2. Множество орграфов регистров с разнонаправленными сдвигами

Теорема 3. Пусть n чётное, орграф Γ_i при чётных i имеет контур $(0,\dots,n-1)$ и дугу $(i,(i{+}l) \bmod n)$, при нечётных i — контур $(n{-}1,\dots,0)$ и дугу $(i,(i{+}\lambda) \bmod n)$. Если НОД$(n,l{-}1){=}1$ или НОД$(n,\lambda{+}1){=}1$, то множество $\hat{\Gamma}$ примитивное и $\exp\hat{\Gamma} \leqslant 2n-2$.

Полученные оценки экспонентов множеств графов имеют порядок $\mathrm{O}(n)$. В то же время экспонент отдельного орграфа множества в ряде случаев имеет порядок $\mathrm{O}(n^2)$ и достигает максимального значения n^2-2n+2.

ЛИТЕРАТУРА

1. *Фомичев В. М., Мельников Д. А.* Криптографические методы защиты информации. В 2 ч. Ч. 1. Математические аспекты. М.: Изд-во Юрайт, 2016. 209 с.
2. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
3. *Авезова Я. Э., Фомичев В. М.* Условия примитивности и оценки экспонентов множеств ориентированных графов // Прикладная дискретная математика. 2017. №1(35). С. 89–101.

УДК 519.7 DOI 10.17223/2226308X/10/26

ПРИМЕНЕНИЕ АЛГОРИТМОВ РЕШЕНИЯ ПРОБЛЕМЫ БУЛЕВОЙ ВЫПОЛНИМОСТИ ФОРМУЛ ДЛЯ ОЦЕНКИ СТОЙКОСТИ БЛОЧНЫХ ШИФРОВ СЕМЕЙСТВА ГОСТ К АЛГЕБРАИЧЕСКОМУ КРИПТОАНАЛИЗУ[1]

Л. К. Бабенко, Е. А. Маро

Представлено применение методов алгебраического анализа к стандартам симметричного шифрования Магма и Present. В качестве способов решения систем булевых нелинейных уравнений выбраны: 1) сведение к задаче выполнимости булевых формул (SAT-задаче) и решение с помощью CryptoMiniSat; 2) применение метода расширенной линеаризации. Для данных методов рассмотрены методики проведения оценки защищённости информации методами алгебраического криптоанализа при использовании симметричных блочных шифров. Проведены эксперименты, показывающие применимость алгебраических методов криптоанализа для сокращённого числа раундов исследуемых шифров. Для шифра Магма выполнен алгебраический анализ при различных заполнениях блоков замены: заданном в стандарте, тождественной замене и замене, являющейся слабой к линейному анализу.

Ключевые слова: *криптография, алгебраический криптоанализ, блочные алгоритмы шифрования, Магма, PRESENT, SAT-решатель, SageMath.*

В современном криптографическом научном сообществе на протяжении последних 15 лет развиваются и совершенствуются методы алгебраического криптоанализа, основанные на использовании нелинейных примитивов алгоритмов шифрования с целью описания алгоритма шифрования в виде систем уравнений, связывающих искомый ключ и известные данные. Повышение производительности современных SAT-решателей привело к возникновению идеи о возможности их применения для вычислительно трудоёмких задач криптоанализа [1 – 3]. Применяются различные методики проведения алгебраического криптоанализа на основе SAT-решения и построения

[1]Работа выполнена при поддержке гранта РФФИ, проект №17-07-00654 А.

Binary Decision Diagram (BDD). Одной из часто используемых методик при использовании SAT-решателей является Guess-and-Determine, которая заключается в фиксировании значений некоторых битов ключа, что позволяет существенно сократить общее время поиска решения рассматриваемой задачи криптоанализа. Методика Guess-and-Determine применена, например, в [4 – 6] к шифру Магма.

Результаты проведения алгебраического анализа шифра PRESENT другими авторами представлены в работах [7, 8].

Моделирование алгебраического анализа шифров выполнялось в среде SageMath [9]. Использовались функции библиотеки sage.sat.converters.polybori для преобразования системы уравнений из АНФ в КНФ (CNFEncoder). Решение системы проведено на основе SAT-решателя CryptoMiniSat и осуществлялось с применением библиотеки sage.sat.boolean_polynomials [10]. Для проведения экспериментов в среде Visual Studio C++ разработана программа формирования и решения систем булевых нелинейных уравнений второй степени методом XL. В качестве блока замены, являющегося слабым к линейному анализу, взята замена, приведённая в [11]. Получены экспериментальные результаты применения алгебраического криптоанализа к шифрам Магма и PRESENT (см. таблицу) на ПК с процессором IntelCore i5 2,8 ГГц и 8 Гбайт оперативной памяти. Проведён поиск всех выполняющих наборов сформированной SAT-задачи. Найденные значения ключей шифрования оказались эквивалентыми на анализируемых парах открытый текст/шифртекст. При проведении эксперимента для восьми раундов Магма были зафиксированы 68 битов ключа (применялся метод Guess-and-Determine).

Результаты экспериментов по алгебраическому анализу шифров PRESENT и Магма

			SAT-метод					XL-метод	
Число пар открытый текст/ шифртекст	Кол-во уравнений	Кол-во неизвестных	Кол-во литералов	Кол-во клозов	Кол-во выполняющих наборов	Время решения, с	Объём памяти, Гбайт	Сложность решения, кол-во операций сложения	Время решения, с
Три раунда шифрования PRESENT									
3	3024	576	16083	274534	$> 10^4$	73,12	0,98	$2^{41,08}$	23,22
5	5040	832	19968	342522	8	3,74	1,39	$2^{43,29}$	107,39
6	6048	960	23863	410800	1	5,01	1,43	$2^{44,08}$	185,78
Четыре раунда шифрования PRESENT									
3	4032	832	18805	313070	$> 2 \cdot 10^3$	3069,35	1,73	$2^{42,33}$	55,21
5	6720	1216	30585	520686	256	379,58	1,82	$2^{44,53}$	253,51
8	10752	1792	48784	832128	16	527,51	2,79	$2^{46,57}$	1044,72
Пять раундов шифрования Магма (со слабыми к линейному анализу блоками замены)									
3	3000	928	5932	39549	4	4,15	1,62	$2^{40,64}$	17,14
7	7000	1952	12459	92707	1	3,36	2,26	$2^{44,30}$	216,27
Пять раундов шифрования Магма (с блоками замены S(X)=X)									
3	3000	928	5338	32873	40	520,89	1,73	$2^{40,64}$	17,14
5	5000	1440	8787	54647	1	4,92	1,85	$2^{42,85}$	79,25
Пять раундов шифрования Магма									
3	3000	928	10596	152045	1	24,96	1,42	$2^{40,64}$	17,14
Восемь раундов шифрования Магма (со слабыми к линейному анализу блоками замены)									
4	5376	2048	15395	110844	4096	1843,67	4,59	$2^{43,92}$	166,3
Восемь раундов шифрования Магма (с блоками замены S(X)=X)									
4	5376	2048	13764	92370	1024	1374,12	3,86	$2^{43,92}$	166,3
Восемь раундов шифрования Магма									
4	5376	2048	30062	431267	1	416,31	3,6	$2^{43,92}$	166,3

ЛИТЕРАТУРА

1. *Courtois N., Bard G., and 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, Report 2007/024, 2007. http://eprint.iacr.org/2007/024
2. *Soos M., Nohl K., and Castelluccia C.* Extending SAT solvers to cryptographic problems // Proc. 12th Intern. Conf. Theory and Applications of Satisfiability Testing. 2009. P. 244–257.
3. *Charfi A.* SAT-Solving in Algebraic Cryptanalysis. Bachelor Thesis, 2014. https://www.cdc.informatik.tu-darmstadt.de/reports/reports/Ahmed_Charfi.bachelor.pdf
4. *Courtois N., Gawinecki J., and Song G.* Contradiction immunity and guess-then-determine attack on GOST // Tatra Mt. Math. Publ. 2012. V. 53. P. 65–79. https://www.sav.sk/journals/uploads/0114113604CuGaSo.pdf
5. *Kazymyrov O., Oliynykov R., and Raddum H.* Influence of addition modulo 2^n on algebraic attacks // Cryptography and Communications. 2016. V. 8. Iss. 2. P. 277–289.
6. *Dinur I., Dunkelman O., and Shamir A.* Improved attacks on full GOST // LNCS. 2012. V. 7549. P. 9–28. https://eprint.iacr.org/2011/558.pdf
7. *Nakahara J., Sepehrdad P., Zhang B., and Wang M.* Linear (hull) and algebraic cryptanalysis of the block cipher PRESENT // 8th Intern. Conf. Cryptology and Network Security CANS'09. N.Y., 2009. P. 58–75.
8. *Lacko-Bartosov L.* Algebraic cryptanalysis of PRESENT based on the method of syllogism // Tatra Mt. Math. Publ. 2012. V. 53. P. 201–212. https://www.sav.sk/journals/uploads/0114111812lackob.pdf
9. The Sage Developers. SageMath, the Sage Mathematics Software System (Version 7.4), 2016. http://www.sagemath.org
10. Sage Reference Manual: Cryptography Release 7.5. http://doc.sagemath.org/pdf/en/reference/cryptography/cryptography.pdf
11. *Бабенко Л. К., Ищукова Е. А.* Анализ алгоритма ГОСТ 28147-89: поиск слабых блоков // Известия ЮФУ. Технические науки. Информационная безопасность. 2014. №2 (151). С. 129–138.

УДК 519.725 DOI 10.17223/2226308X/10/27

КРИПТОГРАФИЧЕСКИЙ АНАЛИЗ ОБОБЩЁННОГО ПРОТОКОЛА ЭЛЬ-ГАМАЛЯ НАД ГРУППОЙ $\mathbf{GL}(8, \mathbb{F}_{251})$[1]

Д. Д. Болотов, Е. А. Магдин

Приводится криптографический анализ обобщённого протокола Эль-Гамаля над группой $\mathrm{GL}(8, \mathbb{F}_{251})$, описанного в работе Педро Хехта. Показано, что существует алгоритм, который эффективно вычисляет формируемый в протоколе ключ. Схема формирования общего ключа в обобщённом протоколе Эль-Гамаля является частным случаем схемы Шпильрайна — Ушакова. Анализ показывает, что рассматриваемый протокол является теоретически и практически нестойким.

Ключевые слова: *криптографический анализ, протокол Эль-Гамаля, протокол Шпильрайна — Ушакова.*

Введение

В работе рассматривается опубликованный в 2017 г. обобщённый протокол Эль-Гамаля [1], который в общем случае строится на группе матриц над конечным полем.

[1]Исследование выполнено при поддержке Российского научного фонда (проект №16-11-10002).