# АППАРАТНО-ЭФФЕКТИВНЫЙ АЛГОРИТМ ФОРМИРОВАНИЯ МАРКЕРА НАЧАЛА СООБЩЕНИЯ

*Файзуллин И.Р., Файзуллин Р.Т.*
*Омский государственный технический университет*

***Аннотация***

Предложен аппаратно, но не программно эффективный криптографический алгоритм для формирования маркера начала передачи информации. Предложена модификация алгоритма, позволяющая передавать информацию в виде специально встроенных ошибок в маркер. Показано, что задача, на которой основана криптографическая стойкость алгоритма, не принадлежит классу NP. В наилучшем для атакующего случае дана оценка числа операций, необходимых для нахождения ключа.

*Ключевые слова:* мастер-ключ, маркер, криптографическая стойкость, автомат без памяти.

## *Введение*

Постоянное увеличение скорости передачи данных и пропускной способности каналов связи приводит к качественному изменению подходов к проблеме защиты информации. Стеганография [1], скрытые каналы [2-3], сегментирование данных [4] из экзотических инструментов становятся одними из наиболее перспективных способов практической защиты информации. В связи с этим остро стоит вопрос о вычислительной эффективности шифроалгоритмов, их доказуемой стойкости и желательном преимуществе аппаратных реализаций алгоритмов перед программными.

В настоящей работе предлагается алгоритм защиты информации, одновременно совмещающий в себе черты стандартных блочных алгоритмов и стеганографии. Оценена стойкость алгоритма и предложен эффективный метод реализации.

Рассмотрим поток данных, состоящий из бит, полученных или с помощью физического генератора псевдослучайных чисел, или с помощью программного датчика псевдослучайных чисел. Задача состоит в том, чтобы встроить в этот поток маркер сообщения, который будет содержать само сообщение. Схожая задача была рассмотрена в работе [5], но там маркер предваряет сообщение и зависит от него, как хэш-код, что представляется не совсем эффективным, т.к. требует офф-лайн обработки больших объёмов данных.

Рассмотрим последовательность байтов $Q^1,..,Q^N$, каждый из которых состоит из $K$ бит, и соответствующий им кортеж бит $q^1,...,q^N$. Будем называть объединение этих кортежей мастер-ключом.

Передающая сторона, или Алиса, генерирует кортеж $X^1, \dots, X^N$ с условиями:

$$X^j \ge Q^j \text{ если } q^j = 0, \quad (1)$$

$$X^j < Q^j \text{ если } q^j = 1.$$

И маркирует начало сообщения операцией побитового сложения байтов.

$X^j, Q^j$:

$$Z_i^j = X_i^j \oplus Q_i^j \; i = 1,..K.$$

Получатель сообщения, или Боб, производит аналогичную операцию $XOR$ над байтом $Z^j$ и байтом $Q^j$, получая в итоге $\overline{X}^j$. Если некоторая последовательность битов $\overline{X}^m,.., \overline{X}^{m+N-1}$ удовлетворяет условиям (1), тот Боб делает вывод о том, что с вероятностью $1–2^{–N}$ эта последовательность байтов маркирует начало сообщения.

Но заметим, что Алиса может специально генерировать некоторые из $X^j$ так, что условия (1) для них не будут выполняться. Если число таких «ошибок» будет относительно мало, например, не более четверти, и окаймлено заранее заданным числом не «ошибок», то Боб, проверяя входной поток, может сделать хорошо обоснованный вывод о наличии специально встроенных Алисой символов «ошибки». Боб должен выбрать из двух гипотез: он получает случайный поток данных или поток данных, созданный Алисой. Учитывая, что случайный поток данных, например, созданный с помощью генератора псевдослучайных чисел BBS, хорошо описывается схемой Бернулли, а при увеличении $N$хорошо описывается нормальным законом, то выделение кортежа $\overline{X}^m,.., \overline{X}^{m+N-1}$ не представляет большого труда, с учётом, например, того, что доверенное лицо проводит тест на открытый текст для наиболее вероятного фрагмента потока данных.

В этом случае Боб может интерпретировать маркер как битовую строку $\overline{q}^j$, $j = 1,..N$, где нулями являются те из $\overline{q}^j$, которые совпадают с $q^j$, а единицами – места «ошибок». Длина слова в этом случае будет равна $N$, а «полезное пространство сообщений» $2^{N-l}$, где $l$ сравнимо с $N$.

Насколько стойкой является предложенная схема шифрования?

Предположим, что аналитик каким-то образом смог выделить несколько кортежей $Z^{js}, j = 1,.., N, s = 1,.., M \; M \ge 2$, отвечающих маркерам, и ему известно, что в маркерах нет «ошибок».

С учётом независимости блоков аналитик может рассматривать только один блок $j$ и отвечающие ему неизвестные $q^j, Q^j, X^{j1},..X^{jM}$.

В этом случае мы получаем систему линейных уравнений в $Z_2$ и неравенств в $R$:

$$z^{js}{}_i = x^{js}{}_i \oplus Q^{js}{}_i \; i = 1,..K, \; s = 1,.., M,$$

$(X^{js} - Q^j)(-1)^{q^j} \geq 0$.

Предполагая, что, например, $q^s = 0$, получим:

$(X^{js} - Q^{js}) \geq 0$.

Попытка решить эту систему прямыми методами обречена на неудачу, т.к. ассоциированные системы линейных алгебраических уравнений имеют ядро размерности, сравнимой с $K$, что делает задачу теоретически неразрешимой.

Предположим, что мы точно знаем расположение $M$ кортежей $Z^j$ в потоке данных и тем самым знаем $z^{js}{}_i = x^{js}{}_i \oplus Q^{js}{}_i \; i = 1,..K, \; s = 1,..,M, \; j = 1,..,N$ для каждых $j, s$. Зафиксируем некоторое $j$ и оценим трудоёмкость определения битов $Q_1^j,...,Q_K^j$ при неизвестном $q$.

Оказывается, что в этом случае верна следующая лемма.

***Лемма 1:***

*В наилучшем для атакующего случае трудоёмкость определения мастер-ключа $Q_1^j,...,Q_N^j$ и $q^1,...,q^N$ не меньше, чем $CNK2^K$.*

Рассмотрим все возможные значения $Q^j$, которые, возможно, являются битами маркера без ошибок. Очевидно, что их число оценивается величиной $2^K$. Для каждого такого $Q^j$ по известному $Z^j$ однозначно определяется $X^j$ и проверяется, например, условие $(X^j - Q^j) \geq 0$. Заметим, что априори нельзя выделить множество таких пробных $Q^j$, для которых всегда будет выполняться только условие $(X^j - Q^j) \geq 0$, кроме, конечно, тривиального случая нулевого вектора. Поэтому мы вынуждены проверять условие в $2^K$ -1 случаях.

По результатам проверки $Q^j$ заносится в одно из множеств $A = \{Q^j, X^j - Q^j \geq 0\}$ или $B = \{Q^j, X^j - Q^j < 0\}$.

Выберем из $M$ кортежей другой байт $Q^j$ и так же образуем множества $A' = \{Q^j, X^{j1} - Q^j \geq 0\}$, $B' = \{Q^j, X^{j1} - Q^j < 0\}$. Предположим, что всё пересечение $A \bigcap A'$ состоит только из одного $H^j$, а пересечение $B \bigcap B'$ пусто.

В этом случае $H^j$ будет искомым байтом, а искомый бит $q^j$ будет определяться однозначно.

Даже в этом простейшем случае мы вынуждены решить системы два раза, для каждого кортежа и число операций побитового сложения для определения $X^j$ пропорционально $K$, т.е. длине байта.

Циклический сдвиг кортежа $q^1,...,q^N$ и встраивание «ошибок» или сообщения решает эту проблему практически, но лемма по существу остаётся верной. Мы с вероятностью 0,25 «успешно» попадаем в отрезок Голомба [6] длины больше, чем единица. Отметим, что мы рассматриваем идеальный случай, в котором выборка и распределение данных в памяти производится мгновенно.

Из леммы следует другой практический вывод о том, что гарантированная на сегодняшний день стойкость, равная $2^{80}$, без учёта операций записи и считывания из памяти, будет обеспечиваться выбором длины байта $K$ большей или равной 64.

Также можно сформулировать очевидную лемму о классе сложности, к которому принадлежит задача криптоанализа данного алгоритма.

***Лемма 2:***

*Задача определения мастер-ключа при известных кортежах $Z^j$ не принадлежит классу $NP$.*

Допустим, что нам известны несколько кортежей $Z^j$ и необходимо проверить, что наборы $Q_1^j,...,Q_N^j$ и $q^1,...,q^N$ являются ключом. Покажем, что, даже если все $X_i^j = Z_i^j \oplus Q_i^j \; i = 1,..K$ удовлетворяют (1), это не означает, что $Q_1^j,...,Q_N^j$ и $q^1,...,q^N$ мастер-ключ. Допустим, что $Z^j$ и $Q^j$ на нескольких общих позициях имеют совпадающие нулевые биты. Тогда $\overline{Q}^j$, полученное произвольной расстановкой единиц в этих позициях, так же позволит сгенерировать $\overline{X}_i^j = Z_i^j \oplus \overline{Q}_i^j \; i = 1,..K$, удовлетворяющие неравенствам (1). Единственный выход – это увеличение числа $M$ в общем случае до величины $2^r$, где $r$ – это число нулевых бит, стоящих в общих позициях у $Z^j$ и $Q^j$. Только в этом случае можно выбрать единственное $Q^j$ из всех возможных $\overline{Q}^j$. Доказательство завершено.

Заметим, что реализация кодирования информации, или создание последовательности $X^1,...X^N$, может быть осуществлена инвертированием бит, например, применением операций И, ИЛИ с битами байта $Q$ и содержимым некоего регистра сдвига с линейной обратной связью. Если, например, $q^j$=0, то некоторые нулевые биты $Q^j$ необходимо инвертировать на единичные (ИЛИ), если же $q^j$=1, то наоборот, необходимо инвертировать единичные биты $Q^j$ (И).

Принимающая сторона может определить набор $q^1,..,q^N$, пропуская его через регистр сдвига и тестируя байты на предмет проверки $(X^{js} - Q^j)(-1)^{q^j} \geq 0$, так же с помощью автомата без памяти (конъюнктивную нормальную форму (КНФ)), предложенного в [7].

Обратим внимание на то немаловажное обстоятельство, что аппаратное шифрование и дешифрование происходит за $O(1)$ время, необходимое для прохождения сигнала через автомат, реализующий КНФ, а программная реализация требует $CKN$ числа операций. Это позволяет сделать вывод о перспективности использования данного подхода в практике корпораций и неэффективности программных реализаций частными лицами.

### *Заключение*

Компьютерное моделирование формирования и распознавания маркера показало, что система работоспособна и не возникает гонок автоматов.

Можно сделать вывод о том, что разработан эффективный алгоритм формирования маркера начала сообщения, доказана его криптографическая стойкость, основанная на решении задачи из класса $EXP$, и определены нижние пределы применимости (по длине ключа). Проведено компьютерное моделирование работы протокола и предложены схемы аппаратной реализации.

### *Литература*


1. **Грибунин, В.Г.** Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: Солон-Пресс, 2002. – С. 6-16.
2. **Столлингс, В.** Криптография и защита сетей: принципы и практика / В. Столлингс. – 2-е изд. – М.: Вильямс, 2003. – С. 123-130.
3. **Грушо, А.А.** Методы защиты информации от атак с помощью скрытых каналов и враждебных программно-аппаратных агентов в распределенных системах / А.А. Грушо, Н.А. Грушо, Е.Е. Тимонина // Вестник РГГУ. – 2009. – № 10. – С. 33-45.
4. **Конахович, Г.Ф.** Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – Киев: МК-Пресс, 2006. – 288 с.
5. **Файзуллин, И.Р.** Крипто-стеганографический алгоритм с использованием хэш-функции для маркировки начала сообщения / И.Р. Файзуллин // Научная сессия МИФИ. Томск. Компьютерные науки. Информационные технологии. – 2007. – № 16. – С. 149-150.
6. **Golomb, S.W.** Run-length encodings / S.W. Golomb // IEEE Trans. Inf. Theor., – 1996. – IT-12, No. 3 – P. 399-401.
7. **Файзуллин, Р.Т.** Алгоритм минимизации функционала, ассоциированного с задачей 3-SAT и его практические применения / Р.Т. Файзуллин, И.Г. Хныкин, В.И. Дулькейт, Е.В. Салаев – Челябинск, 2007. – С. 68-72.


### *References*


1. **Gribunin, V.G.** Digital steganography / V.G. Gribunin, I.N. Okov, I.V. Turintsev – Moscow: "Solon-press" Publisher, 2002 – P. 6-16. – (in Russian).
2. **Stollings, V.** Cryptography and protection of networks: principles and practice / V. Stollings (2 ed.). – Moscow: "Williams" Publisher, 2003. – P. 123-130. – (in Russian).
3. **Grusho, A.A.** Methods of protection of the information from attacks by means of the latent channels and hostile hardware-software agents in the distributed systems / A.A. Grusho, N.A. Grusho, E.E. Timonina // Bulletin RGTU. – 2009. – No. 10. – P. 33-45. – (in Russian).
4. **Konahovich, G.F.** Kompjuternaja steganografija. The theory and practice / G.F. Konahovich, A.J. Puzyrenko – Kiev: "MK-PRESS" Publisher, 2006. – 288 p. – (in Ukraine).
5. **Fayzullin, I.R.** Crypto-algorithm with use of hesh-function for marks of the beginning of the message / I.R. Fayzullin // Scientific session of MEPhI, Computer sciences. Information technology. – 2007. – V. 16 – P. 149-150. – (in Russian).
6. **Golomb, S.W.** Run-length encodings / S.W. Golomb // IEEE Trans. Inf. Theor. – 1996. – IT-12, No. 3. – P. 399-401.
7. **Fajzullin, R.T.** Algorithm of minimization function, associated with a problem 3-SAT and its practical applications, /R.T. Fajzullin, I.G. Hnykin, V.I. Dulkejt, E.V. Salaev – Chelyabinsk, 2007. – P. 68-72. – (in Russian).


## HARDWARE-EFFECTIVE ALGORITHM OF FORMATION OF THE MARKER OF THE BEGINNING OF THE MESSAGE


*R.T. Fayzullin[1], I.R. Fayzullin[2]*

*[1] Omsk State Technical University, [2] Joint-Stock Company TD Perekrostok*



### *Abstract*

It is offered it is hardware, but not software, effective cryptographic algorithm for formation of a marker of the beginning of information transfer. The algorithm updating, allowing to hand over the information, in the form of specially built in errors in a marker is offered.



*Key words:* master key, marker, cryptographic firmness, the automatic machine without memories.


### *Сведения об авторах*


**Файзуллин Рашит Тагирович**, 1956 года рождения. В 1978 г. окончил математический факультет Новосибирского государственного университета. Доктор технических наук (1999 г.). В списке научных работ Р.Т. Файзуллина более 100 статей, 2 монографии.

E-mail: *r.t.faizullin@mail.ru*

**Rashit Tagirovich Fayzullin** (b. 1956) graduated with honours (1978) from the Novosibirsk State University (NSU). He received his Doctor in engineering science in (1999) degrees. He is co-author of more when 100 scientific papers, 2 monographs.



**Файзуллин Ильдар Рашитович**, 1985 года рождения. В 2001 г. окончил факультет компьютерных наук Омского государственного университета. В списке научных работ 8 статей. Область научных интересов: сжатие данных.

E-mail: *blackildar@list.ru*

**Ildar Rashitovich Fayzullin** (b. 1985) graduated (2001) from the Omsk State University (OmSU). He is co-author of 8 scientific papers. His research interests is data compression.



*Поступила в редакцию 20 февраля 2010 г.*