

# Криптографічні хеш-функції на основі клітинних автоматів

доц. Танасюк Ю.В.

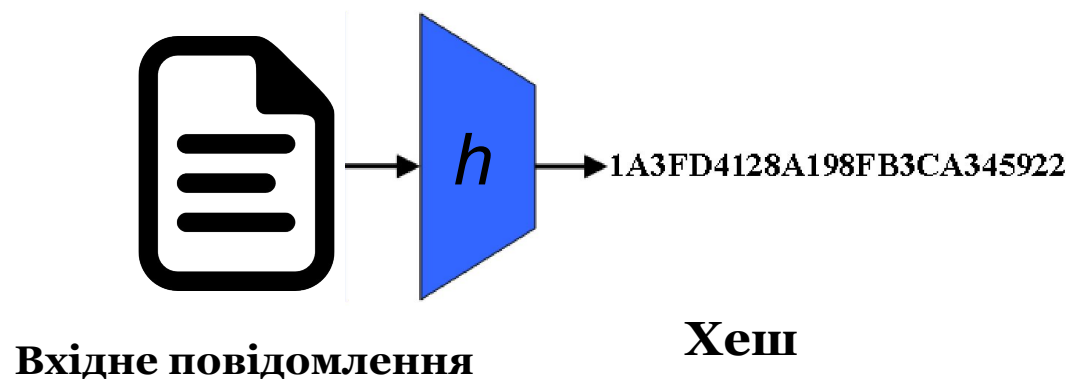
Константинюк Олексій

Мельничук Христина

Петро Бурдейний

Валеріан Гульпак

# Криптографічні хеш-функції

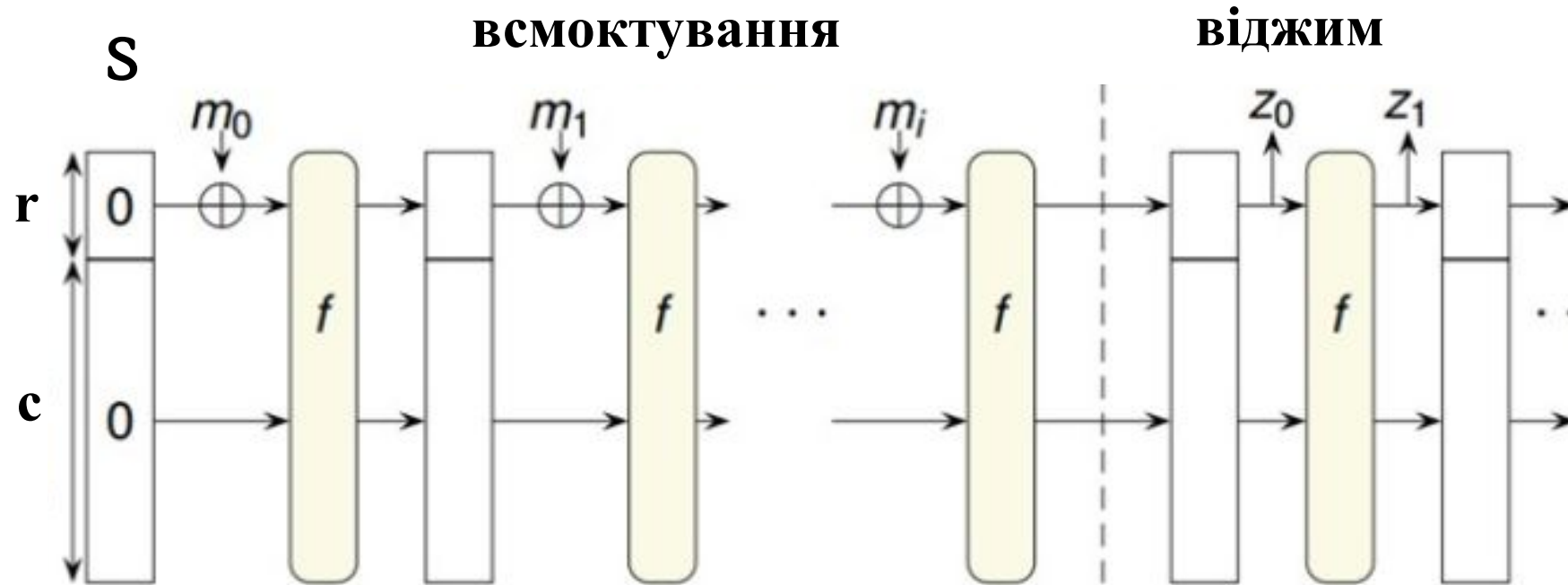


- MD5:  $n = 128$  (Ron Rivest, 1992)
- SHA-1:  $n = 160$  (NSA, NIST, 1995)
- SHA-2:  $n \rightarrow \{224, 256, 384, 512\}$  (NSA, NIST, 2001)

# Алгоритм Кессак

- Переможець конкурсу NIST серед алгоритмів криптографічних хеш-функцій у 2012 р. ([www.nist.gov/itl/csd/sha-100212.cfm](http://www.nist.gov/itl/csd/sha-100212.cfm)).
- Новий стандарт хешування SHA-3 (2015).
- Змінна довжина дайджесту: 224, 256, 384 та 512 бітів.
- Програмна й апаратна реалізація.
- Базується на конструкції губки та псевдовипадкових перетвореннях.

# Конструкція губки

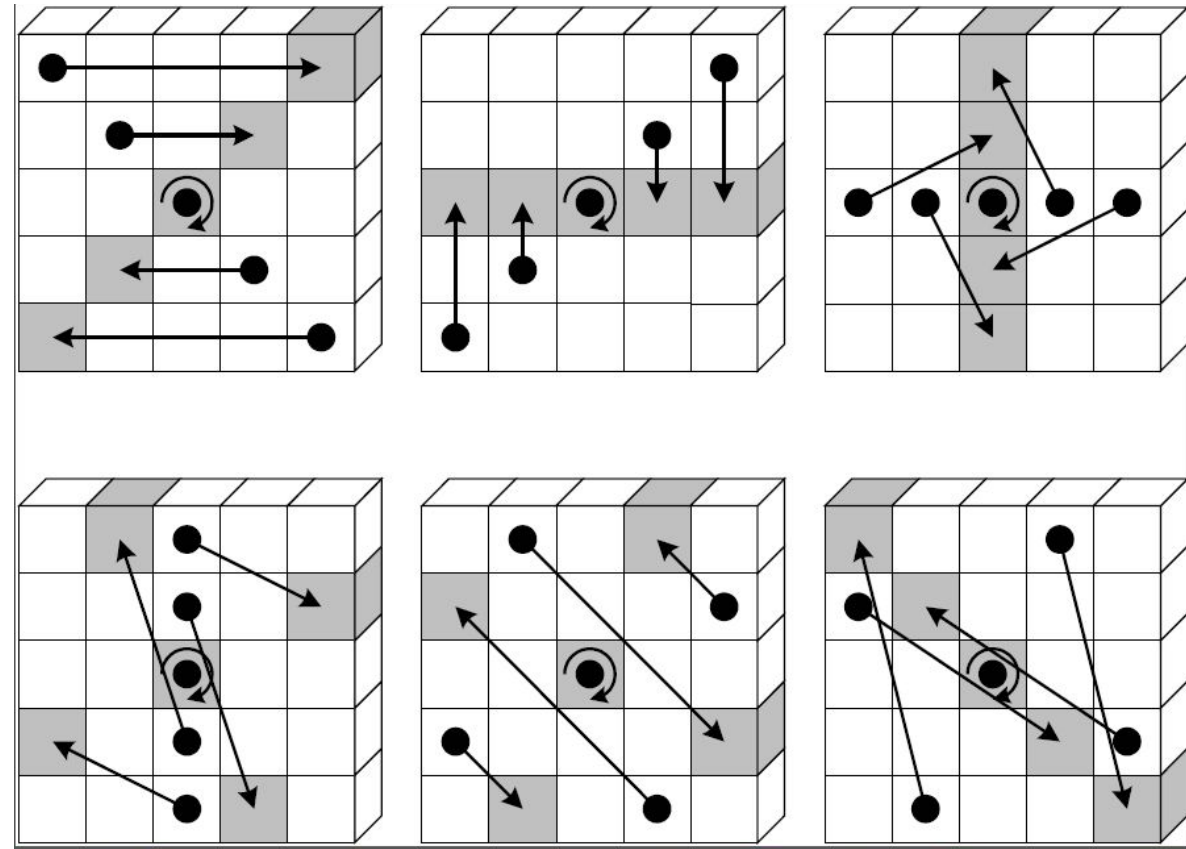
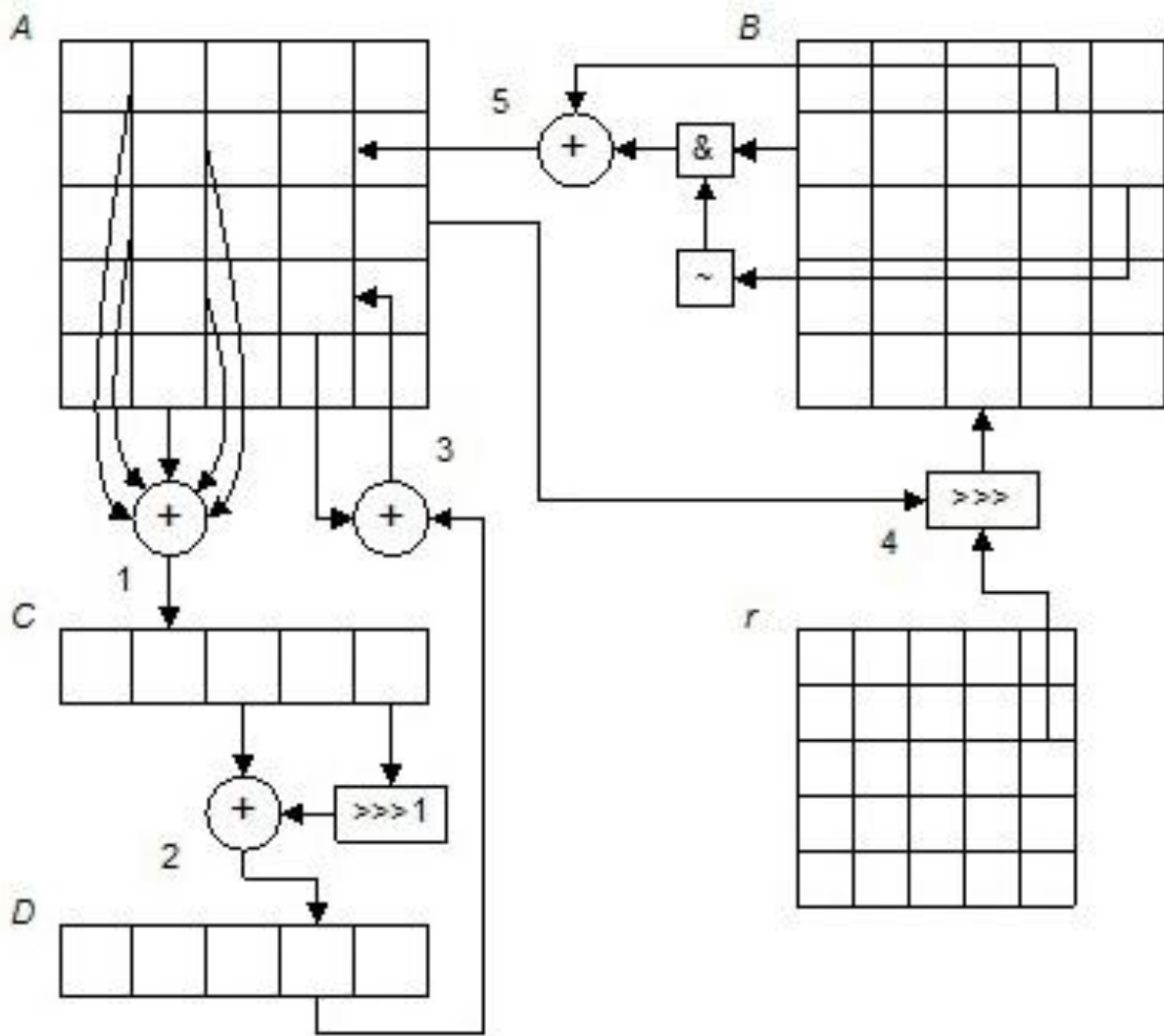


- Інтерактивна конструкція для реалізації псевдовипадкових перестановок за допомогою низки розроблених функцій  $f$ .
- $S$  — внутрішній стан фіксованої довжини  $b$  (бітів).
- $b = r + c$ , де  $r$  — бітова швидкість,  $c$  — потужність.

# Параметри хеш-функції Кессак

- Стандарт SHA-3 використовує стан губки довжиною **1600 бітів**.

Довжина хешу, Z (біти)	Бітова швидкість, r (біти)	Потужність, c (біти)	Рівень захисту, N (біти)
224	1152	448	112
256	1088	512	128
384	832	768	192
512	576	1024	256



Схематичне зображення процедури перестановки Кессак-f стану губки  
<http://n/кессак.noekeon.org/>

# Постановка задачі

- Стан губки – одно-, дво- та тривимірні клітинні автомати (КА).
- Функція перемішування – комбінація правил обробки КА.
- Застосовуються на обох стадіях всмоктування та віджиму.
- Змінна кількість раундів обробки.
- Параметри та довжина хешу відповідають алгоритму Кессак.
- Тестування NIST STS та лавинний ефект.

# Клітинні автомати (КА)

- Самоорганізована статистична система клітин, кожна з яких може перебувати в одному з двох станів 0 або 1
- Розвивається за визначеним правилом, наприклад:

- правило 30:  $C[i]' = C[i-1] \oplus (C[i] \vee C[i+1])$  (1)

- правило 54:  $C[i]' = (C[i-1] \vee C[i+1]) \oplus C[i]$  (2)

- правило 86:  $C[i]' = (C[i-1] \vee C[i]) \oplus C[i+1]$  (3)

- правило 150:  $C[i]' = C[i-1] \oplus C[i] \oplus C[i+1]$  (4)

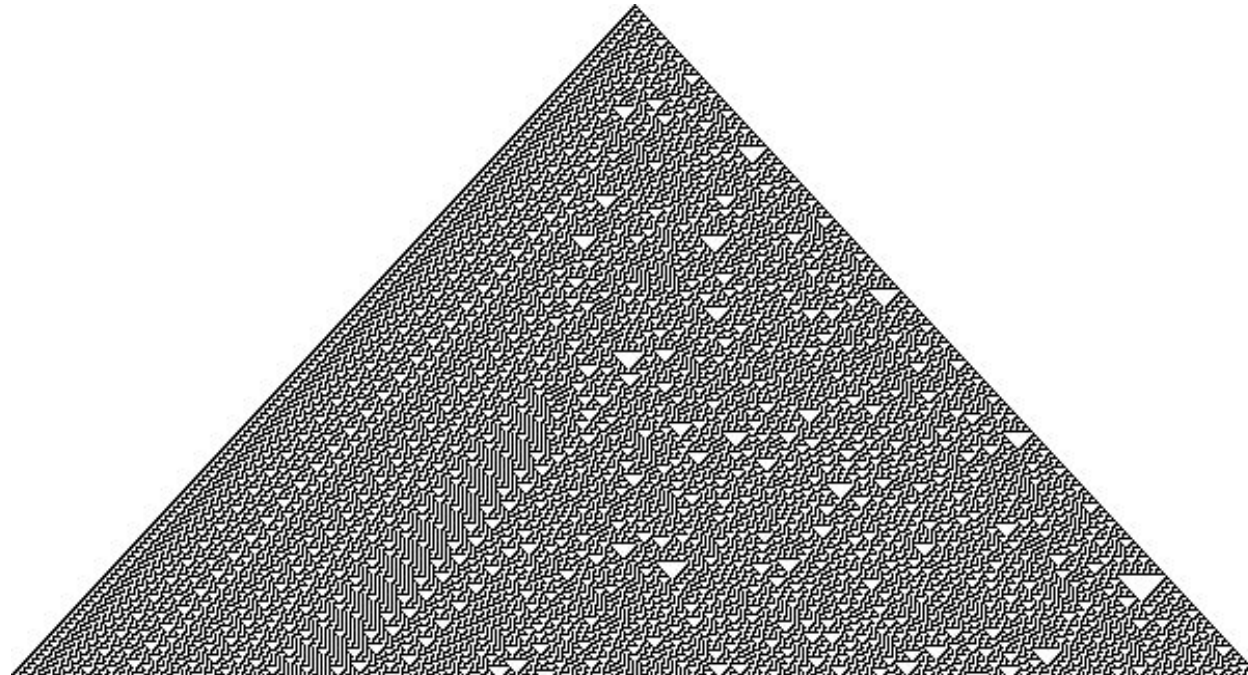
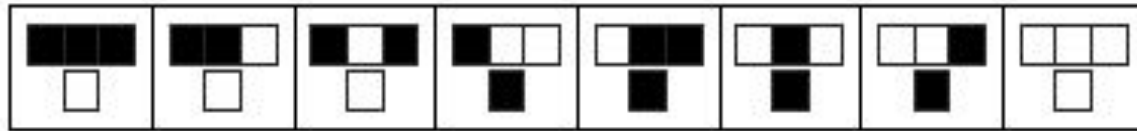
- правило 158:  $C[i]' = C[i-1] \oplus C[i] \oplus C[i+1] \vee C[i] \wedge C[i+1]$  (5)

де  $C[i]$  – поточна клітина,  $C[i]'$  - оновлене значення поточної клітини після застосування правила,  $C[i-1]$ ,  $C[i+1]$  – попередня і наступна сусідні клітини, та  $\oplus$ ,  $\wedge$ ,  $\vee$  - бітові операції XOR, AND, та OR, відповідно.



# Клітинні автомати (КА): правило 30

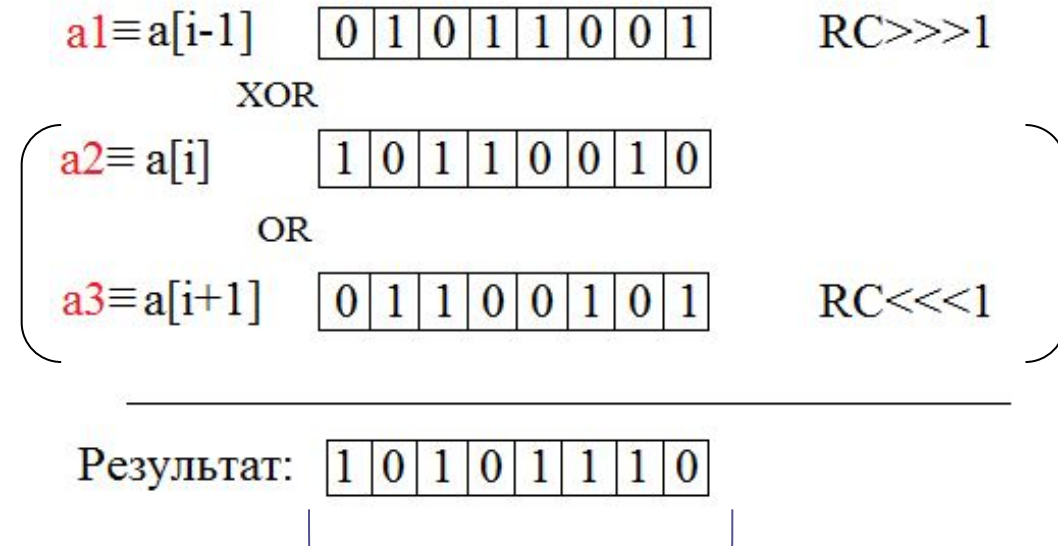
$$C[i]' = C[i-1] \oplus (C[i] \vee C[i+1])$$



# Одновимірні клітинні автомати (КА)

Для оптимізації обробки вектору стану губки RC довжиною 1600 бітів на кожному раунді створювалися два його вектори:

$a2' = a1 \text{ XOR } (a2 \text{ OR } a3)$  – правило №30(1)

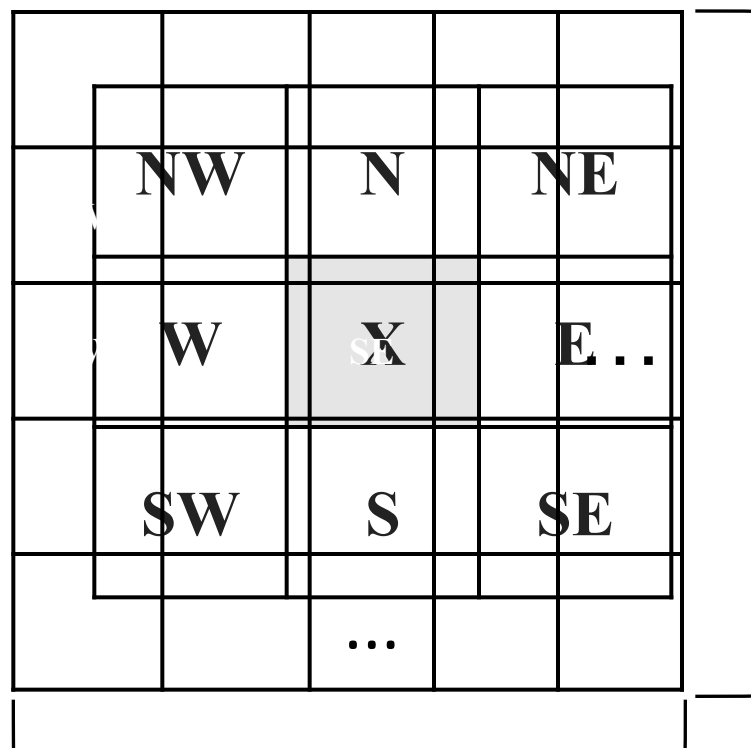


1600 бітів

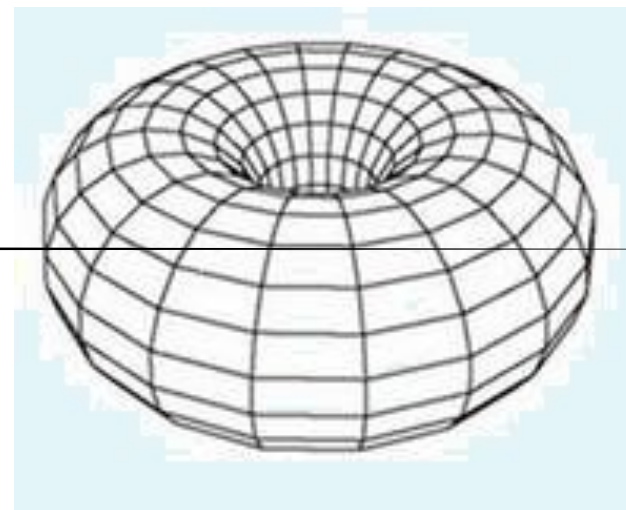
**Збільшення швидкості обробки у 60 разів**

# Двовимірні КА

- 25 рядків довжиною 64 біти, загальний розмір - 1600 бітів
- Локальний окіл Мура: 8 суміжних клітин
- Крайні клітини замикаються в тор.



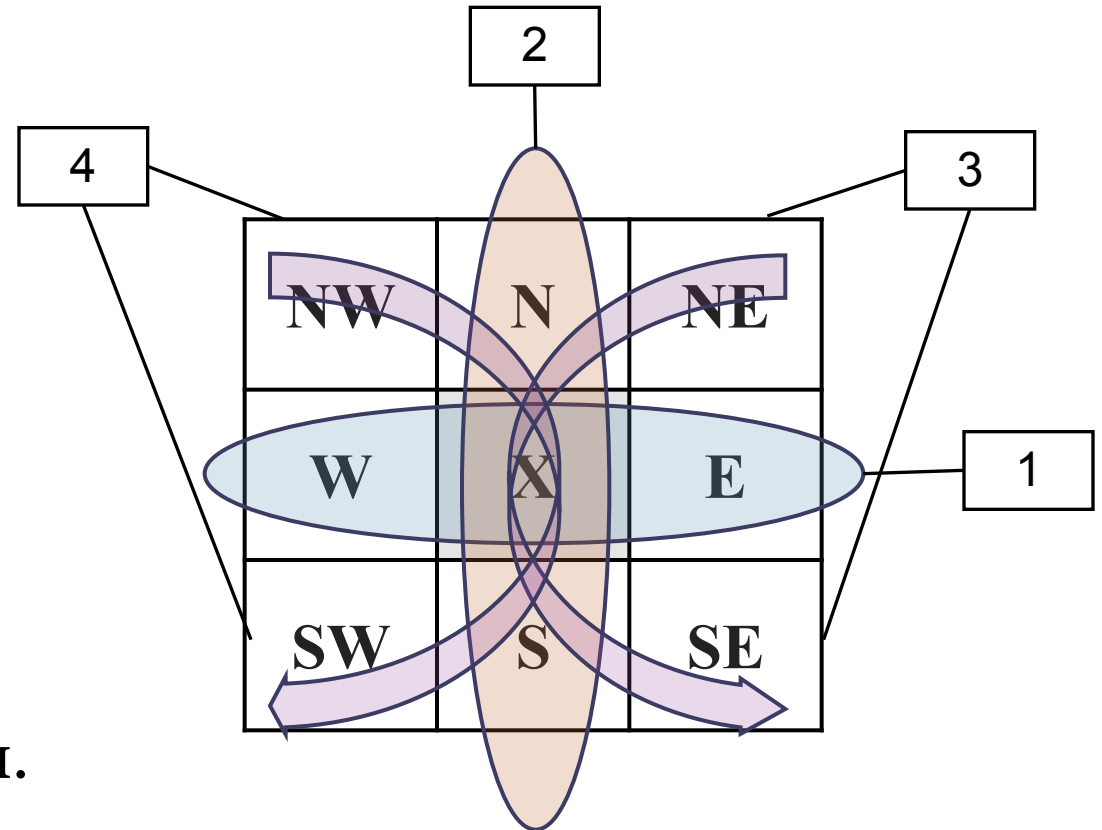
25



64 біти

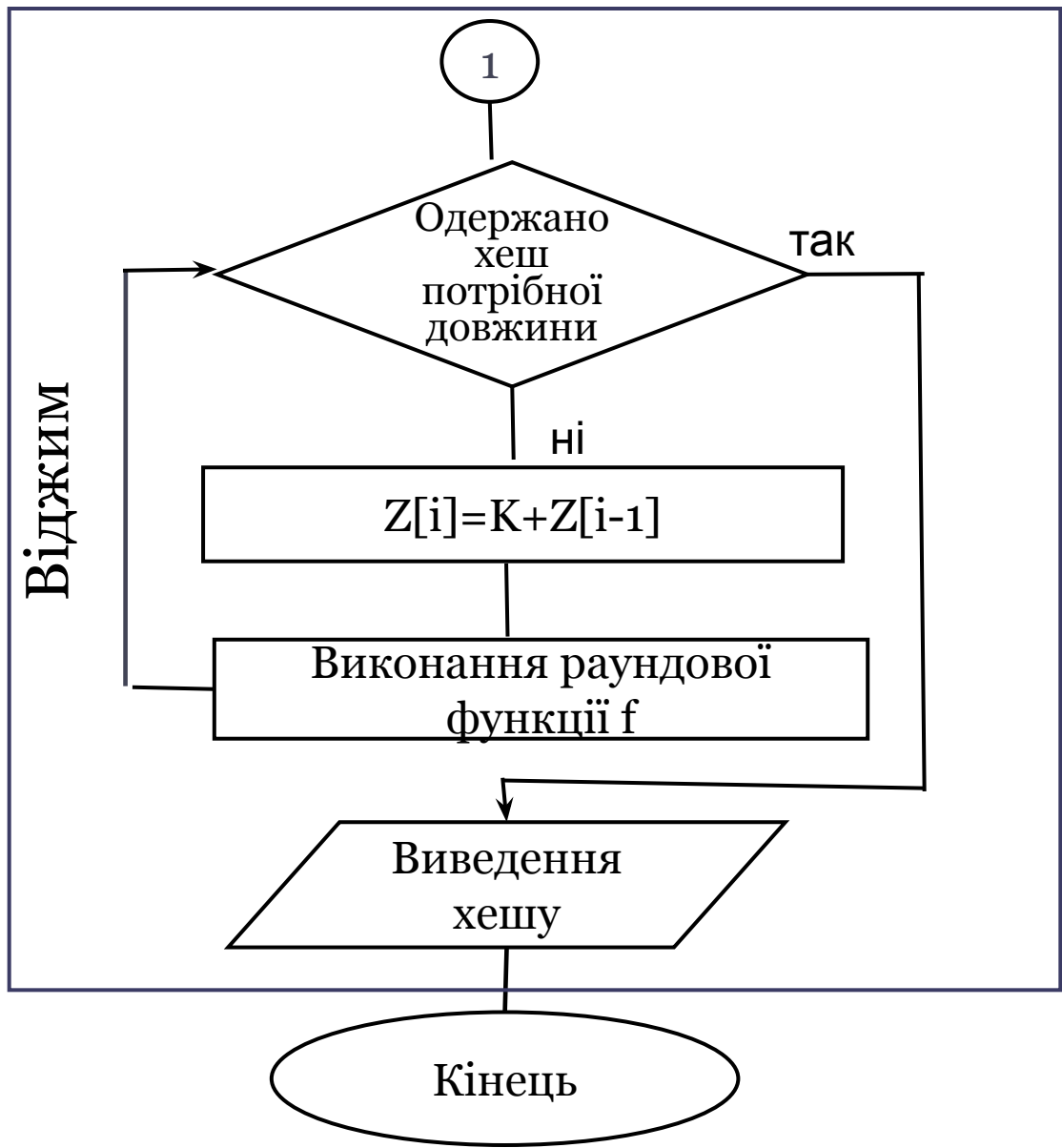
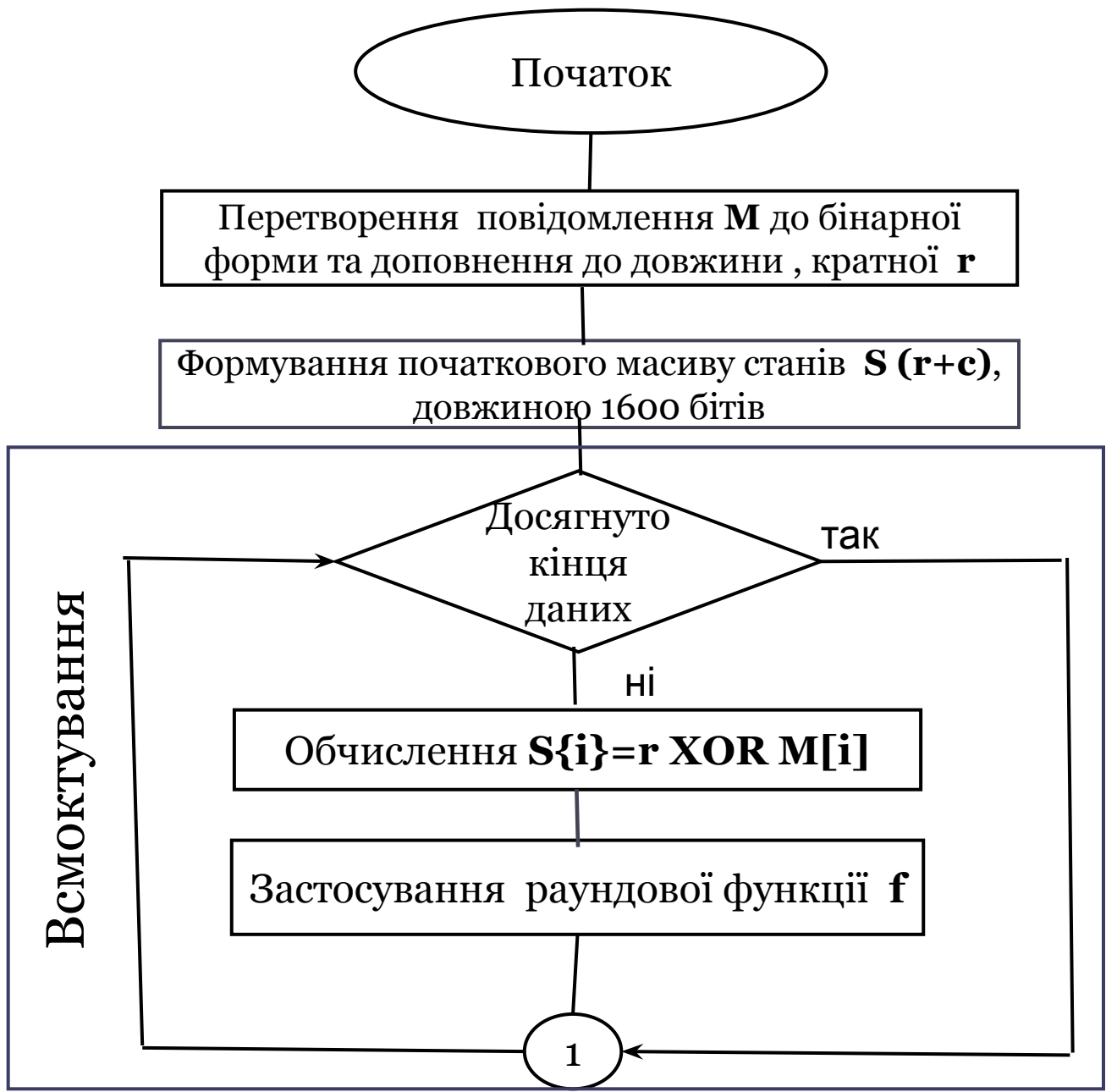
# Схема взаємодії

- 4 способи взаємодії
- N, W, NW, NE – попередні клітини
- S, E, SW, SE – наступні.
- Гібридні клітинні автомати
- Поєднання лінійних (150) та нелінійних (30, 54, 86, 158) правил.

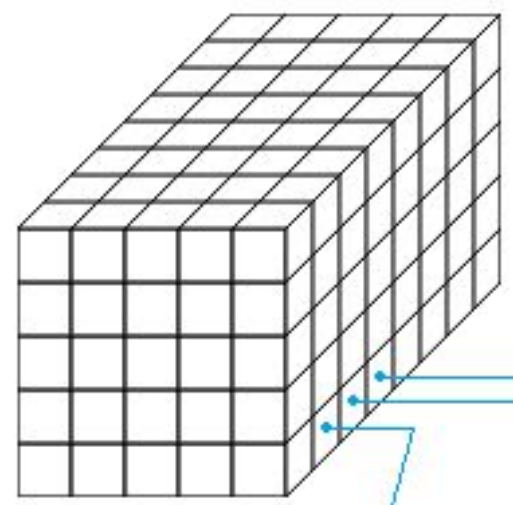


# Різновиди функцій перестановки

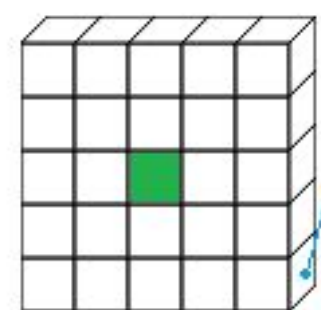
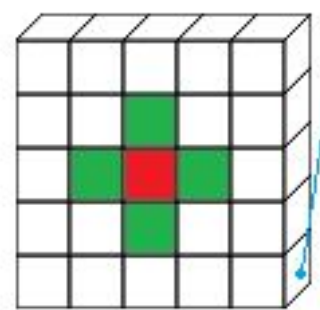
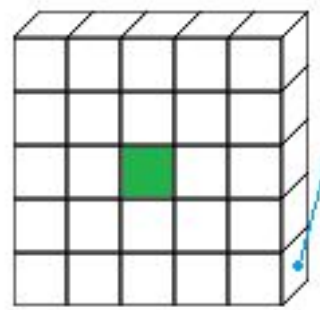
Позначення функцій перемішування	Номер взаємодії	Правило КА	Взаємодія клітин
Rule_30_150_86	1	30	$X' = W \oplus (X \vee E)$
	2	150	$X' = N \oplus X \oplus S$
	3	86	$X' = (NE \vee X) \oplus SE$
	4	86	$X' = (NW \vee X) \oplus SW$
Rule_54_150_86	1	54	$X' = (W \vee E) \oplus X$
	2	150	$X' = N \oplus X \oplus S$
	3	86	$X' = (NE \vee X) \oplus SE$
	4	150	$X' = NW \oplus X \oplus SW$
Rule_54_158_150_86	1	54	$X' = (W \vee E) \oplus X$
	2	158	$X' = N \oplus X \oplus S \vee X \wedge S$
	3	86	$X' = (NE \vee X) \oplus SE$
	4	150	$X' = NW \oplus X \oplus SW$



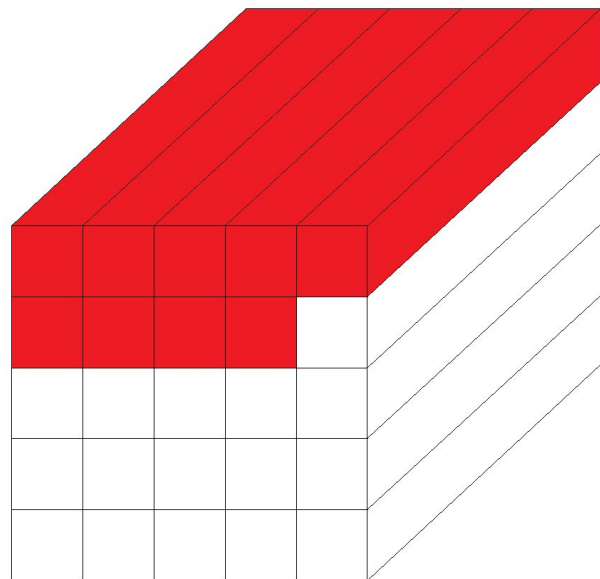
# Тривимірні КА



arrayRC: масив 5x5 64-бітних векторів



# ІНІЦІАЛІЗАЦІЯ



ArrayRC

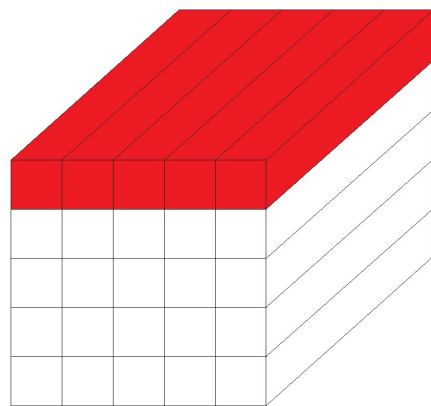
Довжина хешу введена користувачем	RLength
224	1152
256	1088
384	832
Інша довжина	576



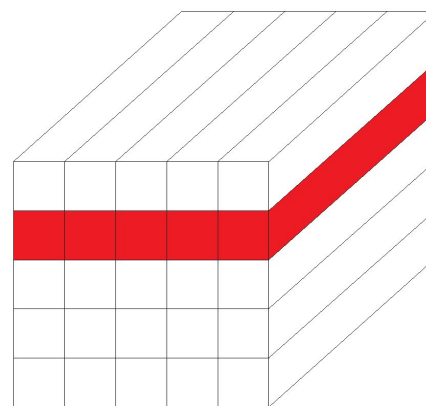
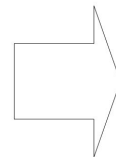
# Правила взаємодії

- Правило 30:  
$$RCArray[i][j] = (\text{nord xor west xor back}) \text{ xor } RCArray[i][j] \mid (\text{south xor east xor face})$$
- Правило 86:  
$$RCArray[i][j] = (\text{nord xor west xor back}) \mid RCArray[i][j] \text{ xor } (\text{south xor east xor face})$$
- Правило 150:  
$$RCArray[i][j] = (\text{nord xor west xor back}) \text{ xor } RCArray[i][j] \text{ xor } (\text{south xor east xor face})$$

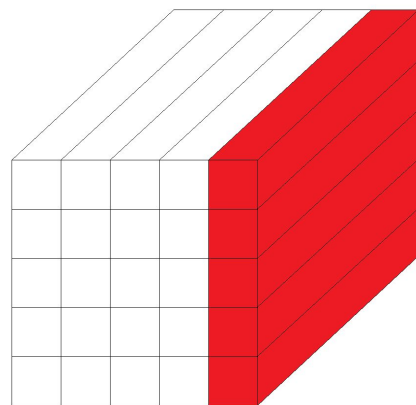
# FBlock



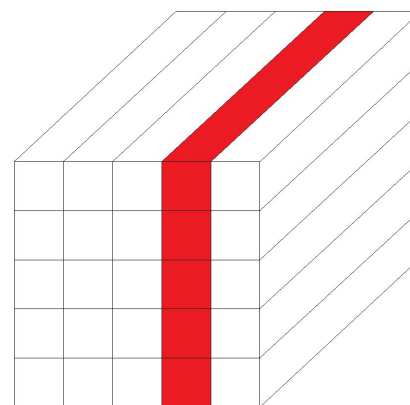
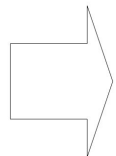
newArrayRC



newArrayRC

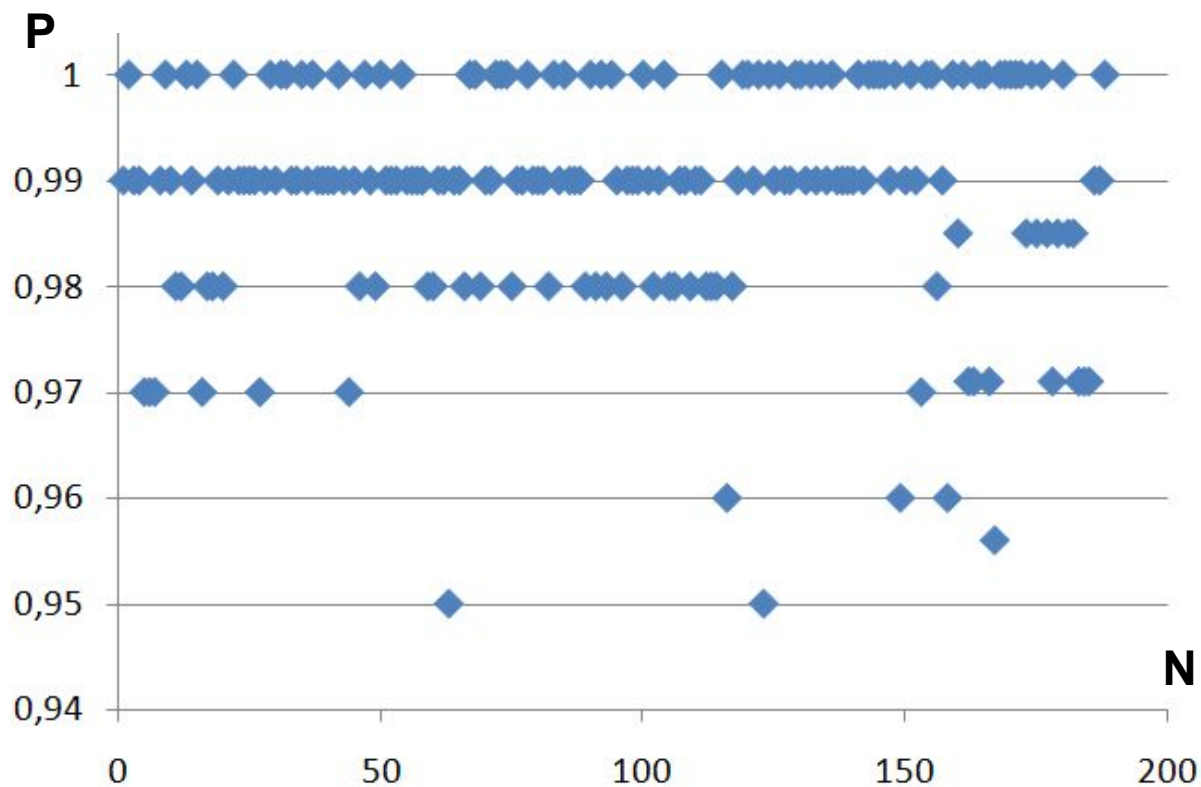


newArrayRC

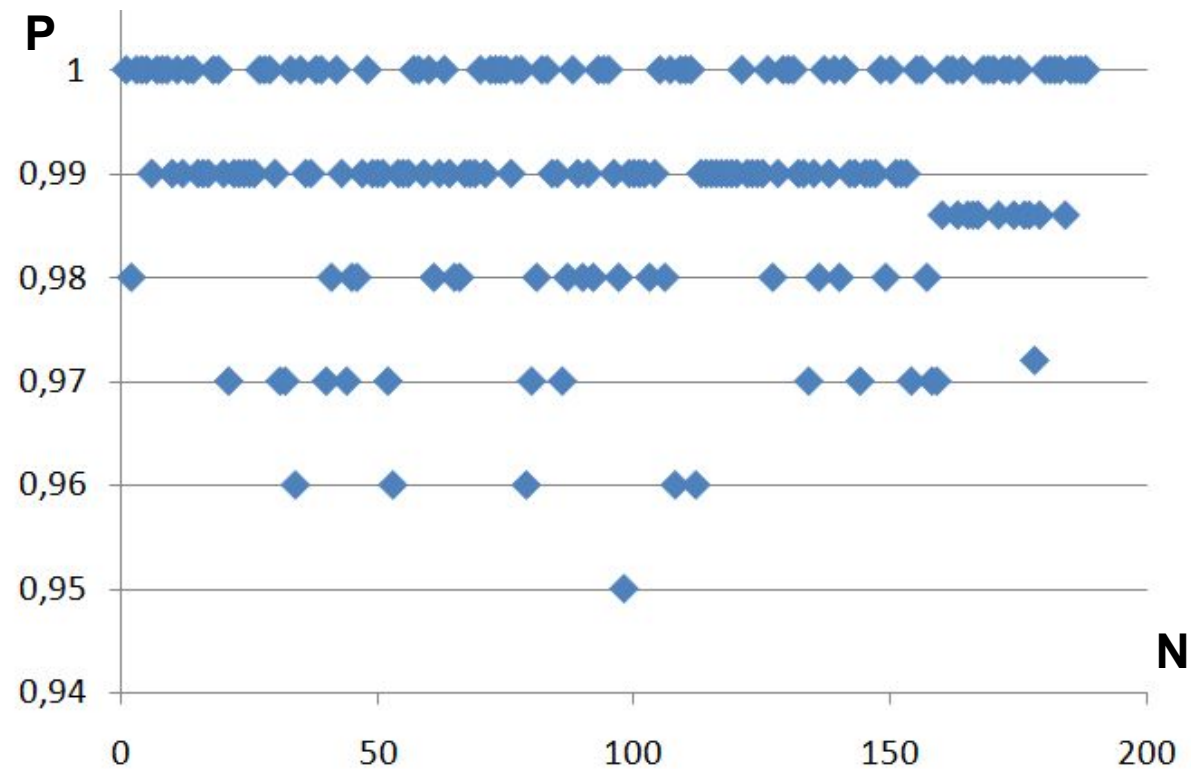


newArrayRC

# Результати статистичного тестування NIST



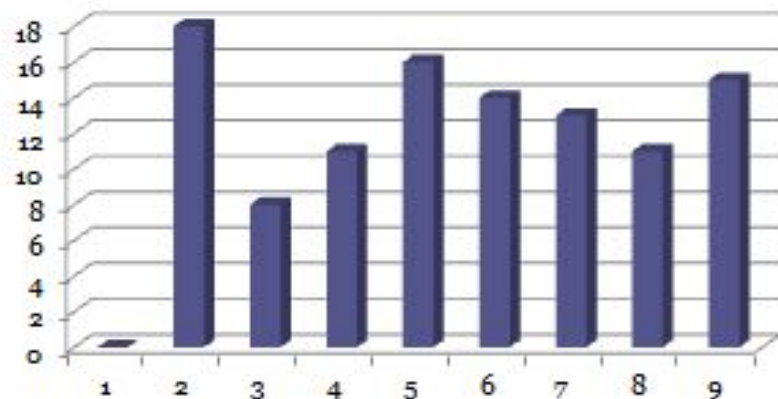
RULE\_54\_150\_86, 5 раундів



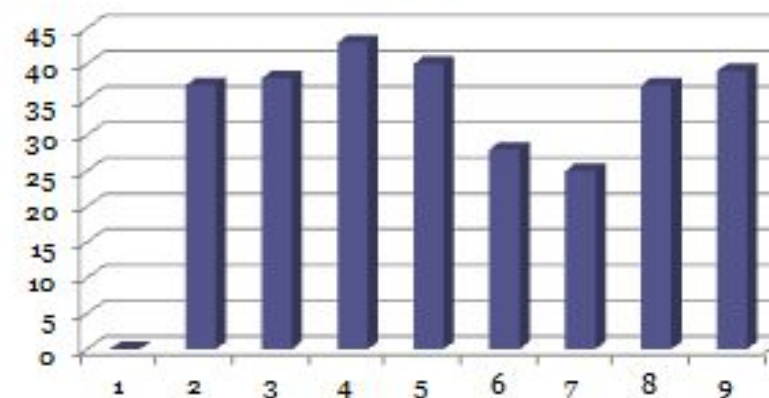
RULE\_54\_150\_86, 10 раундів

# TECTH NIST STS

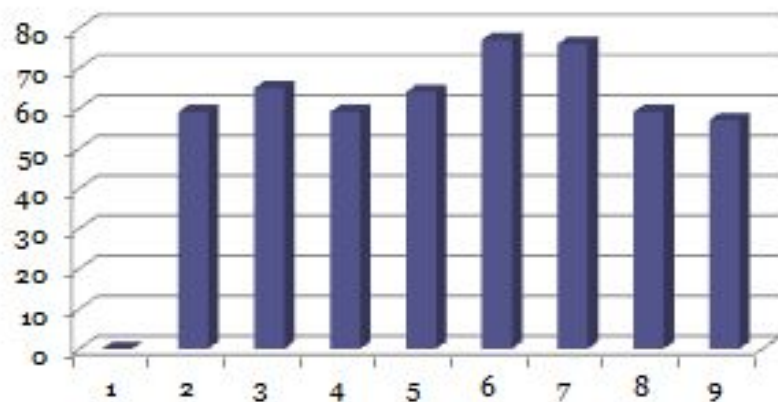
**0,97**



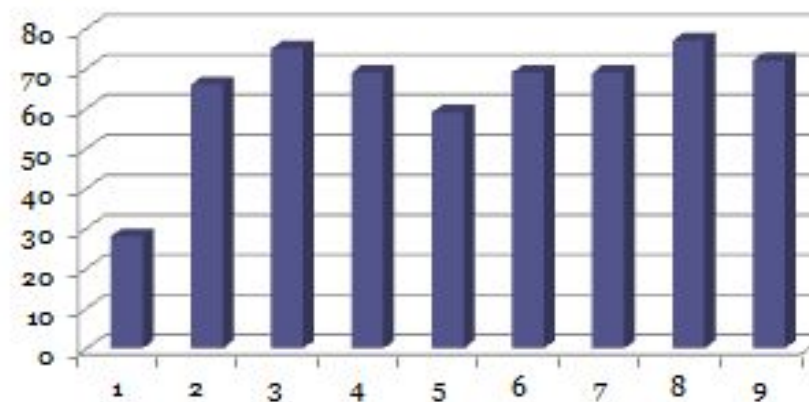
**0,98**



**0,99**



**1**



# ШВИДКОДІЯ

Версія алгоритму хешування	Час формування файлу розміром 100Мб	Час формування 512біт хешу для файлу розміром 1Мб (мс)	Швидкодія (кбайт/с)
1	8хв 8с	7684	133,34
2	6хв 47с	4827	217,23
3	13хв 54с	8335	125,8
4	20хв 21с	11594	90,44
5	26хв 36с	15599	67,22
6	32хв 43с	19201	54,61
7	8хв 15с	5241	200,07
8	9хв 46с	9281	112,98
9	14хв 28с	11104	94,43



# ОДЕРЖАННЯ ХЕШУ

""

```
DFA49F6AA6385B50D868E3B77EB7E71155167ACB2C215AD47E2B8DCC4AE12AFF  
9387D0AD78C20CDA771B018B31F581308CC6E00D1C2F8948CD5033124B911637
```

"The quick brown fox jumps over the lazy dog"

```
20836D916D121E67915BA85B220B7CC318913C6BBA931F7E750623F908CF44A2FC  
9C4EEAF7C21D9D59DF3EF1CE26617B17E08C20E5AA9DA1F5482016FF4C527D
```

"The quick brown fox jumps over the lazy dog."

```
DDE786B38FB7F340CF9D448BD5B726F7B759BE932484A816F8F4E89DC43395ED8DE  
5F556C7CE38D4C210E2FD602A1D11AA68B28FBE6B006E0288EC53BC31DECC
```

"The quick brown fox jumps over the lazy dof"

```
9A604913D0713EB8599C2EBD1E181389505A5C249753D66CEF85685FEA2968660E19  
0C9AD475478026D6C2BDCA108B424CD4B426F305A3A08AD7C6A3470994ED
```

"fhe quick brown fox jumps over the lazy dog"

```
9FCC0C347869380C5E5520F7582FD8945DA3906B903B45A5BBC38FFF193DF711256C  
9944B3017DE5B506CCCC5F08DA5234A1C8866567316A6DFA5BDEEC618AC7
```

"The quick brown fox Fumps over the lazy dog"

```
EA3DCC7EBC18AFD60B23DA110F6E87A6E04E6B240C8D26256F96AC509ADC07358E8A2  
54A12C34A5CD688B12973C80059ACC11C893EF266AD0D3915AB59BF907B
```

**ДЯКУЮ ЗА УВАГУ !**