электронное научно-техническое издание

НАУКА и ОБРАЗОВАНИЕ

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

Обеспечение криптографических свойств обобщенных клеточных автоматов

77-30569/358973

 # 03, март 2012

П.Г. Ключарев

УДК 519.713; 004.056.55

МГТУ им. Н.Э. Баумана
pk.iu8@yandex.ru

Введение

Объем информации, обрабатываемой современными информационными системами, все возрастает. Возрастают и требования к обеспечению информационной безопасности. В связи с этим требуются новые быстрые алгоритмы шифрования. Эта статья продолжает серию работ [1, 2, 3, 4], посвященную исследованиям обобщенных клеточных автоматов в контексте их приложений в криптографии. Концепция построения генераторов псевдослучайных последовательностей, основанных на обобщенных клеточных автоматах, была впервые предложена в работах [5, 6], где, в частности, показано, что на основе клеточных автоматов могут быть созданы новые поточные шифры, отличающиеся высокой скоростью работы.

Одной из важных задач, возникающих в связи с криптографическими применениями обобщенных клеточных автоматов, является разработка методов явного построения локальных функций связи. Решению этой задачи и посвящена настоящая работа.

1. Обобщенные клеточные автоматы

Назовем *обобщенным 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 нее ребра пронумерованы числами $1, \ldots, d_i$.

Опишем теперь работу обобщенного клеточного автомата. В начальный момент времени каждая ячейка памяти m_i, $i = 1, \ldots, N$, 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:

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

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

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

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

В том случае, если все локальные функции связи одинаковы, будем называть такой клеточный автомат *однородным обобщенным 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.

2. Нелинейность и равновесность

Известно, что для обеспечения хороших криптографических свойств преобразования необходимо, чтобы оно имело как можно большую нелинейность. Напомним, что *нелинейностью* [7] булевой функции называется расстояние от этой функции до множества аффинных функций. Кроме того, в работе [5] показано, что для обеспечения равномерности распределения выходной последовательности однородного обобщенного клеточного автомата необходимо и достаточно, чтобы локальная функция связи была равновесной.

Таким образом, требуется равновесная функция, обладающая как можно большей нелинейностью. Для построения такой функции мы воспользуемся методом, основанном на конкатенации бент-функций.

Напомним, что *бент-функцией* [7] называется булева функция от n переменных, все коэффициенты Уолша которой имеют вид $\pm 2^{n/2}$. Такие функции существуют только для

четных n и имеют максимально возможную нелинейность $2^{n-1} - 2^{n/2-1}$, однако не являются равновесными — их вес равен $2^{n-1} \pm 2^{n/2-1}$.

Для построения бент-функций мы воспользуемся методом Ротхауса [8], состоящем в том, что для произвольной булевой функции $s(x_1, \ldots, x_k)$, функция

$$\beta(x_1, y_1, \ldots, x_k, y_k) = \bigoplus_{i=1}^{k} x_i y_i \oplus s(x_1, \ldots, x_k) \tag{3}$$

является бент-функцией.

Пусть β_i, $i = 1, 2, 3, 4$, — бент-функции, такие, что $|\beta_1| + |\beta_2| = 2^n$ и $|\beta_3| + |\beta_4| = 2^n$ (здесь $|\beta|$ — вес функции β). Рассмотрим функции

$$g_1(u, x_1, x_2, \ldots, x_{2k}) = (1 \oplus u)\beta_1(x_1, \ldots, x_{2k}) \oplus u\beta_2(x_1, \ldots, x_{2k}); \tag{4}$$

$$g_2(v, u, x_1, x_2, \ldots, x_{2k}) = (1 \oplus v)\big((1 \oplus u)\beta_1(x_1, \ldots, x_{2k}) \oplus \\ \oplus u\beta_2(x_1, \ldots, x_{2k})\big) \oplus v\big((1 \oplus u)\beta_3(x_1, \ldots, x_{2k}) \oplus u\beta_4(x_1, \ldots, x_{2k})\big). \tag{5}$$

Для этих функций доказано [7], что они являются равновесными, а их нелинейности имеют следующие нижние оценки, близкие к максимально возможным:

$$N_{g_1} \geqslant 2^{2k} - 2^k; \tag{6}$$

$$N_{g_2} \geqslant 2^{2k+1} - 2^{k+1}. \tag{7}$$

Изложенный метод позволяет строить булевы функции большой нелинейности от произвольного числа переменных.

3. Построение локальной функции связи

Одной из важнейших характеристик генераторов псевдослучайных последовательностей является длина периода.

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 $A(t)$. Введем следующие обозначения:

$\delta A = \{v_i | v_{\eta(i,1)} \in A\}$;
$\Delta A = \delta A \cup \big\{v_i \,|\, \eta(j, u) = i,\ u \in \{2, 3, \ldots d_j\},\ v_j \in \delta A\big\}$;
$\Delta^0 A \equiv A$, $\Delta^{j+1} A \equiv \Delta(\Delta^j A)$.

В работе [4] доказана следующая теорема.

Теорема 1. Пусть дан обобщенный клеточный автомат с задающей последовательностью ξ_t, локальные функции связи которого имеют вид $f_i(x_1, \ldots, x_{d_i}) = \psi_i(x_2, \ldots, x_{d_i}) \oplus x_1$. Период набора ячеек M этого автомата 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 $\delta\{w\} \neq \varnothing$.

Из этой теоремы видно, что длину периода можно оценить снизу, если локальная функция связи линейно зависит от одного из своих аргументов и выходом автомата является множество вершин, удовлетворяющее условию теоремы 1.

Итак, необходима как можно более нелинейная и при том равновесная функция, линейно зависящая от одного из своих аргументов. Выберем функции s_1, s_2, s_3 и s_4, для которых выполняются соотношения

$$s_1(x_1, \ldots, x_k) = s_2(x_1, \ldots, x_k) \oplus 1, \quad s_3(x_1, \ldots, x_k) = s_4(x_1, \ldots, x_k) \oplus 1.$$

Теперь, в соответствии с (3), получим четыре бент-функции

$$\beta_j(x_1, y_1, \ldots, x_k, y_k) = \bigoplus_{i=1}^{k} x_i y_i \oplus s_j(x_1, \ldots, x_k), \quad j \in \{1, 2, 3, 4\}.$$

Из них в соответствии с (4) и (5) можно получить равновесные функции g_1 и g_2. Легко видеть, что выполняется

$$g_1(u, x_1, x_2, \ldots, x_{2k}) = \beta_1(x_1, \ldots, x_{2k}) \oplus u; \tag{8}$$

$$\begin{aligned} g_2(v,u,x_1,\ldots,x_{2k}) &= v(\beta_1(x_1,\ldots,x_{2k}) \oplus \beta_3(x_1,\ldots,x_{2k})) \oplus \beta_1(x_1,\ldots,x_{2k}) \oplus u = \\ &= \bigoplus_{i=1}^{k} x_i y_i \oplus s_1(x_1, \ldots, x_k) \oplus v(s_1(x_1, \ldots, x_k) \oplus s_3(x_1, \ldots, x_k)) \oplus u. \end{aligned} \tag{9}$$

Мы получили функции линейно зависящие от одного из своих аргументов, для которых справедливы нижние оценки нелинейности (6) и (7). Поэтому их можно применять в качестве локальных функций связи обобщенного клеточного автомата — необходимо только, чтобы для множества выходных ячеек автомата выполнялось условие теоремы 1.

4. Универсальность обобщенного клеточного автомата

Скажем, что обобщенный клеточный автомат вычисляет булеву функцию $\varphi(x_1, \ldots, x_n)$, если существуют такие числа $j_0 \in \{1, \ldots, N\}$, $t_0 \in \mathbb{Z}^+$ и набор $(j_1, \ldots, j_n) \in \{1, \ldots, N\}^n$ с попарно различными элементами, что выполняется равенство

$$m_{j_0}(t_0) = \varphi(m_{j_1}(0), \ldots, m_{j_n}(0)).$$

Теорема 2. Булеву функцию $\varphi(x_1, \ldots, x_n)$, которая при реализации схемой из функциональных элементов над базисом B имеет сложность l и глубину h, можно вычислить с помощью обобщенного клеточного автомата, локальные функции связи которого принадлежат B, а граф имеет $n + l$ вершин.

◄ Будем рассматривать схему как граф обобщенного клеточного автомата. Пусть у такого клеточного автомата вершины $(v_1, \ldots, v_n)$ соответствуют входам схемы, а остальные вершины — ее элементам. Припишем каждой вершине из множества $\{v_{n+1}, \ldots, v_{n+l}\}$, функцию, вычисляемую соответствующим элементом схемы. Для каждой вершины $v_i \in \{v_1, \ldots, v_n\}$ добавим в граф петлю (v_i, v_i) и припишем ей локальную функцию связи $f_i(x) = x$. Очевидно, что такой клеточный автомат вычисляет функцию φ за h шагов. ►

Если уже по виду локальной функции связи можно определить, что обобщенный клеточный автомат не может вычислить некоторый класс булевых функций, то криптоанализ систем шифрования, основанных на таких автоматах, упрощается. Заметим, что для того, чтобы однородный клеточный автомат мог вычислить произвольную функцию, необходимо, чтобы локальная функция связи являлась шефферовой. Исходя из этого будем считать, что для применений в криптографии необходимо, чтобы локальная функция связи однородного клеточного автомата являлась шефферовой.

Уточним условия, при которых функции (8) и (9) являются шефферовыми. Для этого, согласно теореме Поста, функция не должна принадлежать ни одному из следующих замкнутых классов:

- функций, сохраняющих 0 (T_0);
- функций, сохраняющих 1 (T_1);
- монотонных функций (M);
- самодвойственных функций (S);
- линейных функций (L).

Для начала докажем вспомогательные леммы.

Лемма 1. Соотношение $g_1 \notin T_0 \cup T_1$ верно тогда и только тогда, когда $k + t_1 = 1 \pmod 2$, где t_1 — число ненулевых слагаемых алгебраической нормальной формы функции s_1; при этом свободный член АНФ этой функции равен 1.

◄ Утверждение леммы следует из того, что

$$g_1(0, \ldots, 0) = \beta_1(0, \ldots, 0) = s_1(0, \ldots, 0),$$

а $s_1(0, \ldots, 0)$ равно свободному члену. Кроме того, $g_1(1, \ldots, 1)$ равен сумме $t_1 + k + 1$ единиц. ►

Лемма 2. Соотношение $g_2 \notin T_0 \cup T_1$ верно тогда и только тогда, когда $k + t_3 = 1 \pmod 2$, где t_3 — число ненулевых слагаемых алгебраической нормальной формы функции s_3. При этом свободный член АНФ функции s_1 равен 1.

◄ Действительно, легко видеть, что

$$g_2(0, \ldots, 0) = \beta_1(0, \ldots, 0) \oplus u, \quad g_2(1, \ldots, 1) = \beta_3(1, \ldots, 1) \oplus u.$$

Далее доказательство проводится аналогично доказательству леммы 1. ►

Лемма 3. Имеет место соотношение $g_1 \notin S$.

◄ Вычислим сумму функции g_1 с двойственной ей функцией:

$$g_1 \oplus g_1^* = g_1(u, x_1, y_1, \ldots, x_k, y_k) \oplus \overline{g_1(\overline{u}, \overline{x}_1, \overline{y}_1, \ldots, \overline{x}_k, \overline{y}_k)} =$$

$$= \beta_1(x_1, y_1, \ldots, x_k, y_k) \oplus \beta_1(x_1 \oplus 1, y_1 \oplus 1, \ldots, x_k \oplus 1, y_k \oplus 1) =$$

$$= \bigoplus_{i=1}^{k} x_i y_i \oplus s_1(x_1, \ldots, x_k) \oplus \bigoplus_{i=1}^{k} (x_i y_i \oplus x_i \oplus y_i \oplus 1) \oplus s_1(x_1 \oplus 1, \ldots, x_k \oplus 1) =$$

$$= \bigoplus_{i=1}^{k} x_i \oplus \bigoplus_{i=1}^{k} y_i \oplus k \oplus s_1(x_1, \ldots, x_k) \oplus s_1(x_1 \oplus 1, \ldots, x_k \oplus 1).$$

Рассматриваемая сумма существенно зависит от переменных y_i, но функция s_1 от этих переменных не зависит, следовательно, какова бы не была функция s_1, рассматриваемая сумма не тождественна нулю. Следовательно, $g_1 \notin S$. ►

Лемма 4. Имеет место соотношение $g_2 \notin S$.

◄ Положим $v = 0$ и рассмотрим сумму функции g_2 с двойственной ей функцией:

$$g_2 \oplus g_2^* = \beta_1(x_1, y_1, \ldots, x_k, y_k) \oplus \beta_3(x_1 \oplus 1, y_1 \oplus 1, \ldots, x_k \oplus 1, y_k \oplus 1).$$

Далее доказательство проводится аналогично доказательству леммы 3. ►

Перейдем теперь к основным теоремам этого раздела.

Теорема 3. Функция

$$g_1(u, x_1, y_1, \ldots, x_k, y_k) = \bigoplus_{i=1}^{k} x_i y_i \oplus s_1(x_1, \ldots, x_k) \oplus u$$

является шефферовой тогда и только тогда, когда выполняется $k + t_1 = 1 \pmod 2$, где t_1 — число ненулевых коэффициентов в алгебраической нормальной форме функции s_1; при этом свободный член равен 1.

◄ Действительно, в условиях теоремы выполняется лемма 1, утверждающая, что $g_1 \notin T_0$ и $g_1 \notin T_1$. Из нее следует, что $g_1 \notin M$. По лемме 3 $g_1 \notin S$. Кроме того, по определению $g_1 \notin L$. Из этих фактов следует утверждение теоремы. ►

Теорема 4. Функция

$$g_2(v, u, x_1, y_1, \ldots, x_k, y_k) =$$

$$= (1 \oplus v)(\beta_1(x_1, y_1, \ldots, x_k, y_k) \oplus u) \oplus v(\beta_3(x_1, y_1, \ldots, x_k, y_k) \oplus u) =$$

$$= \bigoplus_{i=1}^{k} x_i y_i \oplus s_1(x_1, \ldots, x_k) \oplus v(s_1(x_1, \ldots, x_k) \oplus s_3(x_1, \ldots, x_k))$$

является шефферовой тогда и только тогда, когда $k + t_3 = 1 \pmod 2$, где t_3 — число ненулевых коэффициентов в алгебраической нормальной форме функции s_3. При этом свободный член АНФ функции s_1 равен 1.

◄ Действительно, в условиях теоремы выполняется лемма 2, утверждающая, что $g_2 \notin T_0$ и $g_2 \notin T_1$. Из нее следует, что $g_2 \notin M$. Согласно лемме 3, $g_2 \notin S$. Кроме того, по определению $g_2 \notin L$. Из этих фактов следует утверждение теоремы. ►

5. Заключение

В работе предложено семейство локальных функций связи обобщенных клеточных автоматов, подходящее для применения в криптографии.

В случае нечетного числа переменных, используется функция

$$g_1(u, x_1, y_1, \ldots, x_k, y_k) = \bigoplus_{i=1}^{k} x_i y_i \oplus s_1(x_1, \ldots, x_k) \oplus u,$$

где $s_1(x_1, \ldots, x_k)$ — произвольная булева функция, причем выполняется сравнение $k+t_1 = 1 \pmod 2$, где t_1 — число ненулевых коэффициентов в алгебраической нормальной форме функции s_1. При этом свободный член равен 1.

Если же число переменных четно, используется функция

$$\begin{aligned} g_2(v, u, x_1, y_1, \ldots, x_k, y_k) = \\ = (1 \oplus v)(\beta_1(x_1, y_1, \ldots, x_k, y_k) \oplus u) \oplus v(\beta_3(x_1, y_1, \ldots, x_k, y_k) \oplus u) = \\ = \bigoplus_{i=1}^{k} x_i y_i \oplus s_1(x_1, \ldots, x_k) \oplus v(s_1(x_1, \ldots, x_k) \oplus s_3(x_1, \ldots, x_k)) \oplus u, \end{aligned}$$

где $s_1(x_1, \ldots, x_k)$ и $s_3(x_1, \ldots, x_k)$ — произвольные булевы функции, причем должно выполняться сравнение $k + t_3 = 1 \pmod 2$, где t_3 — число ненулевых коэффициентов АНФ функции s_3. При этом свободный член АНФ функции s_1 равен 1.

Построенное семейство функций позволяет строить обобщенные клеточные автоматы, допускающие нижнюю оценку периода, а также большую нелинейность выполняемого преобразования. Также, использование этих функций является необходимым условием универсальности обобщенного клеточного автомата, что, по-видимому, способствует повышению криптографической стойкости поточных шифров, основанных на обобщенных клеточных автоматах.

Список литературы

1. *Ключарев 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.

2. *Ключарев П. Г.* NP-трудность задачи о восстановлении предыдущего состояния обобщенного клеточного автомата // Наука и образование. Электронное научно-техническое издание. – 2012. – № 1.
3. *Ключарев П. Г.* Клеточные автоматы, основанные на графах Рамануджана, в задачах генерации псевдослучайных последовательностей // Наука и образование. Электронное научно-техническое издание. – 2011. – № 10.
4. *Ключарев П. Г.* О периоде обобщенных клеточных автоматов // Наука и образование. Электронное научно-техническое издание. – 2012. – № 2.
5. *Сухинин Б. М.* Высокоскоростные генераторы псевдослучайных последовательностей на основе клеточных автоматов // Прикладная дискретная математика. – 2010. – № 2. – С. 34–41.
6. *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.
7. *Cusick T.*, *Stănică P.* Cryptographic Boolean functions and applications. – Academic Press, 2009. – 232 p.
8. *Rothaus O.* On bent functions // Journal of Combinatorial Theory, Series A. – 1976. – V. 20, No. 3. – P. 300–305.

electronic scientific and technical periodical

SCIENCE and EDUCATION

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

On cryptographic properties of generalized cellular automation

77-30569/358973

03, March 2012

P.G. Klyucharev

Bauman Moscow State Technical University
pk.iu8@yandex.ru

We introduce the family of Boolean functions, which can be used as local transition functions in generalized cellular automates. The functions from this family are balanced. The nonlinearity of them is large. The cellular automates based on them have a bottom estimation of period. These properties are important for cryptographic applications of generalized cellular automations.

References

1. *Kliucharev P.G.* Kletochnye avtomaty, osnovannye na grafakh Ramanudzhana, v zadachakh generatsii psevdosluchainykh posledovatel'nostei [Cellular automata, based on Ramanujan graphs, in the problems of pseudorandom sequences generation]. Nauka i obrazovanie, 2011, no. 10. Available at: http://technomag.edu.ru/doc/241308.html.
2. *Kliucharev P.G.* Kriptograficheskie svoistva kletochnykh avtomatov, osnovannykh na grafakh Liubotskogo-Filipsa-Sarnaka [Cryptographic properties of cellular automata based on LPS-graphs]. Bezopasnye informatsionnye tekhnologii. Trudy 2 Vseros. nauch.-tekhn. konf. [Secure information technologies. Proc. 2nd All-Rus. sci.-tech. conf.]. Moscow, Inst. Radioelectron. and Laser Technol. Publ., 2011, pp. 163–173.
3. *Kliucharev P.G.* O periode obobshchennykh kletochnykh avtomatov [About the period of generalized cellular automatons]. Nauka i obrazovanie, 2012, no. 2.
4. *Kliucharev P.G.* NP-trudnost' zadachi o vosstanovlenii predydushchego sostoianiia obobshchennogo kletochnogo avtomata [NP-hard of step backward problem in generalized cellular automaton]. Nauka i obrazovanie, 2012, no. 1.
5. *Sukhinin B.M.* Vysokoskorostnye generatory psevdosluchainykh posledovatel'nostei na osnove kletochnykh avtomatov [High-speed generators of pseudorandom sequences based on cellular automata]. Prikladnaia diskretnaia matematika, 2010, no. 2, pp. 34–41.
6. *Sukhinin B.M.* O nekotorykh svoistvakh kletochnykh avtomatov i ikh primenenii v strukture generatorov psevdosluchainykh posledovatel'nostei [Some properties of cellular automata and

their application in the structure of pseudorandom sequences generators]. Vestnik MGTU im. N.E. Baumana. Ser . Priborostroenie [Herald of the Bauman MSTU. Ser. Instrumentation], 2011, no. 2, pp. 68–76.

7. *Cusick T.W., Stanica P.* Cryptographic Boolean functions and applications. London, Acad. Press, 2009. 232 p.
8. *Rothaus O.S.* On «bent» functions. Journal of Combinatorial Theory, Ser. A, 1976, vol. 20, no. 3, pp. 300–305.