Клеточные автоматы в криптографии txt (v. 1.1)

Клеточные автоматы (КлА) – одна из старейших моделей вычислений, насчитывающая уже более 60 лет.

Станислав Улам, работая в Лос-Аламосской национальной лаборатории в 1940-е годы, изучал рост кристаллов, используя простую решёточную модель[1]. В это же время Джон фон Нейман, коллега Улама, работал над проблемой самовоспроизводящихся систем. Улам предложил фон Нейману использовать более абстрактную математическую модель, подобную той, что Улам использовал для изучения роста кристаллов. Таким образом, возникла первая клеточно-автоматная система.

Конрад Цузе, известный как создатель первого действительно работающего программируемого компьютера Z3 занимался клеточным автоматами на нерегулярных решетках

Также в 1940-е годы, Норберт Винер и Артуро Розенблют разработали клеточно-автоматную модель возбудимой среды. Целью было математическое описание распространения импульса в сердечных нервных узлах.

В 1969 году немецкий инженер Конрад Цузе опубликовал книгу «Вычислимый космос», где выдвинул предположение, что физические законы дискретны по своей природе, и что вся Вселенная является гигантским клеточным автоматом. Это была первая книга из области, называемой сейчас цифровой физикой.

Классический клеточный автомат представляет собой упорядоченный набор ячеек памяти, образующих некоторую регулярную *n*-мерную решетку (на практике наибольшее распространение приобрели клеточные автоматы небольшой размерности – с одно- или двухмерными решетками). Каждая ячейка памяти клеточного автомата может хранить одно значение из некоторого конечного множества (как правило – 1 бит). Время для клеточного автомата изменяется дискретными шагами (тактами). Смена значений всех ячеек решетки происходит синхронно и одновременно при увеличении номера такта, в соответствии с правилами перехода, определяющими новое значение каждой ячейки памяти как функцию от текущих значений других ячеек.

Структура пространственной решетки зависит от формы входящих в нее ячеек. Так, например, в двумерном случае можно рассматривать ячейки прямоугольной, треугольной, шестиугольной формы, а также и иных

конфигураций. Наибольшее внимание получили клеточные автоматы, в которых ячейки имеют квадратную форму, а сами решетки – прямоугольную.

КлА обладает несколькими фундаментальными свойствами физического мира, а именно: массовым параллелизмом, однородностью и локальностью.

- Параллельность – обновления всех клеток происходят независимо друг от друга.
- Локальность – новое состояние клетки зависит только от старого состояния клетки и некоторой её окрестности.
- Однородность – все клетки обновляются по одним и те же правилам.

Другие физические свойства, такие, как обратимость и законы сохранения могут быть обеспечены выбором соответствующих правил обновления. В этой связи не удивительно, что КлА позволяют успешно моделировать различные физические, биологические и даже социальные системы и явления.

В последние 2 десятилетия эта математическая модель получила большое количество приложений в качестве. Основные приложения – имитационное моделирование физических процессов и систем, построение биологических моделей, включая модели самовоспроизводства, обработка изображений, распознаватель языковых конструкций и другие модели структурной лингвистики, архитектура вычислительных систем, теория помехоустойчивого кодирования, теория хаоса, теория фракталов и, наконец, приложения к криптографии. Что касается последней, клеточные автоматы нашли свое применение как в симметричной, так и в асимметричной криптографии, в схемах аутентификации и разделения секрета.

После первого приложения теории КлА к криптографии (1985 г.) и волны публикаций в этом направлении, последовавшей в период конец 80-х – начало 90-х годов, последовало некоторое охлаждение к этой тематике и, как следствие, относительное затишье в числе публикаций. Объясняется это тем, что в первых криптографических алгоритмах, использовавших модель КлА, были обнаружены слабости. Часть работ, как это порой бывает с направлениями, ставшими вдруг «модными», оказалось просто элементарно безграмотными и содержало грубейшие ошибки. Все это не могло не сказаться «авторитете» этой тематики.

Однако, в последнее время вновь наблюдается рост интереса криптографического сообщества к использованию клеточно-автоматных моделей

в криптографии. Количество работ, посвященных приложению КлА к криптографии за последние годы резко выросло. Все это объясняется самой природой КлА, их неотъемлемыми достоинствами и, прежде всего, свойствами параллельности и локальности. Они позволяет организовать одновременную обработку существенных порций информации с помощью достаточно скромных вычислительных ресурсов. Все это соответствует современной тенденции в развитии информационных технологий, когда огромный поток самой разнообразной информации из самых разных источников требует обработки порой в условиях весьма ограниченных вычислительных ресурсов (как то, например, смарт-карты или радиочастотные метки, имеющие выход в Интернет) и образующие сферу так называемого Интернета Вещей.

Первые исследования в области применения клеточных автоматов в криптографии, принадлежат С. Вольфраму и относятся к 1-мерным клеточным автоматам. Вольфрамом и рядом других авторов была рассмотрена возможность применения одномерных клеточных автоматов в качестве генераторов гаммы поточного шифрования.

В настоящее время 1-мерные клеточные автоматы используются в составе генератора псевдослучайных последовательностей в математическом пакете Wolfram Mathematica, разработанном компанией Wolfram Research, однако в остальном не получили широкого распространения.

Возможность применения 2-мерных клеточных автоматов в качестве генераторов гаммы поточного шифрования была рассмотрена в работах …

Machhout Mohsen, Guitouni Zied, Zeghid Medien, Tourki Rached «Design of reconfigurable image encryption processor using 2-D cellular automata generator», International Journal of Computer Science and Applications, Vol. 6, No, 4, pp. 43 - 62 , 2009

Но наибольших успехов это направление получило в работах Б. Сухинина:

- Сухинин Б. М. Разработка генераторов псевдослучайных двоичных последовательностей на основе клеточных автоматов // Наука и образование: электронное научно-техническое издание. 2010. №9. URL: http://technomag.edu.ru/doc/159714.html

- Сухинин Б. М. О влиянии параметров локальной функции связи на распределение значений ячеек двоичных клеточных автоматов // Объединенный научный журнал. 2010. №8. С. 39 – 41.
- Сухинин Б. М. О лавинном эффекте в клеточных автоматах // Объединенный научный журнал. 2010. №8. С. 41 – 46.
- Сухинин Б. М. Высокоскоростные генераторы псевдослучайных последовательностей на основе клеточных автоматов // Прикладная дискретная математика. 2010. №2. С. 34 – 41.
- Сухинин Б. М. Исследование характеристик лавинного эффекта в двоичных клеточных автоматах с равновесными функциями переходов // Наука и образование: электронное научно-техническое издание. 2010. №8. URL: http://technomag.edu.ru/doc/159565.html
- Сухинин, Б.М. Разработка и исследование высокоскоростных генераторов псевдослучайных равномерно распределенных двоичных последовательностей на основе клеточных автоматов. // Диссертация на соискание ученой степени кандидата технических наук. – Москва, 2011. – 224 с.

Для характеристики криптографических свойств 2-мерных клеточного автомата Б. Сухининым было применено понятие лавинного эффекта, введенное в 1973 году Х. Фейстелем для блочных шифров. С криптографической точки зрения – это свойство преобразований при котором небольшие изменения входных данных влекут за собой значительные изменения выходных данных. Оно играет важнейшую роль при изучении свойств блочных шифров и хэш-функций.

Для количественного описания лавинного эффекта в классических клеточных автоматах Сухининым были введены понятия *интегральной* и *пространственной* характеристик лавинного эффекта.

Интегральная характеристика лавинного эффекта $\left(\eta(t)\right)$ определяет временну́ю зависимость распространения лавинного эффекта, и равна отношению числа изменившихся к данному моменту времени ячеек к общему числу ячеек обобщенного клеточного автомата:

$$\eta(t) = \frac{1}{N}\sum_{i=1}^{N}\left(v_i(t) \oplus v_i(t)\right)$$

В свою очередь *пространственная характеристика* $\mu(t)$ показывает скорость с которой изменения распространяются по решетке клеточного автомата.

Так же было введено понятие *оптимального лавинного эффекта*: оптимальным лавинным эффектом называется лавинный эффект при котором изменения распространяются по решетке клеточного автомата равномерно во всех направлениях с максимально возможной скоростью и при этом значение каждой ячейки изменяется с вероятностью 1/2.

В итоге для 2-мерных клеточных автоматов в работах Сухинина было

- исследовано влияние веса локальной функции связи на распределение значений ячеек памяти клеточных автоматов; сформулирован, доказан и подтвержден эмпирически критерий сохранения равномерности распределения;
- получено описание характеристик оптимального лавинного эффекта и эмпирические зависимости характеристик лавинного эффекта от выбора окрестностей ячеек; показано, что клеточные автоматы обладают свойством размножения изменений;
- разработаны новые методы генерации псевдослучайных последовательностей; осуществлен синтез структуры генератора и обоснован выбор его параметров; указан способ обеспечения заданного периода выходной последовательности;
- исследованы статистические свойства выходных последовательностей разработанных генераторов; определены конкретные локальные функции связи и окрестности ячеек клеточных автоматов, обеспечивающие хорошие статистические свойства выходных последовательностей; подтверждено соответствие статистических свойств современным требованиям; разработан программный комплекс автоматизации процесса статистического тестирования;
- разработана и изготовлена в виде устройства на ПЛИС высокоскоростная аппаратная реализация предложенных генераторов на базе 2-мерных клеточных автоматов, превосходящая аналоги по быстродействию.

Обобщенные клеточные автоматы

Обобщенный клеточный автомат был предложен в работе Б. Сухинина [5], где он был назван «неоднородным клеточным автоматом» (в данной работе термин «неоднородный клеточный автомат» будет использоваться в другом смысле). Математически обобщенный КлА можно описать следующим образом:

Пусть задан ориентированный граф $A = (V, E)$, где $V = \{v_1, \dots v_n\}$ – множество вершин графа, E – множество дуг. Пусть d_i – полустепень захода для вершины v_i, при этом входящие в вершину дуги пронумерованы числами 1,…, d_i. Будем считать, что с каждой вершиной v_i ассоциирована ячейка памяти, содержащая булеву переменную m_i, и булева функция $f_i(x_1, \dots, x_{d_i})$ – локальная функция связи *i*-й вершины.

Обобщенный клеточный автомат – это автономный автомат, его внутренним состоянием в момент времени t называется заполнение ячеек $(m_1(t), m_2(t), \dots, m_n(t))$. Тогда работа обобщенного КлА описывается уравнением:

$$m_i(t) = f_i\left(m_{n(i,1)}(t-1), m_{n(i,2)}(t-1), \dots, m_{n(i,d_i)}(t-1)\right),$$

где $m_i(t)$ – состояние *i*-й ячейки памяти в момент времени t, $n\,(i,j)$ – номер вершины, из которой исходит дуга, входящая в вершину *i* и имеющая номер j. Функция переходов является отображением множества состояний в себя и определяет следующее состояние автомата как функцию от текущего состояния.

Однородный обобщенный клеточный автомат – это обобщенный клеточный автомат, граф которого является регулярным по входу и при этом локальная функция связи для всех ячеек одинакова и равна f, т.е. $\forall i \in \{1, \dots, N\} \Rightarrow f_i = f$, где N – число ячеек автомата.

Обобщенный КлА может иметь входную последовательность, загружаемую в его ячейки памяти и задающую внутреннее состояние автомата в начальный момент времени. *Выходом* однородного обобщенного КлА на шаге с номером t будем считать значения первых r ячеек в этот момент времени: $m_0(t), m_1(t), \dots, m_r(t)$. Последовательность:

$$m_0(t_0), m_1(t_0), \dots, m_{r-1}(t_0), m_0(t_0+1), \dots, m_{r-1}(t_0+1), m_0(t_0+2) \dots$$

будем называть выходной последовательностью клеточного автомата.

Переход к обобщенному клеточному автомату позволяет не только сохранить все преимущества классического КлА, но и улучшить многие его характеристики. Для обобщенного КлА выполняются следующие свойства:

- **Параллельность вычислений.** Это дискретная динамическая система с параллельными вычислениями значений ячеек памяти;
- **Свойство локальности.** В отличие от классического клеточного автомата, ячейки памяти могут быть соединены любым способом, подходящим для решения поставленной задачи;
- **Свойство неоднородности**. В общем случае, функции изменения состояния ячеек так же могут быть различны и обладать любыми требуемыми свойствами. Однако локальные функции связи могут быть и одинаковы, как в случае с классическими клеточными автоматами.

Свойства обобщенных клеточных автоматов

Структура однородного обобщенного клеточного автомата полностью определяется структурой соответствующего графа. Соответственно, и криптографические свойства обобщенного клеточного автомата как преобразования, реализующего некоторую однонаправленную функцию, и свойство быть «удобно и эффективно реализуемым» так же напрямую зависят от структуры графа и свойств локальной функции связи.

Интегральная и пространственная характеристики были перенесены на случай обобщенных клеточных автоматов.

Интегральной характеристикой лавинного эффекта в неоднородных клеточных автоматах мы назовем временную зависимость $\eta(t)$ числа изменившихся ячеек к общему их количеству:

$$\eta(t) = \frac{1}{X} \sum_{0 \leqslant x < X} \left(m_{x,t}^{(1)} \oplus m_{x,t}^{(2)} \right),$$

где Σ —обычное арифметическое сложение, а $\oplus$—сложение по модулю 2.

Интегральной характеристикой лавинного эффекта называется зависимость от номера такта доли несовпадающих ячеек для двух идентичных клеточных автоматов, работающих на паре начальных заполнений, отличающихся одним значением переменной:

$$\omega(t) = \frac{1}{n}\sum_{j=1}^{n}\left(m_j{}^{(1)}(0) \oplus m_j{}^{(2)}(t)\right).$$

Пространственной характеристикой лавинного эффекта называется зависимость отношения расстояния от вершины с номером 1 до самой дальней вершины, значение ячейки которой у двух автоматов не совпадает, к эксцентриситету вершины с номером «1»:

$$\mu(t) = \frac{1}{e(1)} \cdot \left(\max_j\left(m_j{}^{(1)}(t) \oplus m_j{}^{(2)}(t)\right) \cdot \Delta(1,j)\right),$$

где $\Delta(i,j)$ – длина минимального пути из вершины i в вершину j, а $e(i)$ – эксцентриситет вершины i. (Эксцентриситетом (eccentricity) $e(v)$ вершины v графа G называется наибольшее из расстояний от вершины v до других вершин графа. Радиус $r(G)$ есть наименьший из эксцентриситетов вершин в графе G, а диаметр $d(G)$ – наибольший из эксцентриситетов.)

ГПСП на основе обобщенных клеточных автоматов

В работе [10], наряду с ГПСП на основе классических клеточных автоматов, были рассмотрены ГПСП на основе обобщенных клеточных автоматов. Было продемонстрировано заметное преимущество ГПСП на основе обобщенных клеточных автоматов по сравнению с классическими в быстродействии и особенно в эффективности аппаратной реализации на ПЛИС (FPGA). Полученный результат объясняется лучшими характеристиками обобщенных клеточных автоматов.

Предложенный в [10] ГПСЧ представляет собой два параллельно работающих обобщенных клеточных автомата C_1 и C_2. На каждом такте работы клеточные автоматы C_1 и C_2 вырабатывают по 256 бит двоичных последовательностей, которые почленно складываются по модулю 2, а результат сложения подается на выход генератора. Поскольку последовательности, вырабатываемые клеточными автоматами, могут рассматриваться как независимые, сложение позволяет улучшить статистические свойства выходной последовательности генератора.

Для исследования статистических свойств генераторов был использован набор специализированных тестов, разработанный и реализованный Национальным институтом стандартов и технологии США.

Характеристики прототипов аппаратной реализации

Были разработаны прототипы аппаратной реализации генератора псевдослучайных последовательностей ККлА на основе классических клеточных автоматов и генератора псевдослучайных последовательностей НКлА на основе обобщенных клеточных автоматов.

Для практической реализации генераторов псевдослучайных последовательностей на основе клеточных автоматов была выбрана микросхема FPGA Cyclone II (EP2C35F672C6) корпорации Altera, относящаяся к семейству недорогих ПЛИС начального уровня.

Было проведено сравнение полученных реализаций с современными аппаратными реализациями поточных шифров (как генераторов псевдослучайных последовательностей, к которым предъявляются наиболее строгие требования как по быстродействию, так и по статистическим свойствам выходных последовательностей). Сравнение показало, что оба прототипа существенно (в несколько раз) превосходят аналоги по скорости выработки выходной последовательности (рис. 7); кроме того, реализация генератора ККлА не уступает, а НКлА значительно превосходит аналоги по эффективности, выраженной в быстродействии на единицу аппаратных ресурсов (рис. 8). Так, например, реализация алгоритма НКлА по показателю абсолютного быстродействия превосходит наиболее быстрый из представленных на конкурс eSTREAM алгоритм Trivium в 1,96 раз, а по показателю приведенного быстродействия – в 4,10 раз.

Эти показатели были достигнуты за счет использования обобщенных клеточных автоматов с локальной функцией связи от 4 переменных, поскольку для таких функций достигается оптимум по затрате логических элементов (LE) микросхемы FPGA. В этом случае для реализации одной ячейки клеточного автомата потребуется всего 1 LE.

Использование других моделей ПЛИС позволит с такой же эффективностью реализовывать обобщенные клеточные автоматы с локальной функцией связи от

бóльшего числа переменных (что ведет к улучшению их криптографических свойств). Таким образом, матрица LE является одной из наиболее удачных платформ для реализации алгоритмов на основе обобщенных клеточных автоматов.

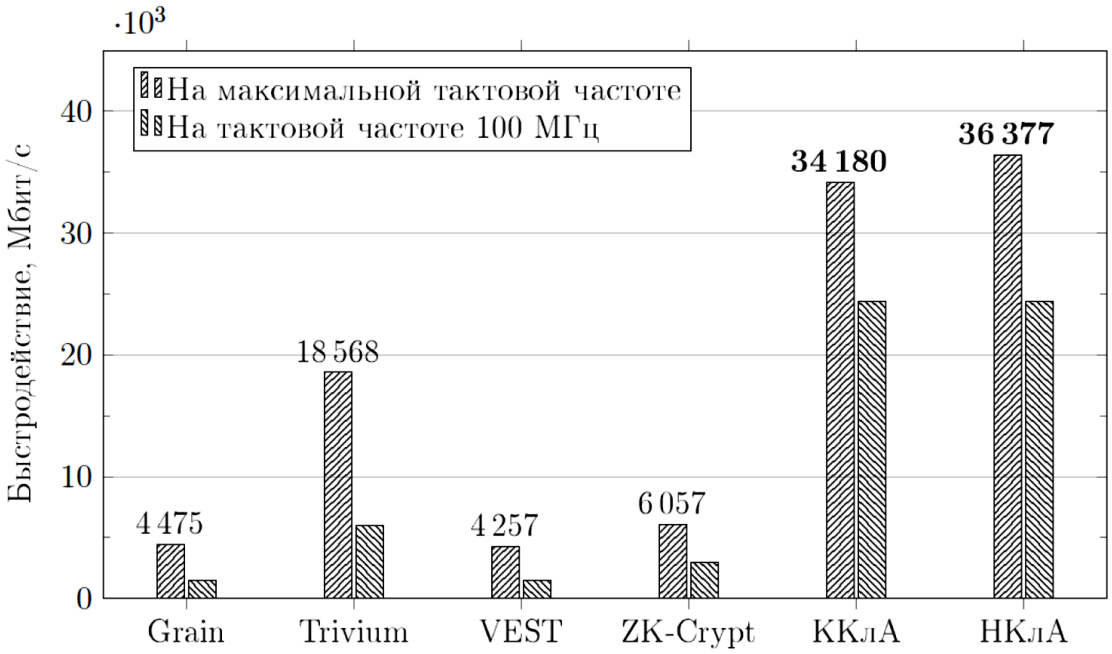

Рис. 7 – Сравнение быстродействия разработанных аппаратных реализаций и генераторов, представленных на конкурс eSTREAM

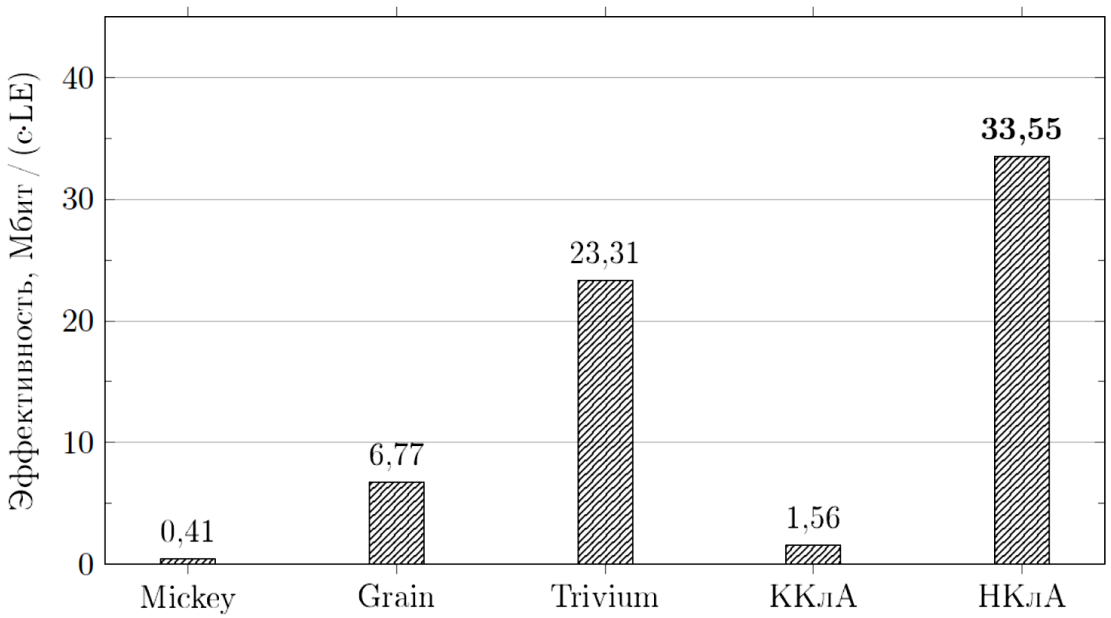

Рис. 8 – Сравнение эффективности разработанных аппаратных реализаций и генераторов, представленных на конкурс eSTREAM

Клеточные автоматы в конструкции блочных шифров

До сих пор попытки использовать клеточные автоматов в конструкции блочных шифров натыкались прежде всего на вопросы обратимости КлА. В то же время имеется значительное число работ, посвященных использованию КлА для построения S-блоков.

SPK-блок – предложенный авторами и потенциально перспективный узел в базисе элементов, которые могут использоваться для построения алгоритмов блочного шифрования.

При построении современных блочных шифров применяются композиции преобразований, реализующих преобразования рассеивания и перемешивания, что достигается с помощью использования так называемых P-блоков (P-box) и S-блоков (S-box). Смешение с ключевой информацией, как правило, осуществляется или с помощью побитового сложения информационного блока с цикловым ключом, который вырабатывается из секретного ключа с помощью специального алгоритма, называемого алгоритмом выработки ключа или (как, например, в алгоритме ГОСТ 28147-89) их сложения по модулю 2^n. Узел, осуществляющий смешение информационного блока с ключевой информацией, в дальнейшем будем называть K-блоком.

Особо отметим, что в случае блочных шифров, имеющих структуру схемы Фейстеля, не требуется обратимость преобразований, входящих в состав основной функции шифрования.

Концепция SPK-блока

В поисках наиболее экономной реализации основных преобразований, задействованных в работе блочного шифра, была предложена концепция SPK-блока, то есть узла, который осуществляет некоторые нелинейные преобразования над входным информационным блоком, при этом осуществляется смешение бит информационного блока с ключевым материалом с одновременным рассеиванием и перемешиванием.

К одной из первых (во всяком случае, из опубликованных в открытой литературе) попыток создания SPK-узла можно отнести конструкцию Лая и Месси, которая была применена в алгоритме блочного шифрования IDEA. Авторами IDEA был предложен MA-узел (Multiplication-Addition), осуществляющий рассеивание, перемешивание и смешение с ключевым материалом входного информационного

вектора и представляющий основную функцию шифрования, используемую в предложенном алгоритме.

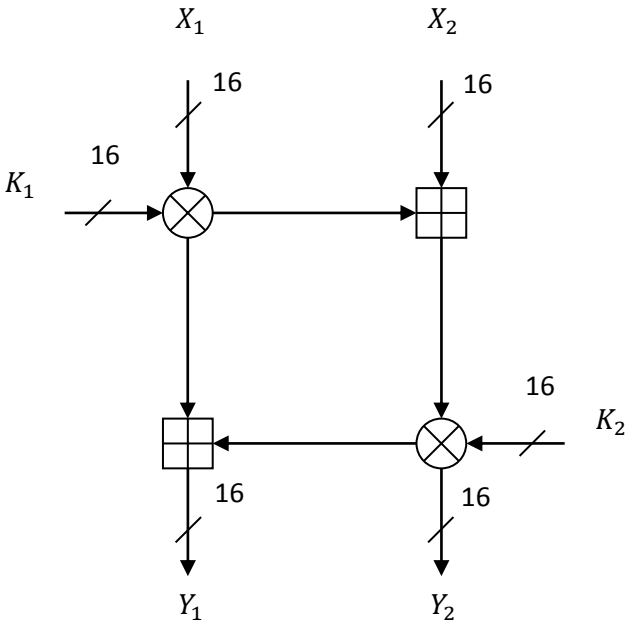

Рис. 9 – Пример SPK-узла в алгоритме IDEA

MA-узел изображен на рис. 9. Здесь X_k – k-я часть входного информационного вектора, Y_k – k-я часть выходного информационного вектора, K_m – m-я часть циклового ключа, $\boxplus$ – операция сложения по модулю 2^{16}, $\otimes$ – операция умножения по модулю $2^{16}+1$. При этом конструкция данного алгоритма шифрования предполагает обратимость всех используемых операций (очевидно, это обстоятельство в основном касается операции умножения по модулю $2^{16}+1$). Хотя для указанных параметров обратимость операции умножения выполняется, ясно, что данный узел не годится для произвольного набора параметров, поскольку далеко не всегда число вида 2^k+1 является простым (простота модуля является необходимым и достаточным условием обратимости модульного умножения).

Будем называть узлы данного типа SPK-узлами, так как они выполняют ту же функцию, что и композиции классических S-блоков, P-блоков с операцией сложения с цикловым ключом, которую мы договорились называть K-блоком.

SPK-блоки на базе клеточных автоматов

Отличным кандидатом на применение в качестве SPK-блока являются обобщенные клеточные автоматы. Данный подход был впервые реализован в [13] и развит в [14].

Другими словами, результатом преобразования SPK-блока на базе обобщенного клеточного автомата будет результат эволюции этого автомата, при которой будет осуществлено и смешение с ключевым материалом, и перемешивание и рассеивание входной информации. При этом, для обеспечения хорошего рассеивания, минимальное число тактов работы обобщенного автомата должно быть не меньше, чем d – диаметр графа этого автомата, а число переменных, от которых должна существенно зависеть функция локальной связи, должно быть равным σ – степени захода обобщенного клеточного автомата.

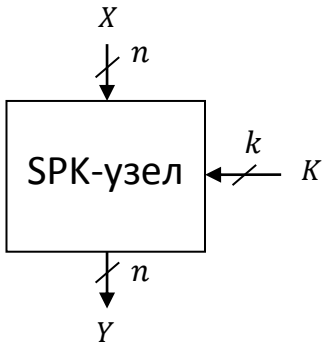

Рис. 10 – Схема SPK-узла

В результате на основании целого ряда проведенных исследований можно утверждать, что реализации шифров, использующих SPK-блоки на основе КлА, являются более эффективными, чем реализации шифров, использующих классические S-, P-, K-блоки, вне зависимости от архитектуры построения шифра: легковесной или производительной.

Легковесная криптография. Проведенные исследования показали, что предложенная концепция SPK-блока хорошо подходит для решения этих задач. Однако, для того, чтобы предлагать SPK-блоки как актуальную замену классическим S-, P-, K-блокам требуется проведение глубокого криптографического анализ предложенной конструкции, что становится важнейшей задачей ближайшего будущего.