# ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ КЛЕТОЧНЫХ АВТОМАТОВ

А.Н. Гамова

На сегодняшний день известно сравнительно небольшое число криптосистем с открытым ключом, причем к ним зачастую предъявляются претензии, как ввиду их малой скорости работы, так и по поводу недостаточного обоснования их стойкости. В основании стойкости таких систем обычно лежит вычислительная трудность решения некоторой задачи для какой-то алгебраической системы, чаще всего с элементами числовой природы. В подавляющем большинстве случаев это или задача факторизации больших чисел, или задача дискретного логарифмирования в циклической группе. Еще более печальны перспективы указанных криптосистем в случае появления квантового компьютера, работающего с тысячами кубит. Поиск же других алгебраических систем, применимых в криптографии с открытым ключом в постквантовом мире, является трудной задачей и требует вовлечения в криптографический обиход новых математических объектов. В этой связи стоит обратить особое внимание на клеточные автоматы, которые представляют собой некоммутативные алгебраические структуры, распараллеленность которых позволяет увеличивать скорость работы и пропускную способность аппаратных реализаций криптоалгоритмов. Эволюция КА развертывается в дискретном пространстве, состоящем из клеток. Законы эволюции локальны, т.е. динамика системы задается неизменным набором правил, по которым осуществляется вычисление нового состояния клеток в зависимости от состояния окружающих ее соседей. Эта смена состояний происходит одновременно и параллельно, а время идет дискретно. Несмотря на простоту построения, КА могут демонстрировать разнообразное и сложное поведение, что дает возможность использовать КА в моделировании природных систем и физических процессов, а также и для генерации случайных чисел. В классических клеточных автоматах набор ячеек представляется в виде упорядоченного множества, элементы которого располагаются в узлах $n$-мерной решетки (наибольшее распространение получили автоматы с одно-, двух- и трехмерными решетками). Кроме того, для классических клеточных автоматов выполняются свойства однородности и локальности. Однородность означает, что все ячейки клеточного автомата являются неразличимы ми по своим свойствам: для них используются одни и те же правила переходов и одинаковые способы выбора окрестности. В окрестность каждой ячейки входит подмножество ячеек, удаленных от данной на расстояние не более заданного и, возможно, она сама. Одной из основных проблем при использовании клеточных

автоматов в генераторах псевдослучайных последовательностей является непредсказуемость их периода в силу нелинейности функции переходов. При этом лавинный эффект позволяет гарантировать, что период последовательности внутренних состояний клеточных автоматов не меньше периода выходной последовательности регистра сдвига. Начальные значения ячеек памяти регистра сдвига также являются ключом выработки псевдослучайной последовательности генератора в целом, т. е. определяют выбор конкретной последовательности из множества возможных.

**Литература**

1. Ефремова А.А., Гамова А.Н. Самопрограммируемые клеточные автоматы в криптографии // Прикладная дискретная математика. 2017. № 10. С. 76–81.