УДК 004.421.5

ВЫСОКОСКОРОСТНЫЕ ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ КЛЕТОЧНЫХ АВТОМАТОВ

Б. М. Сухинин

Клеточным автоматом (КлА) называется модель с дискретным временем, состоящая из множества ячеек памяти, упорядоченных в периодическую n-мерную решетку [1]. Значениями ячеек являются элементы некоторого конечного множества. Для каждой ячейки выбирается ее окрестность, которая используется для определения значения ячейки на следующем такте работы по некоторому заранее заданному правилу.

Для классических клеточных автоматов выполняются свойства однородности и локальности. Однородность означает, что все ячейки КлА являются неразличимыми по своим свойствам; кроме того, для решения проблемы краевых клеток противоположные края решетки отождествляются, то есть двумерная решетка закручивается в тор. В соответствии со свойством локальности в окрестность каждой ячейки входят только ячейки, удаленные от нее на расстояние не более заданного.

В нашей работе мы рассматриваем однородные двумерные булевы клеточные автоматы с прямоугольными ячейками. Окрестность ячейки включает подмножество ячеек, непосредственно смежных с данной, а также, возможно, ее саму. В качестве правила, определяющего новое значение ячейки на следующем такте работы, используется булева функция, которую мы будем называть локальной функцией связи (ЛФС). Аргументами ЛФС являются значения всех ячеек из окрестности данной. Использование КлА с большей размерностью решетки или более широкой окрестностью увеличивает число аргументов ЛФС и делает ее реализацию непрактичной.

Мы вводим понятие лавинного эффекта в клеточных автоматах по аналогии с лавинным эффектом, введенным Хорстом Фейстелем [2] в 1973 г. для оценки свойств криптографических преобразований. Лавинный эффект показывает, насколько сильно изменяется поведение КлА во времени при изменении значения одной ячейки. Если изменения распространяются по решетке равномерно во всех направлениях с максимально возможной линейной скоростью (в данном случае составляющей одну ячейку за такт работы) и при этом затрагивают половину всех ячеек на каждом такте работы, то такой лавинный эффект мы называем оптимальным.

Для оценки лавинного эффекта вводятся две числовые характеристики: интегральная и пространственная. Первая отражает отношение числа изменившихся ячеек к общему их количеству, вторая — линейную скорость распространения изменений по решетке КлА. Компьютерное моделирование показало, что характеристики приближаются к оптимальным по мере увеличения числа аргументов ЛФС, которое совпадает с мощностью окрестности ячейки. При этом характеристики для функций от 8 и 9 аргументов являются практически идентичными.

Также в работе исследуется влияние свойств ЛФС и размеров решетки на функционирование клеточного автомата. Мы показываем, что необходимым условием равномерного заполнения ячеек решетки является равновесность локальной функции связи. Кроме того, рассматриваются пространственные периоды в заполнении решетки, которые существенно снижают временной период КлА. Для уменьшения вероятности возникновения пространственных периодов следует выбирать в качестве размеров решетки простые числа; вероятность также уменьшается при увеличении числа аргументов ЛФС.

В состав генератора ПСП на основе двумерных булевых КлА входят два клеточных автомата и регистр сдвига с линейной обратной связью (РСЛОС). Размеры решетки одинаковы для обоих автоматов и составляют 37×11 ячеек. Окрестность каждой ячейки состоит из ячеек, непосредственно смежных с ней, что соответствует ЛФС от 8 аргументов. В качестве выхода клеточного автомата используются значения ячеек, входящих в подрешетку размера 32×8, что обеспечивает выработку каждым КлА 256 бит за один такт работы. Для каждого клеточного автомата используется своя собственная равновесная локальная функция связи.

Выход РСЛОС на каждом такте работы прибавляется по модулю 2 к значению одной из ячеек каждого клеточного автомата. Лавинный эффект позволяет гарантировать, что период внутренних состояний клеточных автоматов будет не меньше периода выходной последовательности РСЛОС. Мы считаем, что для практического применения генератора достаточно использовать РСЛОС длины 63, что обеспечивает период выходной последовательности КлА не менее $2{,}4 \cdot 10^{21}$ бит.

Выход генератора формируется посредством сложения по модулю 2 выходных последовательностей обоих клеточных автоматов, что позволяет существенно улучшить статистические свойства выходной последовательности генератора, увеличить ее период и затруднить восстановление внутреннего состояния генератора по выходным значениям.

Автором был разработан прототип аппаратной реализации предложенного генератора на ПЛИС Altera Cyclone II (EP2C35F672C6). Выходная последовательность генератора подавалась напрямую на выводы микросхемы ПЛИС, а также записывалась для дальнейшего анализа во внутреннюю память.

Параллельная структура клеточных автоматов позволила достичь формирования выхода генератора за один такт синхронизации схемы. Рабочая частота схемы составила 100 МГц; учитывая, что на каждом такте работы генератор формирует 256 бит выходной последовательности, скорость ее выработки составила 23,8 Гбит/с.

Анализ статистических свойств выходной последовательности проводился при помощи набора тестов NIST [3], предназначенного для выявления статистических отклонений исследуемой последовательности от истинно случайной. В результате тестирования генераторов с различными локальными функциями связи клеточных автоматов были обнаружены функции, при которых генератор успешно проходит все тесты из набора. Для сокращенной версии генератора, в которой один из двух клеточных автоматов отключен и не вырабатывает выходную последовательность, таких функций обнаружено не было; тем не менее сокращенный генератор может использоваться в приложениях с менее жесткими требованиями к статистическим свойствам ПСП.

В настоящее время ведется работа над программной реализацией генератора, использующей в качестве вычислительного устройства графический адаптер ПЭВМ, что позволит говорить о возможности массового применения разработанных алгоритмов. Кроме того, другими объектами исследований являются неоднородные клеточные автоматы, в которых окрестность каждой ячейки выбирается случайным образом, но не изменяется в процессе работы. Неоднородные КлА обладают существенно лучшими характеристиками по сравнению с рассмотренными выше, а также позволяют строить намного более эффективные реализации.

ЛИТЕРАТУРА

1. *Farmer D., Toffoli T., Wolfram S.* Preface to Cellular Automata // Proceedings of an Interdisciplinary Workshop. 1984. P. vii–xii.

2. *Feistel H.* Cryptography and Computer Privacy // Scientific American. 1973. V. 228. No. 5. P. 15–23.
3. http://csrc.nist.gov/publications/nistpubs/800-22-rev1/SP800-22rev1.pdf — NIST SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, revision 1.

УДК 003.26.09

СВЯЗЬ СТРУКТУРЫ МНОЖЕСТВА ОТКРЫТЫХ КЛЮЧЕЙ СО СТОЙКОСТЬЮ КРИПТОСИСТЕМЫ МАК-ЭЛИСА–СИДЕЛЬНИКОВА

И. В. Чижов

Криптосистема Мак-Элиса — одна из старейших криптосистем с открытым ключом. Она была предложена в 1978 г. Р. Дж. Мак-Элисом [1]. Эта криптосистема основывается на $\mathbb{NP}$-трудной проблеме в теории кодирования. В. М. Сидельников в работе [2] предложил использовать для построения криптосистемы Мак-Элиса коды Рида–Маллера $RM(r, m)$, однако, проведя криптоанализ, В. М. Сидельников пришёл к выводу, что на сегодняшний день такая криптосистема не обеспечивает должного уровня стойкости, и в той же работе предложил усиленную модификацию криптосистемы Мак-Элиса на основе РМ-кодов — криптосистему Мак-Элиса–Сидельникова.

Рассмотрим оригинальную криптосистему Мак-Элиса, построенную на кодах Рида–Маллера $RM(r, m)$. При этом предполагается, что выполнено неравенство $2r \leqslant m$, так как именно при таких ограничениях на m и r обеспечивается эффективность алгоритмов декодирования РМ-кода. Будем понимать под взломом как оригинальной криптосистемы Мак-Элиса, так и модифицированной (криптосистемы Мак-Элиса–Сидельникова) восстановление компонентов секретного ключа по открытому ключу. Легко видеть, что в этом случае стойкость оригинальной криптосистемы Мак-Элиса определяется сложностью задачи mcRM (см. далее). Другими словами, если злоумышленник научится эффективно решать задачу mcRM, то он тем самым сможет взломать оригинальную криптосистему Мак-Элиса, построенную на основе РМ-кодов.

Задача mcRM

Вход: матрица $G = H \cdot R \cdot \gamma$, где H — невырожденная двоичная $(k \times k)$-матрица; R — порождающая $(k \times n)$-матрица кода Рида–Маллера $RM(r, m)$; γ — перестановочная $(n \times n)$-матрица.

Найти: невырожденную матрицу H' размера $(k \times k)$ и перестановочную $(n \times n)$-матрицу γ', такие, что $H' \cdot G \cdot \gamma'$ — порождающая матрица кода Рида–Маллера $RM(r, m)$, то есть найдётся невырожденная $(k \times k)$-матрица M, что выполнено равенство $H' \cdot G \cdot \gamma' = M \cdot R$.

Введем в рассмотрение семейство mcRMi задач для $1 \leqslant i \leqslant k$.

Задача mcRMi

Вход: матрица $G = H' \cdot R' \cdot \gamma'$, где H' — невырожденная двоичная $(k-1) \times (k-1)$-матрица; R' — $((k-1) \times n)$-матрица, получающаяся из порождающей матрицы R кода Рида–Маллера $RM(r, m)$ выкидыванием строки с номером i; γ' — перестановочная $(n \times n)$-матрица.

Найти: невырожденную матрицу M' размера $(k-1)\times(k-1)$ и перестановочную $(n\times n)$-матрицу σ', такие, что $M' \cdot G \cdot \sigma'$ — порождающая матрица кода $\mathcal{R}'$, порождаемого матрицей R', то есть найдётся невырожденная $((k-1) \times (k-1))$-матрица L', что выполнено равенство $M' \cdot G \cdot \sigma' = L' \cdot R'$.