УДК 681.03.245 DOI 10.18522/2311-3103-2016-9-3750

Л.К. Бабенко, Е.А. Маро

ПРИМЕНЕНИЕ МЕТОДОВ АЛГЕБРАИЧЕСКОГО АНАЛИЗА ДЛЯ ЗАДАЧ ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ*

Описано применение методов алгебраического анализа для оценки защищенности информации при использовании криптографического преобразования данных симметричными блочными алгоритмами шифрования. В качестве исследуемых алгоритмов выбраны стандарты ГОСТ 34.12-2015 (n=64) и PRESENT. За основу алгебраического анализа взят метод сведения шифрования к задаче булевой выполнимости формул (SAT). Разработаны алгоритмы формирования систем булевых нелинейных уравнений для произвольных заполнений блоков замены и различного числа раундов шифров на основе сети Фейстеля и SP-сети. Предложена методика проведения алгебраического анализа с помощью SAT-решателя CryptoMiniSat, позволяющая предварительно вычислять ожидаемую сложность нахождения наборов решений систем булевых нелинейных уравнений с помощью методов сведения к SAT-задаче. Выделены исследуемые критерии оценки защищенности информации на основе алгебраического анализа криптографических алгоритмов. Разработанные в ходе выполнения исследования алгоритмы и методика могут быть в дальнейшем использованы для оценки защищенности произвольных преобразований на основе операций замены и сложения по модулю 2^n при алгебраическом анализе. В ходе моделирования алгебраического анализа была оценена защищенности данных при сокращенном числе раундов шифрования данных алгоритмов (вычисления проводились с использованием вычислительных ресурсов SageMath Cloud). Для 8 раундов алгоритма «Магма» (ГОСТ 34.12-2015, n=64) ключ шифрования удалось вычислить при известных 4 текстах за 3029,56 сек. Для 4 раундов шифрования PRESENT (ISO 29192-2:2012) 16 наборов ключей были вычислены при наличии 8 текстов за 3268,42 сек.

Оценка защищенности информации; алгебраический анализ; симметричные блочные алгоритмы шифрования; ГОСТ 34.12-2015; PRESENT; задача булевой выполнимости формул (SAT); решатель CryptoMiniSat, алгебраическая нормальная форма (АНФ), конъюнктивная нормальная форма (КНФ).

L.K. Babenko, E.A. Maro

METHODS OF ALGEBRAIC ANALYSIS FOR ASSESSMENT OF INFORMATION SECURITY

This article describes the approach to algebraic analysis methods for the evaluation of data protection by cryptographic algorithms, as an example we have observed the symmetric block ciphers. As the base of research we have selected standards GOST 34.12-2015 (n = 64) and PRESENT. The basis of the algebraic analysis is the method of reduction system of equations to the Boolean formulas satisfiability (SAT) problem. We create a generation algorithms of Boolean systems of nonlinear equations for arbitrary substitution boxes and a different number of encryption rounds (based on a Feistel network and SP-network). We present a methodjlogy of algebraic analysis with a SAT-solver CryptoMiniSat, which allows pre-calculating the expected complexity of finding the sets of solutions of Boolean nonlinear equations systems by the methods of reduction to SAT-problem. Observed criteria for the evaluation of data protection based on the algebraic analysis of cryptographic algorithms are listed. Developed in the course of research algorithms and methodology may be further used to evaluate the security of arbitrary transformations on the basis of operations of replacement and addition modulo 2^n by algebraic analysis. During the modeling of the algebraic analysis we assessed data protection of reduced-rounds encryption al-

* Работа выполнена при поддержке гранта РФФИ 15-37-20007-мол_а_вед.

gorithms (experiments were made using SageMath Cloud computing resources). For 8 rounds "Magma" algorithm (GOST 34.12-2015, n = 64) encryption key was calculated with 4 texts for 3029.56 4 seconds. For 4 rounds encryption PRESENT (ISO 29192-2: 2012) we have calculated 16 keys-sets with 8 texts for 3268.42 seconds.

Evaluation of data protection; algebraic analysis; symmetric block encryption algorithms; GOST 34.12-2015; PRESENT; Boolean formulas satisfiability problem (SAT); solver CryptoMiniSat; algebraic normal form (ANF); conjunctive normal form (CNF).

Введение. Задача анализа надежности применяемых средств защиты информации является основополагающей в сфере безопасности информационных технологий. В современных системах и средствах защиты данных зачастую применяются криптографические алгоритмы, позволяющие обеспечить требование конфиденциальности данных. Например, в качестве алгоритмов защиты информации могут быть использованы симметричные шифры. Несмотря на изначальную высокую надежность предложенных к применению алгоритмов шифрования, важной научной задачей остается проведение исследований стойкости шифров к различным методам анализа.

Перспективным направлением, опираясь на анализ научных работ [1–10], является разработка и исследование алгоритмов и методик проведения оценки защищенности информации на основе алгебраического анализа. Базу алгебраических методов анализа составляет представление преобразований защиты данных в виде систем булевых нелинейных алгебраических уравнений и последующий поиск наборов решений. Были выделены следующие достоинства алгебраического анализа:

- применимость к обширному ряду алгоритмов криптографической защиты информации (как блочным, так и поточным шифрам);
- применение алгебраических методов анализа позволяет вычислять секретную информацию при наличии небольшого числа известных данных;
- эффективный алгоритм алгебраического анализа шифров требует меньших вычислительных ресурсов по сравнению со статистическими методами.

Постановка задачи. Задачей исследовательской работы является разработка алгоритмов формирования и решения систем булевых нелинейных уравнений для преобразований замен и операции сложения по модулю 2^n, отличающиеся от существующих тем, что позволяют обрабатывать произвольные длины векторов, а также выполнять оценку времени решения и требуемых объемов памяти при проведении алгебраического анализа. В ходе исследования была предложена и экспериментально апробирована методика проведения алгебраического анализа на основе метода сведения к SAT-задаче, опирающаяся на разработанные авторами алгоритмы, на примере шифров Магма и PRESENT.

Можно выделить три основных направления в поиске решений систем булевых нелинейных уравнений:

1. SAT-решатели, например, MiniSat2, CryptoMiniSat, PD-SAT.
2. Методы на основе базиса Гребнера, например, алгоритмы Бухбергера, F4, F5.
3. Методы, основанные на принципе линеаризации, например, релинеаризация, расширенная линеаризация, расширенная разреженная линеаризация, ElimLin.

В рамках данной статьи описано применение методов сведения к SAT-задаче и использовании решателя CryptoMiniSat [11]. Алгебраический анализ с применением SAT-решателей можно представить алгоритмом, состоящим из трех основных этапов:

- Представление преобразования защиты информации в виде системы булевых уравнений в АНФ.
- Перевод системы уравнений из АНФ в КНФ.
- Поиск набор решений с помощью SAT-решателей.

После формирования системы уравнений, используя знание структуры исследуемого алгоритма защиты информации, выполняется выражение входных и выходных векторов блока замены через известные тексты. На данном этапе получена система булевых уравнений, представленная в алгебраической нормальной форме (АНФ).

Для перехода к возможности применения SAT-решателей сформированная система булевых уравнений в АНФ должна быть переведена в КНФ. Алгоритм представления уравнений в АНФ, сформированных для блочных алгоритмов, предварительно следует упростить. Воспользуемся следующим алгоритмом [12] приведения сформированной АНФ в КНФ:

1. Замена константы, равной 1, на новую неизвестную, т.к. КНФ не должна содержать констант.
2. Приведение исходной нелинейной системы к линейному виду путем замены всех произведений неизвестных на новые переменные.
3. Дробление длинных цепочек операций сложения по модулю 2 неизвестных на подстроки меньшей длины (например, по 4 неизвестных в сумме).
4. Представление преобразованной системы в КНФ.

В качестве наиболее подходящего SAT-решателя выбран CryptoMiniSat 2.5 [11]. Поиск решений для исследуемых алгоритмов защиты информации осуществлялся в облачной среде математического проектирования SageMath Cloud [13].

Методика проведения алгебраического анализа с помощью SAT-решателя CryptoMiniSat:

1. Формирование подсистем булевых нелинейных уравнений для примитивов замены.
2. Формирование подсистемы булевых нелинейных уравнений, описывающих используемые операции сложения по модулю 2 или 2^n.
3. Формирование подсистемы булевых нелинейных уравнений, описывающих процедуру генерации раундовых ключей шифрования, в случае, если в данной процедуре применяются примитивы замены.
4. Предварительная оценка количества литералов и клозов при конвертации системы булевых нелинейных уравнений из АНФ в КНФ.
5. Конвертация сформированной системы булевых нелинейных уравнений из АНФ в КНФ.
6. Решение системы в КНФ с помощью SAT-решателя CryptoMiniSat на основе разработанного алгоритма.
7. Экспериментальное определение временной сложности, требуемой оперативной памяти и достаточного числа известных текстов для нахождения единственного решения (ключа шифрования) с помощью SAT-решателя.
8. Проверка найденных решений на известных парах текстов.

В качестве критериев защищенности информации на основе алгебраического анализа нами выделены:

1. Параметры итоговой системы булевых нелинейных уравнений, формируемых для заданного числа раундов шифрвоания: количество уравнений, неизвестных и одночленов.
2. Количество текстов, необходимое для нахождения единственно решения системы.
3. Время поиска решений в условиях ограниченных вычислительных ресурсов.
4. Объем данных, обрабатываемых и хранимых в оперативной памяти при проведении вычислений.

Алгебраический анализ алгоритма «Магма». Алгоритм «Магма» является симметричным блочным алгоритмом, построенным по схеме Фейстеля [14]. На вход алгоритма поступает 64-битовый блок данных, который под воздействием 256-битового ключа преобразуется в 64-битовый блок преобразованных данных. В каждом раунде правая часть шифруемого сообщения поступает на вход раундовой функции, где преобразуется с использованием трех операций: сложения данных с раундовым подключом по модулю 2^{32}, замена данных с использованием S-блоков (табл. 1), циклический сдвиг влево на 11 позиций.

Таблица 1

Блоки замены алгоритма ГОСТ Р 34.12-2015

S8	12	4	6	2	10	5	11	9	14	8	13	7	0	3	15	1
S7	6	8	2	3	9	10	5	12	1	14	4	7	11	13	0	15
S6	11	3	5	8	2	15	10	13	14	1	7	4	12	9	6	0
S5	12	8	2	1	13	4	15	6	7	0	10	5	3	14	9	11
S4	7	15	5	10	8	1	6	13	0	9	3	14	11	4	2	12
S3	5	13	15	6	9	2	12	10	11	7	8	1	4	3	14	0
S2	8	14	2	5	6	9	1	12	15	4	11	0	13	10	3	7
S1	1	7	14	13	0	5	8	3	4	15	10	6	9	12	11	2

Выход раундовой функции складывается по модулю 2 с левой частью шифруемого сообщения, после чего правая и левая части меняются местами. Алгоритм содержит 32 раунда, в последнем раунде шифрования правая и левая части местами не меняются. Структура алгоритма «Магма» приведена на рис. 1.

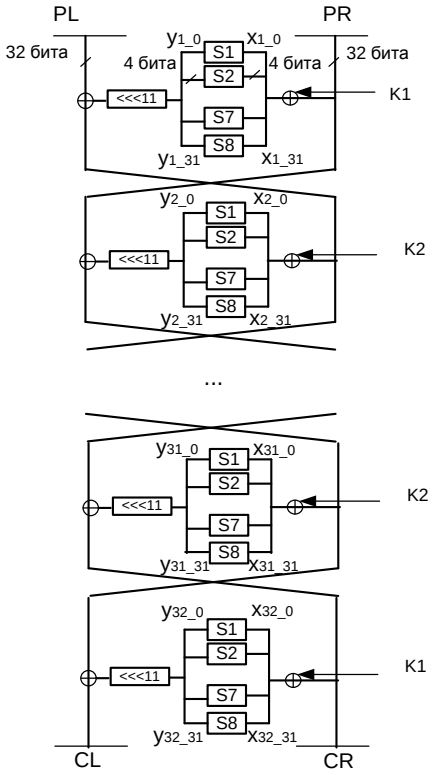

Рис. 1. Алгоритм шифрования «Магма»

Используя алгоритмы, описанные авторами в работах [15–17], сформированы подсистемы для 8 блоков замены. Так для блока замены S8 была составлена следующая подсистема уравнений (x0,x1,x2,x3 – биты входного значения блока замены, y0,y1,y2,y3 – биты выходного значения блока замены):

x0·x1 ⊕ x0·y0 ⊕ x0·y1 ⊕ x0·y3 ⊕ x0=0,
x0·x3 ⊕ x1·x3 ⊕ x0·y0 ⊕ x0·y1 ⊕ x0·y2 ⊕ x0 ⊕ x1 ⊕ x2 ⊕ x3 ⊕ y0 ⊕ y1 ⊕ y3 ⊕ 1=0,
x0·x2 ⊕ x1·x2 ⊕ x0·x3 ⊕ x0·y0 ⊕ x1·y0 ⊕ x0·y1 ⊕ x0·y2 ⊕ x0 ⊕ x2 ⊕ y0=0,
x0·x1 ⊕ x1·x2 ⊕ x0·y0 ⊕ x1·y1 ⊕ x0·y2 ⊕ x2 ⊕ x3 ⊕ y2,
x1·x2 ⊕ x0·y2 ⊕ x1·y2 ⊕ x1 ⊕ y0 ⊕ y1 ⊕ y2 ⊕ y3 ⊕ 1=0,
x0·x1 ⊕ x0·x3 ⊕ x0·y0 ⊕ x0·y1 ⊕ x0·y2 ⊕ x1·y3 ⊕ x0 ⊕ x1 ⊕ x2 ⊕ x3 ⊕ y0 ⊕ y1 ⊕ y3 ⊕ 1=0,
x0·x1 ⊕ x0·x2 ⊕ x1·x2 ⊕ x0·x3 ⊕ x2·x3 ⊕ x0·y0 ⊕ x0·y1 ⊕ x0·y2 ⊕ x2 ⊕ x3 ⊕ y1=0,
x0·x1 ⊕ x1·x2 ⊕ x0·y0 ⊕ x2·y0 ⊕ x1 ⊕ x2 ⊕ y0 ⊕ y1 ⊕ y2 ⊕ y3 ⊕ 1=0,
x0·x3 ⊕ x0·y1 ⊕ x2·y1 ⊕ x0·y2 ⊕ x0 ⊕ x1 ⊕ y1 ⊕ y2 ⊕ y3 ⊕ 1,
x0·x2 ⊕ x0·x3 ⊕ x0·y1 ⊕ x2·y2 ⊕ x3 ⊕ y1=0,
x0·x1 ⊕ x0·y0 ⊕ x2·y3 ⊕ x0 ⊕ x1 ⊕ x3 ⊕ y2 ⊕ y3 ⊕ 1=0,
x0·x1 ⊕ x1·x2 ⊕ x3·y0 ⊕ x0·y1 ⊕ x0·y2 ⊕ x3 ⊕ y0 ⊕ y1=0,
x0·x1 ⊕ x1·x2 ⊕ x0·x3 ⊕ x0·y1 ⊕ x3·y1 ⊕ x0 ⊕ x1 ⊕ x3 ⊕ y0 ⊕ y1 ⊕ y2 ⊕ y3 ⊕ 1=0,
x0·x1 ⊕ x0·x2 ⊕ x1·x2 ⊕ x0·x3 ⊕ x0·y0 ⊕ x0·y1 ⊕ x3·y2 ⊕ x1 ⊕ x3 ⊕ y0 ⊕ y3⊕ 1=0,
x0·x2 ⊕ x0·x3 ⊕ x0·y2 ⊕ x3·y3 ⊕ x3=0,
x0·x1 ⊕ x0·x2 ⊕ x1·x2 ⊕ x0·x3 ⊕ x0·y0 ⊕ y0·y1 ⊕ x0·y2 ⊕ x2,
x0·x1 ⊕ x1·x2 ⊕ x0·x3 ⊕ x0·y0 ⊕ x0·y1 ⊕ x0·y2 ⊕ y0·y2 ⊕ x1 ⊕ x3 ⊕ y0 ⊕ y2 ⊕ y3 ⊕ 1=0,
x0·x1 ⊕ x0·x2 ⊕ x0·x3 ⊕ x0·y0 ⊕ x0·y2 ⊕ y0·y3 ⊕ x0 ⊕ x1 ⊕ x2 ⊕ x3 ⊕ y0 ⊕ y2 ⊕ y3 ⊕ 1=0,
x0·x3 ⊕ x0·y1 ⊕ y1·y2 ⊕ x0 ⊕ x2 ⊕ y0 ⊕ y2=0,
x0·x3 ⊕ x0·y0 ⊕ x0·y2 ⊕ y1·y3 ⊕ x2 ⊕ x3 ⊕ y0=0,
x0·x1 ⊕ x0·y0 ⊕ x0·y2 ⊕ y2·y3 ⊕ x0 ⊕ x2 ⊕ x3 ⊕ y0 ⊕ y1 ⊕ y2=0.

Для описания нелинейной побитовой операции сложения по модулю 2^{32} следует воспользоваться следующей зависимостью, описывающей операцию сложения по модулю в виде нелинейной подсистемы булевых уравнений. Рассмотрим три вектора длиной n-бит каждый: $X = (x_0,...,x_{n-1})$, $Y = (y_0,...,y_{n-1})$, $Z = (z_0,...,z_{n-1})$, для которых выполняется сложение по модулю 2^n:

$$Z = X + Y \bmod 2^n.$$

В операции сложения по модулю 2^n каждый бит z_i зависит от битов $x_{n-1},...,x_i, y_{n-1},...,y_i$. Подобные преобразования можно описать следующим образом через две подсистемы:

$$\begin{cases} z_{n-1} = x_{n-1} \oplus y_{n-1}, \\ z_{n-2} = x_{n-2} \oplus y_{n-2} \oplus x_{n-1}y_{n-1}, \\ z_{n-3} = x_{n-3} \oplus y_{n-3} \oplus x_{n-1}y_{n-1} \oplus (x_{n-2} \oplus y_{n-2})(x_{n-2} \oplus y_{n-2} \oplus z_{n-2}), \\ \dots \\ z_i = x_i \oplus y_i \oplus x_{i+1} \oplus y_{i+1} \oplus (x_{i+1} \oplus y_{i+1})(x_{i+1} \oplus y_{i+1} \oplus z_{i+1}), \\ \dots \\ z_0 = x_0 \oplus y_0 \oplus x_1y_1 \oplus (x_1 \oplus y_1)(x_1 \oplus y_1 \oplus z_1). \end{cases}$$

Тогда операцию сложения по модулю 2^{32} для первого раунда шифрования «Магма» можно описать в виде:

$$\begin{cases} x_{31} = PR_{31} \oplus k_{31}, \\ x_{30} = PR_{30} \oplus k_{30} \oplus PR_{31}k_{31}, \\ x_{29} = PR_{29} \oplus k_{29} \oplus PR_{31}k_{31} \oplus (PR_{30} \oplus k_{30})(PR_{30} \oplus k_{30} \oplus x_{30}), \\ \dots \\ x_i = PR_i \oplus k_i \oplus PR_{i+1} \oplus k_{i+1} \oplus (PR_{i+1} \oplus k_{i+1})(PR_{i+1} \oplus k_{i+1} \oplus x_{i+1}), \\ \dots \\ x_0 = PR_0 \oplus k_0 \oplus PR_1k_1 \oplus (PR_1 \oplus k_1)(PR_1 \oplus k_1 \oplus x_1), \end{cases}$$

где $x_0,...,x_{31}$ – биты входного значения блоков замены, $y_0,...,y_{31}$ – биты выходного значения блоков замены, $k_0,...,k_{31}$ – биты раундового ключа шифрования, $PR_0,...,PR_{31}$ – биты правой части открытого текста.

Выполнив алгебраический анализ алгоритма «Магма» (3–5, 8 раундов) по описанной выше методике, были получены результаты оценки защищенности информации, представленные в табл. 2.

Таблица 2

Результаты алгебраического анализа алгоритма «Магма»

Кол-во раундов	Кол-во известных текстов	Кол-во уравнений	Кол-во неизвестных	Кол-во литералов	Кол-во клозов	Кол-во найденных решений	Общее время вычислений в SageMath Cloud (сек)	Время решения системы булевых уравнений (сек)
3 раунда	1	600	224	1591	19467	$>10^5$	238,45	198,14
	2	1200	352	2819	38811	1	36,55	0,35
4 раунда	2	1600	512	4839	67886	4	93,44	10,27
	3	2400	704	7202	101968	1	202,56	1,32
5 раундов	3	3000	928	10596	152045	1	394,68	24,96
8 раундов	4	5376	2048	30062	431267	1	3029,56	416,31

Для получения сравнительных оценок защищенности информации в зависимости от используемых заполнений блоков замены проведено моделирование алгебраического анализа на алгоритм «Магма» с тождественными блоками замены S(X)=X и с блоками замены, являющимися слабыми к линейному анализу (табл. 3) [18].

Таблица 3

Заполнение слабых к линейному анализу блоков замены

X	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Y	15	7	11	3	13	5	9	1	14	6	10	2	12	4	8	0

В ходе проведенного моделирования получены следующие временные оценки защищенности, представленные в табл. 4.

Для 8 раундов шифрования при моделировании фиксировались значения 68 битов ключа алгоритма «Магма»: 0-15, 51-55, 64-66, 128-130, 179-183, 192-207, 224-231, 244-255.

Таблица 4

Моделирование алгебраического анализа «Магма» при использовании «слабых» блоков замены

Кол-во известных текстов	Кол-во уравнений	Кол-во неизвестных	Кол-во литералов	Кол-во клозов	Кол-во найденных решений	Общее время вычислений в SageMath Cloud (сек)	Время решения системы булевых уравнений (сек)
3 раунда шифрования «Магма» (со слабыми к линейному анализу блоками)							
2	1200	352	1470	9400	8	28,51	0,35
3	1800	480	1965	14084	1	39,91	0,47
3 раунда шифрования «Магма» (с блоками замены S(X)=X)							
2	1200	352	1292	7393	2048	21,11	2,10
3	1800	480	1889	11014	1	37,19	1,07
4 раунда шифрования «Магма» (со слабыми к линейному анализу блоками)							
2	1600	512	2940	16642	128	96,10	0,77
3	2400	704	3869	24982	2	142,36	0,88
4	3200	896	4798	33316	2	195,61	1,23
5	4000	1088	5725	41646	2	294,72	1,51

Кол-во известных текстов	Кол-во уравнений	Кол-во неизвестных	Кол-во литералов	Кол-во клозов	Кол-во найденных решений	Общее время вычислений в SageMath Cloud (сек)	Время решения системы булевых уравнений (сек)
6	4800	1280	6839	49922	2	612,03	4,11
7	5600	1472	7951	58174	1	700,96	2,63
4 раунда шифрования «Магма» (с блоками замены S(X)=X)							
3	2400	704	3726	19280	4	106,76	1,33
4	3200	896	4606	25830	2	144,66	1,10
5	4000	1088	5484	32294	1	242,21	1,24
5 раундов шифрования «Магма» (со слабыми к линейному анализу блоками)							
3	3000	928	5932	39549	4	320,17	4,15
4	4000	1184	7436	52872	2	488,65	4,47
5	5000	1440	9194	66113	2	478,31	2,51
6	6000	1696	10705	79506	2	875,24	6,91
7	7000	1952	12459	92707	1	1135,61	3,36
5 раундов шифрования «Магма» (с блоками замены S(X)=X)							
3	3000	928	5338	32873	40	678,80	520,89
4	4000	1184	7068	43926	2	415,31	28,65
5	5000	1440	8787	54647	1	501,18	4,92
8 раундов шифрования «Магма» (со слабыми к линейному анализу блоками)							
4	5376	2048	15395	110844	4096	5972,41	1843,67
8 раундов шифрования «Магма» (с блоками замены S(X)=X)							
4	5376	2048	13764	92370	1024	4842,31	1374,12

Алгебраический анализ алгоритма PRESENT. Алгоритм PRESENT представляет собой шифр, построенный на принципе сети подстановки-перестановки (SP-сети) [19]. PRESENT содержит 31 раунд, в котором применяются операции сложения по модулю 2 с раундовым ключом, преобразование замены в 16 блоках замены с длинной вектора 4 бита, перестановка битов. В данной работе рассмотрен алгебраический анализ алгоритма PRESENT с независимыми раундовыми ключами (без использования структуры алгоритма генерации раундовых ключей). Структура алгоритма PRESENT приведена на рис. 2. Преобразование замены и перестановки заданы табл. 5, 6 соответственно.

Таблица 5

Замены в блоках алгоритма PRESENT

X	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S(X)	12	5	6	11	9	0	10	13	3	14	15	8	4	7	1	2

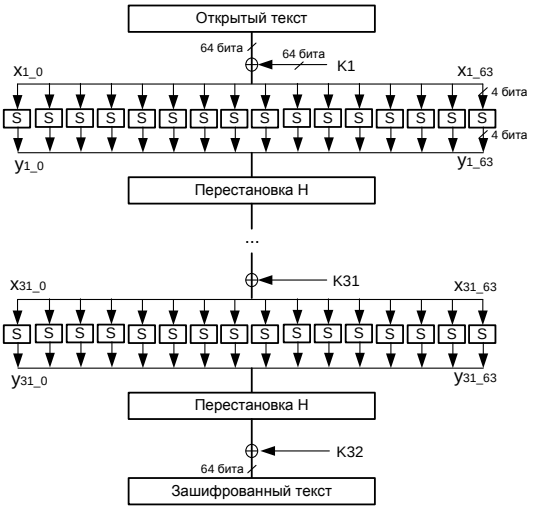

Рис. 2. Структура алгоритма PRESENT

Таблица 6

Перестановка алгоритма PRESENT

b	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
H(b)	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51
b	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
H(b)	4	20	36	52	5	21	37	53	6	22	38	54	7	23	39	55
b	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
H(b)	8	24	40	56	9	25	41	57	10	26	42	58	11	27	43	59
b	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
H(b)	12	28	44	60	13	29	45	61	14	30	46	62	15	31	47	63

Алгоритм выработки раундового ключа из секретного ключа $K = (k_{79},...,k_0)$ заключается в выполнении следующих преобразований:

1. Циклический сдвиг на 61 позиций влево.
2. Выполнение замены старших 4-ех разрядов в S-блоке.
3. Присвоение битам $(k_{19},...,k_{15})$ значения суммы по модулю два $(k_{19},...,k_{15})$ и номера раунда.

Результаты исследований других авторов по алгебраическому анализу алгоритма PRESENT представлены в работах [20, 21].

В ходе выполнения моделирования алгебраического анализа алгоритма PRESENT для блока замены сформированы следующие булевы нелинейные уравнения (x0,x1,x2,x3 – биты входного значения блока замены, y0,y1,y2,y3 – биты выходного значения блока замены):

x1·x2 ⊕ x0 ⊕ x1 ⊕ x3 ⊕ y3=0,

x0·x1 ⊕ x0·x2 ⊕ x0 ⊕ x1 ⊕ y0 ⊕ y2 ⊕ y3 ⊕ 1=0,

x0·x3 ⊕ x1·x3 ⊕ x1·y0 ⊕ x0·y1 ⊕ x0·y2 ⊕ x1 ⊕ x2 ⊕ y2=0,

x0·x3 ⊕ x0·y0 ⊕ x1·y1 ⊕ x0 ⊕ x2 ⊕ y2=0,

x0·x2 ⊕ x0·y0 ⊕ x0·y1 ⊕ x1·y2 ⊕ x1 ⊕ x2 ⊕ x3 ⊕ y2 ⊕ y3=0,

x0·x1 ⊕ x1·x3 ⊕ x1·y3 ⊕ x0 ⊕ x3 ⊕ y3=0,

x0·x2 ⊕ x0·y0 ⊕ x0·y2 ⊕ x0·y3=0,

x0·x1 ⊕ x2·y0 ⊕ x0·y1 ⊕ x0·y2 ⊕ x2 ⊕ x3 ⊕ y1 ⊕ y2 ⊕ y3 ⊕ 1=0,

x0·x1 ⊕ x0·x2 ⊕ x0·x3 ⊕ x2·y1 ⊕ x0·y2 ⊕ x0 ⊕ x2 ⊕ x3 ⊕ y1 ⊕ y3 ⊕ 1=0,

x0·x3 ⊕ x2·x3 ⊕ x0·y0 ⊕ x0·y1 ⊕ x2·y2 ⊕ x1 ⊕ y1 ⊕ y2 ⊕ 1=0,

x0·x2 ⊕ x2·x3 ⊕ x2·y3=0,

x0·x2 ⊕ x3·y0 ⊕ x0 ⊕ x1 ⊕ y1 ⊕ 1=0,

x0·x1 ⊕ x0·x2 ⊕ x0·x3 ⊕ x1·x3 ⊕ x2·x3 ⊕ x0·y1 ⊕ x3·y1 ⊕ x3=0,

x0·x1 ⊕ x3·y2 ⊕ x1 ⊕ x2 ⊕ y1 ⊕ y2 ⊕ 1=0,

x0·x1 ⊕ x1·x3 ⊕ x2·x3 ⊕ x3·y3 ⊕ x1 ⊕ x2 ⊕ x3 ⊕ y1 ⊕ y2 ⊕ 1=0,

x1·x3 ⊕ x0·y1 ⊕ y0·y1 ⊕ x0 ⊕ x1 ⊕ x2 ⊕ y1 ⊕ y3=0,

y0·y2 ⊕ x3 ⊕ y1 ⊕ y3 ⊕ 1=0,

x0·x1 ⊕ x1·x3 ⊕ x0·y1 ⊕ y0·y3 ⊕ x0 ⊕ x1 ⊕ x2 ⊕ x3 ⊕ y1 ⊕ y2 ⊕ y3 ⊕ 1=0,

x2·x3 ⊕ x0·y1 ⊕ y1·y2 ⊕ x1 ⊕ x3 ⊕ y2 ⊕ y3=0,

x0·x1 ⊕ x1·x3 ⊕ x2·x3 ⊕ x0·y0 ⊕ x0·y2 ⊕ y1·y3 ⊕ x0 ⊕ x3=0,

x0·x1 ⊕ x2·x3 ⊕ x0·y1 ⊕ y2·y3 ⊕ x2 ⊕ y2=0.

Преобразования замены в одном блоке могут быть описаны с помощью 21 линейно независимого уравнения. Преобразование перестановки не потребует введения новых переменных, а лишь приводит к перенумерации битов в соответствии с таблицей перестановки. Также для каждого раунда шифрования можно использовать дополнительные уравнения, описывающие применяемые замены в S-блоке к старшим четырем битам ключа, что повлечет формирование 21 уравнения и введения 4 дополнительных неизвестных.

В общем виде преобразования шифрования алгоритма PRESENT могут быть описаны системой из $m = i \cdot 21$ уравнений с $n = i \cdot 8$ неизвестных, где i равно числу используемых при шифровании и формировании раундовых ключей блоков замены. В этом случае преобразования в 31 раунде шифрования алгоритма PRESENT могут быть заданы с помощью системы из 11067 булевых нелинейных уравнений с 4216 неизвестными, число используемых блоков замены составляет $i = 16 \cdot 31 + 31 = 527$.

Используя разработанные алгоритмы, было проведено моделирование алгебраического анализа шифра PRESENT без использования структуры алгоритма выработки раундовых ключей. При анализе трех раундов шифра PRESENT были выполнены следующие замены:

$$X1 = P \oplus K1,$$
$$X2 = H(Y1) \oplus K2,$$
$$X3 = H(Y2) \oplus K3,$$
$$Y3 = H^{-1}(C),$$

где $X1,...,X3$ – 64-х битные входные значения преобразования замены в S-блоках, $Y1,...,Y3$ – 64-х битные выходные значения преобразования замены в S-блоках, $K1,...,K3$ – 64-х битные раундовые ключи, $H()$ – преобразование перестановки, $H^{-1}()$ – преобразование обратное, преобразованию перестановки.

При анализе четырех раундов PRESENT использовалась следующая зависимость между переменными:

$$X1 = P \oplus K1,$$
$$X2 = H(Y1) \oplus K2,$$
$$X3 = H(Y2) \oplus K3,$$
$$X4 = H(Y3) \oplus K4,$$
$$Y4 = H^{-1}(C),$$

где $X1,...,X4$ – 64-х битные входные значения преобразования замены в S-блоках, $Y1,...,Y4$ – 64-х битные выходные значения преобразования замены в S-блоках, $K1,...,K4$ – 64-х битные раундовые ключи, $H()$ – преобразование перестановки, $H^{-1}()$ – преобразование обратное, преобразованию перестановки.

Полученные временные и вычислительные оценки сложности анализа приведены в табл. 7.

Таблица 7

Результаты моделирования алгебраического анализа алгоритма PRESENT

Кол-во текстов	Кол-во уравнений	Кол-во неизвестных	Кол-во литералов	Кол-во клозов	Кол-во решений	Общее время анализа, сек.	Время решения системы, сек	Объем памяти, Гб
3 раунда PRESENT								
2	2016	448	8786	137530	$>10^5$	338,85	33,42	0,75
3	3024	576	16083	274534	$>10^4$	421,91	73,12	0,98
4	4284	704	16057	273914	16	490,96	2,56	1,26
5	5040	832	19968	342522	8	635,28	3,74	1,39
6	6048	960	23863	410800	1	1005,68	5,01	1,43
4 раунда PRESENT								
2	2688	640	13012	209258	$>10^4$	711,64	205,65	1,27
3	4032	832	18805	313070	$>2\cdot10^3$	4156,61	3069,35	1,73
4	5376	1024	24794	417010	1028	1626,16	428,15	1,67
5	6720	1216	30585	520686	256	1654,79	379,58	1,82
8	10752	1792	48784	832128	16	3268,42	527,51	2,79

Заключение. Разработанные в ходе выполнения исследования алгоритмы и методика могут быть в дальнейшем использованы для оценки защищенности произвольных преобразований на основе операций замены и сложения по модулю 2^n при алгебраическом анализе. В ходе моделирования алгебраического анализа была оценена защищенность данных при сокращенном числе раундов шифрования данных алгоритмов (вычисления проводились с использованием вычислительных ресурсов SageMath Cloud). Для 8 раундов алгоритма «Магма» (ГОСТ 34.12-2015, n=64) ключ шифрования удалось вычислить при известных 4 текстах за 3029,56 сек. Для 4 раундов шифрования PRESENT (ISO 29192-2:2012) 16 наборов ключей были вычислены при наличии 8 текстов за 3268,42 сек.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Семенов А.А., Заикин О.С., Беспалов Д.В., Ушаков А.А.* SAT-подход в криптоанализе некоторых систем поточного шифрования // Вычислительные технологии. – 2008. – Т. 13, № 6.
2. *Семенов А.А.* Алгоритмы решения задачи о булевой выполнимости (SAT) и их применение в криптоанализе // PHDays 2015.
3. *Soos M., Nohl K., Castelluccia C.* Extending SAT Solvers to Cryptographic Problems // Theory and Applications of Satisfiability Testing – SAT, 2009. – P. 244-257.
4. *Sepehrdad P.* Statistical and Algebraic Cryptanalysis of Lightweight and Ultra-lightweight Symmetric Primitives: PhD Dissertation, 2012. – 180 p.
5. *Erickson J., Ding J., Christensen C.* Algebraic Cryptanalysis of SM4: Grobner Basis Attack and SAT Attack Compared // 12th International Conference, Seoul, Korea, 2009. – P. 73-86.
6. *Albrecht M.* Tools for Algebraic Cryptanalysis // Proceedings of the ECRYPT Workshop on Tools for Cryptanalysis. – 2010. – P. 13-14,
7. *Courtois N.* Algebraic Complexity Reduction and Cryptanalysis of GOST. –http://www.nicolascourtois.com/papers/gostac11.pdf.
8. *Weinmann R.-P.* Algebraic Methods in Block Cipher Cryptanalysis. PhD Dissertation, 2009. – 113 p.
9. *Bulygin S.* Algebraic cryptanalysis of the round-reduced and side channel analysis of the full PRINTCipher-48. – http://eprint.iacr.org/2011/287.pdf.
10. *Otpuschennikov I., Semenov A., Gribalova I., Zaikin O., Kochemazov S.* Encoding Cryptographic functions to SAT Using TRANSALG system // ECAI 2016: 22nd European Conference on Artificial Intelligence. – 2016. – P. 1594-1595.
11. *Soos M.* CryptoMiniSat 2.5.1. – http://www.msoos.org/wordpress/wp-content/uploads/2010/08/cryptominisat-2.5.1.pdf.
12. *Bard G., Courtois N., Jefferson C.* Efficient Methods for Conversion and Solution of Sparse Systems of Low-Degree Multivariate Polynomials over GF(2) via SAT-Solvers // Cryptology ePrint Archive. – 2007. – Vol. 24. – https://eprint.iacr.org/2007/024.pdf.
13. SageMath, the Sage Mathematics Software System, The Sage Developers, 2016. – http://www.sagemath.org.
14. ГОСТ Р 34.12-2015. Криптографическая защита информации. – http://tc26.ru/standard/gost/GOST_R_3412-2015.pdf.
15. *Бабенко Л.К., Маро Е.А.* Анализ стойкости блочных алгоритмов шифрования к алгебраическим атакам // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 110-119.
16. *Babenko L. K., Maro E.A., Anikeev M.V.* Modeling of algebraic analysis of GOST+ cipher in SageMath // 7th international conference on Security of information and networks. – 2016. – P. 100-103.
17. *Babenko L.K., Ishchukova E.A., Maro E.A.* Algebraic analysis of GOST encryption algorithm // 4th International conference on Security of information and networks. – 2011. – P. 57-62.
18. *Бабенко Л.К., Ищукова Е.А* Анализ алгоритма ГОСТ 28147-89: поиск слабых блоков // Извести ЮФУ. Технические науки. – 2014. – № 2 (151). – С. 129-138.
19. *Bogdanov A., Knudsen L.R., Leander G., Paar C., Poschmann A., Robshaw M.J., Seurin B., Vikkelsoe C.* PRESENT: An ultra-light--weight block cipher // Cryptographic Hardware and Embedded Systems- -CHES ’07, 9th International Workshop, Vienna, Austria, 2007. – Vol. 4727. – P. 450-466.

20. *Bard G.* Algebraic Cryptanalysis. – 2009. – 356 p.
21. *Nakahara J., Sepehrdad P., Zhang B., Wang M.* Linear (Hull) and Algebraic Cryptanalysis of the Block Cipher PRESENT // 8th International Conference on Cryptology and Network Security, CANS '09, New York, 2009. – P. 58-75.

REFERENCES

1. *Semenov A.A., Zaikin O.S., Bespalov D.V., Ushakov A.A.* SAT-podkhod v kriptoanalize nekotorykh sistem potochnogo shifrovaniya [SAT-approach in the cryptanalysis of certain stream encryption systems], *Vychislitel'nye tekhnologii* [Computational technologies], 2008, Vol. 13, No. 6.
2. *Semenov A.A.* Algoritmy resheniya zadachi o bulevoy vypolnimosti (SAT) i ikh primenenie v kriptoanalize [Algorithms for solving the problem of Boolean satisfiability (SAT) and their use in cryptanalysis], *PHDays 2015*.
3. *Soos M., Nohl K., Castelluccia C.* Extending SAT Solvers to Cryptographic Problems, *Theory and Applications of Satisfiability Testing – SAT, 2009*, pp. 244-257.
4. *Sepehrdad P.* Statistical and Algebraic Cryptanalysis of Lightweight and Ultra-lightweight Symmetric Primitives: PhD Dissertation, 2012, 180 p.
5. *Erickson J., Ding J., Christensen C.* Algebraic Cryptanalysis of SM4: Grobner Basis Attack and SAT Attack Compared, *12th International Conference, Seoul, Korea, 2009*, pp. 73-86.
6. *Albrecht M.* Tools for Algebraic Cryptanalysis, *Proceedings of the ECRYPT Workshop on Tools for Cryptanalysis*, 2010, pp. 13-14.
7. *Courtois N.* Algebraic Complexity Reduction and Cryptanalysis of GOST. Available at: http://www.nicolascourtois.com/papers/gostac11.pdf.
8. *Weinmann R.-P.* Algebraic Methods in Block Cipher Cryptanalysis. PhD Dissertation, 2009, 113 p.
9. *Bulygin S.* Algebraic cryptanalysis of the round-reduced and side channel analysis of the full PRINTCipher-48. Available at: http://eprint.iacr.org/2011/287.pdf.
10. *Otpuschennikov I., Semenov A., Gribalova I., Zaikin O., Kochemazov S.* Encoding Cryptographic functions to SAT Using TRANSALG system, *ECAI 2016: 22nd European Conference on Artificial Intelligence,* 2016, pp. 1594-1595.
11. *Soos M.* CryptoMiniSat 2.5.1. Available at: http://www.msoos.org/wordpress/wp-content/uploads/2010/08/cryptominisat-2.5.1.pdf.
12. *Bard G., Courtois N., Jefferson C.* Efficient Methods for Conversion and Solution of Sparse Systems of Low-Degree Multivariate Polynomials over GF(2) via SAT-Solvers, *Cryptology ePrint Archive*, 2007, Vol. 24. Available at: https://eprint.iacr.org/2007/024.pdf.
13. SageMath, the Sage Mathematics Software System, The Sage Developers, 2016. Available at: http://www.sagemath.org.
14. GOST R 34.12-2015. Kriptograficheskaya zashchita informatsii [Cryptographic protection of information]. Available at: http://tc26.ru/standard/gost/GOST_R_3412-2015.pdf.
15. *Babenko L.K., Maro E.A.* Analiz stoykosti blochnykh algoritmov shifrovaniya k algebraicheskim atakam [Analysis of resistance block ciphers against algebraic cryptanalysis], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2011, No. 12 (125), pp. 110-119.
16. *Babenko L. K., Maro E.A., Anikeev M.V.* Modeling of algebraic analysis of GOST+ cipher in SageMath, *7th international conference on Security of information and networks,* 2016, pp. 100-103.
17. *Babenko L.K., Ishchukova E.A., Maro E.A.* Algebraic analysis of GOST encryption algorithm, *4th International conference on Security of information and networks,* 2011, pp. 57-62.
18. *Babenko L.K., Ishchukova E.A.* Analiz algoritma GOST 28147-89: poisk slabykh blokov [Analysis of algorithm GOST 28147-89: research of weak s-boxes], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2014, No. 2 (151), pp. 129-138.
19. *Bogdanov A., Knudsen L.R., Leander G., Paar C., Poschmann A., Robshaw M.J., Seurin B., Vikkelsoe C.* PRESENT: An ultra-light--weight block cipher, *Cryptographic Hardware and Embedded Systems-CHES '07, 9th International Workshop, Vienna, Austria, 2007,* Vol. 4727, pp. 450-466.
20. *Bard G.* Algebraic Cryptanalysis, 2009, 356 p.

21. *Nakahara J., Sepehrdad P., Zhang B., Wang M.* Linear (Hull) and Algebraic Cryptanalysis of the Block Cipher PRESENT, *8th International Conference on Cryptology and Network Security, CANS '09, New York, 2009,* pp. 58-75.

Статью рекомендовал к опубликованию д.т.н., профессор К.Е. Румянцев.

Бабенко Людмила Климентьевна – Южный федеральный университет; e-mail: blk@fib.tsure.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 88634312018; кафедра безопасности информационных технологий; профессор.

Маро Екатерина Александровна – e-mail: marokat@gmail.com; тел.: 88634371905; кафедра безопасности информационных технологий; ассистент.

Babenko Lyudmila Klimentevna – Southern Federal University; e-mail: blk@fib.tsure.ru; 2, Chehov street, Taganrog, 347928, Russia; phone: +78634312018; the department of security of information technologies; professor.

Maro Ekaterina Aleksandrovna – e-mail: marokat@gmail.com; phone: +78634371905; the department of security of information technologies; assistant.

УДК 004.067 DOI 10.18522/2311-3103-2016-5057

Ю.А. Брюхомицкий

ИММУНОЛОГИЧЕКИЙ МЕТОД ВЕРИФИКАЦИИ РУКОПИСИ С ИСПОЛЬЗОВАНИЕМ ВЕКТОРНОГО ПРЕДСТАВЛЕНИЯ ДАННЫХ

Предлагается метод текстонезависимого онлайн-анализа рукописи, использующий принципы функционирования искусственных иммунных систем, ориентированный на задачу верификации личности по рукописи. Метод основан на использовании иммунологической модели отрицательного отбора. Метод может применяться для анализа произвольных текстов произвольного объема. Особенностью метода является представление информационных потоков рукописи в виде последовательности информационных единиц фиксированного формата и размера, с последующей их децентрализованной обработкой. Для этого применяется двойное квантование во времени исходных информационных потоков рукописи. Информационные единицы рукописи, в свою очередь, представляются векторами в многомерном пространстве признаков, характеризующих положение пера. Предлагаемый метод верификации рукописи обладает рядом преимуществ. По сравнению известным методом онлайн-анализа рукописи на основе частотного разложения, пригодным исключительно для анализа сильно ограниченных объемов текстов, представленных предопределенными словами или короткими фразами, предлагаемый метод не имеет таких ограничений и позволяет проводить анализ произвольных рукописных текстов произвольного объема. За счет значительного увеличения объема используемых рукописных данных, характеризующих особенности личности, точность анализа повышается. Другим принципиальным отличием предлагаемого иммунологического онлайн-анализа является переход от интегральной оценки рукописных данных за некоторый фиксированный период времени к непрерывной оценке их временной структуры с возможностью своевременного принятия правильного верификационного решения в темпе поступления рукописных данных. Такая схема распознавания дает преимущества при решении определенных классов задач, критичных ко времени принятия верификационного решения.

Текстонезависимый онлайн-анализ рукописи; верификация личности по рукописи; принципы работы искусственных иммунных систем; векторное представление информационных единиц рукописи.