электронное научно-техническое издание

НАУКА и ОБРАЗОВАНИЕ

Эл № ФС77 - 30569. Государственная регистрация №0421100025. ISSN 1994-0408

О периоде обобщённых клеточных автоматов

77-30569/340943

 # 02, февраль 2012

П.Г. Ключарёв

УДК 519.713; 004.056.55

МГТУ им. Н.Э. Баумана

1. Введение

Эта статья является продолжением серии работ [2, 3, 1], посвященной исследованию возможности применения обобщённых клеточных автоматов в качестве криптографических примитивов. Концепция построения генераторов псевдослучайных двоичных последовательностей, базирующихся на обобщённых клеточных автоматах была впервые предложена в работах [4, 5]. Важной проблемой из этой области является построение клеточных автоматов, для которых можно получить нижнюю оценку периода выходной последовательности. Решению этой проблемы и посвящена настоящая работа.

2. Основные понятия

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

- булева переменная m_i, называемая *ячейкой*;
- булева функция $f_i(x_1, \ldots, x_{d_i})$, называемая локальной функцией связи i-ой вершины.

При этом для вершины v_i, входящие в неё ребра пронумерованы числами $1 \ldots d_i$.

Опишем теперь работу обобщённого клеточного автомата. В начальный момент времени каждая ячейка памяти $m_i, i = 1...N$ имеет некоторое начальное значение $m_i(0)$. Далее автомат работает по шагам. На шаге с номером t с помощью локальной функции связи вычисляются новые значения ячеек:

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

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

Назовем *однородным обобщённым клеточным автоматом* обобщённый клеточный автомат, у которого локальная функция связи для всех ячеек одинакова и равна f, то есть для любого $i \in \{1, ..., N\}$ выполняется $f_i = f$. Степени захода вершин такого клеточного автомата, очевидно, одинаковы: $d_1 = d_2 = \ldots = d_N = d$. Обобщённый клеточный автомат, не являющийся однородным, будем называть *неоднородным*.

Пусть задана двоичная последовательность $\{\xi_t\}$. Назовем *обобщённым клеточным автоматом с задающей последовательностью* (ОКАЗП) обобщённый клеточный автомат, у которого для вычисления одной из ячеек m_r (будем её называть задающей ячейкой), вместо формулы (1) используется формула

$$m_r(t) = f_r\left(m_{\eta(r,1)}(t-1), m_{\eta(r,2)}(t-1), \ldots, m_{\eta(r,d_r)}(t-1)\right) \oplus \xi_t. \qquad (2)$$

В том случае, если все локальные функции связи одинаковы, будем называть такой клеточный автомат *однородным обобщённым клеточным автоматом с задающей последовательностью*.

Некоторый набор ячеек клеточного автомата будем называть *выходом*. *Выходной последовательностью* клеточного автомата назовем функцию, аргументом которой является номер шага, а значением — значение выхода на этом шаге.

3. Нижняя оценка периода

Важнейшей характеристикой генераторов псевдослучайных последовательностей является длина периода. В особенности, эта характеристика важна в случае необходимости обеспечения криптографического качества псевдослучайной последовательности, вырабатываемой генератором. Именно с целью

обеспечения минимальной длины периода и было введено понятие задающей последовательности.

Пусть A — некоторое множество вершин клеточного автомата. Рассмотрим набор ячеек, ассоциированных с вершинами из этого множества, упорядоченными по возрастанию номеров. Набор значений этих ячеек на шаге t обозначим как $A(t)$. Теперь рассмотрим множество вершин, первый аргумент локальных функций связи которых берется из A:

$$\delta A = \{v_i | v_{\eta(i,1)} \in A\}. \tag{3}$$

Далее, рассмотрим множество

$$\Delta A = \delta A \cup \{v_i | \eta(j,u) = i, u \in \{2,3,\dots d_j\}, v_j \in \delta A\}\,. \tag{4}$$

Теперь введем обозначения

$$\Delta^0 A \equiv A, \tag{5}$$

$$\Delta^{j+1} A \equiv \Delta(\Delta^j A). \tag{6}$$

Теорема 1. Если для некоторого множества вершин A обобщённого клеточного автомата, локальная функция связи которого имеет вид $f_i(x_1,\dots,x_{d_i}) = \psi_i(x_2,\dots,x_{d_i}) \oplus x_1$, последовательность $A(t), t = 0,1,\dots$ имеет период длины L_A и, при этом, для каждой вершины $w \in A$, $\delta\{w\} \neq \varnothing$, то последовательность $\Delta A(t)$ имеет период длины $L_{\Delta A} \geqslant L_A$.

◄ Предположим, что $L_{\Delta A} < L_A$. Тогда существуют такие a_1, a_2 и b, что

$$A(a_1 L_{\Delta A} + b) \neq A(a_2 L_{\Delta A} + b). \tag{7}$$

В то же время, по определению периода,

$$\Delta A(a_1 L_{\Delta A} + b - 1) = \Delta A(a_2 L_{\Delta A} + b - 1), \tag{8}$$

$$\Delta A(a_1 L_{\Delta A} + b) = \Delta A(a_2 L_{\Delta A} + b). \tag{9}$$

Заметим, что для всех $v_i \in \delta A$, в формуле $f_i(x_1,\dots,x_{d_i}) = \psi_i(x_2,\dots,x_{d_i}) \oplus x_1$, переменная x_1 берется из ячейки, вершина которой принадлежит A. Учитывая формулу (7), а также то, что для каждой вершины $w \in A$ множество $\delta\{w\}$ не пусто, получаем, что хотя бы для одной вершины $v_i \in \delta A$ выполняется

$$m_i(a_1 L_{\Delta A} + b) = m_i(a_2 L_{\Delta A} + b) \oplus 1. \tag{10}$$

Следовательно, выполняется

$$\Delta A(a_1 L_{\Delta A} + b) \neq \Delta A(a_2 L_{\Delta A} + b), \tag{11}$$

что противоречит формуле (9). Это противоречие и доказывает теорему. ►

На основе доказанной теоремы предложим способ построения обобщённого клеточного автомата с заданным периодом.

Теорема 2. Период набора ячеек M обобщенного клеточного автомата с задающей последовательностью ξ_t имеет длину не меньшую чем длина периода задающей последовательности, если $\Delta^u\{v_r\} \subseteq M$, для задающей вершины v_r и некоторого $u \in \mathbb{N}$ и, при этом, для любого $w \in \Delta^j\{v_r\}$, для всех $j \in \{0, 1, \ldots, u-1\}$, выполняется $\delta\{w\} \neq \varnothing$.

◄ Если считать, что значения последовательности ξ_t принимает некоторая дополнительная ячейка v_{N+1}, от которой линейно зависит ячейка v_r, то перенумеровав переменные локальной функции связи этой ячейки и применив теорему 1, получим утверждение теоремы. ►

Итак, из доказанной теоремы видно, что если локальная функция связи линейно зависит от одного из своих аргументов и выходом автомата является множество вершин, удовлетворяющее условию теоремы 2, то нижней оценкой длины периода выходной последовательности обобщённого клеточного автомата является длина периода задающей последовательности. Породить задающую последовательность можно с помощью любого генератора псевдослучайных последовательностей, для которого известна нижняя оценка периода. Причем не предъявляется никаких требований к криптографическому качеству выходной последовательности такого генератора. Например, можно использовать линейный регистр сдвига с обратной связью, характеристический многочлен которого является примитивным.

4. Заключение

В работе предложен способ построения обобщённых клеточных автоматов, допускающих нижнюю оценку периода. Этот способ позволит доказывать нижнюю оценку длины периода выходной последовательности поточных шифров и

генераторов псевдослучайных последовательностей, основанных на обобщённых клеточных автоматах.

Автор выражает благодарность Д. А. Жукову за ценное обсуждение.

Список литературы

1. Ключарёв П. Г. Клеточные автоматы, основанные на графах Рамануджана, в задачах генерации псевдослучайных последовательностей // Наука и образование. Электронное научно-техническое издание. 2011. № 10. http://technomag.edu.ru/doc/241308.html.
2. Ключарёв П. Г. Криптографические свойства клеточных автоматов, основанных на графах Любоцкого-Филипса-Сарнака // Безопасные информационные технологии. Сборник трудов Второй всероссийской научно-технической конференции. М.: НИИ радиоэлектроники и лазерной техники, 2011. С. 163–173.
3. Ключарёв П. Г. NP-трудность задачи о восстановлении предыдущего состояния обобщенного клеточного автомата // Наука и образование. Электронное научно-техническое издание. 2012. № 1. http://technomag.edu.ru/doc/312834.html
4. Сухинин Б. М. Высокоскоростные генераторы псевдослучайных последовательностей на основе клеточных автоматов // Прикладная дискретная математика. 2010. № 2. С. 34–41.
5. Сухинин Б. М. О некоторых свойствах клеточных автоматов и их применении в структуре генераторов псевдослучайных последовательностей // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия: Приборостроение. 2011. № 2. С. 68–76.

electronic scientific and technical periodical

SCIENCE and EDUCATION

El № FS77 - 30569. №0421100025. ISSN 1994-0408

On period of generalized cellular automation

77-30569/340943

02, February 2012

P. Klyucharev

Bauman Moscow State Technical University

We introduce the method of constructing the generalized cellular with designated lower bounds of period. This property is very important for construction of stream ciphers based on generalized cellular automations.

References

1. Klyucharev P. G. Kletochnye avtomaty, osnovannye na grafah Ramanudzhana, v zadachah generacii psevdosluchajnyh posledovatel'nostej // Nauka i obrazovanie. Jelektronnoe nauchno-tehnicheskoe izdanie. 2011. № 10. http://technomag.edu.ru/doc/241308.html.
2. Klyucharev P. G. Kriptograficheskie svojstva kletochnyh avtomatov, osnovannyh na grafah Ljubockogo-Filipsa-Sarnaka // Bezopasnye informacionnye tehnologii. Sbornik trudov Vtoroj vserossijskoj nauchno-tehnicheskoj konferencii. M.: NII radiojelektroniki i lazernoj tehniki, 2011. C. 163–173.
3. Klyucharev P. G. NP-trudnost' zadachi o vosstanovlenii predydushchego sostojanija obobshchennogo kletochnogo avtomata // Nauka i obrazovanie. Jelektronnoe nauchno-tehnicheskoe izdanie. 2012. № 1. http://technomag.edu.ru/doc/312834.html
4. Suhinin B. M. Vysokoskorostnye generatory psevdosluchajnyh posledovatel'nostej na osnove kletochnyh avtomatov // Prikladnaja diskretnaja matematika. 2010. № 2. C. 34–41.
5. Suhinin B. M. O nekotoryh svojstvah kletochnyh avtomatov i ih primenenii v strukture generatorov psevdosluchajnyh posledovatel'nostej // Vestnik

Moskovskogo gosudarstvennogo tehnicheskogo universiteta im. N.Je. Baumana. Serija: Priborostroenie. 2011. № 2. C. 68–76.