С. С. Агафьин

LW-МОДИФИКАЦИЯ АЛГОРИТМА ШИФРОВАНИЯ ГОСТ 28147-89

Одним из наиболее быстро развивающихся направлений в сфере компьютеризированных небольших устройств являются RFID-системы. RFID — это метод автоматической идентификации объектов, в котором посредством радиосигналов считываются или записываются данные, хранящиеся в так называемых RFID-метках [1].

Для шифрования информации, циркулирующей в подобных системах, используются алгоритмы, изучаемые LW-криптографией. Этот раздел криптографии ставит своей целью разработку алгоритмов для применения в устройствах, которые не способны обеспечить большинство существующих шифров достаточными ресурсами для функционирования.

Поскольку до сих пор не разработан универсальный шифр, удовлетворяющий всем предъявленным к алгоритмам требованиям [2], рассмотрим возможность создания нового LW-алгоритма. Очевидно, что если начинать данную работу «с нуля», то у разработанного шифра будет, как минимум, один серьезный недостаток — он будет совершенно не изучен и может нести в себе потенциальные уязвимости. Поэтому для разработки нового LW-шифра был выбран путь модификации уже известного алгоритма.

Выбор алгоритма

Для исследования был выбран единственный алгоритм шифрования, разрешенный в России к использованию в сертифицированных средствах защиты информации, — ГОСТ 28147-89 [3].

Алгоритм был представлен в 1989 г. и прошел более чем через 20 лет криптографических исследований. Данный шифр успешно применяется в большом числе отечественных средств защиты информации, однако малоизвестен в других странах. Вследствие этого в открытой печати не появлялось подробных работ, посвященных возможности применения ГОСТ 28147-89 в RFID-системах.

RFID-системы накладывают значительные ограничения на применяемый алгоритм шифрования, поэтому для обоснования возможности использования алгоритма ГОСТ 28147-89 в данных системах необходимо сначала оценить логическую сложность алгоритма. Для этого было проведено его моделирование в пакете Altera Quartus II Version 10.1 Build 197. Выбор данного программного продукта обоснован его бесплатностью и наличием необходимого функционала.

Однако пакет имеет недостаток — невозможность определения частоты, т. е. фактически невозможна оценка быстродействия. Бесплатных программ, позволяющих провести данную оценку, найдено не было. Тем не менее, так как алгоритм успешно реализовывается в различных

средствах защиты уже более 20 лет, можно предположить, что его характеристики быстродействия окажутся приемлемыми для применения в системах радиочастотной идентификации.

Алгоритм шифрования был реализован на языке VHDL и исследован в режиме симуляции. Реализация алгоритма шифрования потребовала 1078 эквивалентных вентилей, что является приемлемым результатом для использования в пассивных RFID-метках при граничном значении в 2000 вентилей.

И хотя полученная логическая сложность стала одним из лучших показателей среди современных симметричных блочных шифров, она достигнута без оптимизационных преобразований, которые могут улучшить данный результат.

Одно из таких преобразований — удаление семи S-блоков и выбор оставшегося таким образом, чтобы данное изменение серьезно не повлияло на стойкость алгоритма [4]. В описании алгоритма шифрования ГОСТ 28147-89 нет указаний на то, какие S-блоки нужно выбирать, более того, не сказано, что они должны быть различными. Таким образом, приведенная выше модификация полностью вписывается в стандарт и может использоваться в сертифицированных средствах криптографической защиты.

Для определения выигрыша в сложности алгоритма модифицированная версия ГОСТ 28147-89 была реализована на языке VHDL. Единственный S-блок был описан как тривиальный, так как в данном случае его вид не влияет на результат.

Логическая сложность данной модификации алгоритма оказалась равна 731 логическому вентилю, что на 32 % меньше, чем сложность базового алгоритма с восьмью различными узлами замен.

Одну из целей реализации можно считать достигнутой: полученный алгоритм по слабости запутанности логической структуры уступает лишь алгоритмам семейства KATAN/KTANTAN (688 логических вентилей). Однако использование данного семейства шифров не представляется возможным из-за существующей криптографической атаки, позволяющей по 4 парам открытого/закрытого текста получить ключ с временной сложностью 2^{73}.

Выбор узлов замен

Так как в приведенной выше модификации используется один S-блок вместо восьми, встает вопрос о его выборе. Данный узел должен обладать хорошими перемешивающими свойствами, быть стойким к линейному и разностному анализу.

Для определения узла, отвечающего данным требованиям, были проведены следующие действия.

Сначала были сгенерированы перестановки длины 16, множество которых полностью соответствует множеству узлов замен 4x4. Для упрощения данной процедуры была использована лемма из [5], которая позволила сократить без нарушения общности данное множество до 11 (!), путем фиксации 5 координат значениями, совпадающими с индексом координаты.

Затем были подсчитаны значения приведенных ниже характеристик для множества перестановок, которые описывают стойкость алгоритма к линейному и разностному криптографическим анализам.

Определим степень линейности булевой функции f от 4 переменных как

$Lin(f) = \max|f^{w}(a)|$.

Чем больше значение $Lin(f)$, тем ближе функция к линейной или аффинной, другими словами, существует линейная или аффинная функция, которая является аппроксимацией функции f. Максимальное значение, которое может принимать данная величина, равно 2^n, и оно достижимо только в случае линейной или аффинной функции.

Пусть S: $V_4 \to V_4$. Определим функцию S_b как координатную функцию S
$S_b: V_4 \to V_1,\ x \mapsto \langle b,\ S(x) \rangle$.

Эта функция, является булевой функцией, полученной из функции S-блока путем фиксации суммы выходных битов, определенных b.

Запишем степень линейности S-блока $Lin(S)$:

$$Lin(S) = \max_{a \in V_4,\ b \in V_4 \setminus \{0\}} |S_b^{w}(a)| .$$

Данная величина показывает степень стойкости S-блока к линейному анализу. Чем меньше это значение, тем более стойким к данной атаке является узел замен.

Для оценки стойкости блока к разностному анализу определим для каждого вектора a:

$\Delta_{S,a}: V_4 \to V_4,\ x \mapsto S(x)+S(x+a)$

$$Diff(S) = \max_{a \neq 0,\ b \in V_4} |\Delta_{S,a}^{-1}(b)| .$$

Характеристика $Diff(S)$ связана с максимальной вероятностью того, что для любой фиксированной ненулевой входной разности после преобразования S-блоком будет получена определенная выходная разность. Для фиксированной разности a значение $|\Delta_{S,a}^{-1}(b)|$ является числом пар $(x,x+a)$, таких, что их выходная разность равна b.

В работе [5] доказано, что для обеспечения максимальной стойкости к линейному анализу $Lin(S)$ должно быть равно 8, так как это наименьшее значение, которое может принимать данная характеристика, в случае, если S является биективным преобразованием множества. Также в данной работе показано, что не существует S-блоков с $Diff(S)$, значение которой меньше 4.

Для определения всех S-блоков, отвечающих данным условиям, и фильтрации остальных, на языке программирования C# была написана программа, поддерживающая параллельные вычисления, и потрачено 78 часов машинного времени на ее выполнение.

Результатом работы стало подмножество, состоящее из 1395850 перестановок, что составляет приблизительно 3,4 % от исходного множества мощностью 11!

Для описания данного множества было произведено его разбиение на классы аффинной эквивалентности, представители которых приведены в таблице 1.

Таблица 1. Представители классов эквивалентности

Номер класса	**Представитель класса эквивалентности**
0	0 1 2 3 4 6 9 10 8 5 12 14 7 13 15 11
1	0 1 2 3 4 6 9 10 8 5 12 14 7 15 13 11
2	0 1 2 3 4 6 9 10 8 5 12 14 11 13 15 7
3	0 1 2 3 4 6 9 10 8 5 12 15 13 11 14 7
4	0 1 2 3 4 6 9 12 8 5 15 13 11 7 10 14
5	0 1 2 3 4 6 9 10 8 11 12 14 5 13 15 7
6	0 1 2 3 4 6 9 10 8 11 12 14 7 15 13 5
7	0 1 2 3 4 6 9 10 8 11 12 14 13 5 7 15
8	0 1 2 3 4 6 9 10 8 11 12 14 15 7 5 13
9	0 1 2 3 4 6 9 10 8 12 5 13 7 14 15 11
10	0 1 2 3 4 6 9 10 8 12 5 13 11 14 15 7
11	0 1 2 3 4 6 9 10 8 12 11 13 5 15 14 7

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

Исходя из алгоритма выбора данных перестановок можно заключить, что для обеспечения стойкости к линейному и разностному анализу модифицированного алгоритма можно использовать перестановку, относящуюся к любому из полученных классов.

Заключение

Путем простой модификации классического алгоритма шифрования ГОСТ 28147-89 был получен шифр, который может использоваться в сертифицированных средствах защиты информации при наличии серьезных ограничений на доступные ресурсы, например таких, которые выдвигаются для подсистем шифрования, реализуемых на RFID-метках.

Поскольку в ГОСТ 28147-89 не определены узлы замен, нужно выбрать такую перестановку, которая имела бы хорошие криптографические свойства, достаточные для того, чтобы замена восьми разных S-блоков на один повторяющийся не повлияла на стойкость алгоритма.

В процессе поиска такого узла было определено множество перестановок, которые могут использоваться в алгоритме шифрования.

Также для проверки утверждений, на которых основывался процесс определения этого множества, произвольным образом была выбрана одна перестановка, которая была использована в реализации модифицированного алгоритма на языке программирования C++. К данной реализации были применены методы линейного и разностного криптографического анализа. Полученные результаты позволяют судить о достаточной стойкости модифицированного алгоритма.

СПИСОК ЛИТЕРАТУРЫ:

1. *Poschmann A. Y.* Lightweight Cryptography: Cryptographic Engineering for a Pervasive World // Cryptology ePrint Archive. Report 516. 2009.
2. *Агафьин С. С.* LW-криптография: шифры для RFID-систем // Безопасность информационных технологий. 2011. № 1. С. 30–33.
3. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Введ. 1990-01-07. М.: Изд-во стандартов, 1996. – 28 с.
4. *Leander G., Paar C., Poschmann A., Schramm K.* New Lightweight DES Variants // Lecture Notes in Computer Science. 2007. Vol. 4593. P. 196–210.
5. *Leander G., Poschmann A.* On the Classification of 4 Bit S-Boxes // Lecture Notes in Computer Science. 2007. Vol. 4547. P. 159–176.