DOI: 10.17117/nv.2015.03.038

Поступила (Received): 24.09.2015

<http://ucom.ru/doc/nv.2015.03.038.pdf>

info@sfedu.ru

Бабенко Л.К., Ищукова Е.А., Алексеев Д.М.
Реализация поиска слайдовых пар для алгоритма
шифрования Магма с использованием технологии MPI

Babenko L.K., Ischukova E.A., Alekseev D.M.
Implementing of slide pairs' searching for encryption
algorithm Magma with using MPI technology

В статье рассмотрены основные механизмы применения слайдовой атаки к симметричным блочным шифрам. Рассмотрена возможность применения слайдовой атаки для оценки стойкости алгоритма шифрования данных Магма в случае использования слабых ключей шифрования. Приведен пример слайдовой пары для рассматриваемой схемы анализа применительно к шифру Магма. Основной задачей при слайдовой атаке является поиск слайдовых пар. Для сокращения времени анализа разработан и реализован параллельный алгоритм, осуществляющий непересекающийся полный перебор правой части парного текста для поиска слайдовой пары с использованием технологии MPI. На основе готовой реализации получены обширные экспериментальные данные, отражающие скорость поиска слайдовой пары в зависимости от параметров исследуемого шифра, а также конфигурации вычислительной сети. По полученным практическим данным построены и проанализированы графики временных зависимостей. В заключении статьи дана оценка эффективности самого подхода к поиску слайдовых пар, сделаны предположения о дальнейших направлениях развития данного метода анализа

Ключевые слова: криптография, блочный шифр

The article describes the basic mechanisms of the application of the slide attack to symmetric block ciphers. In the article there is described the possibility of using a slide attack for assessing the stability of the algorithm encryption Magma in the case of weak encryption keys. There is given an example of a slide pair for the scheme of analysis in relation to the code of Magma. The main objective of the slide attack is searching for slide pairs. To reduce the time of analysis we developed and implemented a parallel algorithm that performs disjoint exhaustive search of the right side of a pair of text to search for a pair of slide technology with MPI. On the basis of the final implementation was received the extensive experimental data that reflect the search of the speed slide pair depending on the parameters of the test code number, and configuration of the computer network. The graphs of time dependences are constructed and analyzed on the derived test data. In conclusion of the article there is given the appraisal of effectiveness of the approach to the search for slide pairs, the assumptions about the future directions of development of this method of the analysis are made

Key words: cryptography, block cipher

Бабенко Людмила Климентьевна
Доктор технических наук, профессор
Южный федеральный университет
г. Таганрог, ул. Чехова, 2

Babenko Ludmila Klimentievna
Doctor of Technical Sciences, Professor
Southern Federal University
Taganrog, Chehov st., 2

Ищукова Евгения Александровна
Кандидат технических наук, профессор
Южный федеральный университет
г. Таганрог, ул. Чехова, 2

Ischukova Evgeniya Alexandrovna
Candidate of Technical Sciences, associate Professor
Southern Federal University
Taganrog, Chehov st., 2

Алексеев Дмитрий Михайлович
Студент
Южный федеральный университет
г. Таганрог, ул. Чехова, 2

Alekseev Dmitry Mihaylovich
Student
Southern Federal University
Taganrog, Chehov st., 2

*Работа выполнена при поддержке гранта
РФФИ № 15-37-20007-мол-а-вед.*

Введение (Introduction)

С 1 января 2016 года в России в силу вступит новый криптографический стандарт ГОСТ Р 34.12-2015 "Информационная технология. Криптографическая защита информации. Блочные шифры"[1, с.2]. В его состав войдут два алгоритма шифрования: ныне действующий стандарт шифрования ГОСТ 28147-89 и новый блочный алгоритм шифрования Кузнечик. В составе нового стандарта действующий алгоритм шифрования ГОСТ 28147-89 именуется как Магма.

Магма представляет собой симметричный блочный алгоритм шифрования с размером блока входных данных 64 бита, секретным ключом 256 бит и 32 раундами шифрования. Подробнее ознакомиться с работой алгоритма шифрования данных Магма можно в [1, с. 9].

Исходя из того, что ныне действующий стандарт шифрования ГОСТ 28147-89 вошел и в состав нового стандарта шифрования (как шифр «Магма»), его анализ является весьма актуальной задачей. Дело в том, что современный мир криптоанализа предлагает достаточно большой объем исследований в области таких популярных методов атак на алгоритм ГОСТ 28147-89 как дифференциальный и линейный криптоанализ[2, с. 80 – 84; 3, 34 – 61; 4, 132 – 140], в то время как слайдовая атака применительно к данному шифру рассмотрена не так основательно. В связи с этим актуальность рассмотрения именно слайдовой атаки применительно к шифру «Магма» наиболее целесообразна.

Метод слайдовой атаки впервые был предложен А. Бирюковым и Д. Вагнером[2, с. 245; 3, с. 589]. Рассмотрим подробнее основные механизмы слайдовой атаки.

На рис. 1 показан процесс зашифрования n -битового открытого текста X_0 , в результате которого получается шифр-текст X_r . Здесь X_j обозначает промежуточное значение данных после j -го раунда зашифрования, так что

$$X_j = F_j(X_{j-1}, k_j),$$

где $j = 1, 2, 3 \dots r$.

Рис. 1. Схема обычного блочного алгоритма шифрования

Функция F называется слабой в том случае, если при известных двух равенствах $F(x_1, k) = y_1$ и $F(x_2, k) = y_2$ ключ k легко определяется. На рис. 2 показано,

как может быть применена слайдовая атака к алгоритмам шифрования такого типа [4, с. 192; 5, с. 102].

Рис. 2. Схема обычной слайдовой атаки

Идея заключается в том, что можно сопоставить один процесс зашифрования с другим таким образом, что один из процессов будет «отставать» от другого на один раунд. Пусть, X_0 и X_0' обозначают исходные открытые тексты, $X_j = F_j(X_{j-1})$ и $X_j' = F_j(X_{j-1}')$, где $j = 1, 2, 3 \dots r$. Идея заключается в том, что если мы имеем такую пару значений, что $X_1 = X_0'$, то мы также будем иметь соответствующую им пару значений, такую что $X_r = X_{r-1}'$. Предположим, что $X_j = X_{j-1}'$, тогда мы можем сказать, что $X_{j+1} = F(X_j) = F(X_{j-1}') = X_j'$. Пара открытых текстов и соответствующих им шифр-текстов (P, C) , (P', C') называется слайдовой парой в том случае, если $F(P) = P'$ и $F(C) = C'$ [4, с. 192; 5, с. 102].

Слайдовая атака проходит следующим образом. Мы получаем $2^{n/2}$ пар открытый – закрытый текст (P_i, C_i) , и ищем среди них слайдовые пары. Согласно парадоксу дней рождений, мы ожидаем найти хотя бы одну пару индексов i, i' , такую, что $F(P_i) = P_{i'}$ и $F(C_i) = C_{i'}$ одновременно выполняются для некоторого ключа. После того, как слайдовая пара найдена, мы можем найти некоторые биты подключа. В том случае, если раундовая функция слабая, мы можем найти весь подключ данного раунда. Для нахождения оставшихся битов секретного ключа необходимо определить следующую слайдовую пару, и с ее помощью провести анализ. Таким образом, достаточно найти всего несколько слайдовых пар для полного определения битов секретного ключа, что и является задачей, стоящей перед криптоаналитиком. Подробнее о применении слайдовой атаки можно прочесть в работе [2, с. 245-259; 3, с. 589-606; 6, с. 43].

Таким образом, целью нашей работы является разработка параллельного алгоритма (с использованием технологии MPI) поиска слайдовых пар применительно к алгоритму шифрования «Магма», а также оценка временных характеристик как процесса шифрования, так и самого поиска слайдовых пар.

Решение данных задач предполагает выполнение следующих этапов исследования:

1. Реализация алгоритма шифрования данных «Магма»;
2. Реализация параллельного алгоритма шифрования данных;
3. Разработка и реализация параллельного алгоритма поиска слайдовых пар.

Предполагается, что параллельность алгоритма позволит повысить скорость его работы, увеличивая число процессов.

Материалы и методы (Materials and Methods)

Помимо актуальности и современности слайдовой атаки, есть и практический аспект ее применения к шифру «Магма». В связи с тем, что для данного алгоритма шифрования отсутствует функция выработки подключей, существует возможность использования однотипных подключей.

В данной работе нами была рассмотрена задача поиска слайдовой пары для случая, когда в алгоритме шифрования Магма используется один и тот же раундовый подключ, который используется в каждом из 32 раундов шифрования. Это теоретически возможно в 2^{32} случаях из 2^{256} , так как в Магме отсутствует функция выработки раундовых подключей. Поиск слайдовой пары путем полного перебора правой части парного текста представлен на рис. 3. Сначала необходимо зафиксировать один текст (входную 64-х битную последовательность) и левую часть парного текста, равную правой (исходной) части фиксированного текста. Правая часть парного текста определяется путем полного перебора. Затем обе входные последовательности для каждой перебираемой правой части парного текста шифруются с помощью блочного алгоритма шифрования Магма. После чего проверяется критерий правильности правой части (что позволяет определить, является ли исходная пара текстов слайдовой парой), а именно: левая часть шифр-текста, полученная для фиксированного текста, должна быть равна правой части шифр-текста, полученной для парного текста, в котором перебирается правая часть.

В результате был разработан и реализован алгоритм, состоящий из следующих шагов:

1. Зафиксировать один текст (входную 64-х битную последовательность) и левую часть парного текста, равную правой (исходной) части фиксированного текста.
2. Определить правую часть путем полного перебора ее возможных значений (от 0x00000000 до 0xffffffff).
3. Зашифровать фиксированный текст, а также парный текст (с перебираемой на текущем этапе правой частью).
4. Проверить критерий отбора слайдовых пар: левая часть шифр-текста, полученная для фиксированного текста, должна быть равна правой части шифр-текста, полученной для парного текста, в котором перебирается правая часть. Перейти к шагу 2.
5. После полного перебора правой части парного текста сформировать результат о поиске слайдовых пар.

Рассмотрим пример слайдовой пары.

Пусть, исходный открытый фиксированный текст представляет собой следующую 64-х битовую последовательность: 0xfedcba9876543210, где 0xfedcba98 – левая часть, а 0x76543210 – правая часть фиксированного текста. При ключе шифрования

$K = 0xffeedddccffeedddccffeedddccffeedddccffeedddccffeedddccffeedddcc$

слайдовой парой к данному фиксированному тексту будет являться следующая 64-х битовая последовательность: 0x7654321028da3b14. Проверим, так ли это. Зашифруем исходный фиксированный текст. Результат зашифрования

представляет собой: 0xef04eacbbad969b9. Теперь зашифруем парный текст. Результат зашифрования представляет собой: 0xeb2e2421ef04eacb.

Рис. 3. Схема поиска слайдовой пары

Проверим критерии отбора слайдовых пар:

1. Левая часть парного текста равна правой (исходной) части фиксированного текста (0x76543210).

2. Левая часть шифр-текста, полученная для фиксированного текста, равна правой части шифр-текста, полученной для парного текста (0x ef04eacb).

Рассмотрим теперь реализацию параллельного алгоритма с использованием технологии MPI для поиска слайдовых пар текстов, необходимых для проведения слайдовой атаки на алгоритм шифрования Магма.

MPI – это интерфейс передачи сообщений (MessagePassingInterface), ориентированный, в первую очередь, на разработку программ для систем с распределенной памятью. По сути, MPI представляет собой библиотеку функций и описания типов данных, предназначенную для распараллеливания программ,

написанных на языках программирования Си и Фортран. Средства библиотеки MPI направлены на облегчение взаимодействия (которое сводится к обмену данными и синхронизации) процессов параллельной программы [6, с. 99].

Одним из достоинств программ, разработанных с использованием библиотеки MPI, является возможность их использования как на специально оборудованном кластере, так и на кластере, состоящем из обычных ПЭВМ, связанных между собой сетью [6, с. 99].

Пожалуй, самой распространенной реализацией MPI является MPICH. Данная реализация разработана исследователями из Аргонской национальной лаборатории США (ArgonneNationalLaboratory, USA). Данная библиотека является свободно распространяемой [6, с. 100]. Важным достоинством использования данной реализации является тот факт, что существуют версии данной библиотеки для всех популярных операционных систем. Именно поэтому для выполнения поставленной задачи мы используем пакет MPICH.

Рассмотрим применимость данной технологии к параллельному поиску правых частей парных текстов. В начале работы программы осуществляется шифрование фиксированного текста. После того, как инициализирована библиотека MPI, выполняется функция определения числа процессов `size` и функция определения рангов (идентификаторов) `myrank` процесса.

```
MPI_Init(&argc, &argv);  
MPI_Comm_rank(MPI_COMM_WORLD, &myrank);  
MPI_Comm_size(MPI_COMM_WORLD, &size);
```

Затем каждый процесс получает свой диапазон для вычислений, а именно, правую часть парного фиксированному текста. Левая часть парного текста, как упоминалось нами ранее, равна правой части фиксированного текста. Правая часть парного текста программно определяется, как сумма ранга (идентификатора) процесса и числа процессов. Таким образом, правая часть парного текста будет перебираться параллельно всеми процессами в рамках своего диапазона. Тот факт, что каждый процесс имеет свой уникальный ранг, и то, что нумерация ранга начинается с нуля, обеспечит полный неповторяющийся для разных процессов перебор правой части. После того, как процесс обработал и проверил на «слайдовость» текущую правую часть, он увеличивает ее значение на количество процессов. Описанное выше программно реализовано следующим образом:

```
right_slaid = myrank;  
while(right_slaid <= (0xffffffff - size + 1))  
{  
    right_slaid_result = find_slaid(right_slaid);  
    right_slaid = right_slaid + size;  
    if(right_slaid_result != 0)  
    {  
        fprintf(slaid_file, "Slaid pair: %x \n",  
right_slaid_result);  
        fflush(slaid_file);  
    }  
}
```

Наглядно алгоритм распараллеливания процесса поиска слайдовых пар представлен на рис. 4.

Результаты (Results)

Прежде, чем рассмотреть временные характеристики поиска слайдовой пары, необходимо оценить временные характеристики применительно к процессу шифрования, который, очевидно, будет являться основой для поиска слайдовой пары.

Рис. 4. Алгоритм распараллеливания

Экспериментальные данные при шифровании блоков алгоритмом Магма получены с использованием IntelCore i5 – 3320M CPU, 2.60 GHz, 4 Gb RAM. Так, шифрование одного блока данных осуществляется около 0.000007 сек. Результаты измерений времени для различного количества входных блоков представлены в таблице 1.

Таблица 1. Результаты измерений времени для различного кол-ва входных блоков

Количество входных блоков	Время шифрования, мсек
1	0.007
512	2.967
1024	5.706
4096	22.785
8192	47.713
16384	91.175

По полученным результатам построен график зависимости времени от количества шифруемых входных блоков. График представлен на рис. 5.

Рис. 5. График зависимости времени от количества шифруемых входных блоков

Теперь проведем временную оценку шифрования 16384 блоков с помощью алгоритма «Магма» для разного количества процессов (параллельное вычисление). Так, например, шифрование 16384 блоков одним процессом занимает 91.175 мсек. Результаты измерений времени для различного количества процессов представлены в таблице 2.

Таблица 2. Результаты измерений времени шифрования для различного количества процессов

Количество процессов	Время шифрования, мсек
1	91.175
2	48.698
4	37.797
8	22.674
16	12.368

По полученным результатам построен график зависимости времени от количества процессов при шифровании 16384 блоков данных. График представлен на рис. 6.

Рис. 6. График зависимости времени шифрования от количества процессов

Рассмотрим временные характеристики при осуществлении поиска слайдовых пар путем полного перебора правой части фиксированного текста. Результаты измерений времени для различного количества процессов представлены в таблице 3.

Таблица 3. Результаты измерений времени поиска слайдовых пар для различного кол-ва процессов

Количество процессов	Время шифрования, сек
1	26900,979194
2	16765.134295
4	9913.899299
8	5943.140347

По полученным результатам построен график зависимости времени поиска слайдовых пар от количества процессов. График представлен на рис. 7.

Рис. 7. График зависимости времени поиска слайдовых пар от количества процессов

Обсуждение и заключение (Discussion and Conclusion)

Очевидно, что при оценке временных характеристик процесса шифрования согласно алгоритму «Магма» без применения параллельных технологий получена практически линейная зависимость (некоторые искажения связаны с погрешностью времени при проведении шифрования), отражающая увеличение времени шифрования при увеличении количества шифруемых блоков. Однако цель проведения таковой оценки состояла не в выявлении столь очевидной характеристики, а в демонстрации быстроедействия реализации алгоритма.

В целом же, шифрование данных осуществляется с достаточно высокой скоростью. Это связано с тем, что всей операции при шифровании программно реализованы с использованием только лишь двоичных операций.

Практически полученная зависимость времени шифрования от количества шифрующих процессов отражает снижение количества времени, затрачиваемого на шифрование одинакового количества блоков, при увеличении количества процессов (некоторые искажения связаны также с погрешностью оценки времени при проведении шифрования).

Отметим, что полный перебор какой-либо величины – задача, решение которой требует больших затрат временного ресурса. В связи с этим, нами и был реализован алгоритм, осуществляющий параллельный непересекающийся перебор правой части парного текста. Как уже было сказано ранее, принцип его работы представлен на рис. 4. В ходе исследований показано, что параллельность алгоритма позволяет повысить скорость его работы, увеличивая число процессов. Так, например, поиск слайдовой пары при использовании двух процессов занимает в 1,7 раза больше времени, чем аналогичное вычисление для четырех процессов.

Разработанный и реализованный параллельный алгоритм является достаточно эффективным с точки зрения реализации, но сам подход к поиску слайдовых пар основывается на однотипности подключей и назвать его максимально эффективным нельзя. В связи с этим наши дальнейшие исследования в области слайдовой атаки на шифр «Магма» связаны с разработкой алгоритма поиска слайдовых пар для 2-х и 4-х однотипных подключей, а затем его применение к анализу полного шифра.

Список используемых источников:

1. Криптографическая защита информации Блочные шифры.
URL: https://www.tc26.ru/standard/gost/GOST_R_3412-2015.pdf
2. Бирюков А., Вагнер Д. Слайдовые атаки // Труды быстрого программного шифрования, 1999. №1636. Лекции в области компьютерных наук. С. 245-259.
3. Бирюков А., Вагнер Д. Расширенная слайдовая атака. Достижения в криптологии // Еврокрипт. 2000. № 1807. Лекции в области компьютерных наук. С. 589-606.
4. Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа. Москва.: Гелиос АРВ, 2006. 376 с.
5. Бабенко Л.К., Ищукова Е.А. Криптоанализ современных систем защиты информации. Актуальные аспекты защиты информации. Монография. Т.: Изд-во ТТИ ЮФУ, 2011. С. 102-180.
6. Бабенко Л.К., Ищукова Е.А., Сидоров И.Д. Параллельные алгоритмы для решения задач защиты информации. М.: Горячая линия Телеком, 2014. 304 с.
7. Бабенко Л.К., Ищукова Е.А., Сидоров И.Д. Применение параллельных вычислений при решении задач защиты информации // Программные системы: теория и приложения. 2013. Т. 4. № 3-1 (17). С. 25-42.
8. Babenko L.K., Ishchukova E.A., Maro E.A., Research about Strength of GOST 28147-89 Encryption Algorithm. Proceedings of the 5th international conference on Security of information and networks. NY, 2012. P. 80-84.
9. Babenko L., Ischukova E., Maro E. GOST Encryption Algorithm and Approaches to its Analysis. Theory and Practice of Cryptography Solutions for Secure Information Systems, IGI Global book series Advances in Information Security, Privacy, and Ethics (AISPE) Book Series, Published in the United States of America by Information Science Reference. P. 34-61.
10. Babenko L., Ishchukova E. Influence of S-Boxes to the Resistance of GOST Algorithm against Linear Cryptanalysis. Proceedings of the 6th international conference on Security of information and networks. NY, 2013. P. 132-140.

References:

1. Cryptography Block ciphers. URL: https://www.tc26.ru/standard/gost/GOST_R_3412-2015.pdf
2. A. Biryukov, D. Wagner, Slide attacks // *Proceedings of fast software encryption 1999*. No. 1636. *Lectures in computer science*. P. 245-259.
3. Biryukov A., Wagner D. Advanced slide attacks. *Advances in cryptology // Eurocrypt. 2000*. No. 1807. *Lectures in computer science*. P. 589-606.
4. Babenko L. K., E. A. Isakova *Modern block encryption algorithms and methods of analysis*. Moscow.: Gelios ARV, 2006. 376 p.
5. Babenko L. K., E. A. Isakova *Cryptanalysis of modern systems of information protection. Current aspects of information security*. Monograph. T: Izd-vo TTI yufu, 2011. P. 102-180.
6. Babenko L. K., Isakova E. A., Sidorov I. D. *Parallel algorithms for solving problems of information security*. M.: hotline Telecom, 2014. 304 p.
7. Babenko L. K., Isakova E. A., Sidorov I. D. Application of parallel computing in solving problems of information protection // *Program systems: theory and applications*. 2013. Vol. 4. No. 3-1 (17). P. 25-42.
8. Babenko L.K., Ishchukova E.A., Maro E.A., Research about Strength of GOST 28147-89 Encryption Algorithm. *Proceedings of the 5th international conference on Security of information and networks*. NY, 2012. P. 80-84.
9. Babenko L., Ischukova E., Maro E. *GOST Encryption Algorithm and Approaches to its Analysis. Theory and Practice of Cryptography Solutions for Secure Information Systems*, IGI Global book series *Advances in Information Security, Privacy, and Ethics (AISPE) Book Series*, Published in the United States of America by Information Science Reference. P. 34-61.
10. Babenko L., Ishchukova E. Influence of S-Boxes to the Resistance of GOST Algorithm against Linear Cryptanalysis. *Proceedings of the 6th international conference on Security of information and networks*. NY, 2013. P. 132-140.

© 2015, Бабенко Л.К., Ищуклова Е.А., Алексеев Д.М.
Реализация поиска слайдовых пар для алгоритма
шифрования Магма с использованием технологии
MPI

© 2015, Babenko L.K., Ischukova E.A., Alekseev D.M.
Implementing of slide pairs' searching for encryption
algorithm Magma with using MPI technology