Наука и Образование
МГТУ им. Н.Э. Баумана
Сетевое научное издание
ISSN 1994-0448

Наука и Образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2014. №9. С. 194–202.
DOI: 10.7463/0914.0727086
Представлена в редакцию: 07.09.2014

УДК 004.056.55+519.713

Об устойчивости обобщенных клеточных автоматов к некоторым типам коллизий

Ключарёв П. Г.[1,*]

[*]pk.iu8@yandex.ru

[1]МГТУ им. Н.Э. Баумана, Москва, Россия

Статья посвящена некоторым вопросам синтеза обобщенных клеточных автоматов, предназначенных для использования в составе различных криптографических алгоритмов. Вводится понятие коллизии в обобщенном клеточном автомате. Исследуются вопросы построения обобщенных клеточных автоматов, устойчивых к определенному типу коллизий. Получено достаточное условие отсутствия одношаговых коллизий веса 1, состоящее в том, что локальная функция связи должна линейно зависеть от одного из аргументов, а соответствующие этим аргументам ребра графа клеточного автомата, вместе с инцидентными им вершинами, должны образовывать 2-фактор. Рассматривается вопрос существование 2-фактора в таком графе и приводится метод его нахождения за полиномиальное время.

Ключевые слова: криптография, клеточный автомат, коллизия.

Введение

Современные информационные технологии, активно развиваясь, предъявляют все новые требования как к уровню защищенности каналов связи, так и к их пропускной способности. В этой связи активно развиваются криптографические методы. Криптографии посвящено очень большое количество источников, в частности, [7, 9, 13, 14], существует большое количество различных криптоалгоритмов (хороший обзор можно найти в [5]). Однако в свете интенсификации развития так называемой легковесной (lightweight) криптографии [15, 18], многие из них не удовлетворяют современным требованиям в части производительности и эффективности. Это приводит к необходимости разработки новых криптоалгоритмов.

В работах [1, 4] и ряде других, автором были разработаны принципы построения симметричных криптоалгоритмов на основе обобщенных клеточных автоматов. Эти криптоалгоритмы имеют очень высокую производительность при аппаратной реализации. Данная работа продолжает это направление исследований. В ней исследуются коллизии, возникающие при работе обобщенных клеточных автоматов и решается оставленный ранее открытым

важный для обеспечения криптостойкости вопрос о нумерации ребер графа клеточного автомата. Основной задачей настоящей статьи является разработка метода построения обобщенных клеточных автоматов, устойчивых к определенному виду коллизий. Именно такие автоматы и должны быть использованы в криптографических алгоритмах.

1. Обобщенные клеточные автоматы

Назовем обобщенным клеточным автоматом ориентированный мультиграф $A(V, E)$, где $V = \{v_1, \ldots, v_N\}$ — множество вершин, а E — мультимножество ребер. С каждой его вершиной v_i ассоциированы:

• булева переменная m_i, которая называется ячейкой;

• булева функция $f_i(x_1, \ldots, x_{d_i})$, которая называется локальной функцией связи i-й вершины.

При этом каждой паре (ребро v, инцидентная ему вершина e) будет соответствовать номер аргумента локальной функции связи, вычисляемой в вершине v. Мы будем называть его номером ребра e относительно вершины v.

Здесь мы рассматриваем только клеточные автоматы, графы которых не имеют кратных ребер.

Опишем теперь работу обобщенного клеточного автомата. В начальный момент времени каждая ячейка m_i, $i = 1...N$, имеет некоторое начальное значение $m_i(0)$. Автомат работает пошагово. Так, значения ячеек на шаге номер t вычисляются по формуле:

$$m_i(t) = f_i(m_{\eta(i,1)}(t-1), m_{\eta(i,2)}(t-1), \ldots, m_{\eta(i,d_i)}(t-1)), \tag{1}$$

где $\eta(i, j)$ — номер вершины, из которой исходит ребро, заходящее в вершину i и имеющее относительно этой вершины номер j. Заполнением клеточного автомата $M(t)$ на шаге t будем называть набор значений ячеек $(m_1(t), m_2(t), \ldots, m_N(t))$.

Обобщенный клеточный автомат будем называть однородным, если для любого $i \in \{1, \ldots, N\}$ выполняется $f_i = f$, т.е. локальная функция связи для всех ячеек одинакова. Степени захода вершин такого клеточного автомата, очевидно, одинаковы: $d_1 = d_2 = \ldots = d_N = d$.

Назовем обобщенный клеточный автомат неориентированным, если для любого ребра (u, v) в его графе существует и ребро (v, u). Граф такого автомата можно рассматривать как неориентированный, если заменить каждую пару ориентированных ребер (u, v) и (v, u) на неориентированное ребро $\{u, v\}$.

Здесь мы будем использовать лишь неориентированные однородные обобщенные клеточные автоматы, для краткости называя их просто обобщенными клеточными автоматами.

Для криптостойкости шифров большое значение имеет выбор графа обобщенного клеточного автомата. Согласно работе [3], хорошим выбором являются графы Рамануджана [8, 10, 12].

Кроме того, важным является правильный выбор локальной функции связи обобщенного клеточного автомата, требования к которой сформулированы автором в работе [3]. Семейство функций, удовлетворяющих этим требованиям построено автором в работе [2]. В настоящей статье мы получим новые требования к таким функциям (сразу заметим, что семейство функций из работы [2] удовлетворяет и им).

2. Коллизии в обобщенных клеточных автоматах

Выходной последовательностью клеточного автомата A назовем функцию F_A: $B^n \times \mathbb{N} \to$ $\to B^n$, аргументами которой является начальное заполнение и номер шага, а значением — заполнение на этом шаге.

Будем называть t-шаговой коллизией веса w такие два различных заполнения обобщенного клеточного автомата $x_1,\ x_2 \in \{0,\ 1\}^N$, что $|x_1 \oplus x_2| = w$ и $F_A(x_1, t) = F_A(x_2, t)$, но $F_A(x_1, t-1) \neq F_A(x_2, t-1)$, где $|x|$ — вес вектора x.

Заметим, что любая t-шаговая коллизия одновременно является и $(t+\tau)$-шаговой коллизией, для любого натурального τ.

Очевидно, что существование коллизий в обобщенном клеточном автомате, при условии наличия эффективных алгоритмов их нахождения, резко ухудшает криптографические свойства основанных на нем криптоалгоритмов. Поэтому очень важны методы синтеза обобщенных клеточных автоматов, для которых коллизии либо отсутствуют, либо их нахождение является вычислительно-трудной задачей. Такие автоматы мы будем называть устойчивыми к коллизиям.

В данной работе мы изучим устойчивость к одношаговым коллизиям веса 1.

Итак, пусть в клеточном автомате A существует одношаговая коллизия веса 1: (x_1, x_2). Пусть $x_2 = x_1 \oplus \varepsilon$, где $|\varepsilon| = 1$. Пусть единица в ε соответствует ячейке клеточного автомата с номером j. Тогда для любой ячейки v_i смежной с v_j должны существовать такие значения $a_1,\ \ldots,\ a_{k-1},\ a_{k+1},\ a_d \in \{0,\ 1\}$, что выполняется:

$$f(a_1, \ldots, a_{k-1}, 0, a_{k+1}, \ldots, a_d) = f(a_1, \ldots, a_{k-1}, 1, \ldots, a_{k+1}, a_d), \tag{2}$$

где k — номер относительно вершины v_i ребра (v_j, v_i).

Для того чтобы рассматриваемых коллизий не существовало, достаточно, чтобы для некоторого k нельзя было найти $a_1,\ \ldots,\ a_{k-1},\ a_{k+1},\ \ldots,\ a_d \in \{0,\ 1\}$, удовлетворяющие уравнению (2). При этом, нумерация ребер графа должна быть такой, чтобы каждой вершине было инцидентно ребро, имеющее номер k относительно какой-либо другой вершины.

Отсюда возникает два вопроса:

• какой должна быть локальная функция связи?

• какой должна быть нумерация ребер и каким требованиям должен удовлетворять граф обобщенного клеточного автомата?

Далее мы подробно остановимся на этих вопросах.

3. Локальная фукция связи

Итак, построим такую локальную функцию связи $f(x_1, \ldots, x_d)$. Представим эту функцию в виде

$$f(x_1, \ldots, x_d) = x_k g_1(x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_d) \oplus g_2(x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_d),$$

где g_1 и g_2 — $(d-1)$-местные булевы функции.

Тогда для того, чтобы не существовало набора аргументов, для которых выполнялось бы условие (2), необходимо и достаточно, чтобы $g_1(x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_d) = 1$, т.е. функция f линейно зависела от одной из своих переменных:

$$f(x_1, \ldots, x_d) = x_k \oplus g_2(x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_d).$$

Действительно, если функция g_1 не равна тождественно единице, то существует такой набор $a_1, \ldots, a_{k-1}, a_{k+1}, \ldots, a_d$, что $g_1(a_1, \ldots, a_{k-1}, a_{k+1}, \ldots, a_d) = 0$ и условие (2) выполняется. Если же $g_1 = 1$, то переменная x_k является существенной независимо от значений остальных переменных и, следовательно, условие (2) не выполняется.

4. Строение графа обобщенного клеточного автомата

Как было отмечено выше, граф должен быть такой, чтобы каждой вершине было инцидентно ребро, имеющее номер k относительно какой-нибудь другой вершины. То есть, при использовании локальной функции связи, предложенной в предыдущем разделе, от каждой ячейки клеточного автомата должна линейно зависеть какая-либо другая ячейка. Легко видеть, что для этого достаточно, чтобы ребра, имеющие номер k относительно каких-либо вершин вместе с этими вершинами образовывали 2-фактор графа обобщенного клеточного автомата.

Напомним, что s-фактором графа G называется его s-регулярный подграф на том же множестве вершин, а s-факторизацией графа называется множество его s-факторов, объединение которых совпадает с графом, но множества ребер попарно различны. Хороший обзор современного состояния теории факторизации графов можно найти в работе [17].

В том случае, если 2-фактор является связным, он называется гамильтоновым циклом и его поиск является NP-трудной задачей. Однако если связность не требуется, он может быть найден за полиномиальное время.

Сначала выясним условия существования 2-фактора. В этой связи известны следующие теоремы.

Теорема 1 (Петерсен [16]). Граф имеет 2-факторизацию тогда и только тогда, когда он регулярен и имеет четную степень.

Теорема 2 (Беблер [19]). Любой 2-реберносвязный регулярный мультиграф, имеющий нечетную степень, содержит 2-фактор.

Таким образом, учитывая, что в однородных обобщенных клеточных автоматах используются регулярные графы, 2-фактор существует, если степень графа четная, либо если граф является 2-реберно-связным, что на практике всегда выполняется.

Теперь приведем способ, позволяющий найти 2-фактор в данном графе $G(V, E)$.

Построим двудольный граф $G_1 = (V_2, E_1)$, где $V = V \cup V_1$, V и V_1 — две доли графа, $|V| = |V_1|$, $V = \{v_1, \ldots, v_n\}$, $V_1 = \{u_1, \ldots, u_n\}$. Множество ребер E_1 построим следующим образом: ребро $(v_i, u_j) \in E_1$ тогда и только тогда, когда $(v_i, v_j) \in E$

Теперь остается найти в графе G_1 максимальное паросочетание. Для поиска максимального паросочетания в двудольном графе существует ряд алгоритмов, наиболее удачным из которых считается алгоритм Хопкрофта — Карпа [11], имеющий сложность $O(|E|\sqrt{|V|})$.

Полученному паросочетанию и соответствует искомый 2-фактор.

Найдя посредством вышеприведенного метода произвольный 2-фактор, следует для каждой его связной компоненты, являющейся циклом вида $v_1, e_1, v_2, e_2, \ldots, v_m, e_m, v_1$, сопоставить каждому ребру номер k, относительно следующей в цикле вершины, где k — номер переменной, от которой линейная функция связи зависит линейно. Вопрос о правильной нумерации остальных ребер все еще остается открытым. По-видимому, их можно пронумеровать произвольно (но так, чтобы относительно каждой вершины инцидентные ей ребра имели номера $1, 2, \ldots, d$).

5. О практическом применении

Криптографические алгоритмы, основанные на клеточных автоматах, могут найти широкое применение в различных областях, где требуется как легковесное шифрование (в том числе, для связи с беспилотными летательными аппаратами), так и обычное шифрование (например, для защиты электронных документов, в САПР [6]) и т.д.

Заключение

В статье развита теория обобщенных клеточных автоматов, свободных от одношаговых коллизий веса 1, которые очень важны для криптографических применений. Разработан метод построения таких автоматов, работающий за полиномиальное время.

Список литературы

1. Ключарёв П.Г. Блочные шифры, основанные на обобщённых клеточных автоматах // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2012. № 12. С. 361–374. DOI: 10.7463/0113.0517543
2. Ключарёв П.Г. Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2012. № 3. Режим доступа: http://technomag.bmstu.ru/doc/358973.html (дата обращения 01.08.2014).
3. Ключарёв П.Г. Построение псевдослучайных функций на основе обобщенных клеточных автоматов // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2012. № 10. С. 263–274. DOI: 10.7463/1112.0496381

4. Ключарёв П.Г. Криптографические хэш-функции, основанные на обобщенных клеточных автоматах // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2013. № 1. С. 161–172. DOI: 10.7463/0113.0534640
5. Панасенко С. Алгоритмы шифрования. Специальный справочник. СПб.: БХВ-Петербург, 2009. 576 с.
6. Чичварин Н. Выбор методов защиты проектной документации от несанкционированного доступа // Информационные технологии. 2014. № 5. С 41–48.
7. Buchmann J. Introduction to Cryptography. Springer New York, 2004. 338 p. (Ser. Undergraduate Texts in Mathematics). DOI: 10.1007/978-1-4419-9003-7
8. Davidoff G., Sarnak P., Valette A. Elementary number theory, group theory and Ramanujan graphs. Cambridge: Cambridge University Press, 2003. 154 p. (London Mathematical Society Student Texts; vol. 55).
9. Hoffstein J., Pipher J., Silverman J. An Introduction to Mathematical Cryptography. Springer New York, 2008. (Ser. Undergraduate Texts in Mathematics). DOI: 10.1007/978-0-387-77993-5
10. Hoory S., Linial N., Wigderson A. Expander graphs and their applications // Bulletin of the American Mathematical Society. 2006. Vol. 43, no. 4. P. 439–562.
11. Hopcroft J.E., Karp R.M. An n^5/2 algorithm for maximum matchings in bipartite graphs // SIAM Journal on computing. 1973. Vol. 2, no. 4. P. 225–231.
12. Lubotzky A., Phillips R., Sarnak P. Ramanujan graphs // Combinatorica. 1988. Vol. 8, no. 3. P. 261–277. DOI: 10.1007/BF02126799
13. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. Taylor & Francis, 1996. 816 p.
14. Paar C., Pelzl J. Understanding Cryptography: A Textbook for Students and Practitioners. Springer Berlin Heidelberg, 2010. 372 p. DOI: 10.1007/978-3-642-04101-3
15. Panasenko S., Smagin S. Lightweight cryptography: Underlying principles and approaches // International Journal of Computer Theory and Engineering. 2011. Vol. 3, no. 4. P. 516–520. DOI: 10.7763/IJCTE.2011.V3.360
16. Petersen J. Die theorie der regulären graphs // Acta Mathematica. 1891. Vol. 15, no. 1. P. 193–220. DOI: 10.1007/BF02392606
17. Plummer M.D. Graph factors and factorization: 1985–2003: a survey // Discrete Mathematics. 2007. Vol. 307, no. 7. P. 791–821. DOI: 10.1016/j.disc.2005.11.059
18. Preneel B. Stream ciphers and lightweight cryptography // Proc. of the 2nd International Workshop on ZUC Algorithm and Related Topics. Beijing, China, 2011.
19. Von Baebler F. Über die zerlegung regulärer streckenkomplexe ungerader ordnung // Commentarii Mathematici Helvetici. 1937. Vol. 10, no. 1. P. 275–287.

Science & Education of the Bauman MSTU
Electronic journal
ISSN 1994-0448

Science and Education of the Bauman MSTU, 2014, no. 9, pp. 194–202.
DOI: **10.7463/0914.0727086**
Received: 07.09.2014

On Collision Resistance of Generalized Cellular Automata

Klyucharev P. G.[1,*]

[*]pk.iu8@yandex.ru

[1]Bauman Moscow State Technical University, Moscow, Russia

Keywords: cryptography, cellular automata, collision

The author had previously developed the principles for creating the symmetric cryptoalgorithms based on the generalized cellular automata. In hardware implementation these cryptoalgorithms are of high efficiency. This work continues studies in this field. It investigates collisions arising during the operation of generalized cellular automata.

The main objective of the work is to develop a method for creating the generalized cellular automata to be resistant to a certain type of collisions.

Two various initial fillings of the generalized cellular machine gun differing in w categories and giving identical fillings after t steps shall be called a t-step collision of weight w. We notice that any t-step collision at the same time is also a step collision (t+u).

It is obvious that collisions existing in generalized cellular automata, provided that there are efficient algorithms to detect them, sharply worsen cryptographic properties of the crypto-algorithms based on it. Therefore methods for synthesis of generalized cellular automata, which are resistant to collisions are very important. This work studies resistance to the single-step collisions of weight 1.

The work shows that for a lack of single-step collisions of weight 1 it is enough that any other cell is linearly dependent on each cell of the cellular automata. For this, it is sufficient that the k-numbered edges with regard to any tops form, together with these tops, a 2-factor of the graph of the generalized cellular automata while a local function of relation has to be linear in k- numbered argument.

Existence conditions of 2-factor are given. The method to find the 2-factor in this graph is given. It is based on the search algorithm of the maximum bipartite matching.

Thus, the article develops a theory of the generalized cellular automata, free from single-step collisions of weight 1. Such automata are important for cryptographic applications. The method is developed to create such cellular automata operating in polynomial time.

References

1. Kliucharev P.G. Block ciphers based on generalized cellular automata. *Nauka i obrazovanie MGTU im. N.E. Baumana = Science and Education of the Bauman MSTU*, 2012, no. 12, pp. 361–374. DOI: 10.7463/0113.0517543 (in Russian).
2. Kliucharev P.G. On cryptographic properties of generalized cellular automation. *Nauka i obrazovanie MGTU im. N.E. Baumana = Science and Education of the Bauman MSTU*, 2012, no. 3. Available at: http://technomag.bmstu.ru/doc/358973.html, accessed 01.08.2014. (in Russian).
3. Kliucharev P.G. Construction of pseudo-random functions based on generalized cellular automata. *Nauka i obrazovanie MGTU im. N.E. Baumana = Science and Education of the Bauman MSTU*, 2012, no. 10, pp. 263–274. DOI: 10.7463/1112.0496381 (in Russian).
4. Kliucharev P.G. Cryptographic hash functions based on generalized cellular automata. *Nauka i obrazovanie MGTU im. N.E. Baumana = Science and Education of the Bauman MSTU*, 2013, no. 1, pp. 161–172. DOI: 10.7463/0113.0534640 (in Russian).
5. Panasenko S.P. *Algoritmy shifrovaniia. Spetsial'nyi spravochnik* [Reference book of encryption algorithms]. St. Petersburg, BKhV-Peterburg Publ., 2009. 576 p. (in Russian).
6. Chichvarin N.V. The Choice of Methods of Protection Design Documents from Unauthorized Access. *Informatsionnye tekhnologii*, 2014, no. 5, pp. 41–48. (in Russian).
7. Buchmann J. *Introduction to Cryptography*. Springer New York, 2004. 338 p. (Ser. *Undergraduate Texts in Mathematics*). DOI: 10.1007/978-1-4419-9003-7
8. Davidoff G., Sarnak P., Valette A. *Elementary number theory, group theory and Ramanujan graphs*. Cambridge, Cambridge University Press, 2003. 154 p. (*London Mathematical Society Student Texts*; vol. 55).
9. Hoffstein J., Pipher J., Silverman J. *An Introduction to Mathematical Cryptography*. Springer New York, 2008. (Ser. *Undergraduate Texts in Mathematics*). DOI: 10.1007/978-0-387-77993-5
10. Hoory S., Linial N., Wigderson A. Expander graphs and their applications. *Bulletin of the American Mathematical Society*, 2006, vol. 43, no. 4, pp. 439–562.
11. Hopcroft J.E., Karp R.M. An n^5/2 algorithm for maximum matchings in bipartite graphs. *SIAM Journal on Computing*, 1973, vol. 2, no. 4, pp. 225–231.
12. Lubotzky A., Phillips R., Sarnak P. Ramanujan graphs. *Combinatorica*, 1988, vol. 8, no. 3, pp. 261–277. DOI: 10.1007/BF02126799
13. Menezes A., van Oorschot P., Vanstone S. *Handbook of Applied Cryptography*. Taylor & Francis, 1996. 816 p.
14. Paar C., Pelzl J. *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer Berlin Heidelberg, 2010. 372 p. DOI: 10.1007/978-3-642-04101-3

15. Panasenko S., Smagin S. Lightweight cryptography: Underlying principles and approaches. *International Journal of Computer Theory and Engineering*, 2011, vol. 3, no. 4, pp. 516–520. DOI: 10.7763/IJCTE.2011.V3.360

16. Petersen J. Die theorie der regularen graphs. *Acta Mathematica*, 1891, vol. 15, no. 1, pp. 193–220. DOI: 10.1007/BF02392606

17. Plummer M.D. Graph factors and factorization: 1985–2003: a survey. *Discrete Mathematics*, 2007, vol. 307, no. 7, pp. 791–821. DOI: 10.1016/j.disc.2005.11.059

18. Preneel B. Stream ciphers and lightweight cryptography. *Proc. of the 2nd International Workshop on ZUC Algorithm and Related Topics*. Beijing, China, 2011.

19. Von Baebler F. Über die zerlegung regulärer streckenkomplexe ungerader ordnung. *Commentarii Mathematici Helvetici*, 1937, vol. 10, no. 1, pp. 275–287.