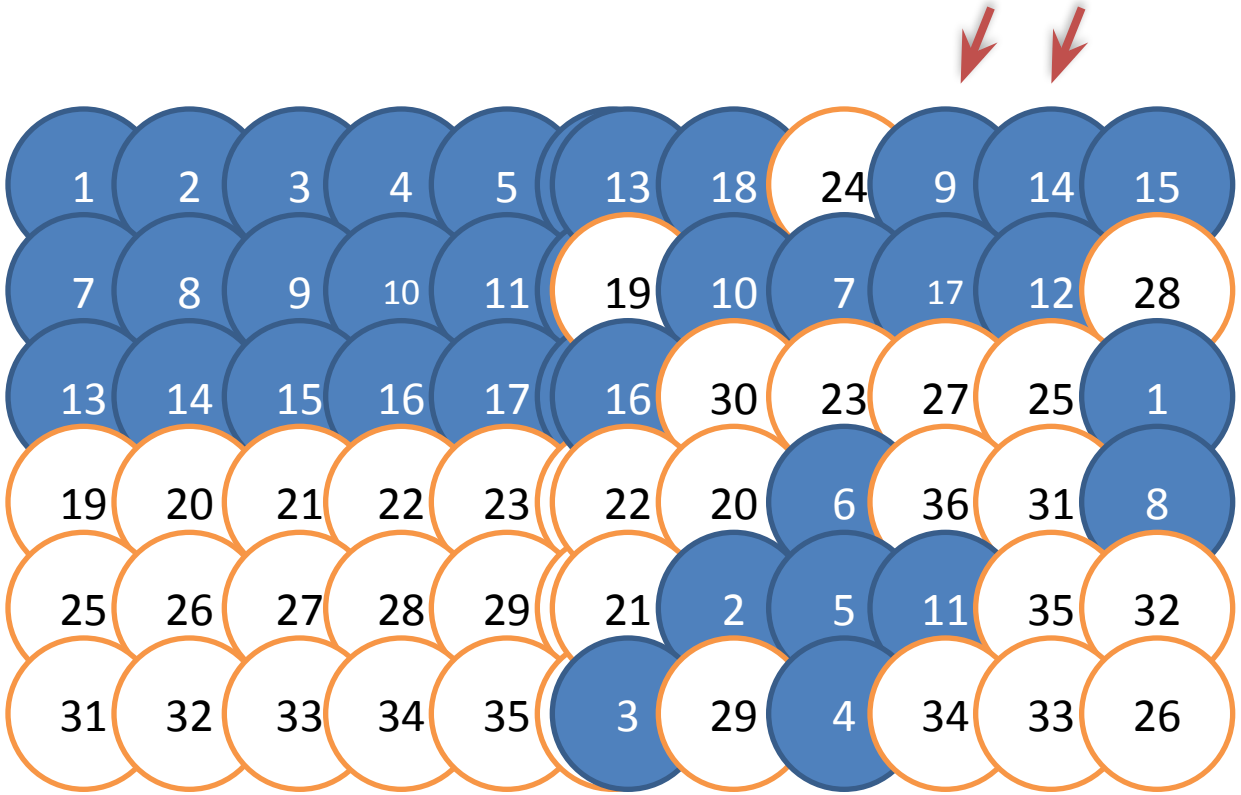
Модификация алгоритма перемешивания для генерации случайных числовых последовательностей

Автор: ст. гр. И-31д, АВТ, СНТУ
Иван Игнатьев
Руководитель: канд. техн. наук, доцент
Иван Владимирович Кудрявченко

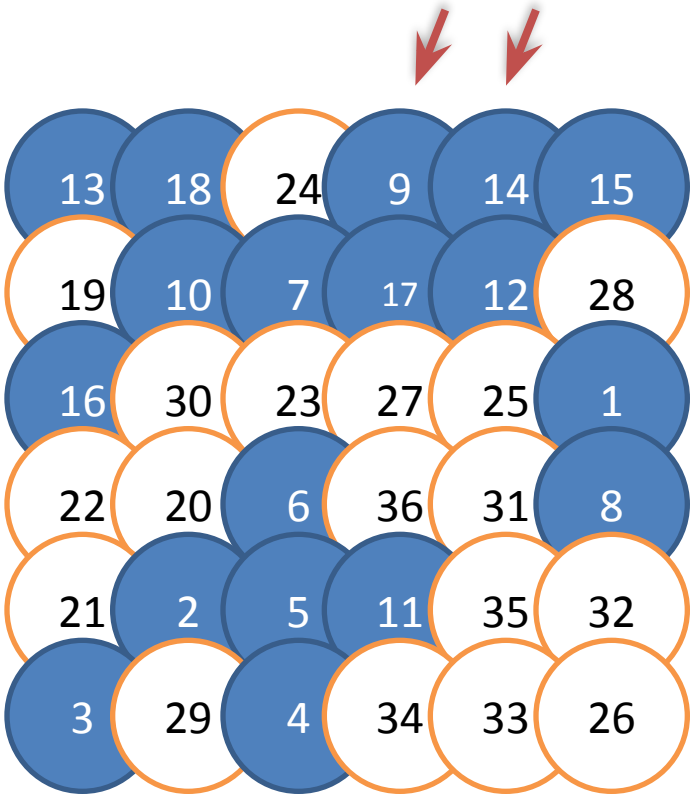
«Случайность»

Алгоритм перемешивания «Фигуры»



Т.к. от итерации к итерации алгоритм построения фигуры не меняется, то на всём множестве зависимость предыдущего элемента от следующего одинакова.

Так же подобный подход приводит к тому, что последовательность становится периодичной.



11111111111111111000000000000000000

11011101111100001000100101111001010000

00101000111000101001101111110000101 1

Преимущества

- Возможность применения в ГСЧП, распределенных по равномерному закону
- Простота реализации и понимания
- Высокая скорость работы, с двоичными словами большой длины
- Используя операцию перестановок, можно генерировать последовательность двоичных слов любой длинны

Предлагаемая модификация

Преимущества

- Преимущества алгоритма «Фигуры»
- Возможность применения в криптографических системах ГСЧП на базе модификации алгоритма
- Простое и доступное устройство в качестве источника энтропии, позволяющие быстро получать новую фигуру

Последний слайд

Ваши вопросы

?

Контакты:
Иван Игнатьев
E-mail: ivan@ignatiev.su
ICQ: 288-220-137

Библиографический список

Кудрявченко И.В. Исследование алгоритма перемешивания для генерации случайных числовых последовательностей [Текст] / И.В. Кудрявченко, В.В. Кудрявченко // Восточно-европейский журнал передовых технологий. – 2005. – №5. – С. 108—110.