x:

$$\delta_{\max} = \max_{(\Delta x \neq 0, \Delta y) \in \mathrm{F}_2^n} \#\left\{ x \in \mathrm{F}_2^n \;\middle|\; \left(S(x) + S(x + \Delta x)\right) = \Delta y \right\}, \quad P_S^{<dc>} = \delta_{\max} / 2^n .$$

3. Максимальная вероятность линейной аппроксимации S-блока $P_S^{<lc>}$.

Данный показатель определяется по таблице отклонений линейных аппроксимаций S-блока [5]. Индексы по строкам и столбцам этой таблицы соответствуют входному Λx и выходному Λy шаблонам (маскам), а элементы $\lambda(\Lambda x, \Lambda y)$ в ячейках таблицы соответствуют величине *отклонения* (от среднего значения) количества случаев выполнения соответствующей линейной аппроксимации, на полном пространстве аргументов x:

$$\lambda_{\max} = \max_{(\Lambda x, \Lambda y \neq 0) \in \mathrm{F}_2^n} \left| \#\left\{ x \in \mathrm{F}_2^n \;\middle|\; x \cdot \Lambda x = S(x) \cdot \Lambda y \right\} - 2^{n-1} \right|, \quad P_S^{<lc>} = \left(2 \times \lambda_{\max} / 2^n \right)^2 .$$

4. Максимальная вероятность отклонения «критерия распространения» $P_S^{<pc>}$.

Показатель определяется как максимальное отклонение (от среднего значения) вероятности изменения суммы некоторого не пустого множества Λ выходов S-блока под действием фиксированной разности Δ на его входе [6]:

$$\xi_{\max} = \max_{(\Delta \neq 0,\ \Lambda \neq 0) \in \mathrm{F}_2^n} \left| \#\left\{ x \in \mathrm{F}_2^n \;\middle|\; \Lambda \cdot S(x) = \Lambda \cdot S(x \oplus \Delta) \right\} - 2^{n-1} \right|, \quad P_S^{<pc>} = \xi_{\max} / 2^n .$$

5. Максимальная вероятность «частичного однобитного» дифференциала $P_S^{<td>}$.

Показатель оценивает степень не равновероятности «активизации» некоторого бита выходной разности при «активизации» или «не активизации» некоторого бита входной разности:

$$\mu_{\max} = \max_{\substack{\Delta x, \Delta y \in \mathrm{F}_2, \\ 0 \le i, j < n}} \left| \#\left\{ x, \Delta \in \mathrm{F}_2^n \;\middle|\; \Delta x = [\Delta]_i,\ \Delta y = \left[S(x) \oplus S(x \oplus \Delta) \right]_j \right\} - 2^{2n-2} \right|, \quad P_S^{<td>} = \mu_{\max} / 2^{2n},$$

где операция $[x]_i$ возвращает значение i-го разряда вектора x.

6. Минимальная алгебраическая степень булевых полиномов S-блока $\deg_y(S)$.

Алгебраическая степень S-блока определяется по минимальной степени булевых полиномов s_i, соответствующих отдельным выходным разрядам S-блока: $y_i = s_i(x_0,\ldots,x_{n-1})$, т.е. $s_i: \mathrm{F}_2^n \to \mathrm{F}_2$:

$$\deg_y(S) = \min_{0\le i<n} \deg(s_i).$$

7. Минимальная алгебраическая степень переменных булевых полиномов S-блока $\deg_x(S)$.

Минимальная алгебраическая степень аргументов S-блока определяется по минимальному значению степени $\deg_{x_j}(s_i)$ каждой из переменных x_j булевого полинома s_i каждого из выходов S-блока:

$$\deg_x(S) = \min_{0\le i<n,\, 0\le j<n} \deg_{x_j}(s_i).$$

8. Минимальное количество термов булевого полинома S-блока $\mathrm{term}(S)$.

Показатель определяется как минимальное количество термов в булевых полиномах s_i, соответствующих отдельным выходным разрядам y_i S-блока:

$$\mathrm{term}(S) = \min_{0\le i<n} \mathrm{term}(s_i),$$

где $\mathrm{term}(s_i)$ – количество термов в полиноме s_i.

9. Минимальное количество термов булевого полинома S-блока, содержащих некоторую переменную $\mathrm{term}_x(S)$.

Показатель определяется как минимальное количество термов в булевых полиномах s_i, соответствующих отдельным выходным разрядам y_i S-блока, содержащих каждую из переменных x_j, т.е.:

$$\mathrm{term}_x(S) = \min_{0\le i<n,\, 0\le j<n} \mathrm{term}_{x_j}(s_i).$$

При выборе конструкции S-блока необходимо обеспечить выполнение показателя 1, а также стремиться к минимизации показателей 2–5 и максимизации показателей 6–9 вплоть до предельно достижимых значений. Рассмотренные показатели дальше будем называть *показателями нелинейности*. Отметим, что показатели 6,7 отражают устойчивость алгоритма к атаке криптоанализа методом дифференциалов высших порядков, а показатели 8, 9 — к интерполяционной атаке.

3. Предельно нелинейные S-блоки

Для защиты от атак криптоанализа цикловой функции S-блоки должны удовлетворять определённым ограничениям на перечисленные выше показатели нелинейности.

Задача формирования S-блоков, удовлетворяющих определённым требованиям, является не тривиальной и может решаться двумя способами:

1) формирование случайных подстановок и проверка показателей их нелинейности;

2) построение S-блоков в соответствии с некоторой конструкцией, обеспечивающей удовлетворение соответствующим требованиям.

Первый способ является более универсальным, однако менее эффективным. В соответствии со вторым способом, можно сравнительно просто построить подстановки, удовлетворяющие только некоторому подмножеству требований, предъявляемых к S-блокам. Поэтому для построения S-блоков предлагается использовать комбинированную методику, включающую оба подхода.

В качестве основы для построения S-блока воспользуемся *«биективными предельно нелинейными преобразованиями»*, которые представляют собой биективные преобразования, обладающие свойствами предельно близкими к свойствам *«совершенно нелинейных (или бент-) преобразований»* [7]. Использование в качестве основы преобразований указанного вида позволяет получить предельно достижимые, для выбранной разрядности, значения 2 - 4-го показателей нелинейности. При этом, если S-блок имеет нечётную разрядность, то соответствующее преобразование является *«почти совершенно нелинейным»* [7].

Особый интерес среди конструкций «биективных предельно нелинейных преобразований» представляет конструкция Динга [8] (или её частный случай – конструкция Ниберг [9]), которая сочетает

свойства «предельной нелинейности» и максимальной алгебраической степени (показатель 6). Эта конструкция имеет вид

$$S(x) = x^{2^n - 2^i}, \quad 1 \le i < n, \quad x \in \mathrm{F}_{2^n},$$

где в качестве полинома, образующего поле может использоваться любой неприводимый полином степени n над $\mathrm{F}_2[x]$. В конструкции Ниберг [9] используется случай ($i = 1$), т.е. вычисление обратного элемента. Эта конструкция была использована разработчиками алгоритма Rijndael [10], победителя проекта AES [11].

Несмотря на достижение предельных значений 2–4 и 6-го показателей нелинейности, а также выполнение условия биективности (показатель 1), конструкция Ниберг–Динга не гарантирует получение оптимальных значений показателей 5–9. Однако известно [9], что группой симметрии «совершенно нелинейных» и «предельно нелинейных» преобразований является множество аффинных невырожденных преобразований, т.е. показатели нелинейности 2–4, а также 1 и 6 не зависят от вида (наличия) аффинного невырожденного преобразования на входе и/или выходе базового преобразования. При этом показатели 5, 7–9 зависят от линейных преобразований входа / выхода. Поэтому, используя в качестве основы конструкцию Ниберг–Динга, дополненную невырожденным аффинным преобразованием входа / выхода, можно получить конструкцию S–блока с оптимальными значениями показателей 5, 7–9. Таким образом, нелинейное преобразование, достигающее предельных значений по показателям 2–9, может быть описано следующим образом:

$$S(X) = \mathrm{M_y} \times \left[\left(\mathrm{M_x} \times X \oplus \mathrm{V_x} \right)^{2^n - 2} \right]_B \oplus \mathrm{V_y}, \quad X, \mathrm{V_x}, \mathrm{V_y} \in \mathrm{F}_2^n, \quad \mathrm{M_x}, \mathrm{M_y} \in \mathrm{GL}\left(n, \mathrm{F}_2\right),$$

где B – некоторый базис над $\mathrm{GF}(2^n)$, определяемый образующим (неприводимым) полиномом; $\times$ – операция матричного умножения; $\oplus$ – операция сложения векторов из F_2^n.

Отметим, что для упрощения записи, в последнем соотношении опущены операции транспонирования векторов, и предполагается, что преобразование «вектор-строка» $\leftrightarrow$ «вектор-столбец» выполняется «по умолчанию».

Фактические значения достижимых показателей нелинейности зависят от разрядности S-блока n. При выборе разрядности S-блока следует учитывать, что большая разрядность S-блоков позволяет «быстрее» (за меньшее число циклов) достигнуть необходимого уровня криптостойкости, однако ограничивающим фактором является сложность реализации многоразрядных S-блоков. На современных CPU, с приемлемой сложностью, фиксированный S-блок может быть реализован двумя способами:

1) табличным (разрядность 4-12 бит);
2) аналитическим (разрядность 4 бита).

В силу байт-ориентированности большинства современных процессоров наиболее эффективно табличным способом могут быть реализованы байтовые подстановки (8→8 бит). Кроме того, длина полного блока данных обычно является степенью 2 и желательно, чтобы длина S-блока делила длину блока.

Применение аналитического способа (вычисление булевых выражений) оправдано только на процессорах большой разрядности (64 и больше бит), позволяющих распараллелить вычисление соответствующего числа S-блоков. С другой стороны, учитывая, что табличный способ выполняет нелинейное смешивание последовательно расположенных битов некоторого регистра («слова» в памяти), достоинством аналитического способа реализации является *межрегистровое* нелинейное смешивание битов блока без применения дополнительных операций перестановки битов.

Таким образом, наиболее предпочтительными, с точки зрения простоты реализации, являются 4-х и 8-ми битные S-блоки. Предельные значений показателей 2–4 и 6 (обеспечиваемые конструкцией Ниберг–Динга), для выбранных разрядностей, приведены в табл. 1. Оценка предельных значений показателей 5, 7–9, достижимых на базе конструкции Ниберг–Динга, была выполнена экспериментально. Полученные значения приведены в табл. 2. Соответствующие вероятности приведены в табл. 3. Кроме того, в качестве дополнительного требования использовалось ограничение максимальной вероятности «однобитного перехода» значением 2^{1-n}, т.е.

$$W_H(\Delta x) = W_H(\Delta y) = 1 : \delta(\Delta x, \Delta y) = 2,$$

а также «отбраковывались» S-блоки, имеющие «фиксированные точки», т.е. $S(x) = x$.

Таблица 1

Разрядность	δ_{max}	λ_{max}	ξ_{max}	$\deg_y(S)$
4 бита	4	4	4	3
8 бит	4	16	16	7

Таблица 2

Разрядность	μ_{max}	$\deg_x(S)$	$\mathrm{term}_y(S)$	$\mathrm{term}_x(S)$
4 бита	4	3	8	3
8 бит	196	7	124	56

Таблица 3

Разрядность	$P_S^{<dc>}$	$P_S^{<lc>}$	$P_S^{<pc>}$	$P_S^{<td>}$
4 бита	2^{-2}	2^{-2}	2^{-2}	2^{-6}
8 бит	2^{-6}	2^{-6}	2^{-4}	$49/2^{14}$

4. Управляемые S-блоки

Сложность построения многих криптоатак может быть существенно повышена, если шифр использует переменные (ключезависимые) подстановки (например, в ГОСТ 28147-89 [12] подстановки определяются долговременным ключом). При этом необходимо, чтобы используемые S-блоки выбирались из множества подстановок, удовлетворяющих ограничениям на рассмотренные выше показатели.

Группой симметрии для рассмотренных показателей S-блока будет являться множество операций инвертирования и перестановки входов и/или выходов. Т.е. указанные преобразования не влияют на рассмотренные показатели нелинейности S-блока. Если перестановку координат (битов) сделать управляемой цикловым ключом, то мы получим управляемый S-блок с фиксированными показателями криптостойкости. Назовём такое управляемое преобразование PS-блоком.

Выбирая конструкцию PS-блока, следует учитывать, что общее количество перестановок n элементов составляет $n!$, а для $n > 2$ указанное значение не может быть степенью 2, в то время как ключ, используемый для выбора одной из перестановок, будет числом в двоичной системе счисления, каждый бит которого равновероятно может принимать как значение 0, так и 1. Поэтому если для выбора перестановки битов (из полного множества) использовать ключ длиной $\lceil \log_2 n! \rceil$ или больше, то различные перестановки будут не равновероятны, что негативно скажется на статистической безопасности алгоритма.

Для решения этой проблемы можно ограничиться выбором перестановок из усечённого множества размерностью $2^k < n!$. Однако и в этом случае необходимо контролировать статистические параметры перестановки: негативной является ситуация, когда вероятности перестановки некоторого разряда в различные позиции зависят от позиции источника и/или получателя.

Для решения обоих указанных задач может использоваться следующая схема выбора перестановки по (двоичному) ключу. Предлагаемый алгоритм выбора перестановок основан на следующем свойстве.

Лемма 1. n различных перестановок может быть получено путём циклического сдвига (вращения) любой перестановки n элементов.

Так как любой фрагмент длиной k некоторой перестановки также является перестановкой k элементов, то к нему также применима лемма 1, и, следовательно, справедлива следующая лемма.

Лемма 2. Ни одна из новых $k_1 \times k_2 - 1$ перестановок, полученных различными циклическими сдвигами (вращением) двух не пересекающихся непрерывных фрагментов длиной k_1 и k_2 ($k_1, k_2 > 0$) некоторой перестановки длиной n ($n \geq k_1 + k_2 > 2$), не может быть получена из исходной перестановки путём применения любого из $n - 1$ не нулевого циклического сдвига.

Это связано с изменением «циклического» порядка расположения элементов исходной перестановки длины n при циклическом сдвиге любого её фрагмента.

Посредством итеративного применения лемм 1 и 2 (для случая $k_1 = 1$) можно сформировать все возможные $n!$ перестановок, однако для обеспечения равновероятности получения любой перестановки «управляющий сигнал» должен быть M-ичным.

Для динамического формирования 2^k различных перестановок из 2^m элементов, удовлетворяющих требованию равновероятности перестановки каждого элемента в любую позицию, на основе лемм 1 и 2 можно определить следующий алгоритм.

Алгоритм.

1) Присвоить $n = m$, $t = 1$, в качестве исходной взять тождественную перестановку длиной $N = 2^m$;
2) поместить указатель перестановки в её начало $p = 1$;
   поместить указатель «управляющей последовательности» в её начало $k = 1$;
3) на основе n разрядов «управляющей последовательности» выполнить циклический сдвиг 2^n соседних элементов перестановки;
4) сместить указатель в «управляющей последовательности» на n разрядов ($k = k + n$);
   сместить указатель позиции перестановки на 2^n элементов ($p = p + 2^n$);
5) $t = t - 1$, если $t > 0$, то перейти к пункту 3;
6) $n = n - 1$; $t = m - n + 1$;
7) если $n > 0$, то перейти к пункту 2, иначе выход.

Количество разрядов k, необходимое для задания всех 2^m перестановок указанного вида, можно определить из следующего соотношения

$$k = \sum_{1 \le i \le m} i \times 2^{m-i} . \qquad (1)$$

Схема «вращения» перестановки, в соответствии с последним алгоритмом, может быть представлена следующей диаграммой (см. рисунок).

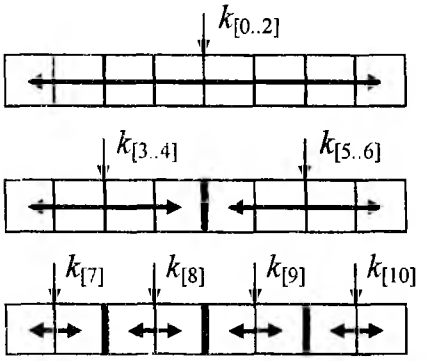

Рис.

Конструкция PS-блоков позволяет получить множество различных (ключезависимых) S-блоков с требуемыми характеристиками на основе одного нелинейного преобразования.

В соответствии с соотношением (1) для интересующих нас длин S-блоков можем определить длину (ключевой) «управляющей последовательности»: для $n = 4 \Rightarrow k = 4$, для $n = 8 \Rightarrow k = 11$.

Алгоритм выбора перестановки по ключу для $n = 4$ ($k = 4$) может быть реализован в виде булевых выражений, а для $n = 8$ ($k = 11$) — таблично. При этом в последнем случае для сокращения затрат памяти k может быть представлено в виде 8+3, где 8 бит (на диаграмме рис. 1 биты $k_{[3..10]}$) определяют вход в таблицу из 256 ячеек, содержащих по 8 элементов, содержащих номер позиции, в которую должен быть переставлен соответствующий бит. Оставшиеся 3 бита ключа (на диаграмме рис. 1 биты $k_{[0..2]}$) используются для определения величины сдвига содержимого выбранной ячейки.

Отметим, что направление циклического сдвига фрагмента перестановки значения не имеет, но для однозначности представления перестановки «управляющим сигналом» направление должно быть фиксированным.

Перестановки малого числа битов (например, четырёх) могут быть эффективно реализованы в виде матричного умножения:

$$x_i' = \bigoplus_{j=0}^{3} a_{i,j} \wedge x_j, \quad i = \overline{0,3}, \quad a_{i,j}, x_j \in \{0,1\},$$

где $A = \{a_{i,j}\}$ – матрица перестановки (т.е. содержит в каждой строке и столбце только по одной единице), и, если $a_{i,j} = 1$, то $x_i' = x_j$.

В соответствии с соотношением (1) получаем, что общее количество матриц перестановки 4 элементов составляет $2^4 = 16$. Если в качестве «управляющего сигнала» для выполнения перестановки используется цикловой ключ, то соответствующие матрицы перестановки могут быть сформированы

на стадии «разворачивания ключа». В силу высокой «разряжённости» этих матриц, задача их без избыточного кодирования может быть решена весьма эффективно.

Выводы

Предложенный метод построения управляемых предельно нелинейных преобразований (PS-блоков) позволяет динамически формировать «секретные» S-блоки с предельно достижимыми показателями устойчивости к известным атакам криптоанализа. При этом множество различных PS-блоков может быть реализовано на базе одного фиксированного S-блока путём добавления операции ключезависимой перестановки координат (битов). Эта операция не коммутативна с операцией сложения по модулю 2 (XOR), используемой обычно для ввода ключа. Кроме того, обе указанные операции не влияют на нелинейные свойства базового S-блока, т.е. криптостойкость PS-блока не зависит от используемого ключа, в то время как сложность линейного и дифференциального криптоанализа возрастает в случае неопределённости позиций входных / выходных координат. Предложенная конструкция S-блоков, благодаря максимизации алгебраической степени и количества термов отдельных аргументов, оптимизирована для применения в составе цикловых функций с SPN-структурой.

Список литературы: 1. «Supporting Document on E2», Nippon Telegraph and Telephone Corporation, June 14, 1998. 2. *Zhang X.-M., Zheng Y.*, Cryptographically resilient functions // IEEE Transactions on Information Theory, September 1997. 3. *Nyberg K., Knudsen L.R.* Provable Security Against a Differential Attack // Journal of Cryptology. Vol. 8, No. 1. P. 27–37. 1995. 4. *Biham E., Shamir A.* Differential Cryptanalysis of the Data Encryption Standard. Springern Verlag, New York, 1993. 5. *Matsui M.* Linear cryptanalysis method for DES cipher. Advances in Cryptology – EUROCRYPT '93, LNCS 765. 1994. P. 386-397. 6. *Preneel B., Van Leekwijck W., Van Linden L., Govaerts R., Vandewalle J.* Propagation characteristics of boolean functions in *LNCS 473. Advances in Cryplology: Proc. Eurocrypt'90,* 1. Damgard, Ed., Aarhus, Denmark, May 21-24. Berlin: Springer-Verlag. 1990. P. 161-173. 7. *Meier W., Staffelbach O.* "Nonlinearity criteria for cryptographic functions," in *LNCS 434; Advances in Cryptology; Proc. Eurocrypt'89,* J.-J. Quisquater and J. Vandewalle, Eds., Houthalen, Belgium, April 10-23, 1989, pp. 549-562. Berlin: Springer-Verlag, 1990. 8. *Beth T., Ding C.* «On Almost Perfect Nonlinear Permutations», Advances in Cryptology, Proceedings Eurocrypt'93, LNCS 765, T. Helleseth, Ed., Springer-Verlag, 1994. 9. *Nyberg K.* «Differentially uniform mappings for cryptography», Advances in Cryptology, Proceedings Eurocrypt'93, LNCS 765, T. Helleseth, Ed., Springer-Verlag, 1994, pp. 55-64. 10. Daemon J., Rijmen V. AES Proposal: Rijndael, 1999. 11. AES discussion forum: http://aes.nist.gov 12. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. М.: Госстандарт СССР.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 2.10.2001