Ассоциация РусКрипто

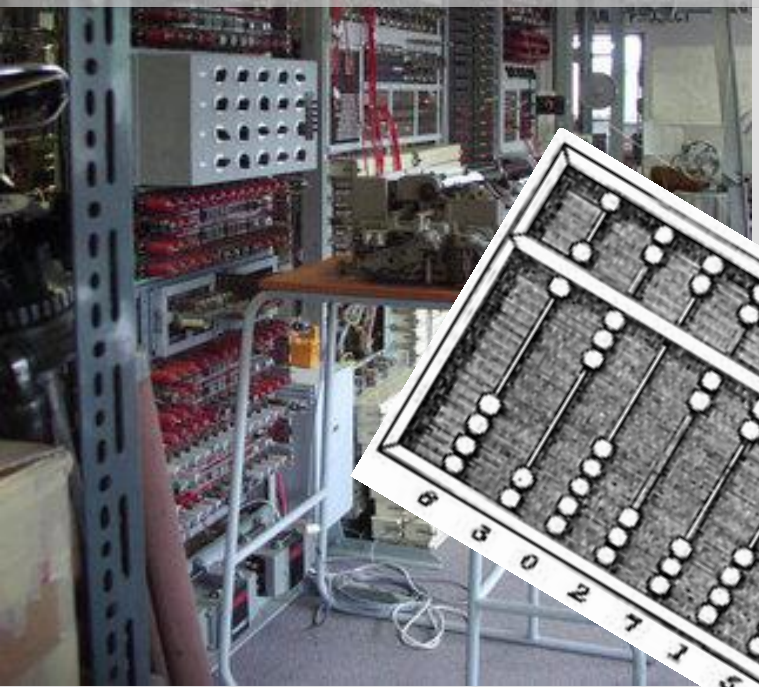
РусКрипто 2016

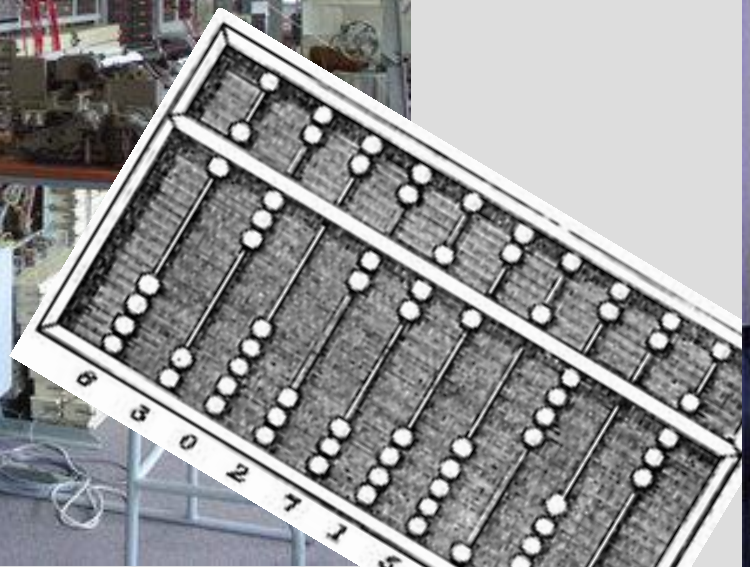
Клеточные автоматы в криптографии

Ассоциация РусКрипто

Клеточные автоматы

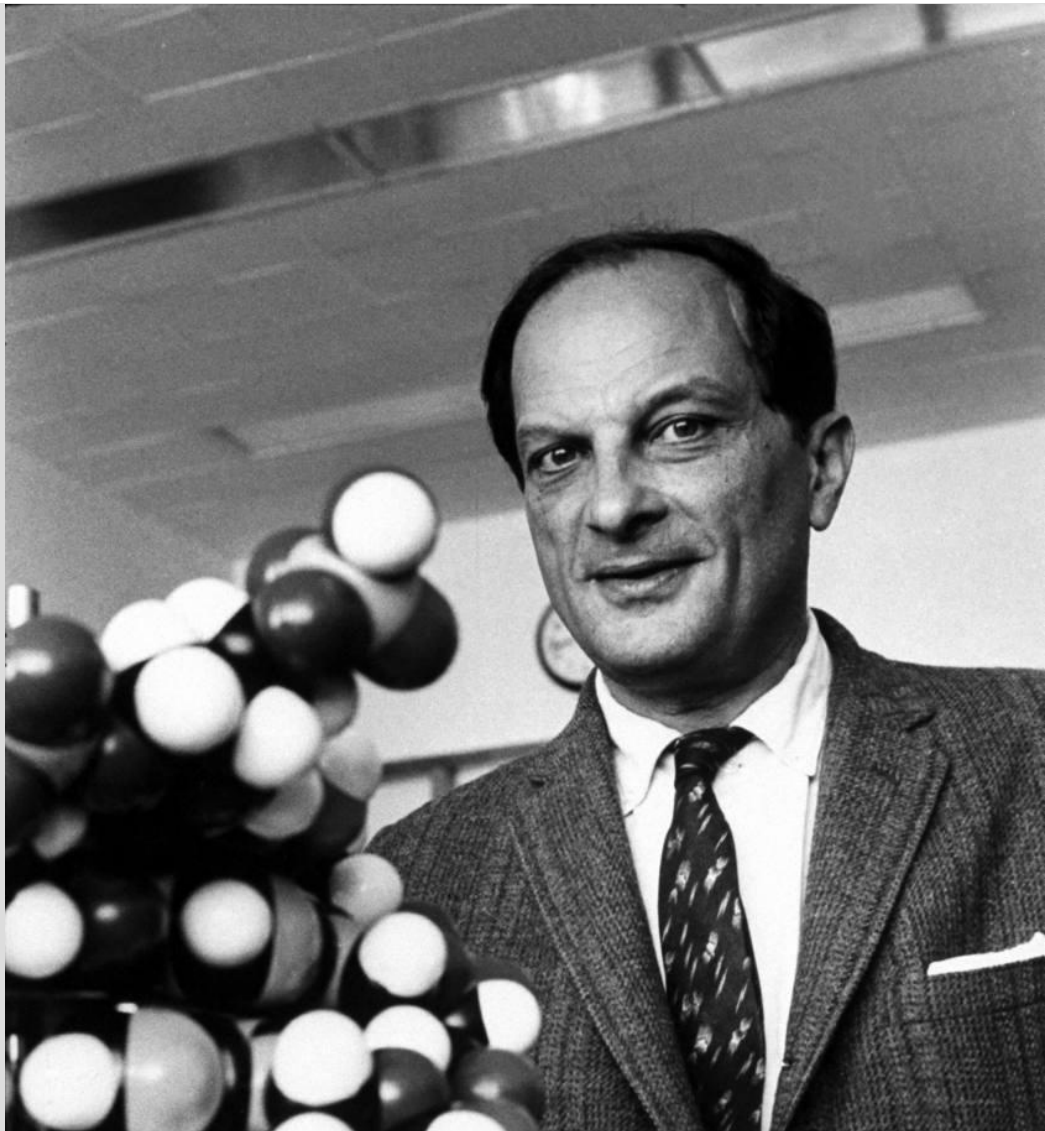
Клеточный автомат – одна из старейших вычислительных моделей...





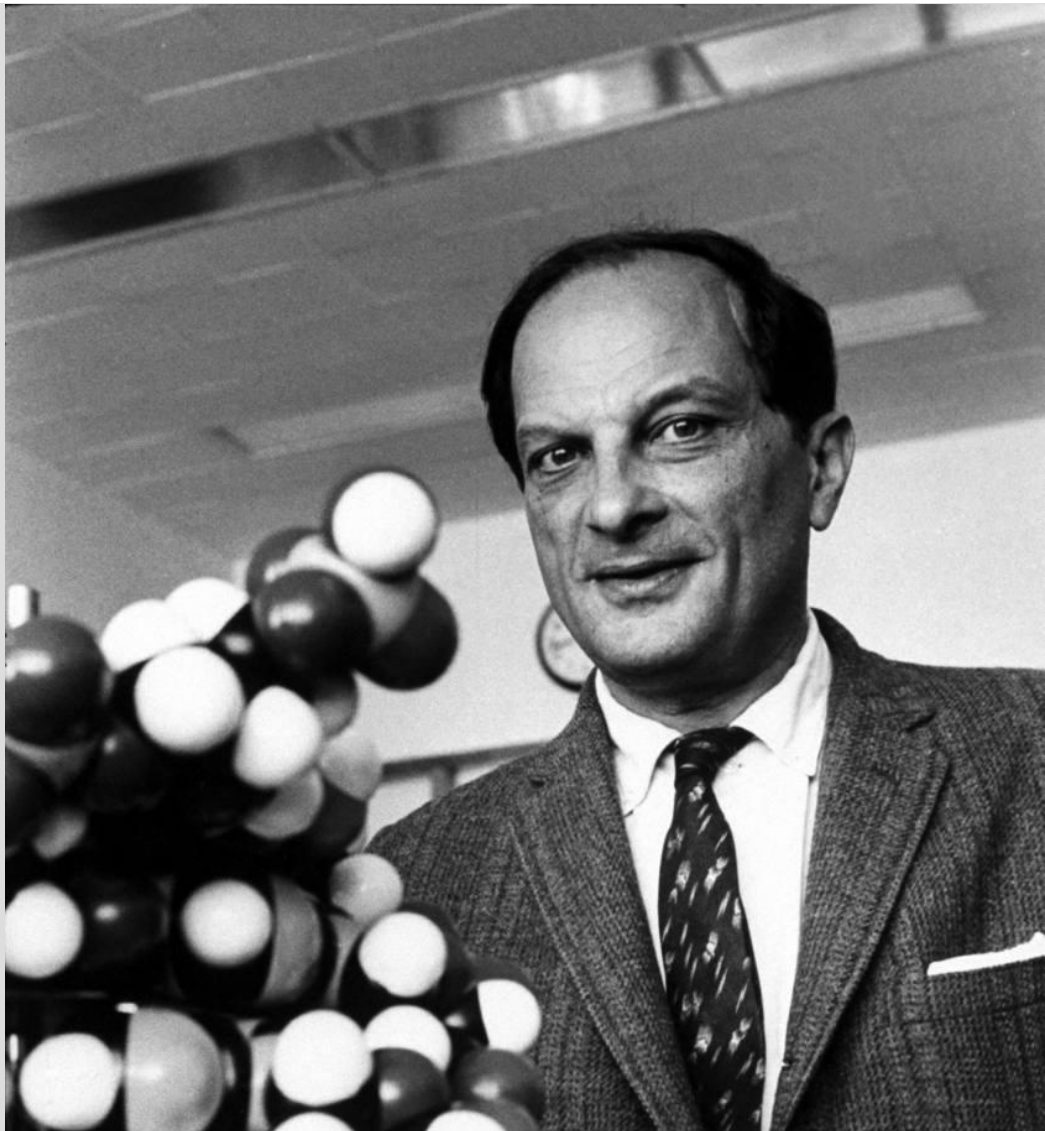
Ассоциация РусКрипто

Клеточные автоматы



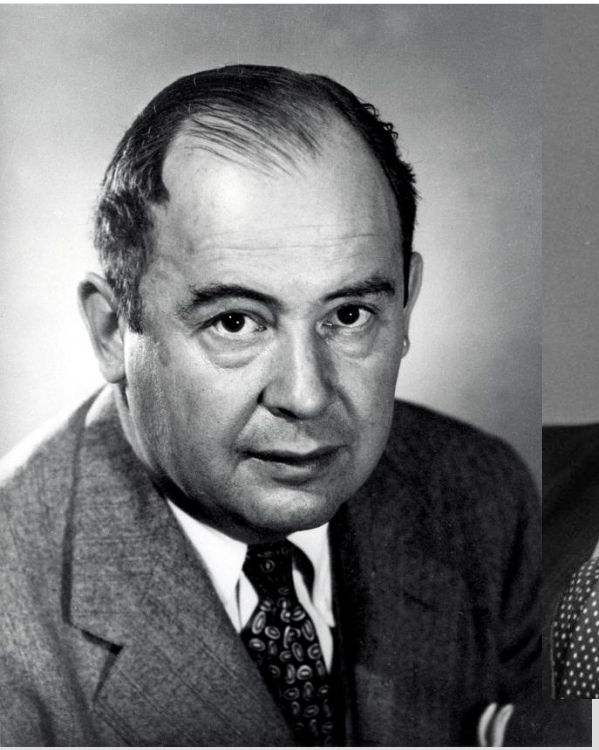
Ассоциация РусКрипто

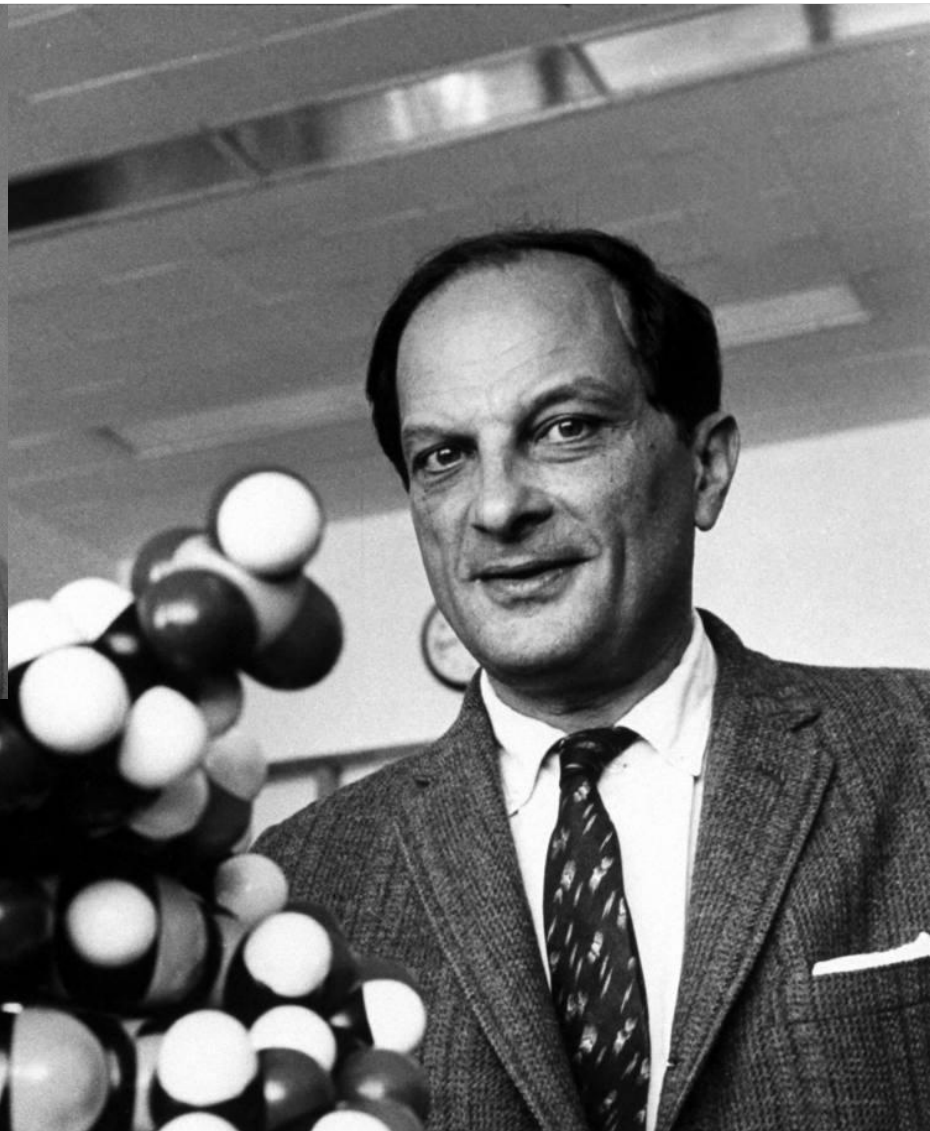
Клеточные автоматы



Ассоциация РусКрипто

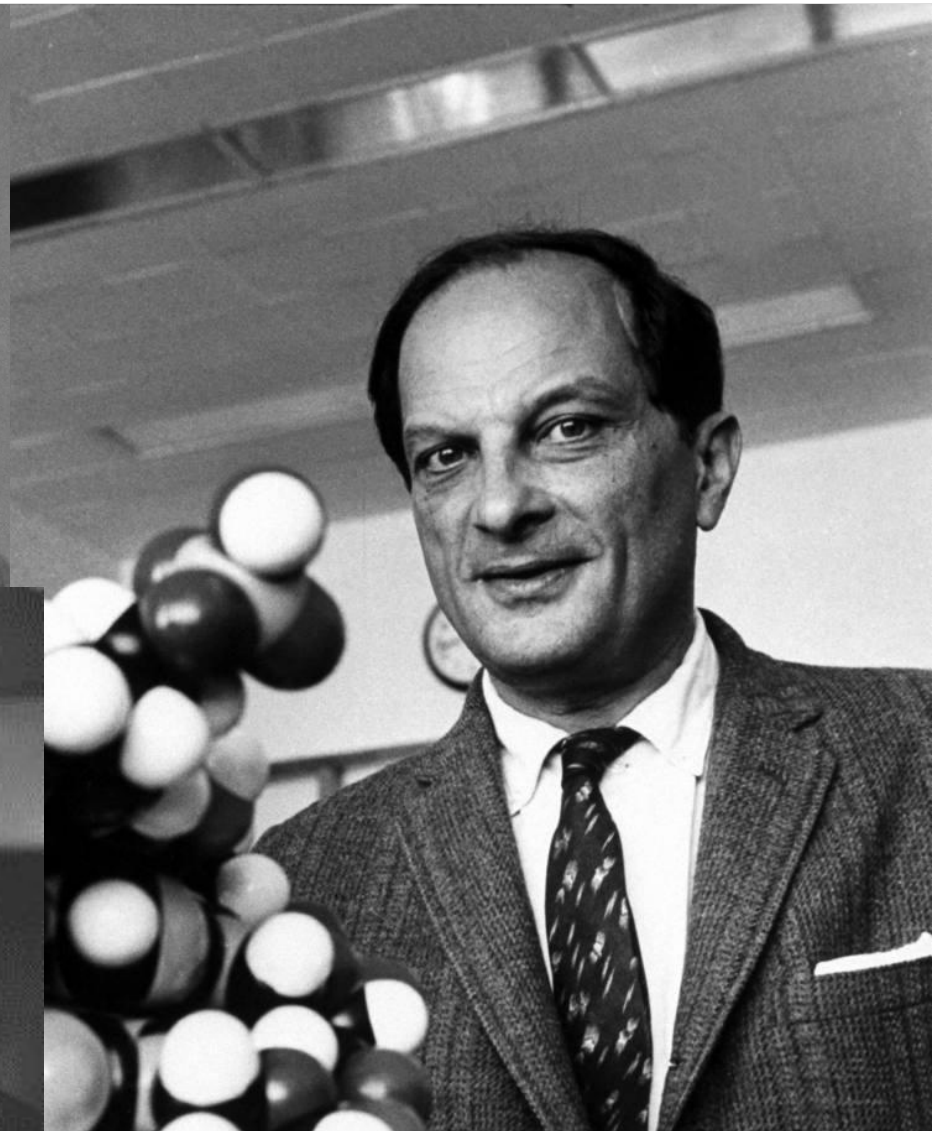
Клеточные автоматы





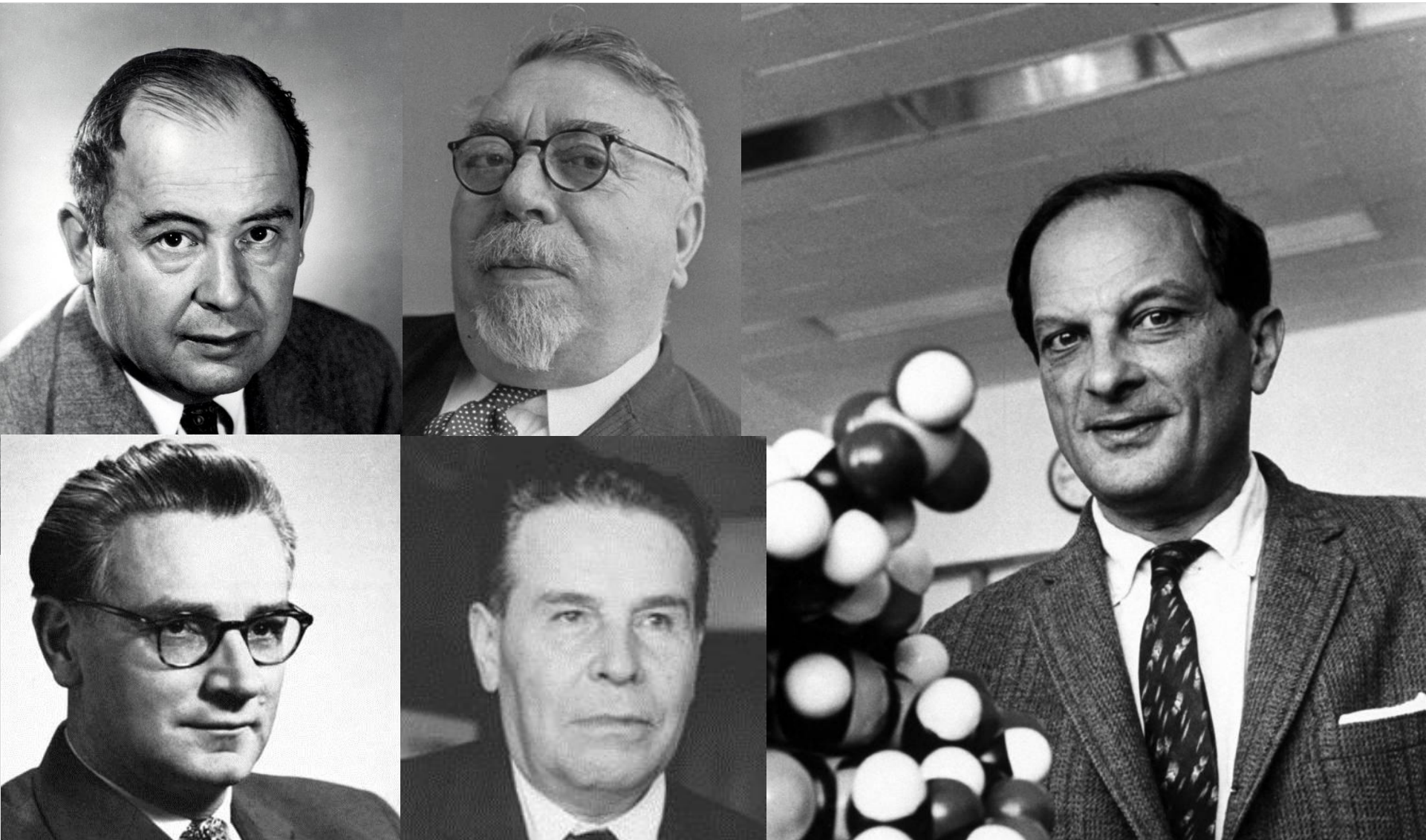
Ассоциация РусКрипто

Клеточные автоматы



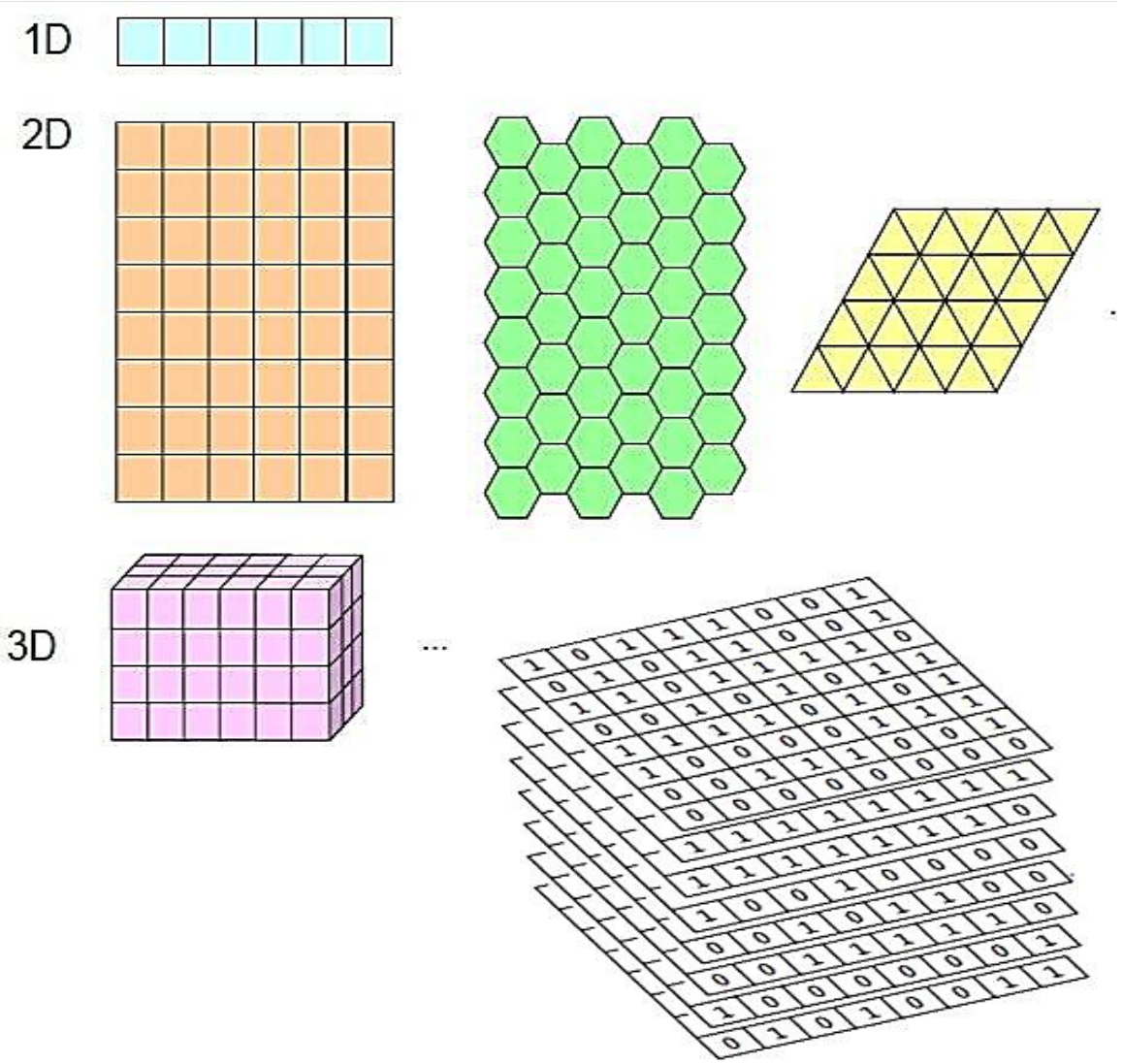
Ассоциация РусКрипто

Клеточные автоматы



Ассоциация РусКрипто

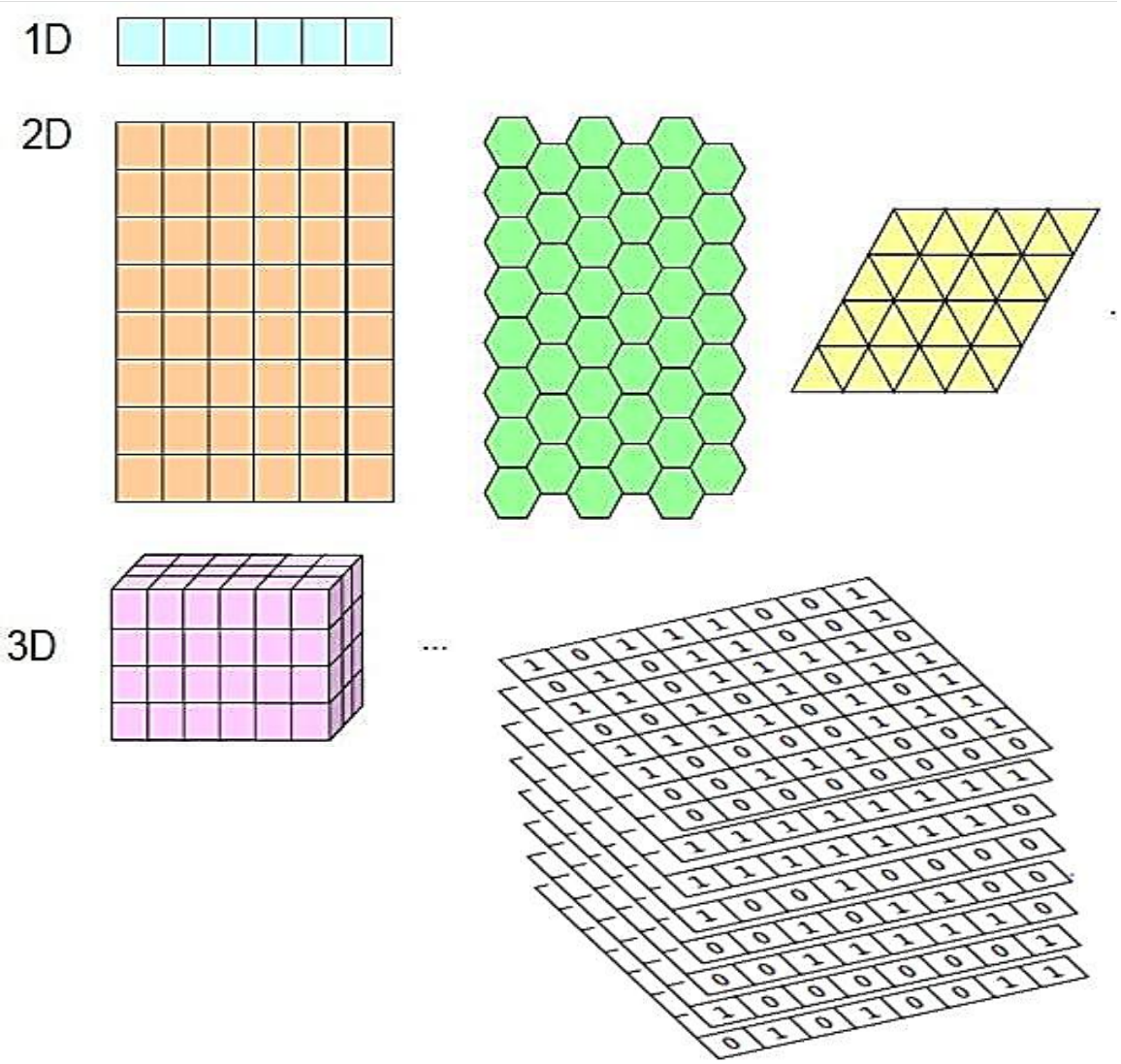
Классические клеточные автоматы



Классический клеточный автомат представляет собой упорядоченный набор ячеек памяти, образующих некоторую регулярную *n*-мерную решетку.

Ассоциация РусКрипто

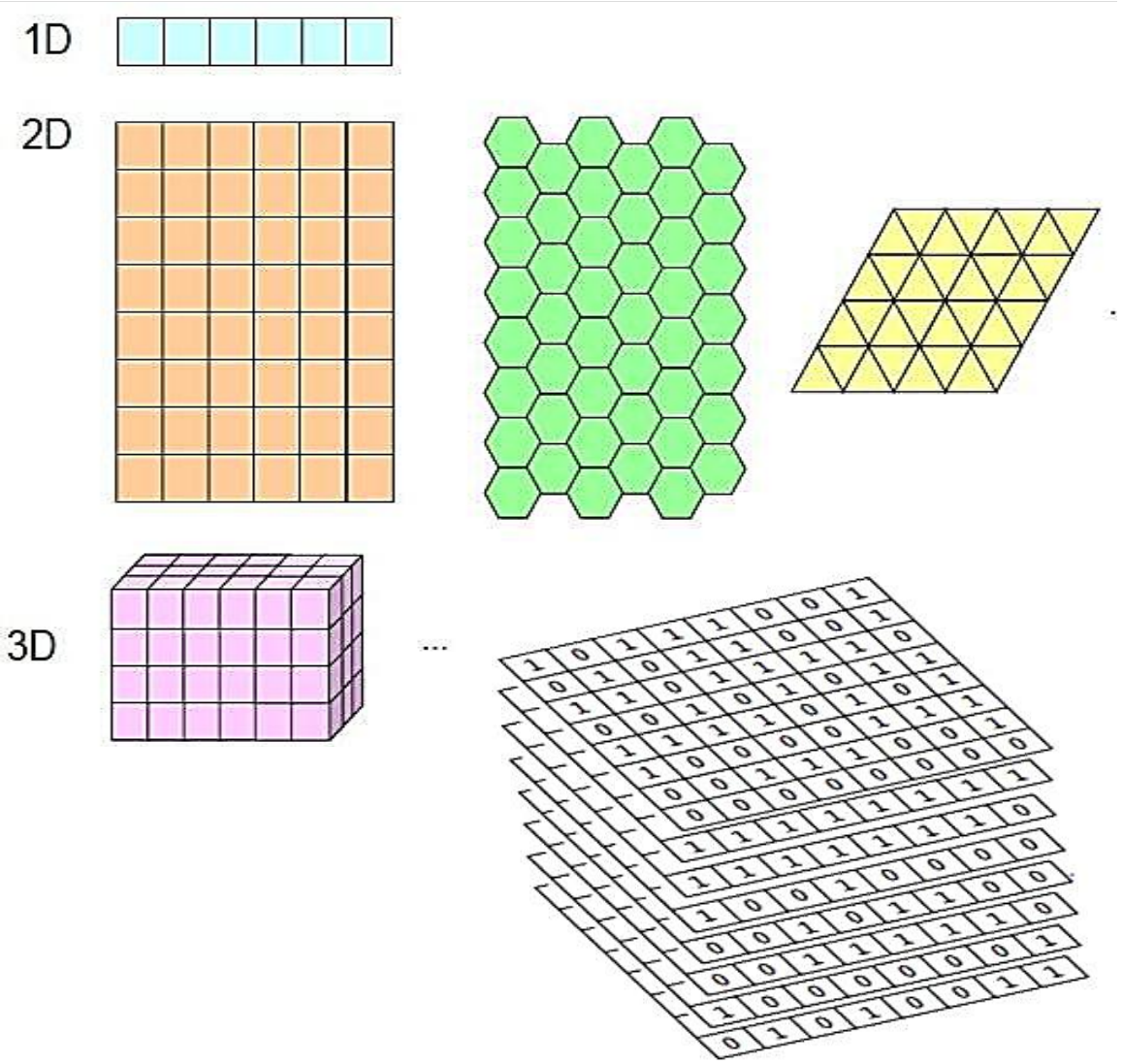
Классические клеточные автоматы



Каждая ячейка памяти клеточного автомата может хранить одно значение из некоторого конечного множества (как правило – 1 бит).

Ассоциация РусКрипто

Классические клеточные автоматы



Время для клеточного автомата изменяется дискретными шагами (тактами).

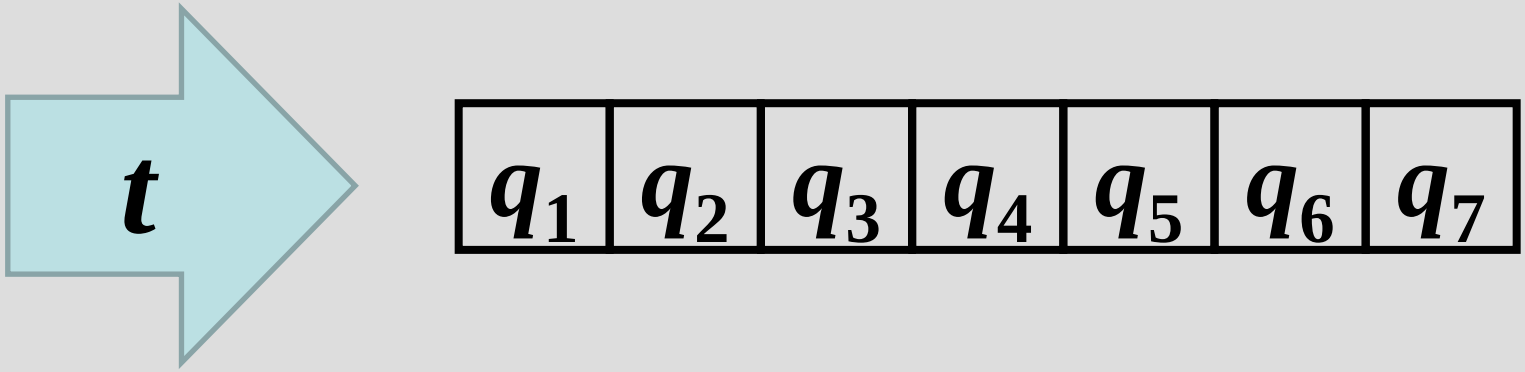
Ассоциация РусКрипто

Одномерный клеточный автомат

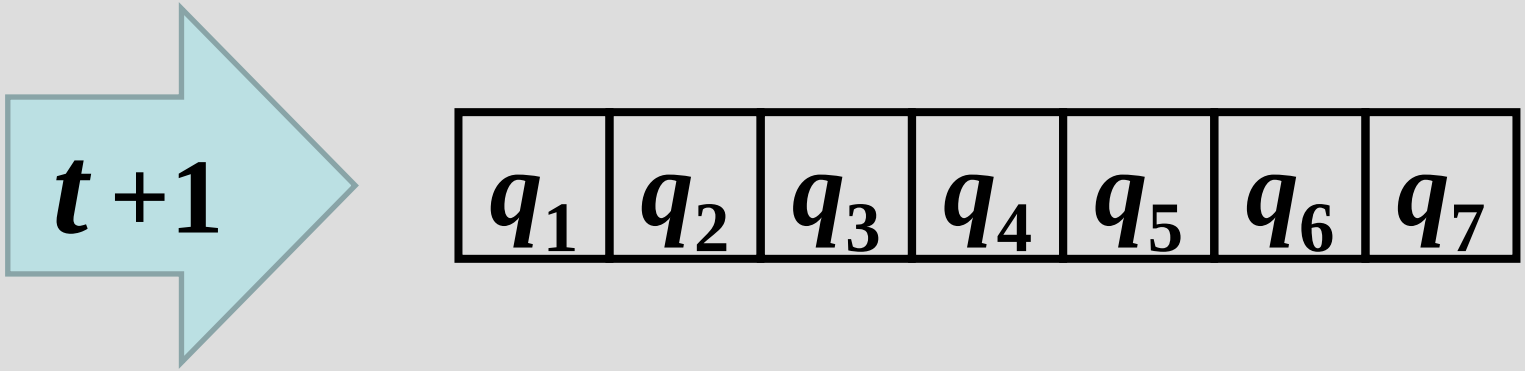
Классический клеточный автомат представляет собой упорядоченный набор ячеек памяти, образующих некоторую регулярную n-мерную решетку. Каждая ячейка памяти клеточного автомата может хранить одно значение из некоторого конечного множества (как правило – 1 бит).

Ассоциация РусКрипто

Одномерный клеточный автомат

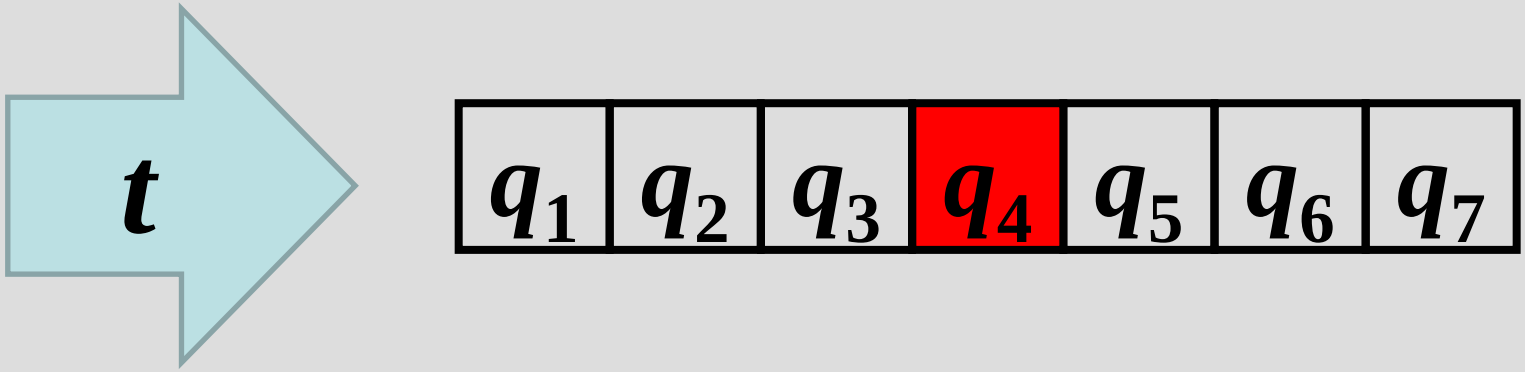


Время для клеточного автомата изменяется дискретными шагами (тактами).

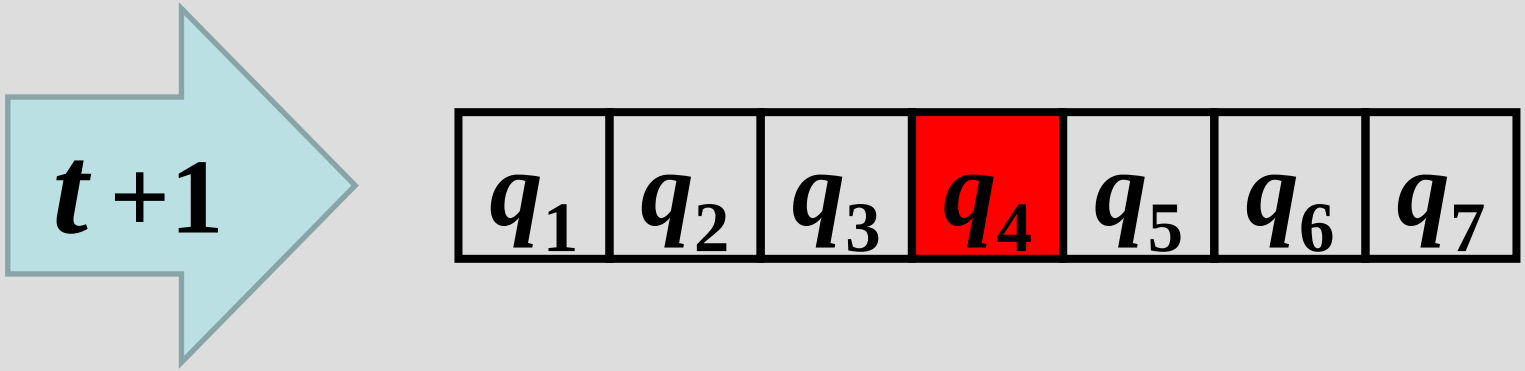


Ассоциация РусКрипто

Одномерный клеточный автомат

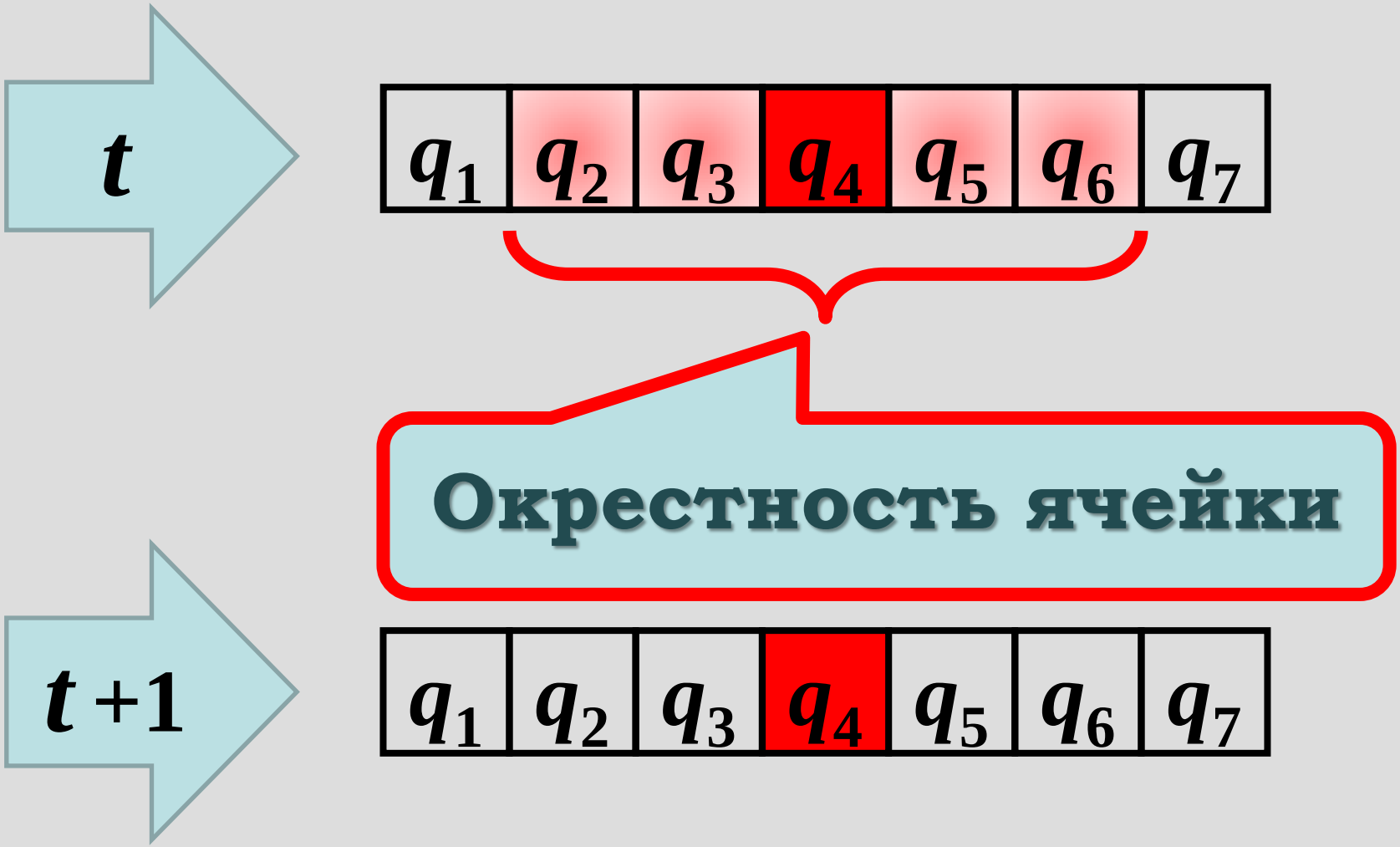


Время для клеточного автомата изменяется дискретными шагами (тактами).



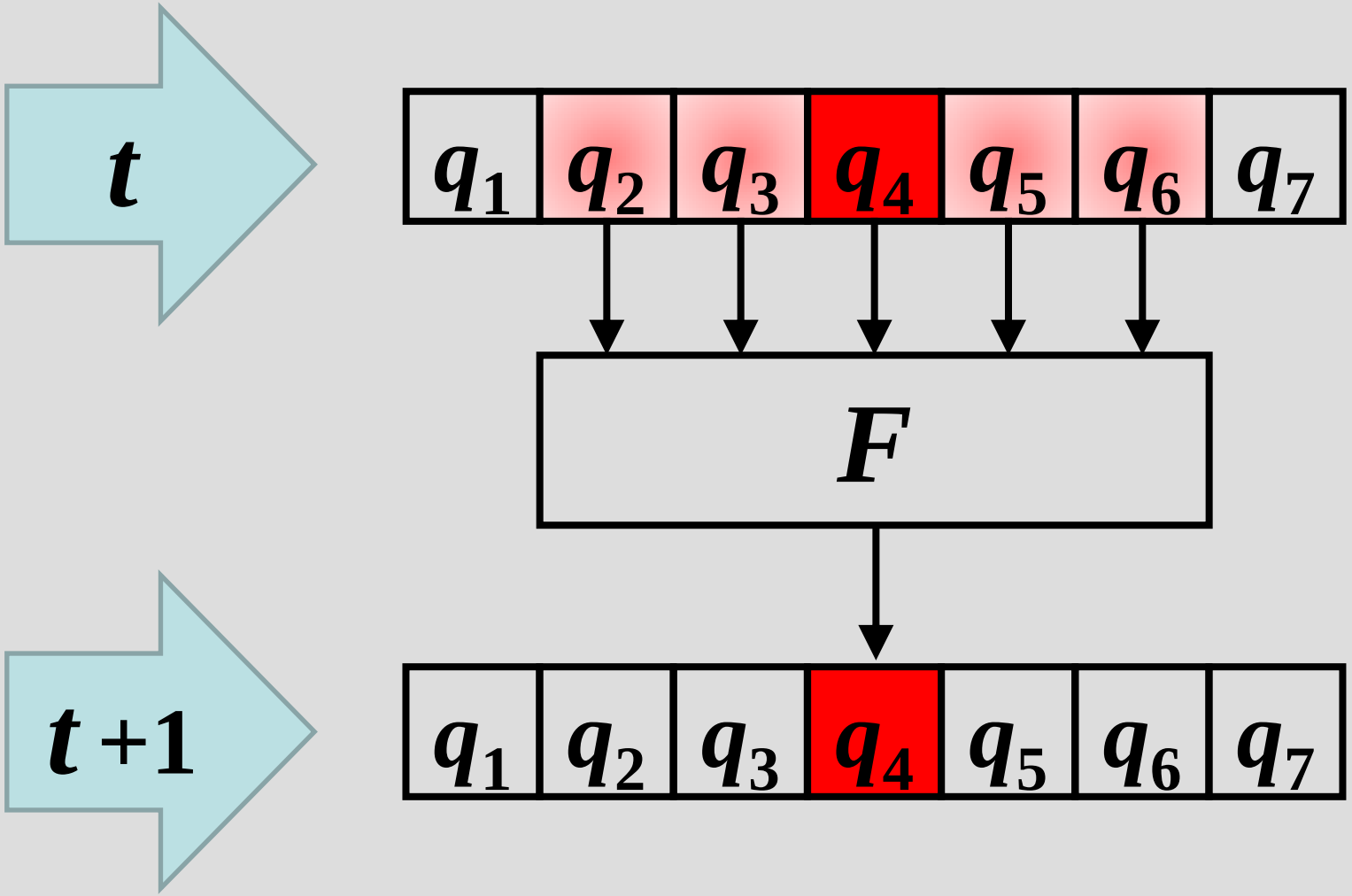
Ассоциация РусКрипто

Одномерный клеточный автомат



Ассоциация РусКрипто

Одномерный клеточный автомат



Ассоциация РусКрипто

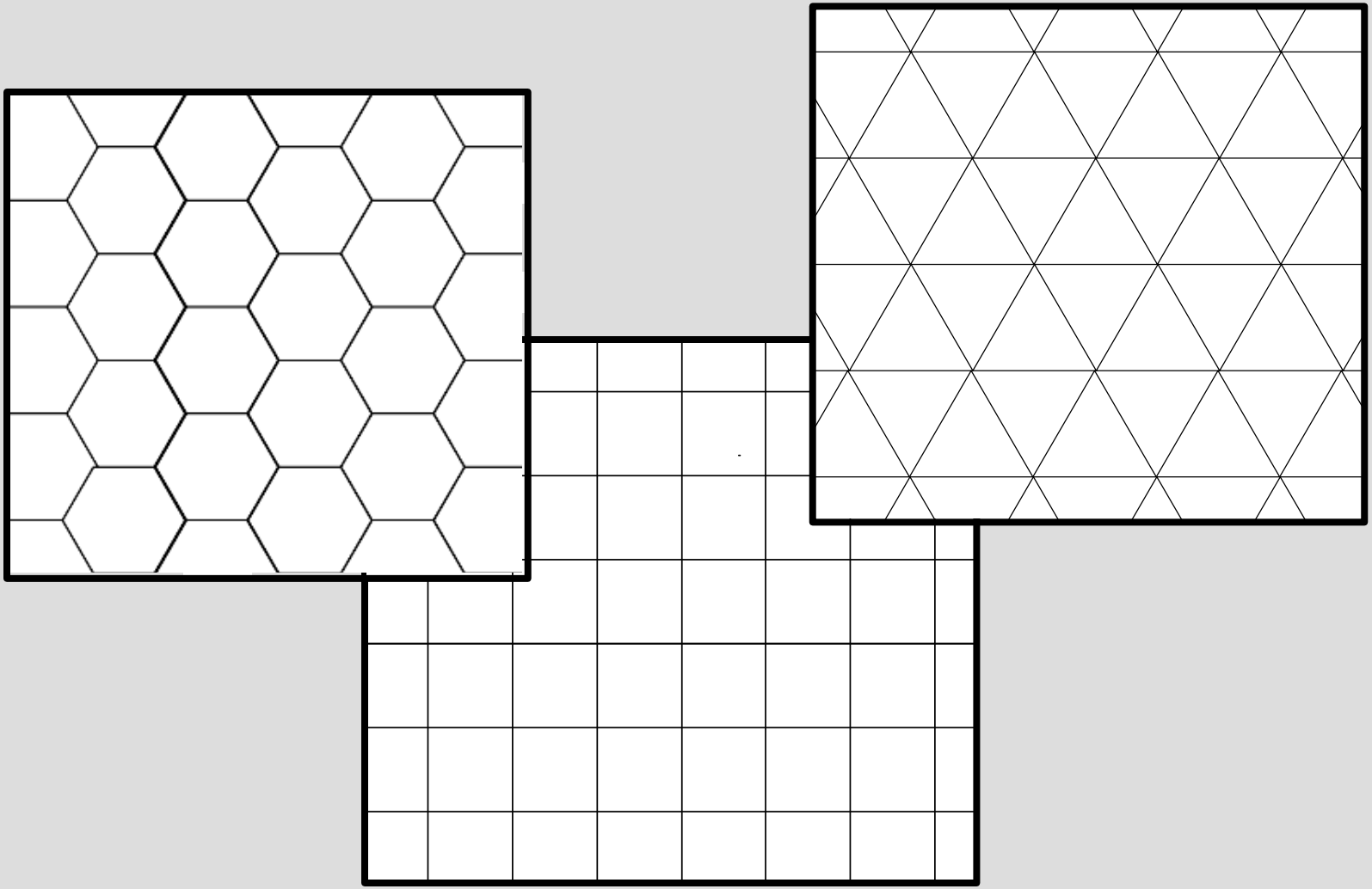
Одномерный клеточный автомат

$$q_i(t+1) =$$

$$=F(q_{i-k}(t),\ldots, q_{i-1}(t), q_i(t), q_{i+1}(t),\ldots, q_{i+k}(t))$$

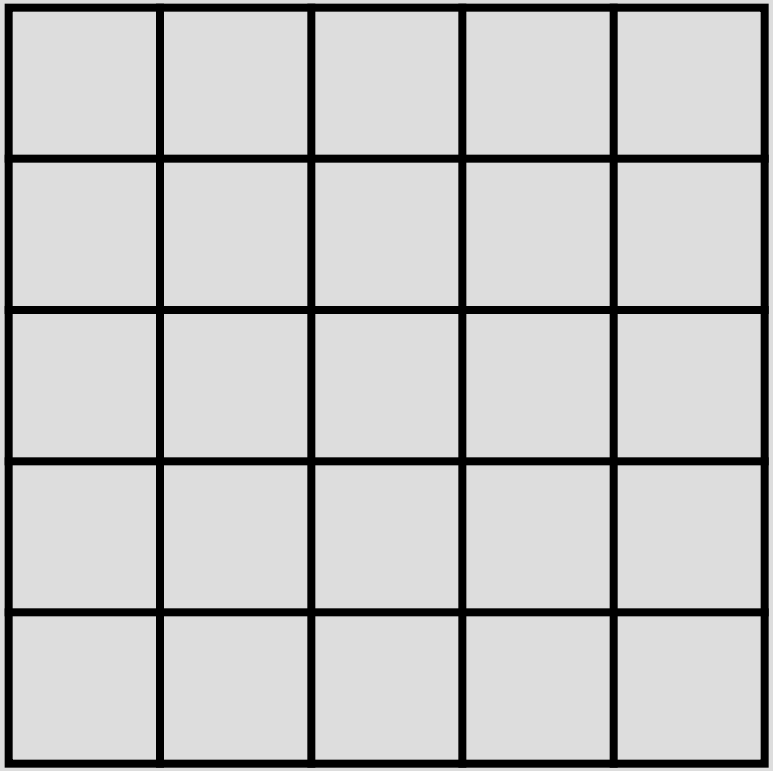
Ассоциация РусКрипто

Двумерный клеточный автомат



Ассоциация РусКрипто

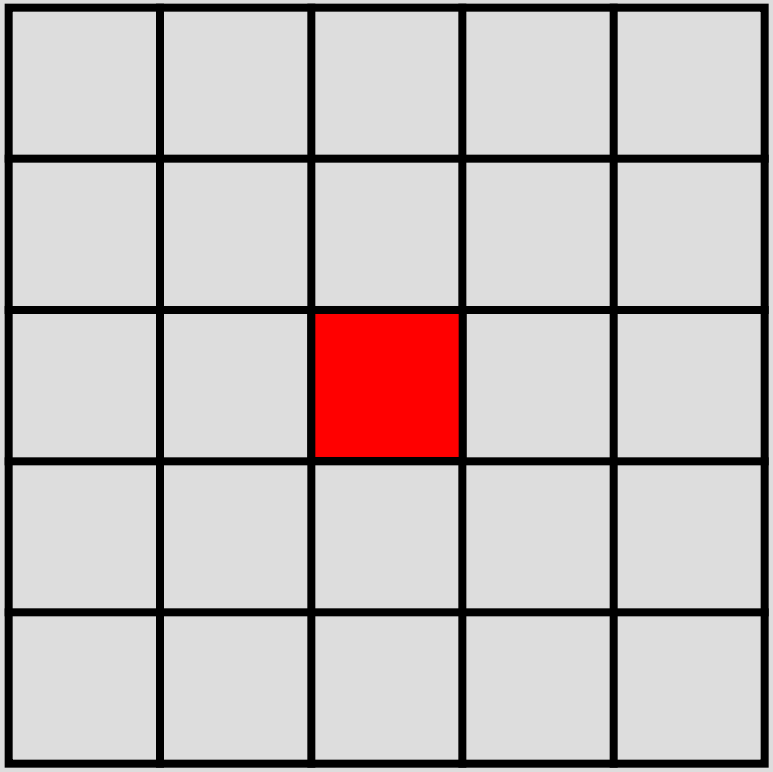
Двумерный клеточный автомат



Ассоциация РусКрипто

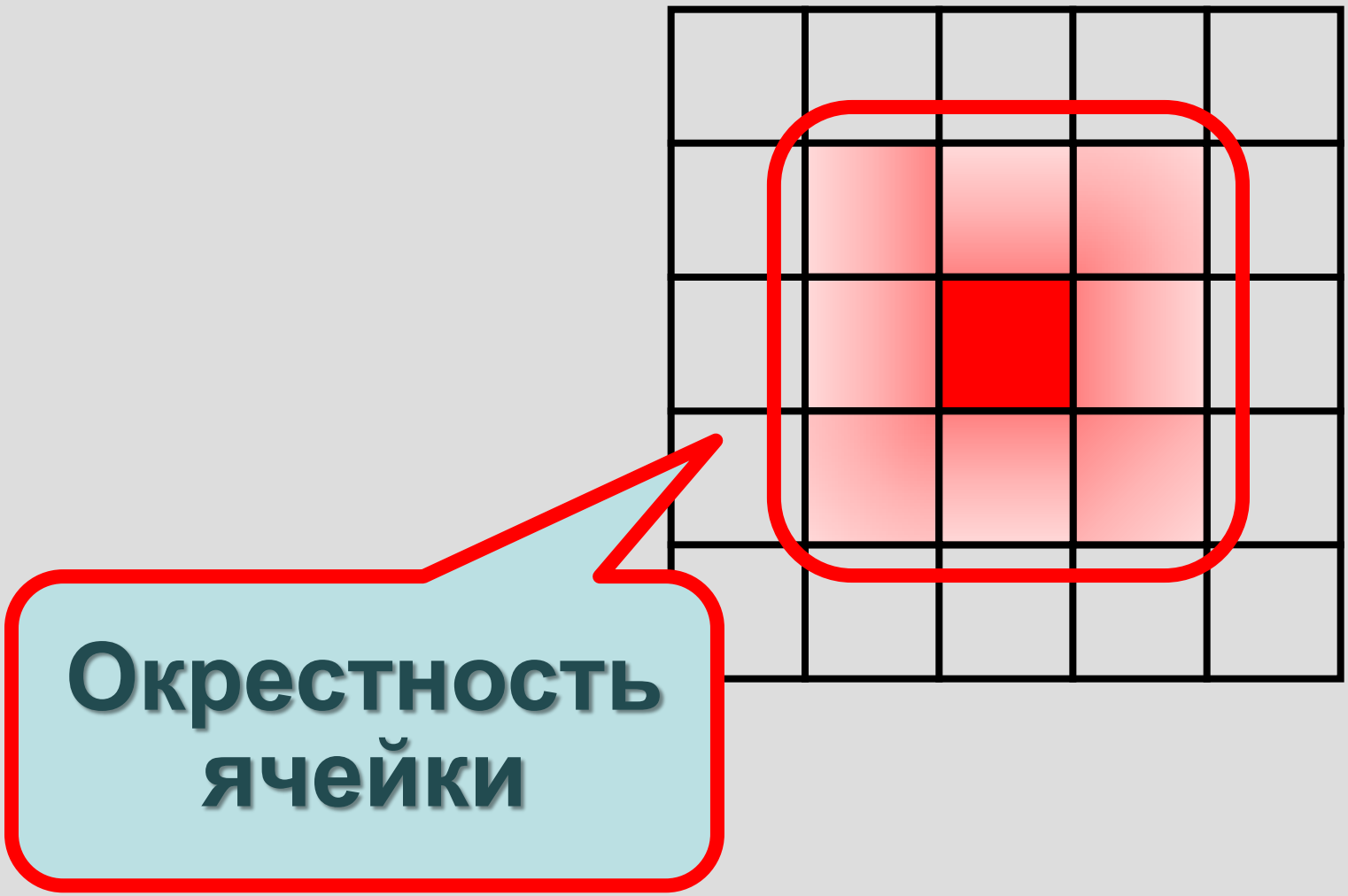
Двумерный клеточный автомат

$t \Rightarrow t+1$



Ассоциация РусКрипто

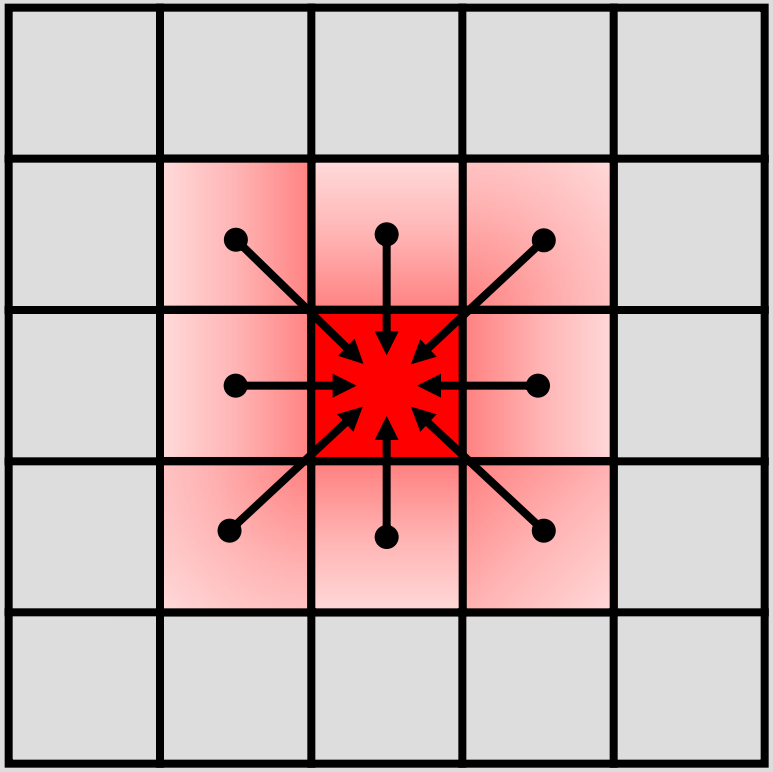
Двумерный клеточный автомат



Ассоциация РусКрипто

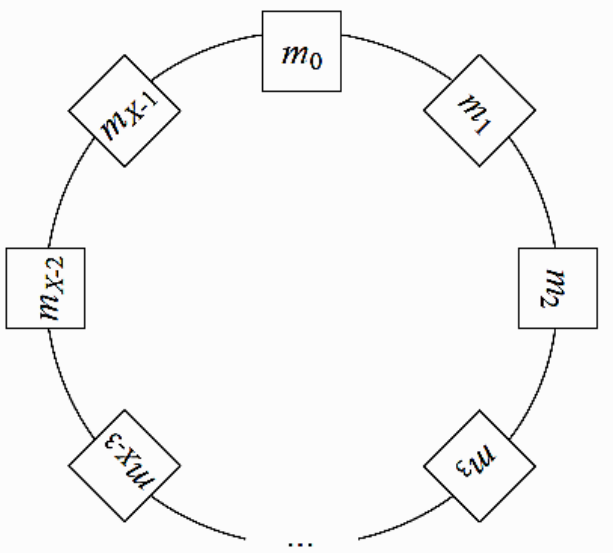
Двумерный клеточный автомат

$$f: \Omega^{|\Psi_r|} \to \Omega$$

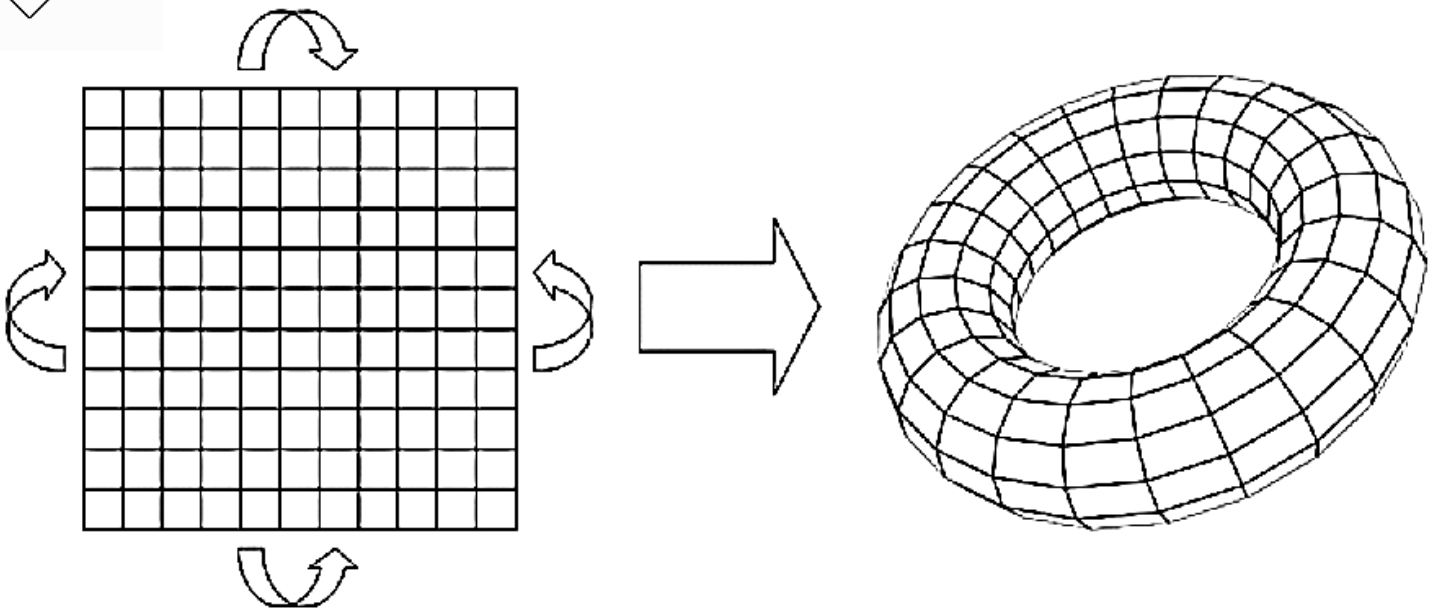


Ассоциация РусКрипто

Классические клеточные автоматы



Нулевые и периодические границы



Ассоциация РусКрипто

Классические клеточные автоматы

- **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.

Ассоциация РусКрипто

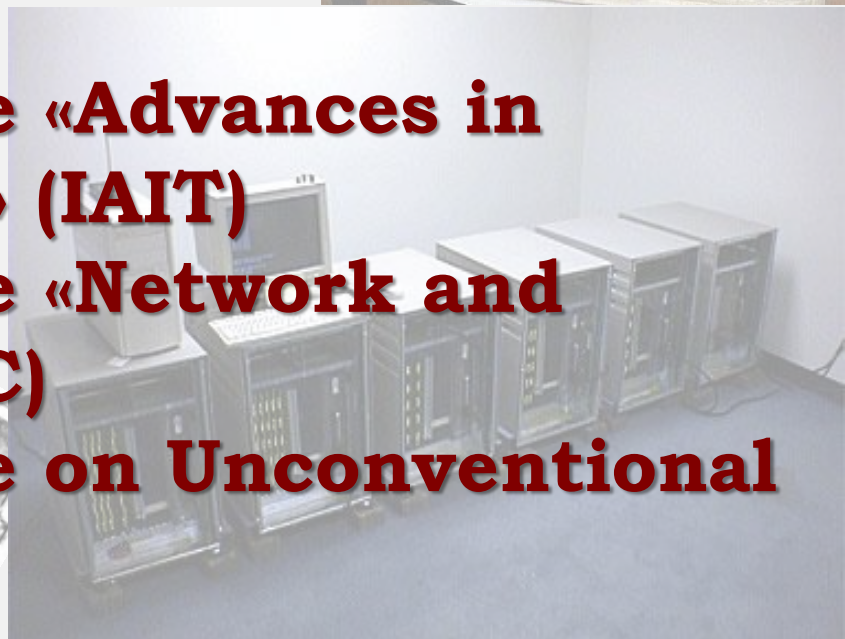
Классические клеточные автоматы

- имитационное моделирование физических процессов и систем,
- построение биологических моделей, включая модели самовоспроизводства,
- обработка изображений,
- модели структурной лингвистики,
- архитектура вычислительных систем,
- теория помехоустойчивого кодирования,
- теория хаоса,
- теория фракталов,
- и, наконец, приложения к криптографии

Ассоциация РусКрипто

Клеточные автоматы

- International Conference on Cellular Automata for Research and Industry (ACRI) – с 1994 г.
- International Workshop on Cellular Automata and Discrete Complex Systems (AUTOMATA) – с 1995 г.
- International Conference «Advances in Information Technology» (IAIT)
- International Conference «Network and Parallel Computing» (NPC)
- International Conference on Unconventional Computation (UC)



Ассоциация РусКрипто

Клеточные автоматы и криптография

Ассоциация РусКрипто

Клеточные автоматы в криптографии (2013)

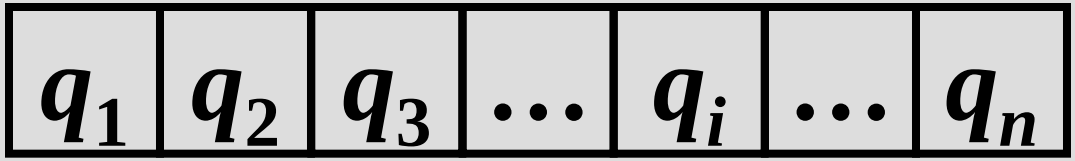
- An Application of Non-Uniform Cellular Automata for Efficient Cryptography (A. Kumaravel, O.N. Meetei) Indian Journal of Science and Technology, Vol. 6 (5S) (2013), pp. 4560-4566
- A Note on the Reversibility Of Elementary Cellular Automaton 150 With Periodic Boundary Conditions (A.M. del Rey) Romanian Journal of Information Science and Technology, Vol. 16, No 4 (2013), pp. 365–372
- Applications of natural computing in cryptology: NLFSR based on hybrid cellular automata with 5-cell neighborhood (R. Dogaru, I. Dogaru) Proceedings of the Romanian Academy, Ser. A, Vol. 14, Spec. Iss. (2013), pp. 365–372
- Amorphous computing: examples, mathematics and theory (W. R. Stark) Nat. Comput., 12 (2013), pp. 377–392
- Cryptography Using Cellular Automata (H. Bhasin, R. Kumar, N. Kathuria) International Journal of Computer Science and Information Technologies, Vol. 4 (2) (2013), pp. 355-357
- Improving Resistance against Attack of L2DCASKE Encryption Algorithm by using RCA Rule 30 based S-Box (K.J. Jegadish Kumar et al.), International Journal of Computer Applications, Vol. 70, No.16 (2013)
- Analysis of Hash Functions and Cellular Automata Based Schemes (J.-C. Jeon), International Journal of Security and Its Applications Vol. 7, No. 3 (2013), pp. 303-316
- Cellular Automata in Cryptographic Random Generators (J. Spencer) – M.S. thesis, DePaul University, 2013
- Image steganography based on cellular automata (B. Jana et al.), International Journal of Pure and Applied Mathematics Vol. 83, No. 5 (2013), pp. 701-715

Клеточные автоматы в криптографии (2014)

- Cellular Automata and Cryptography (T. Santos) – M.S. thesis, Universidade do Porto, 2014
- FPGA Implementation of Cellular Automata Based Stream Cipher: YUGAM-128 (K.J.J. Kumar, et al.) International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 3, Spec. Iss. 3 (2014), pp. 313-317
- A Fast Cryptosystem Using Reversible Cellular Automata (S. Bouchkaren, S. Lazaar) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 5 (2014), pp. 207-210
- Cryptographic Algorithm Using Cellular Automata Rules (A. Singh, S.S. Mishra), International Journal of Computer Application, Iss. 4, Vol. 3 (2014), pp. 57-64

Ассоциация РусКрипто

Одномерный клеточный автомат



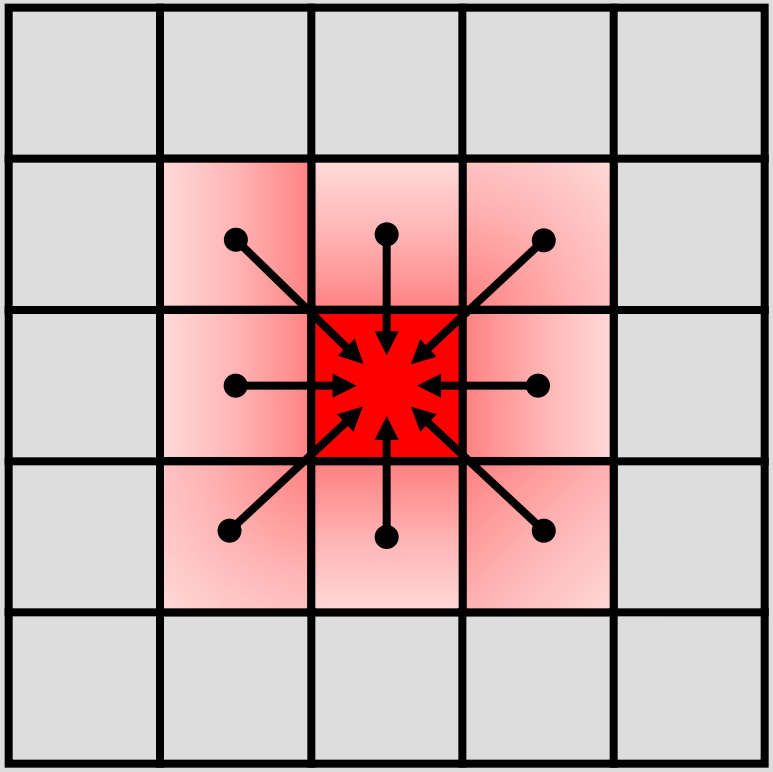
- **Wolfram S. Cryptography with Cellular Automata. Advances in Cryptology: Crypto '85 Proceedings, Lecture Notes in Computer Science, v. 218 (Springer-Verlag, 1986), pp. 429-432**

$$q_i(t+1) = $$

$$= q_{i-1}(t) \oplus q_i(t) \oplus q_{i+1}(t) \oplus q_i(t)\, q_{i+1}(t)$$

Ассоциация РусКрипто

Двумерный клеточный автомат



Двумерный клеточный автомат

- **Сухинин, Б.М. Разработка и исследование высокоскоростных генераторов псевдослучайных равномерно распределенных двоичных последовательностей на основе клеточных автоматов. // Дисс. к.т.н. – Москва, 2011. – 224 с.**
- **Сухинин Б.М. Высокоскоростные генераторы псевдослучайных последовательностей на основе клеточных автоматов // Прикладная дискретная математика. 2010. №2. С. 34 – 41.**
- **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.**

Ассоциация РусКрипто

Двумерный клеточный автомат

- исследовано влияние веса локальной функции связи на распределение значений ячеек памяти клеточных автоматов;
- сформулирован, доказан и подтвержден эмпирически критерий сохранения равномерности распределения.

Ассоциация РусКрипто

Двумерный клеточный автомат

- для характеристики криптографических свойств 2-мерных клеточного автомата Б. Сухининым было применено понятие лавинного эффекта, введенное в 1973 году Х. Фейстелем для блочных шифров.
- для количественного описания лавинного эффекта в классических клеточных автоматах были введены понятия *интегральной* и *пространственной* характеристик лавинного эффекта.

Двумерный клеточный автомат

Интегральная характеристика **лавинного эффекта определяет временну́ю зависимость распространения лавинного эффекта, и равна отношению числа изменившихся к данному моменту времени ячеек к общему числу ячеек обобщенного клеточного автомата:**

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

Ассоциация РусКрипто

Двумерный клеточный автомат

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

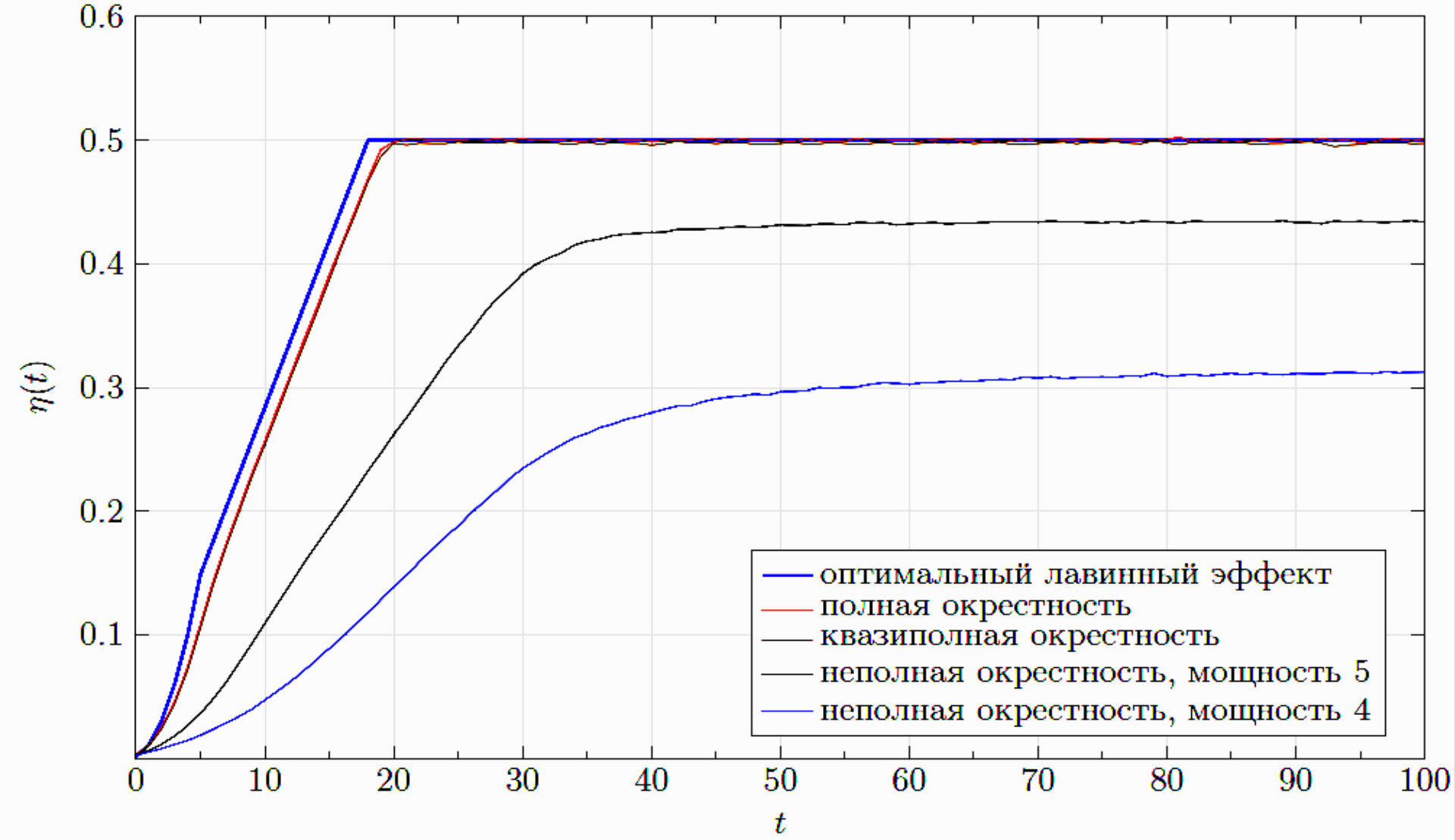
Ассоциация РусКрипто

Двумерный клеточный автомат

- 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.

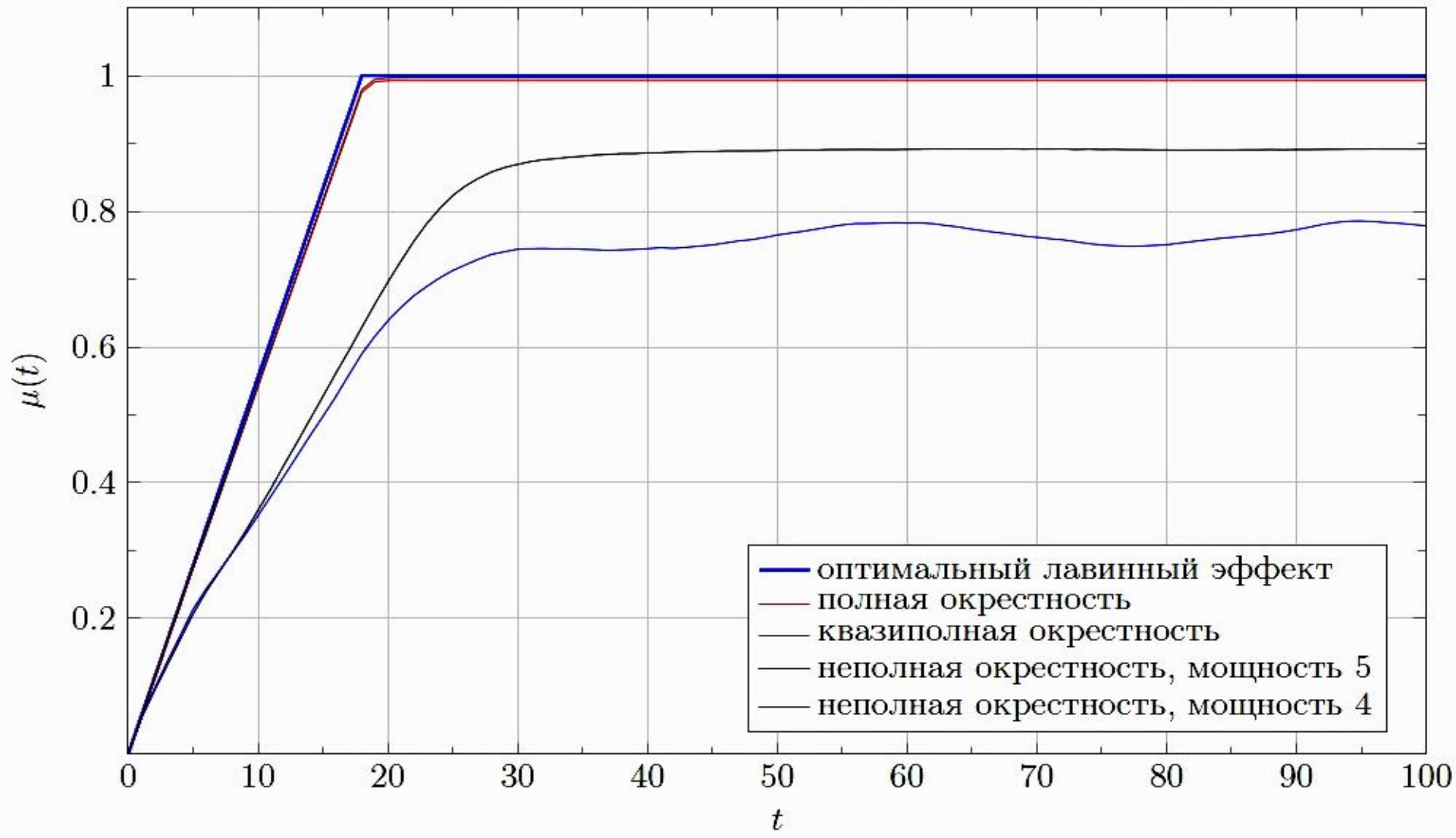
Ассоциация РусКрипто

Интегральные характеристики лавинного эффекта в классических двумерных клеточных автоматах



Ассоциация РусКрипто

Пространственные характеристики лавинного эффекта в классических двумерных клеточных автоматах



Ассоциация РусКрипто

Двумерный клеточный автомат

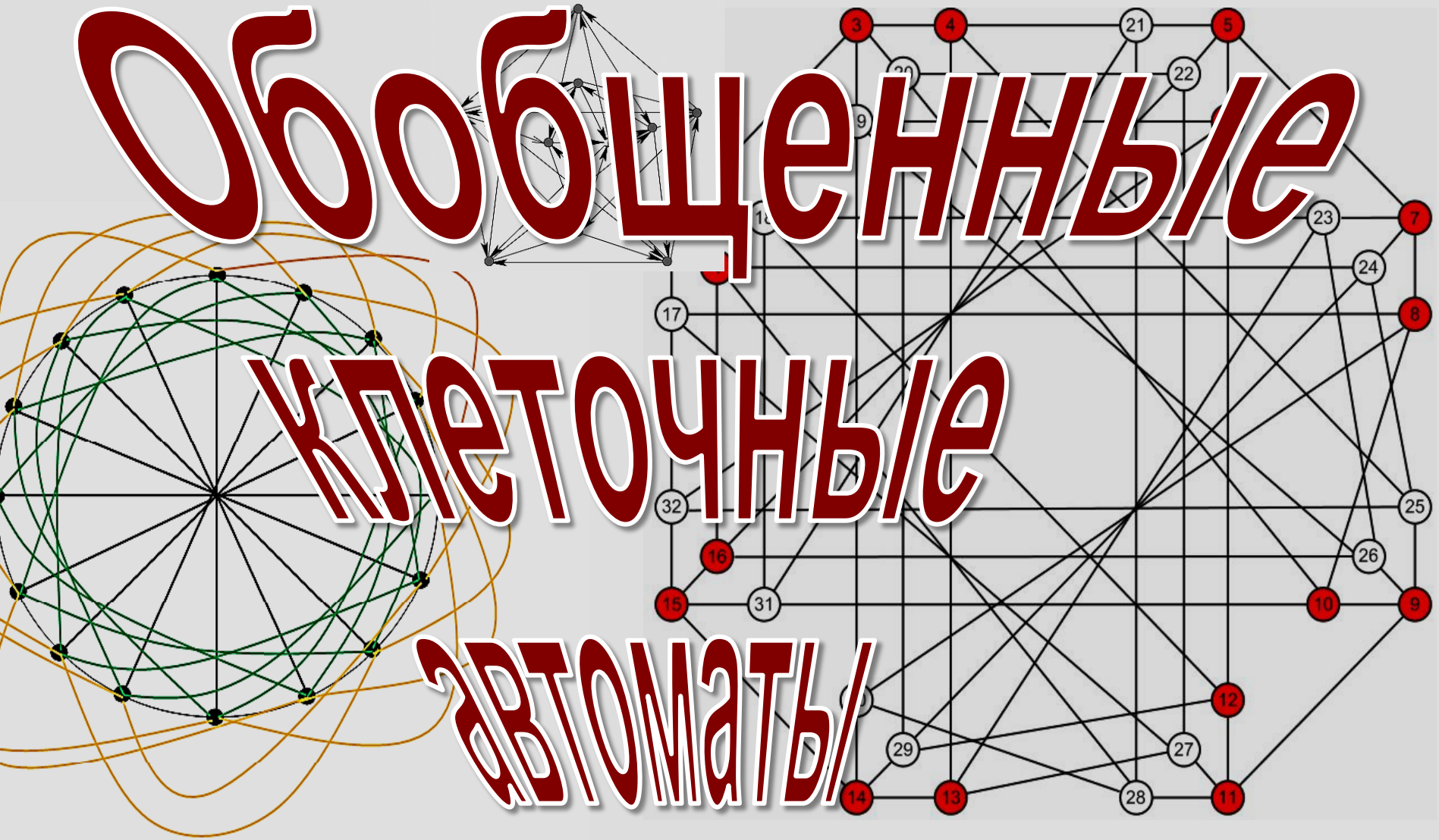
- исследованы статистические свойства выходных последовательностей разработанных генераторов; определены конкретные локальные функции связи и окрестности ячеек клеточных автоматов, обеспечивающие хорошие статистические свойства выходных последовательностей; подтверждено соответствие статистических свойств современным требованиям; разработан программный комплекс автоматизации процесса статистического тестирования;

Ассоциация РусКрипто

Двумерный клеточный автомат

- 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

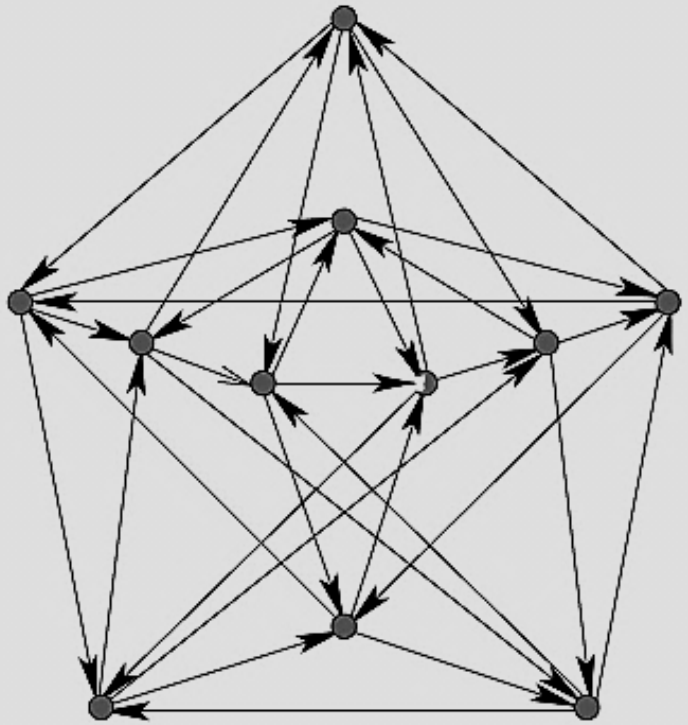


Ассоциация РусКрипто

Обобщенные клеточные автоматы

$$G = (V, E)$$

$$V = \{v_1, v_2, \ldots, v_N\}$$



$$v_i(t) = f_i\left(v_{i_1}(t-1), v_{i_2}(t-1), \ldots, v_{i_m}(t-1)\right)$$

Ассоциация РусКрипто

Обобщенные клеточные автоматы

- **Параллельность вычислений.**
- **Свойство локальности. В отличие от классического КлА, ячейки памяти могут быть соединены любым способом;**
- **Свойство неоднородности. Локальные функции связи могут быть различны и обладать любыми требуемыми свойствами. Однако локальные функции связи могут быть и одинаковы, как в случае с классическими клеточными автоматами.**

Ассоциация РусКрипто

Обобщенные клеточные автоматы

- ***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:**

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

Ассоциация РусКрипто

Обобщенные клеточные автоматы

- ***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»:**

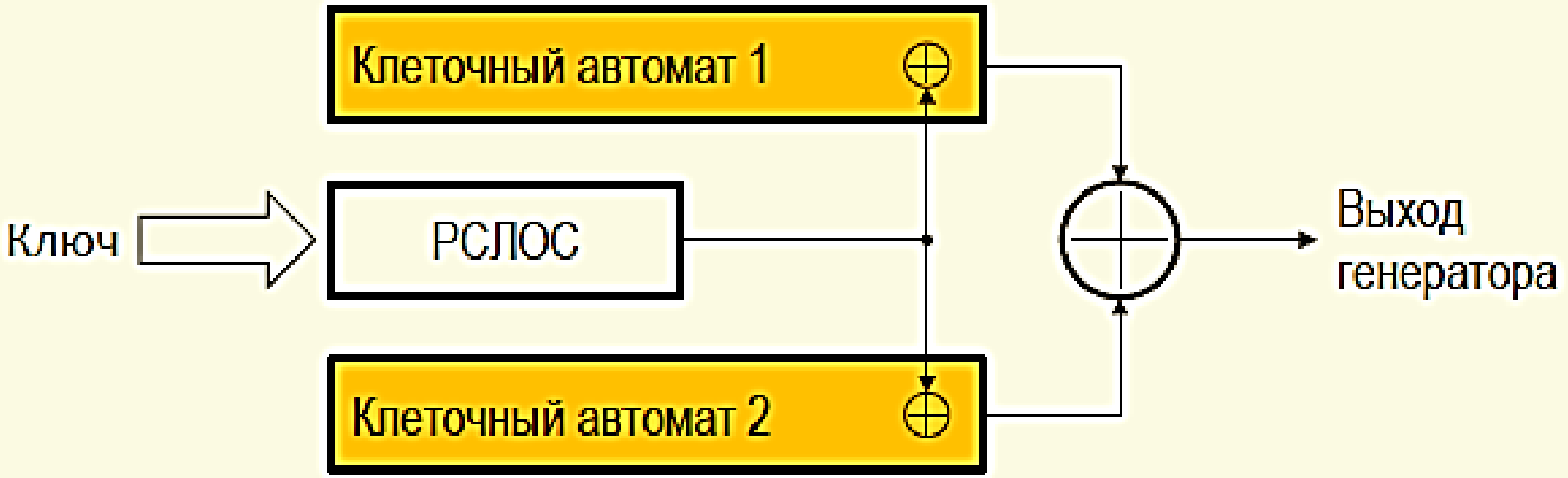
$$\mu(t) = \frac{1}{e(1)} \cdot \left(\max_j \left(m_j^{(1)}(t) \oplus m_j^{(2)}(t) \right) \cdot \Delta(1, j) \right)$$

где $\Delta(i, j)$ – длина минимального пути из вершины i в вершину j,
а $e(i)$ – эксцентриситет вершины i.

Ассоциация РусКрипто

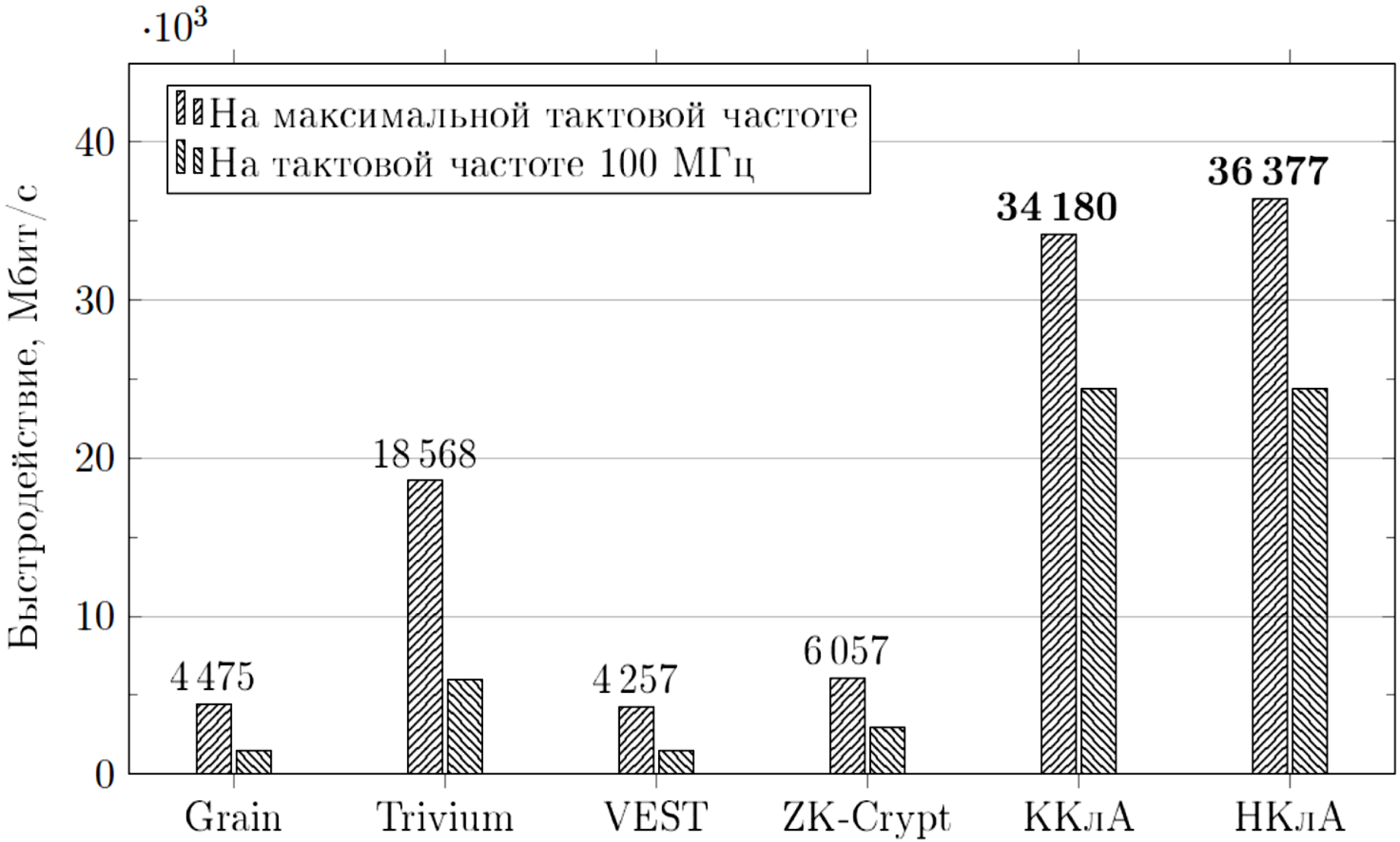
ГПСП на основе обобщенных клеточных автоматов

FPGA Cyclone II (EP2C35F672C6) Altera.



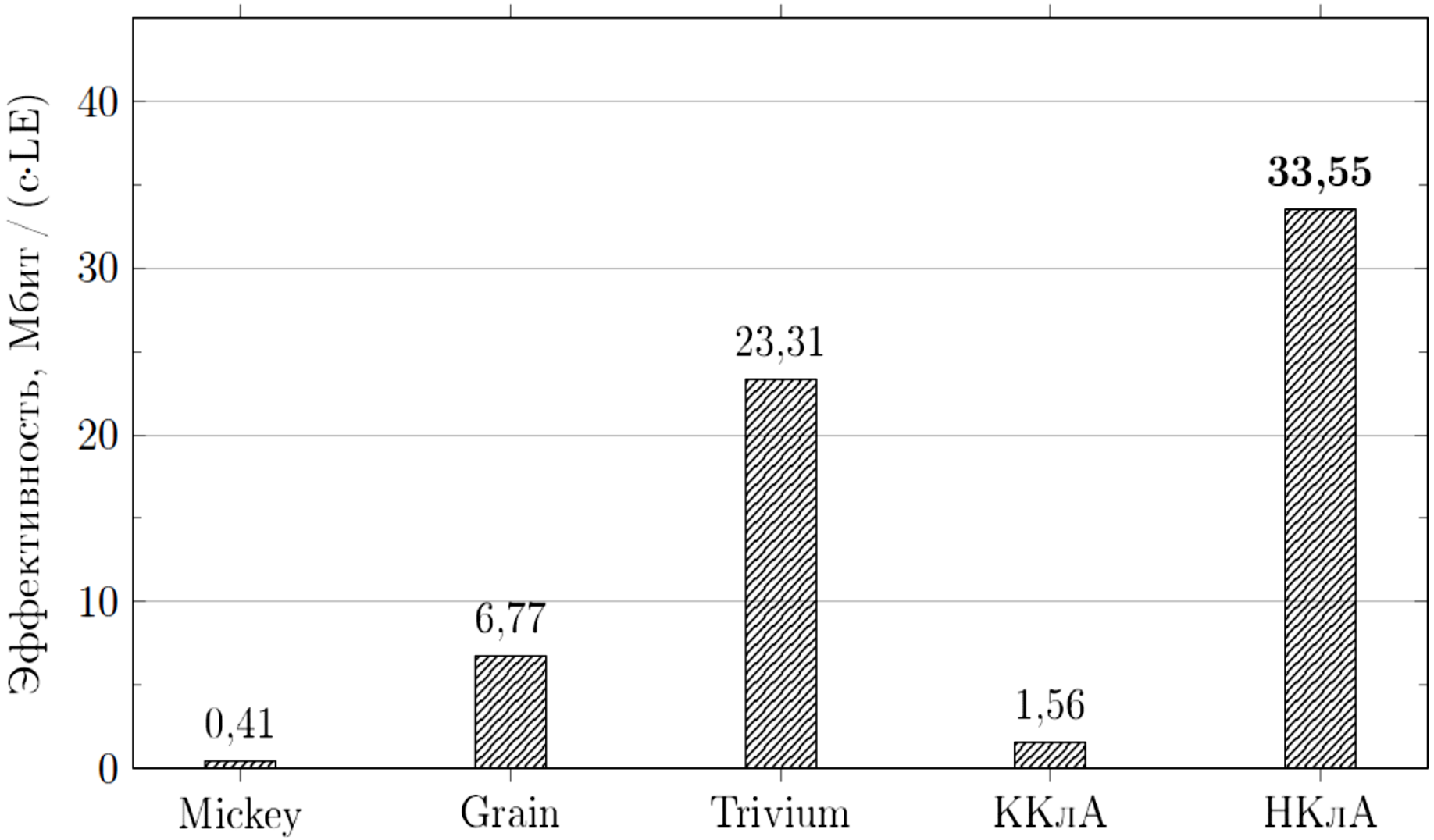
Ассоциация РусКрипто

ГПСП на основе обобщенных клеточных автоматов



Ассоциация РусКрипто

ГПСП на основе обобщенных клеточных автоматов

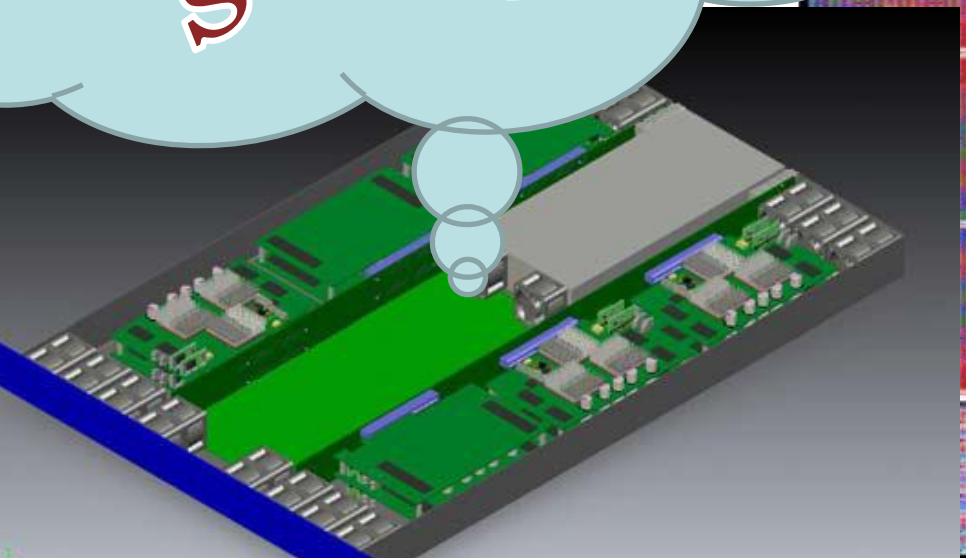



Ассоциация
РусКрипто
Клеточные
автоматы
в конструкции
блочных шифров

Ассоциация РусКрипто

Клеточные автоматы в конструкции блочных шифров

В конструкции S-блоков

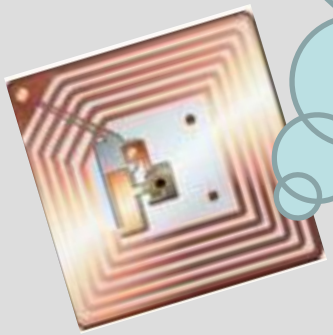


Обратимые клеточные автоматы

Ассоциация РусКрипто

Клеточные автоматы в конструкции блочных шифров

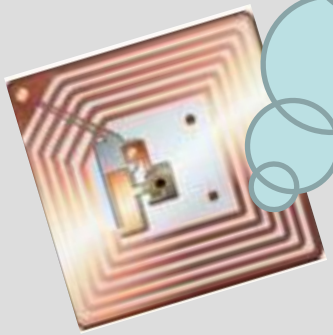
Концепция SPK-блока



Ассоциация РусКрипто

Клеточные автоматы в конструкции блочных шифров

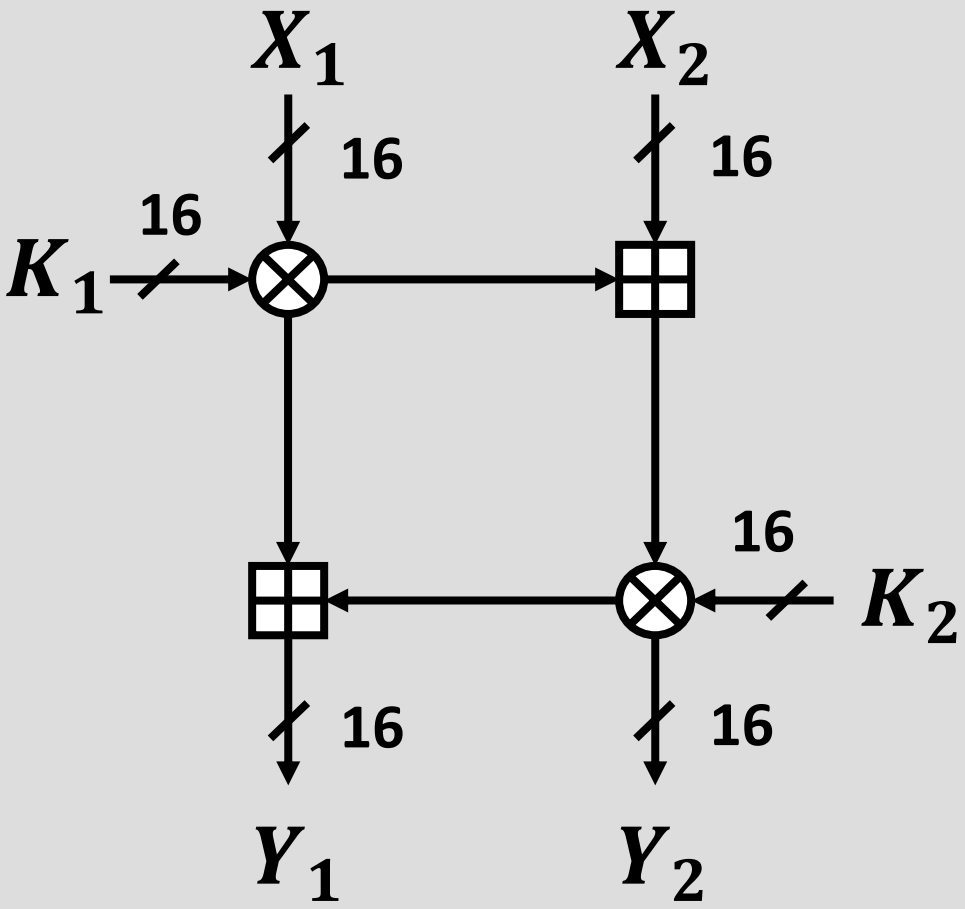
S-блок+
P-блок+
K-блок



Ассоциация РусКрипто

SPK-блок

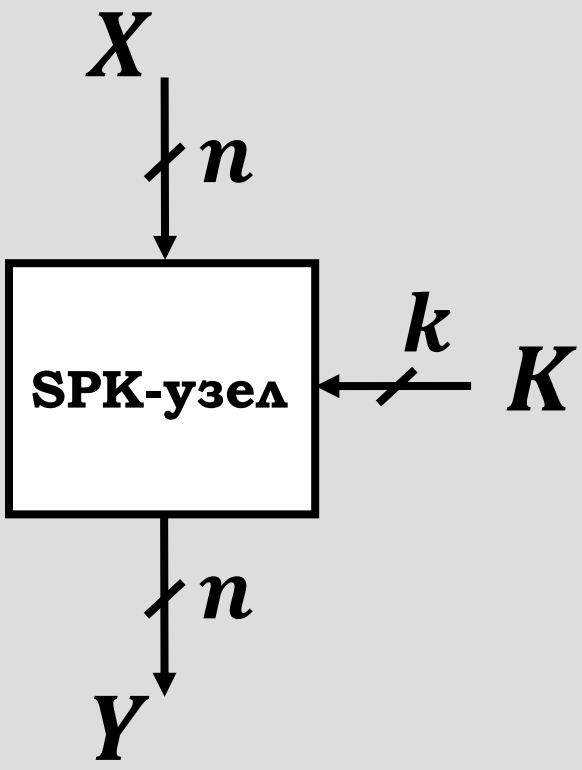
Lai X., Massey J. A Proposal for a New Block Encryption Standard, Advances in Cryptology: EUROCRYPT 1990 Proceedings. – Lecture Notes in Computer Science, vol. 473, Springer-Verlag, 1991. – pp. 389–404.



MA-узел (Multiplication-Addition)

Ассоциация РусКрипто

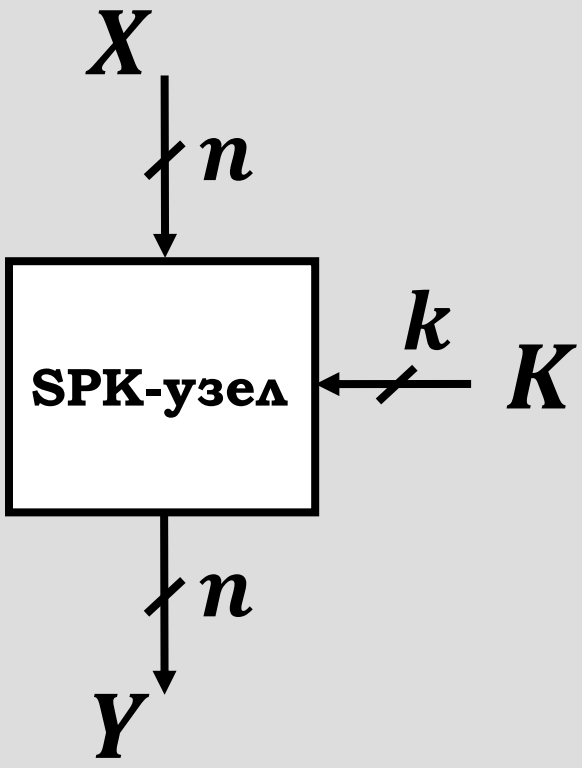
SPK-блок на базе обобщенных клеточных автоматов



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.

Ассоциация РусКрипто

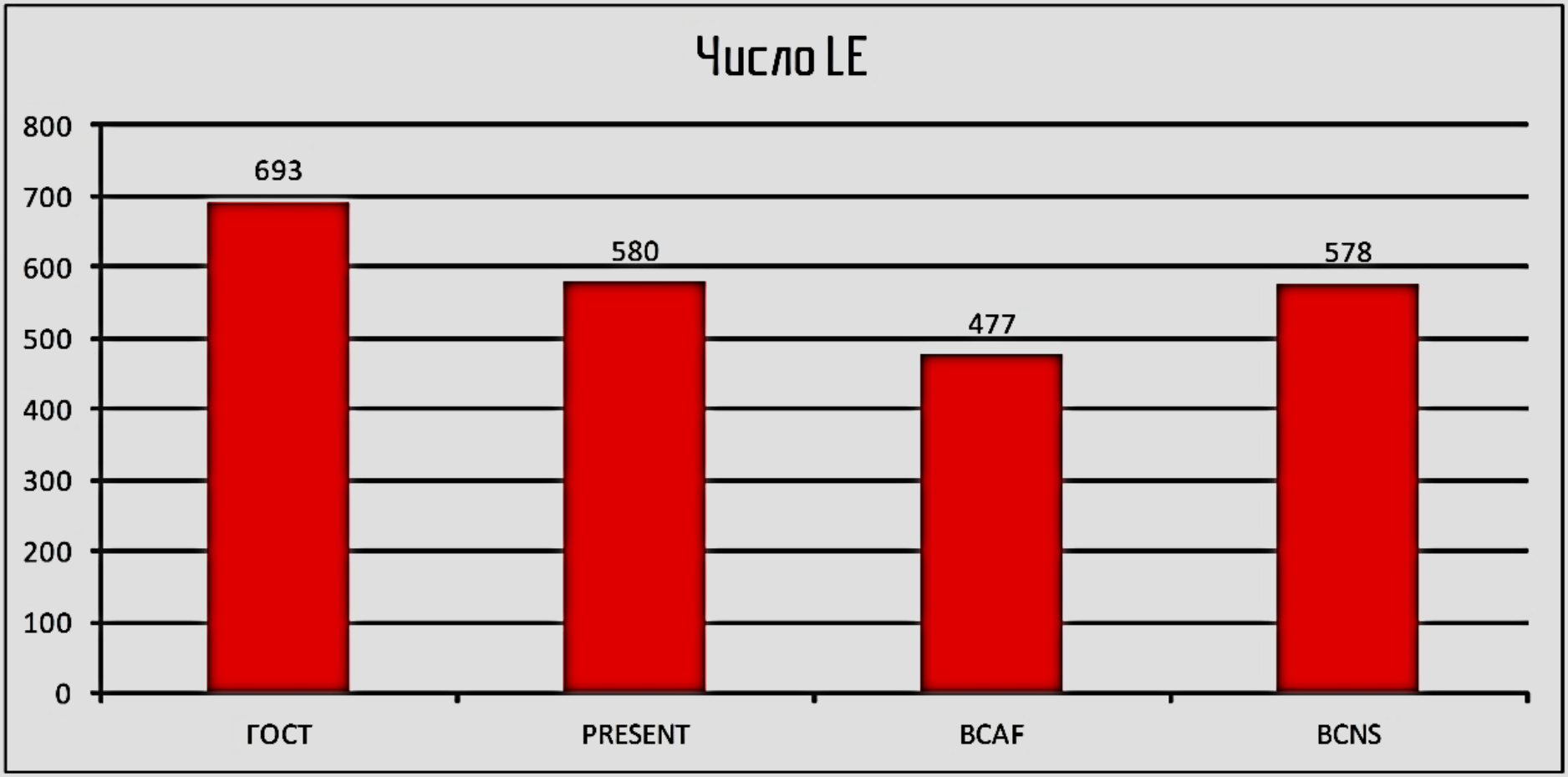
SPK-блок на базе обобщенных клеточных автоматов



Минимальное число тактов работы автомата должно быть не меньше, чем d – диаметр орграфа этого автомата, а число переменных, от которых должна существенно зависеть функция локальной связи, должно быть равным σ – степени захода орграфа автомата.

Ассоциация РусКрипто

SPK-блок на базе обобщенных клеточных автоматов



Ассоциация РусКрипто

Невнятное прошлое

Перспективное будущее

Ассоциация РусКрипто

Обобщенные клеточные автоматы

Проведенные исследования показали, что использование обобщенных клеточных автоматов в конструкции управляющей части поточных шифров, а также предложенная концепция SPK-блока хорошо подходит для решения задач низкоресурсной криптографии. Однако, для того, чтобы предлагать эти конструкции как актуальную замену классическим требуется проведение глубокого криптографического анализ предложенных конструкций, что становится важнейшей задачей ближайшего будущего.

Ассоциация РусКрипто

Клеточные автоматы