Инженерный вестник Дона, №4 (2015)
ivdon.ru/ru/magazine/archive/n4y2015/3284

Дифференциальные свойства S-блоков замены для алгоритма ГОСТ 28147-89

Е.А. Ищукова[1], *И.А. Калмыков*[2]

[1]*Южный федеральный университет, Таганрог*
[2]*Северо-Кавказский федеральный университет, Ставрополь*

Аннотация: В работе представлены основные дифференциальные свойства, выявленные для S-блоков замены алгоритма ГОСТ 28147-89, включенных в стандарт шифрования данных ГОСТ 34.12-2015, который вступает в силу с 1 января 2016 года. Выявленные свойства могут быть использован для анализа с использованием таких методов анализа, как дифференциальный криптоанализ и метод невозможных дифференциалов.
Ключевые слова: алгоритм шифрования, симметричное шифрование, блочный шифр, блок замены, дифференциальный криптоанализ, невозможные дифференциалы, дифференциальные свойства.

Введение

Алгоритм шифрования ГОСТ 28147-89 (далее просто ГОСТ) представляет собой блочный алгоритм шифрования, построенный по схеме Фейстеля. ГОСТ преобразует 64-битовые блоки данных и использует при шифровании 256-битовый ключ, что сразу значительно повышает стойкость данного алгоритма к методу полного перебора.

Примечательно то, что для действующего сейчас алгоритма ГОСТ 28147-89 блоки замены являются не фиксированным элементом и могут быть выбраны произвольным образом. Считается, что даже при выборе слабых блоков, 32 раундов алгоритма шифрования ГОСТ будет достаточно для того, чтобы обеспечить требуемую стойкость. Известны блоки замены, которые использовались в приложении для Центрального Банка РФ [1], однако до сих пор нет каких-либо сведений об анализе алгоритма даже с имеющимися известными данными. Отдельно стоит отметить, что буквально два месяца назад в нашей стране был утвержден новый стандарт шифрования данных ГОСТ 34.12-2015, который вступает в силу с 1 января 2016 года. Данный стандарт содержит два алгоритма шифрования, одним из которых является алгоритм шифрования ГОСТ28147-89, для которого зафиксированы блоки

замены. В стандарте данный алгоритм назван Магма (Magma) [2]. В связи с этим большой научный интерес представляет всестороннее изучение свойств для выбранного набора блоков. В настоящей работе будут рассмотрены дифференциальные свойства S-блоков замены для алгоритма ГОСТ с целью их дальнейшего использования для анализа с использованием невозможных дифференциалов

Исследуемые блоки замены

Согласно стандарту [2] для алгоритма ГОСТ утвержден набор блоков замены, приведенный в таблице №1. В соответствии с [2] в данной интерпретации (в стандарте данные блоки обозначены как π и имеют нумерацию от 0) блок S1 применяется к самому младшему байту, а S8 – к самому старшему байту преобразуемого блока данных.

Таблица №1

Блоки замены для алгоритма ГОСТ 34.12-2015

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

Интересен тот факт, что для каждого из представленных в стандарте блоков замен имеются входы, которые после прохождения через S-блок остаются неизменными. В таблице №1 эти позиции выделены цветом.

Алгоритм анализа S-блоков

В общем случае показано[4-7], что если входная разность в блок замены имеет нулевую разность (то есть тексты, которые образуют данную разность, равны), то на выходе такого преобразования разность также будет иметь нулевое значение (несмотря на то, что она будет образована новыми значениями, полученными в результате применения преобразования замены) [8-10]. Если же входная разность имеет ненулевое значение, то она может быть преобразована в различные значения с некоторыми вероятностями (в некоторых случаях даже в значение, равное 0, как например это было показано для алгоритма шифрования DES [3]). В общем случае алгоритм определения соответствия входных и выходных разностей может быть представлен в следующем виде

Алгоритм анализа блока замены

1. Определяется блок замены, на вход которого поступает n бит.
2. В таблице анализа для данного блока замены все исходные значения полагаются равными 0.
3. Определяется первое возможное значение входной разности $\Delta A=0$.
4. Определяется значение первого входа $X=0$ в анализируемый S-блок.
5. Вычисляется второе значение входа $X' = X \oplus \Delta A$.
6. Для входов X и X’ в соответствии с принципом работы S-блока определяются соответственно выходы Y и Y’.
7. Вычисляется значение выходной разности $\Delta C = Y \oplus Y'$.
8. В таблице анализа увеличивается на 1 значение, стоящее на пересечении строки с номером ΔA и столбца с номером ΔC.
9. Значение X увеличивается на 1.
10. Если $X<2^n$, то происходит переход к пункту 5.
11. Значение ΔA увеличивается на 1.
12. Если $\Delta A < 2^n$, то происходит переход к пункту 4.

13. Если не все блоки замены проанализированы, то происходит переход к пункту 1, иначе алгоритм заканчивает свою работу.

Выявленные свойства S-блоков

В результате применения алгоритма анализа S-блоков, было получено восемь таблиц, отражающих дифференциальные зависимости для каждого из S-блоков, представленных в таблице №1. Анализ построенных таблиц позволил выявить следующие закономерности:

1. Сумма всех значений одной горизонтальной линии, то есть количества различных значений выходных разностей ΔC, соответствующих одному и тому же значению входной разности ΔA всегда равна 2^4.

2. Ненулевое значение входной разности ΔA ни в одном из блоков не может быть заменено на значение ΔC = 0.

3. В таблицах анализа нет пар разностей (ΔA, ΔC) с вероятностью больше, чем ¼.

4. Для блока замены S1:
   - входная разность ΔA=14 приведет к разностям ΔC, у которых старший бит всегда будет равен 0;
   - входные разности ΔA=5 и ΔA=11 приведут к разностям ΔC, у которых старший бит всегда будет равен 1.

5. Для блока замены S2:
   - входная разность ΔA=8 приведет к разностям ΔC, у которых старший бит всегда будет равен 0;
   - входные разности ΔA=7 и ΔA=15 приведут к разностям ΔC, у которых старший бит всегда будет равен 1.

6. Для блока замены S5:
   - входная разность ΔA=8 приведет к разностям ΔC, у которых старший бит всегда будет равен 0;

- входные разности $\Delta A=1$ и $\Delta A=9$ приведут к разностям ΔC, у которых старший бит всегда будет равен 1.

7. Для блока замены S6:
   - входная разность $\Delta A=9$ приведет к разностям ΔC, у которых младший бит всегда будет равен 0;
   - входная разность $\Delta A=14$ приведет к разностям ΔC, у которых младший бит всегда будет равен 1;
8. Для блока замены S7:
   - входная разность $\Delta A=13$ приведет к разностям ΔC, у которых старший бит всегда будет равен 0;
   - входные разности $\Delta A=3$ и $\Delta A=14$ приведут к разностям ΔC, у которых старший бит всегда будет равен 1.

Выявленные закономерности представляют собой большой интерес и будут использованы в дальнейшем при разработке алгоритма поиска связей для невозможных дифференциалов. Следует отметить, что остается интересным выбор именно такого набора блоков для нового стандарта шифрования данных ГОСТ 34.12-2015. Например, анализ вышеупомянутых S-блоков, которые использовались в приложении для Центрального Банка РФ [1], не позволял выявить свойства с 4 по 8 пункт. Несмотря на то, что 32 раундов алгоритма шифрования ГОСТ будет достаточно для того, чтобы обеспечить требуемую стойкость, авторы настоящей работы считают, что выбранный набор блоков замен требует тщательного всестороннего изучения.

Работа выполнена при поддержке гранта РФФИ №15-37-50856-мол-нр.

Литература

1. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. – М.:ТРИУМФ, 2002. – 648 с.

2. Криптографическая защита информации Блочные шифры // URL: tc26.ru/standard/gost/GOST_R_3412-2015.pdf

3. Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа. – М.: Гелиос АРВ, 2006. – 376 с.

4. 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.

5. Ищукова Е.А. Оценка стойкости блочных алгоритмов шифрования с использованием линейного криптоанализа // Международный журнал прикладных и фундаментальных исследований №11, 2014. - С.560 - 564. URL: rae.ru/upfs/?section=content&op=show_ article&article_id=6180.

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. Маро Е.А. Алгебраический анализ стойкости криптографических систем защиты информации // Инженерный вестник Дона, 2013, №4 URL: ivdon.ru/magazine/archive/n4y2013/1996.

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 (SIN 2012), ACM, New York, NY, USA, pp. 80-84.

9. L. Babenko, E. Ischukova, E. Maro, 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. – pp. 34 – 61.

10. Бегляров В.В., Берёза А.Н. Гибридный эволюционный алгоритм решения систем линейных алгебраических уравнений, описывающих

электрические цепи // Инженерный вестник Дона, 2013, №1 URL: ivdon.ru/magazine/archive/n1y2013/1540.

References

1. Shnajer B. Prikladnaja kriptografija: Protokoly, algoritmy, ishodnye teksty na jazyke Si. [Applied cryptography: Protocols, algorithms, source texts in the C language] M.: TRIUMF, 2002. 648 p.

2. Kriptograficheskaja zashhita informacii Blochnye shifruю URL: tc26.ru/standard/gost/GOST_R_3412-2015.pdf

3. Babenko L.K., Ishhukova E.A. Sovremennye algoritmy blochnogo shifrovanija i metody ih analiza [Modern algorithms of block ciphers and methods of their analysis]. M.: Gelios ARV, 2006. 376 p.

4. Babenko L.K., Ishhukova E.A. Kriptoanaliz sovremennyh sistem zashhity informacii Aktual'nye aspekty zashhity informacii. Monografija [Cryptoanalysis of modern systems of information security]. T.: Izd-vo TTI JuFU, 2011. pp. 102-180.

5. . Ishhukova E.A. Ocenka stojkosti blochnyh algoritmov shifrovanija s ispol'zovaniem linejnogo kriptoanaliza [Strenght assessment of block ciphers with use of a linear cryptoanalysis]. Mezhdunarodnyj zhurnal prikladnyh i fundamental'nyh issledovanij №11, 2014. pp.560-564. URL: rae.ru/upfs/?section=content&op=show_ article&article_id=6180.

6. Babenko L.K. Ishhukova E.A. Sidorov I.D. Parallel'nye algoritmy dlja reshenija zadach zashhity informacii [Parallel algorithms for the solution of cryptoanalysis problem]. M.: Gorjachaja linija Telekom, 2014. 304 p.

7. Maro E.A. Inženernyj vestnik Dona (Rus), 2013, № 4 URL: ivdon.ru/magazine/archive/n4y2013/1996.

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 (SIN 2012), ACM, New York, NY, USA, pp. 80-84.

9. L. Babenko, E. Ischukova, E. Maro, 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. pp. 34 – 61.

10. Begljarov V.V., Berjoza A.N. Inženernyj vestnik Dona (Rus), 2013, №1. URL: ivdon.ru/magazine/archive/n1y2013/1540.