Методы и средства генерации нелинейных узлов замены для симметричных криптоалгоритмов

Казимиров Александр Владимирович
младший научный сотрудник
кафедры БИТ ХНУРЭ

Научный руководитель:
к.т.н., доц. каф. БИТ
Олейников Роман Васильевич

Харьков 2014

Актуальность

Многие зарубежные страны, включая Россию и Белоруссию, за последние несколько лет приняли новые улучшенные стандарты криптографических преобразований, например ГОСТ Р 34.11-2012 или СТБ 34.101.31-2011. На сегодняшний день в Украине используются стандарты блочного симметричного шифрования и хэш-функции, принятые более 20 лет назад, которые имеют как теоретические слабости, так и ограничения в производительности. Для преодоления отставания необходимо разработать новые симметричные криптосистемы, основными компонентами которых являются нелинейные узлы замены.

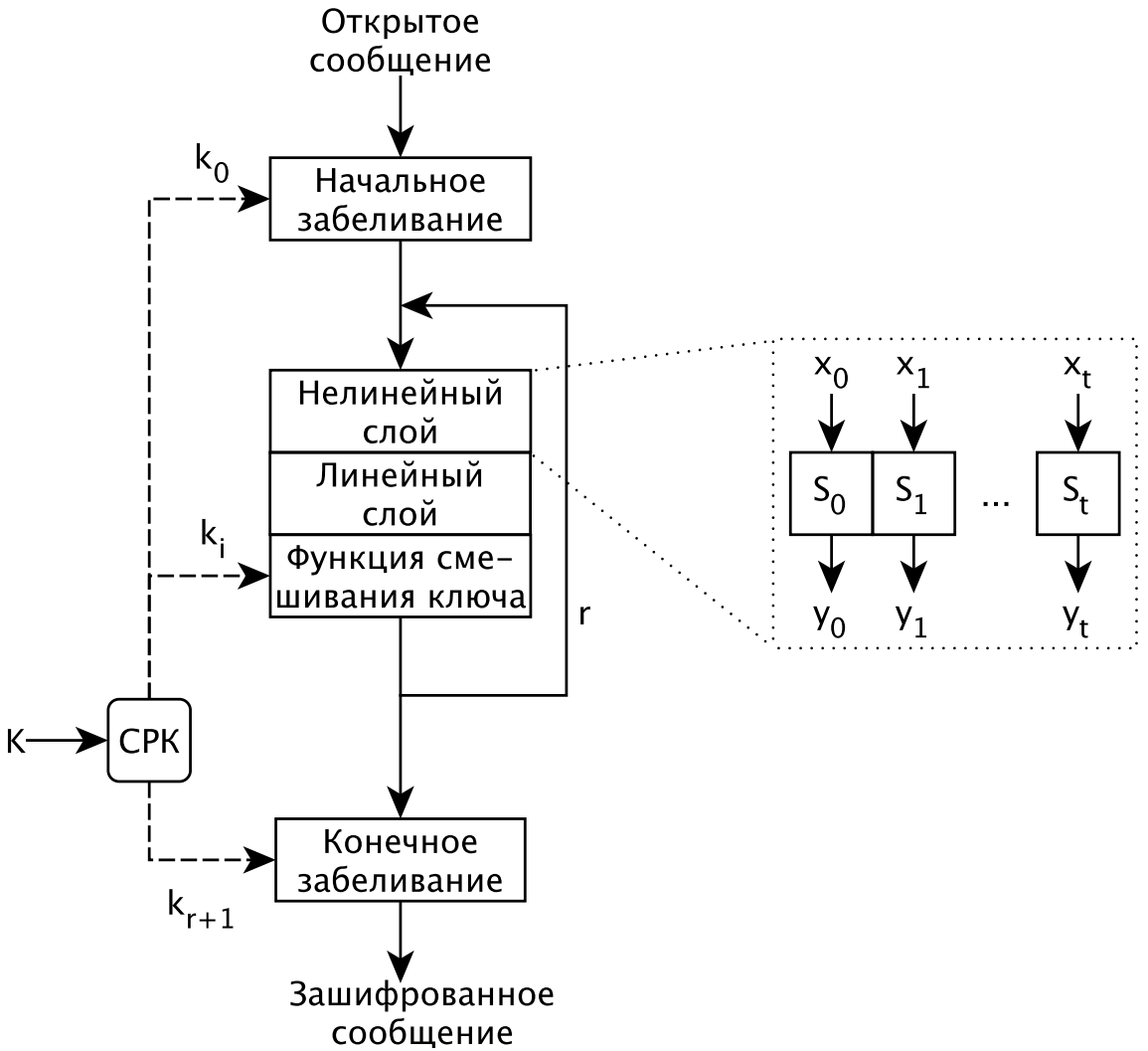
Цель исследования

Разработка методов генерации нелинейных узлов замены, применение которых на этапе проектирования современных итеративных криптографических примитивов приводит к обеспечению высокого уровня стойкости к дифференциальному, линейному и алгебраическому криптоанализам.

Задачи исследования

1. Провести анализ методов формирования нелинейных отображений в симметричной криптографии.
2. Разработать математическую модель представления линейных отображений, заданных над полем, в матричном виде для уменьшения сложности проверки на эквивалентность нелинейных отображений.
3. Усовершенствовать метод оценки стойкости блочных симметричных шифров относительно алгебраической атаки на основе решения системы нелинейных уравнений над полем $\mathbb{F}_2$.
4. Разработать метод формирования долговременных ключевых элементов (ДКЭ) для шифра ДСТУ ГОСТ 28147:2009, подстановки которых принадлежат различным классам PA-эквивалентности.
5. Разработать эффективный метод генерации нелинейных узлов замены для перспективных блочных симметричных шифров.

Итеративный блочный симметричный шифр



Расширенно аффинная (PA) эквивалентность

Две функции F и G называются PA-эквивалентными если

$$F(x) = A_1 \circ G \circ A_2(x) + L_3(x) \tag{1}$$

для некоторых аффинных перестановок $A_1(x) = L_1(x) + c_1$, $A_2(x) = L_2(x) + c_2$ и линейной функции $L_3(x)$.

Функции F и G называются частично PA-эквивалентные (ЧPA), если некоторые из функций $\{L_1, L_2, L_3, c_1, c_2\}$ равны 0 или x. Два особых случая

- линейная эквивалентность: $\{L_3, c_1, c_2\} = \{0, 0, 0\}$
- аффинная эквивалентность: $L_3 = 0$

Предложенный метод преобразования линейных функций

Для произвольной линейной функции $L : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ сложность предложенного метода нахождения $m \times n$ матрицы M

$$L(x) = \sum_{i=0}^{n-1} \delta_i x^{2^i} = M \cdot x, \quad \delta_i \in \mathbb{F}_{2^m}. \tag{2}$$

равна $O(n)$.

Применение к ГОСТ Р 34.11-2012

Восстановлена алгебраическая структура российской функции хэширования, которая задана в стандарте в виде алгоритмов над полем $\mathbb{F}_2$.

Проверка на ЧРА-эквивалентность

Постановка проблемы

С целью поиска изоморфных представлений цикловых функций (S-блоков) необходимо при известных векторных булевых функциях $F, G : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ найти такие M_1, M_2, M_3, V_1 и V_2, чтобы выполнялось равенство

$$F(x) = M_1 \cdot G(M_2 \cdot x \oplus V_2) \oplus M_3 \cdot x \oplus V_1 \qquad (3)$$

Метод полного перебора

Сложность полного перебора при проверке на РА–эквивалентность двух функций из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$ равна $O(2^{3n^2+2n})$. Уже для $n = 6$ сложность равна 2^{120}.

Сравнение методов решения проблемы ЧРА-эквивалентности

№	Частичная РА-эквивалентность	Сложность	$G(x)$
1	$F(x) = M_1 \cdot G(M_2 \cdot x)$	$O\left(n^2 \cdot 2^n\right)$	П
2	$F(x) = M_1 \cdot G(M_2 \cdot x \oplus V_2) \oplus V_1$	$O\left(n \cdot 2^{2n}\right)$	П
3	$F(x) = M_1 \cdot G(x \oplus V_2) \oplus V_1$	$O\left(2^{2n+1}\right)$	†
4	$F(x) = M_1 \cdot G(x \oplus V_2) \oplus V_1$	$O\left(n \cdot 2^{3n}\right)$	Л
5	$F(x) = G(M_2 \cdot x \oplus V_2) \oplus V_1$	$O\left(n \cdot 2^n\right)$	П
6	$F(x) = G(x \oplus V_2) \oplus M_3 \cdot x \oplus V_1$	$O\left(n \cdot 2^n\right)$	Л
7	$F(x) = M_1 \cdot G(x \oplus V_2) \oplus M_3 \cdot x \oplus V_1$	$O\left(2^{2n+1}\right)$	‡
8	$F(x) = M_1 \cdot G(x \oplus V_2) \oplus M_3 \cdot x \oplus V_1$	$O\left(n \cdot 2^{3n}\right)$	Л

† - G при выполнении условия $\{2^i \mid 0 \leq i \leq n-1\} \subset \mathrm{img}(G')$, где $G'(x) = G(x) \oplus G(0)$.

‡ - G при выполнении условия $\{2^i \mid 0 \leq i \leq n-1\} \subset \mathrm{img}(G')$, где $G'(x) = G(x) \oplus L_G(x) \oplus G(0)$.

Сравнение методов решения проблемы ЧРА-эквивалентности

Результаты расчётов приведены в логарифмическом виде с основанием 2.

№	$n = 6$		$n = 8$		$n = 10$		$n = 12$	
	СПП	СИМ	СПП	СИМ	СПП	СИМ	СПП	СИМ
1	69	12	125	14	197	17	285	20
2	81	15	141	19	217	24	309	28
3	47	13	79	17	119	21	167	25
4		21		27		34		40
5		12		14		17		20
6	48	9	80	11	120	14	168	16
7	83	13	143	17	219	21	311	25
8		21		27		34		40

СПП - сложность полного перебора

СИМ - сложность известных методов

Предложенные критерии

Расширенный критерий алгебраического иммунитета

Подстановка обеспечивает более высокую стойкость к алгебраической атаке, если система уравнений описывающая S-блок

1. имеет более высокую степень;
2. обладает меньшим количеством уравнений;
3. является менее разреженной (количество ненулевых термов в системе больше).

Критерий к нескольким нелинейным узлам замены

Подстановки $S_1, S_2, \ldots, S_k$, используемые в нелинейном слое, должны принадлежать различным классам эквивалентности для уменьшения количества изоморфных представлений.

Совершенно нелинейные подстановки

S-блок – отображение n-битного входного сообщения в некоторое выходное размерностью m бит.

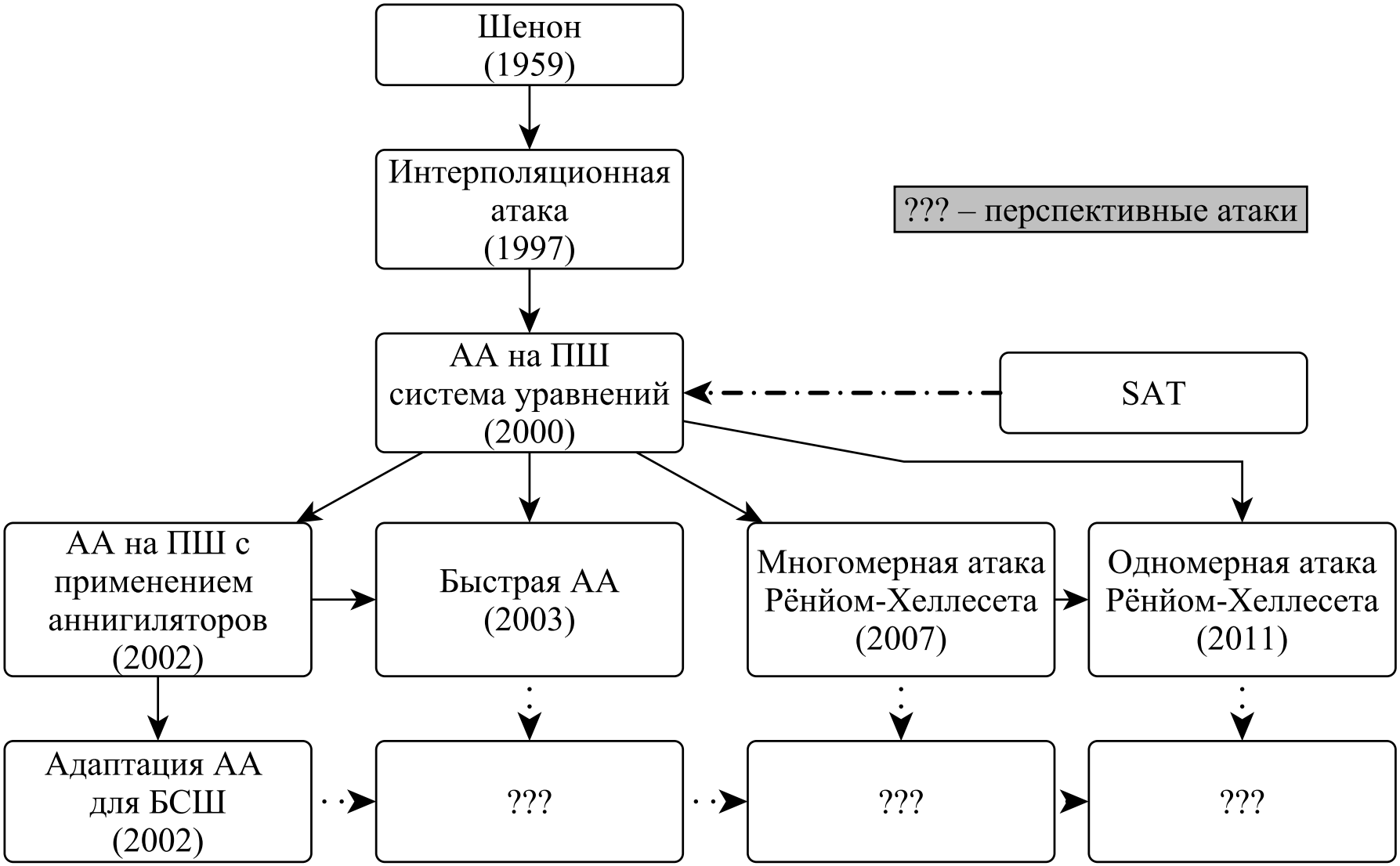
- Минимальная степень
- Сбалансированность
- Нелинейность
- Корреляционный иммунитет
- δ-равномерность
- Циклическая структура
- Алгебраический иммунитет
- Абсолютный индикатор
- Отсутствие фиксированных точек
- Критерий распространения
- ГЛХ «сумма квадратов»
- ...

Характеристики подстановки шифра AES

Таблица: Характеристики S-блока шифра AES

Свойства	Показатель
Сбалансированность	Да
Биективность	Да
Нелинейность	112
Максимум таблицы линейных аппроксимаций	16
Максимальное значение автокорреляции	32
ГЛХ «сумма квадратов»	133120
Критерий распространения	0
Корреляционный иммунитет	0
t-устойчивость	0
Строгий лавинный критерий	Нет
Максимум дифференциальной таблицы	4
Минимальная степень	7
Циклические свойства	43:27, 242:87, 99:59, 124:81, 143:2
Алгебраический иммунитет	2(39)

Развитие алгебраической атаки



Оптимальные подстановки

Подстановка является оптимальной, если достигнута совокупность, известная на текущий момент, предельных значений показателей, определяющих стойкость симметричного преобразования к методам дифференциального, линейного и алгебраического криптоанализов.

Критерии оптимальной подстановки для БСШ.

- заранее заданные
  - биективность (перестановка);
  - наибольшее значение минимальной степени;
  - отсутствие фиксированных точек;
  - максимальный алгебраический иммунитет.
- варьирующиеся
  - минимальное значение δ-равномерности;
  - максимальное значение нелинейности.

Пример критериев оптимальности для $n = m = 8$

Оптимальная перестановка без фиксированных точек должна иметь

- минимальную степень 7;
- алгебраический иммунитет 3 (441 уравнения);
- δ-равномерность не больше 8;
- нелинейность не меньше 104.

Метод случайной генерации

Алгоритм

Сгенерировать случайную перестановку и проверить её на оптимальность.

Результаты проведённого анализа

После 12 часов работы, кластер с 4096 ядрами нашёл 27 перестановок ($NL = 100$), 4 из них оказались КШЗ-неэквивалентными.

Вычислительные ограничения метода

Дополнительный поиск подстановок с $NL = 102$ после 48 часов (22 года на одном ядре) не выдал ни одного результата.

Предложенный метод генерации подстановок

Пусть $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ – биективная перестановочная векторная булева функция с максимальным показателем нелинейности и минимальным значением δ-равномерности.

Алгоритм генерации

- генерация подстановки S на основе выбранной функции F (например, $F = x^{-1}$);
- случайный обмен местами NP значений подстановки S и формирование подстановки S_t;
- последовательная проверка критериев, в зависимости от их вычислительной сложности. При несоответствии хотя бы одному из критериев осуществляется переход к предыдущему пункту.

Результаты применения предложенного метода

Результаты проведённого анализа

В течение 1 часа работы кластера было получено 1152 оптимальных подстановок, с нелинейностью 104 и алгебраическим иммунитетом 3.

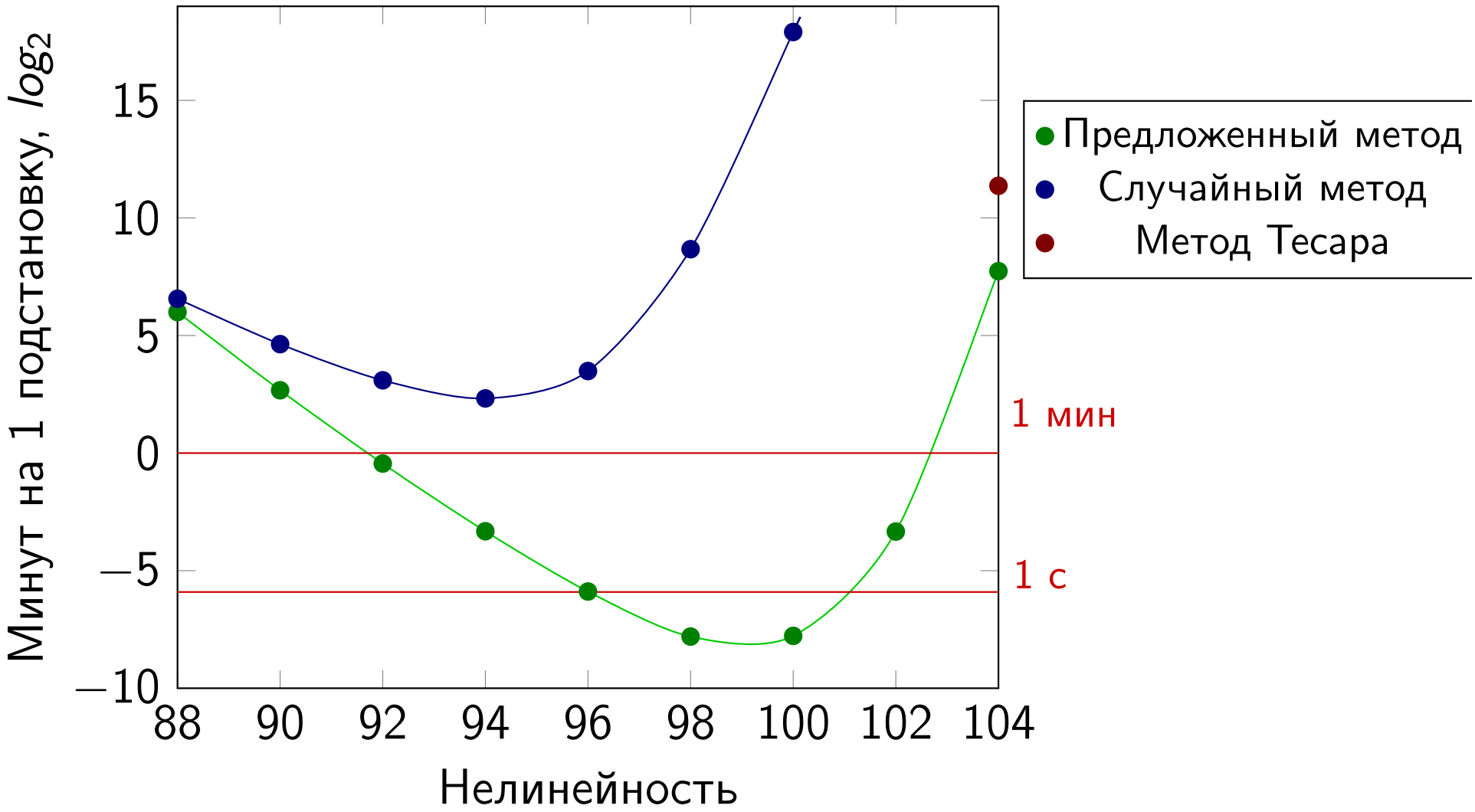
Эффективность предложенного метода

Если функция обмена значений является случайной, то время, необходимое на генерацию одной оптимальной подстановки на однопроцессорном ПК, в среднем равно 3.5 часам.

Вычислительные ограничения метода

Кластер не нашёл ни одной оптимальной подстановки с нелинейностью 106 и алгебраическим иммунитетом 3 в течение 107 часов работы (50 лет на одном ядре).

Производительность известных методов



Сравнительная характеристика узлов нелинейной замены

Свойства	AES	ГОСТ Р 34.11-2012	СТБ 34.101.31-2011	Калина S0	Полученный S-блок
δ-равномерность	4	8	8	8	8
Нелинейность	112	100	102	96	104
Абсолютный индикатор	32	96	80	88	80
ГЛХ «сумма квадратов»	133120	258688	232960	244480	194944
Минимальная степень	7	7	6	7	7
Алгебраический иммунитет	2(39)	3(441)	3(441)	3(441)	3(441)

Рассматриваемые подстановки

Набор подстановок	Характеристики				
	NL	δ	AI	Разреженность	Количество уравнений
О	96	8	3	0.1739	441
П	104	8	3	0.1719	441
С	90	10	3	0.1740	441
C_{max}	100	8	3	0.1719	441
D_{min}	100	8	2	0.4453	1
А	102	8	2	0.4700	13
AES	112	4	2	0.3127	39

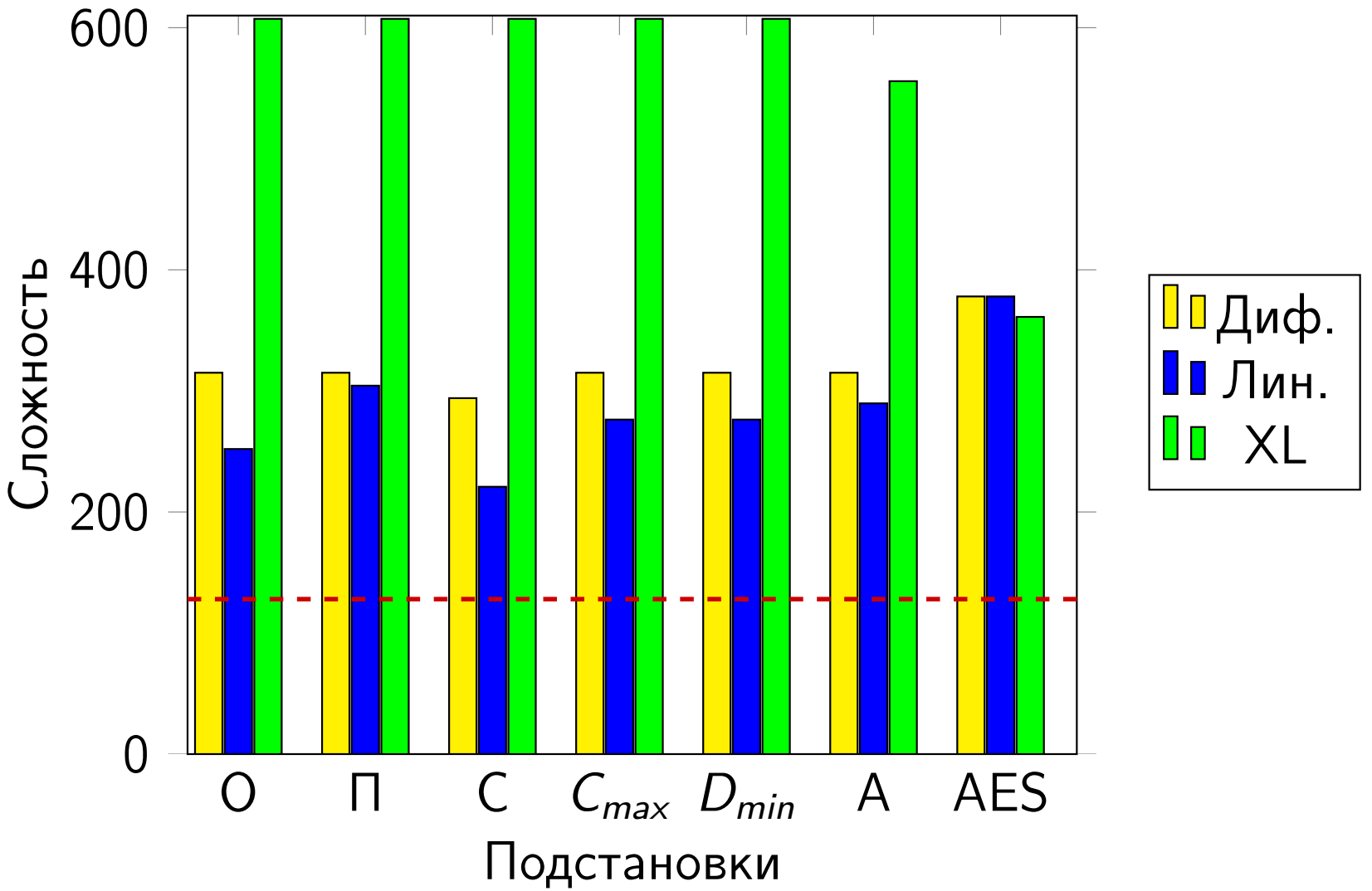
Таблица: Характеристики подстановок используемых при анализе шифра «Калина 128/128»

Сложность криптоаналитических атак на примере шифра «Калина 128/128»

Набор подстановок	Сложность криптоанализа		
	Диф.	Лин.	XL $\omega = 2.4$
O	2^{315}	2^{252}	$2^{607,3}$
П	2^{315}	$2^{304,3}$	$2^{607,3}$
C	2^{294}	$2^{220,8}$	$2^{607,3}$
C_{max}	2^{315}	$2^{276,3}$	$2^{607,3}$
D_{min}	2^{315}	$2^{276,3}$	$2^{607,3}$
A	2^{315}	$2^{289,7}$	$2^{555,8}$
AES	2^{378}	2^{378}	$2^{361,1}$

Таблица: Расчёт сложности атак на шифр «Калина 128/128» с различными нелинейными слоями

Сложность криптоаналитических атак на примере шифра «Калина 128/128»



Обозначим через g примитивный элемент поля $\mathbb{F}_{2^4}$, образованного при помощи примитивного полинома $f(z) = z^4 + z + 1$.

F_i	Полином
F_1	$x^{14}+g^{11}x^{13}+gx^{12}+g^3x^{11}+g^5x^9+g^7x^8+g^8x^7+g^4x^6+g^11x^5+g^2x^4+g^4x^3+g^{11}x^2$
F_2	$x^{14} + g^{11}x^{13} + g^7x^{12} + gx^{11} + g^8x^{10} + g^{13}x^9 + g^{11}x^8 + g^2x^6 + gx^5 + g^2x^4 + g^7x^3 + gx^2 + g^8x$
F_3	$x^{14} + g^{13}x^{13} + g^9x^{12} + g^6x^{11} + g^{10}x^{10} + g^7x^9 + g^{10}x^8 + g^7x^7 + g^8x^6 + g^{12}x^5 + g^{12}x^4 + x^3 + g^{11}x^2 + g$
F_4	$x^{14} + g^4x^{13} + g^3x^{12} + g^2x^{11} + x^{10} + g^{11}x^9 + g^2x^8 + gx^7 + g^2x^6 + g^9x^5 + g^4x^4 + g + x^3 + g^{12}x^2 + g^{11}x$
F_5	$x^{14}+gx^{13}+g^9x^{12}+gx^{11}+g^7x^{10}+g^6x^7+g^{10}x^6+gx^5+g^8x^4+g^2x^3+g^6x^2+g^9x$
F_6	$x^{14} + gx^{13} + x^{12} + g^7x^{11} + g^{13}x^{10} + gx^9 + g^{11}x^8 + g^{14}x^7 + g^3x^6 + g^6x^5 + gx^4 + g^{14}x^3 + g^{14}x^2 + g^9x$
F_7	$x^{14} + g^{10}x^{13} + gx^{12} + g^4x^{11} + g^{14}x^{10} + g^4x^9 + g^5x^8 + g^2x^7 + g^9x^6 + g^4x^5 + g^8x^4 + g^{14}x^3 + g^5x^2 + x$
F_8	$x^{14} + g^{12}x^{13} + g^8x^{12} + g^8x^{11} + g^{14}x^{10} + gx^9 + g^8x^8 + g^{14}x^7 + g^6x^6 + x^5 + g^{14}x^4 + g^{12}x^3 + gx^2 + g^{14}x$

Таблица: РА-неэквивалентные перестановочные векторные булевы функции

Метод генерации ДКЭ для ДСТУ ГОСТ 28147:2009

1. Каждой из 8 подстановок ДКЭ $(K_1, \ldots, K_8)$ ставится в соответствие векторная булева функция $F_1, \ldots, F_8$.
2. К каждому полиному последовательно применяются аффинно-эквивалентные преобразования до тех пор, пока функция (подстановка) не будет удовлетворять циклическим свойствам.

Верхняя граница мощности множества ДКЭ ДСТУ ГОСТ 28147:2009 построенных по предлагаемой методике равна

$$\left(\prod_{i=1}^{4}\left(2^4 - 2^{i-1}\right)\right)^2 \cdot 2^8 \cdot 8! \approx 2^{51}$$

Пример ДКЭ

Каждая из подстановок $K_1, \ldots, K_8$ обладает:

- нелинейностью 4;
- δ-равномерностью 4;
- минимальной степенью 3.

№	Ключ
K_1	$[5, 11, 13, 10, 8, 4, 1, 0, 6, 12, 3, 15, 2, 9, 7, 14]$
K_2	$[7, 8, 12, 10, 2, 1, 15, 14, 11, 13, 5, 9, 0, 3, 6, 4]$
K_3	$[15, 14, 7, 5, 3, 13, 9, 2, 10, 6, 11, 1, 8, 0, 12, 4]$
K_4	$[15, 8, 9, 14, 1, 4, 13, 11, 3, 5, 6, 12, 0, 2, 7, 10]$
K_5	$[5, 10, 6, 15, 8, 4, 2, 3, 9, 7, 13, 0, 14, 1, 12, 11]$
K_6	$[7, 9, 12, 8, 10, 2, 13, 14, 0, 5, 4, 6, 3, 15, 1, 11]$
K_7	$[8, 14, 11, 5, 1, 4, 7, 6, 13, 2, 9, 15, 3, 10, 12, 0]$
K_8	$[13, 14, 6, 10, 2, 15, 0, 5, 12, 1, 11, 4, 9, 8, 3, 7]$

Таблица: Пример ДКЭ сгенерированных по предложенному методу

Выводы

1. Основными критериями для подстановок, применяемых в БСШ, являются биективность, отсутствие фиксированных точек, δ-равномерность, минимальная степень, алгебраический иммунитет и нелинейность.
2. Предложенный критерий для множества подстановок позволяет уменьшить количество изоморфных представлений алгоритма шифрования.
3. Расширенный критерий алгебраического иммунитета позволяет отбирать нелинейные узлы замены обеспечивающие максимальную защиту от алгебраической атаки.
4. Применение метода генерации оптимальных нелинейных узлов замены для национальных симметричных алгоритмов шифрования (при $n = 8$) позволяет получить перестановку с отсутствием фиксированных точек и показателями: δ-равномерность 8, нелинейность 104, минимальная степень 7, алгебраический иммунитет 3.

Выводы

5. Применение предложенного метода генерации оптимальных нелинейных узлов замены позволяет получить ДКЭ для шифра ДСТУ ГОСТ 28147:2009, состоящие из подстановок принадлежащих различным PA-эквивалентным классам, и обеспечивающий высокий уровень стойкости к дифференциальному и линейному криптоанализам.
6. Проведённый анализ S-блоков показал превосходство оптимальных нелинейных узлов замены, полученных с применением предложенного метода, над подстановками, используемыми в распространённых симметричных криптопреобразованиях, включая стандарты СТБ 34.101.31-2011, ГОСТ Р 34.11-2012 и представителей украинского национального конкурса по выбору перспективного алгоритма шифрования, проведённого в 2007-2009 годах.

Научная новизна

1. Впервые предложен метод генерации узлов нелинейной замены для перспективных блочных симметричных шифров с одновременным учётом δ-равномерности, нелинейности и алгебраических показателей на основе векторных булевых функций, что позволяет находить подстановки с улучшенными показателями алгебраического иммунитета и нелинейности при малых затратах ресурсов.
2. Впервые предложен метод формирования долговременных ключевых элементов на основе классов эквивалентностей векторных булевых функций, что позволяет генерировать узлы нелинейной замены, которые принадлежат различным классам PA-эквивалентности и имеют максимальные показатели защиты от дифференциального и линейного криптоанализов.

Научная новизна

3. Усовершенствован метод нахождения матрицы линейного отображения, заданного в виде полинома над полем $\mathbb{F}_2$, который в отличие от известных для решения системы матричных уравнений использует набор входных векторов бинарного вида с единичным весом Хемминга, использование которого позволяет уменьшить сложность нахождения алгебраической формы высокоуровневых конструкций криптографических алгоритмов и проверки векторных булевых функций на частично расширенную аффинную эквивалентность.
4. Получил дальнейшее развитие метод оценки стойкости блочных симметричных шифров к алгебраической атаке, который отличается от известных учётом показателей количества уравнений в системе и её разреженностью, что позволяет уточнить значение верхней границы скложности атаки.

Научная новизна

5. Получил дальнейшее развитие метод отбора подстановок для блочных симметричных шифров, который основан на критериальном подходе, в частности с учётом пердложеного алгебраического критерия, и отличается от известных комплексной оценкой стойкости, что позволяет генерировать S-блоки, использование которых в симметричных алгоритмах шифрования увеличивает сложность криптоаналитических атак.

Практическая значимость полученных результатов

1. Разработана программная реализация предложенного метода нахождения 8-битовых перестановок с отсутствием фиксированных точек, нелинейностью 104, минимальной степенью 7, алгебраическим иммунитетом 3 и 8-равномерных на однопроцессорном компьютере со средним значением времени работы 3.5 часа.
2. Разработана программная реализация быстрой генерации ДКЭ для шифра ДСТУ ГОСТ 28174:2009 с оптимальными показателями на основе предложенного метода.
3. Разработано программное обеспечение для расчёта большинства известных на сегодняшний день показателей, включая нелинейность, корреляционный иммунитет, δ-равномерность, алгебраический иммунитет, произвольных векторных булевых функций, которые применяются в качестве узлов нелинейной замены в симметричных криптопримитивах.
4. Разработана программная реализация вычисления оценки верхней границы эффективности случайного метода генерации подстановок в распределённых кластерных системах.

Публикации

Основные результаты исследований опубликованы в 10 научных специализированных изданиях Украины и в 3 зарубежных изданиях, которые входят в научно-метрические базы, а также прошли апробацию на 18 научно-технических конференциях и международных форумах проводимых в Украине и за рубежом.

Апробация результатов

Результаты исследований, проведённых в работе, докладывались на

- 4-х международных форумах проводимых в Украине:
  - 3-й Международный радиоэлектронный форум «Прикладная радиоэлектроника. состояние и перспективы развития» (2008)
  - 12-, 14-, 15-й Международный молодёжный форум «Радиоэлектроника и молодёжь в XXI веке» (2008, 2010, 2011)
- 3-х зарубежных международных конференциях:
  - WAIFI'12 (г. Бохум, Германия)
  - RusCrypto13 (г. Москва, Россия)
  - CTCrypt 2013 (г. Екатеринбург, Россия)

Апробация результатов

- 9-ти научно-практических конференциях:
  - XII, XIII Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах» (2009, 2010)
  - Научно-техническая конференция с международным участием «Компьютерное моделирование в наукоёмких технологиях» (2010)
  - Международная научно-практическая конференция «Перспективы развития информационных и транспортных технологий в налоговой сфере, внешнеэкономической деятельности и управлении организациями» (2011)
  - ...
- 3-х исследовательских школах:
  - Winter School in Information Security 2012 (г. Финсе, Норвегия)
  - ECRYPT II Summer School on Tools 2012 (о. Миконос, Греция)
  - IceBreak 2013 (г. Рейкьявик, Исландия)