# О статистических свойствах последовательностей, формируемых физически неклонируемыми функциями, для использования в механизмах идентификации и аутентификации

Бондаренко А.И., Маршалко Г.Б., Романенков Р.А., Уривский А.В., Щербакова А.О.

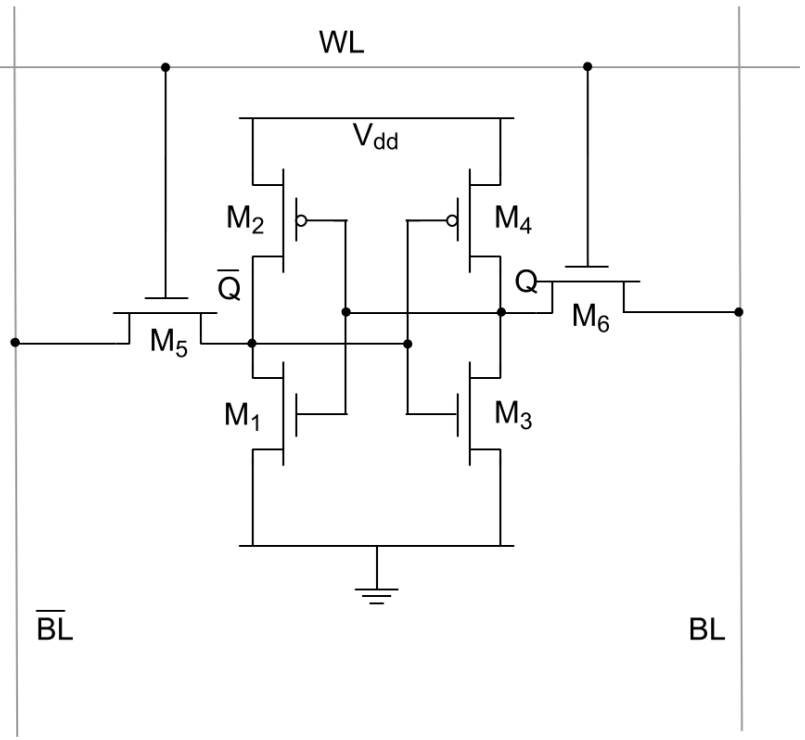
24 марта 2022 г.

# Что такое физически неклонируемая функция (ФНФ)?

- Это функция, такая что ее реализация на конкретном устройстве, существенным образом зависит от физических характеристик этого устройства, определяемых технологическими допусками процесса производства.
- При этом для конкретного устройства некоторые значения функции характеризуются определенной стабильностью, а для различных устройств для одних и тех же входных значений, в целом, различаются.
- Это позволяет использовать данный примитив как для задач идентификации, так и для выработки случайных чисел.

# ФНФ на статической памяти с произвольным доступом (SRAM)

- SRAM - энергозависимая память с произвольным доступом.
- Каждая ячейка памяти имеет свое вероятное состояние при включении.
- ФНФ типа SRAM считывает дампы памяти, которые определяют значение функции для каждого устройства.



# Эксперимент

## Модель

Будем моделировать ФНФ как семейство $\mathbb{A}$ вероятностных автоматов $\mathcal{A}_i = (C, S, X, P_{I,E}, \xi_{I,E})$, где $C, S, X$ – входное множество, множество внутренних состояний, выходное множество $P_{I,E} : C \times S \to S \times X$ – функция поведения ФНФ, $\xi_{I,E}$ – начальное распределение на $S$.

## Параметризация

- I – внутренние параметры (технологические допуски)
- E – внешние параметры (температура, влажность, напряжение)

## ФНФ типа SRAM

$C = \emptyset$, $P_{I,E}(s) = (s, s), s \in S$. То есть поведение ФНФ описывается распределением $\xi_{I,E}$ .

# Эксперимент

## Задача

Задача состоит в описании свойств семейства распределений $\xi_{I,E}$ и проверке гипотез о

- Уникальности, $\forall I \neq I^* \xi_{I,E} \neq \xi_{I^*,E}$

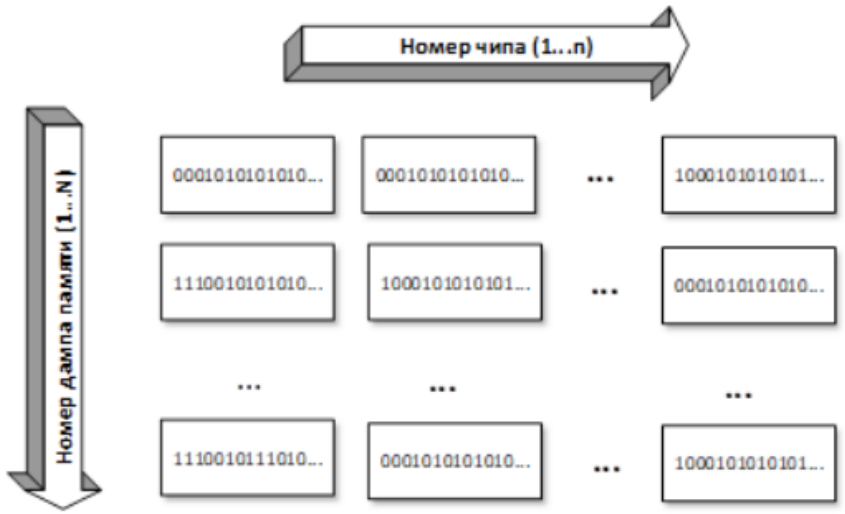
А для конкретного семейства распределений $\xi_i I; *$ проверке гипотез о

- Стабильности, $\forall E \neq E^* \xi_{I,E} = \xi_{I,E^*}$, в том числе конкретных битов: $P(\xi_{I,*}(x) = a) = 1, a = 0, 1$
- Случайности конкретных битов, $P(\xi_{I,*}(x) = a) = 1/2, a = 0, 1$

Такие характеристики рассматриваются в ISO/IEC 20897-1:2020 Information security, cybersecurity and privacy protection — Physically unclonable functions — Part 1: Security requirements

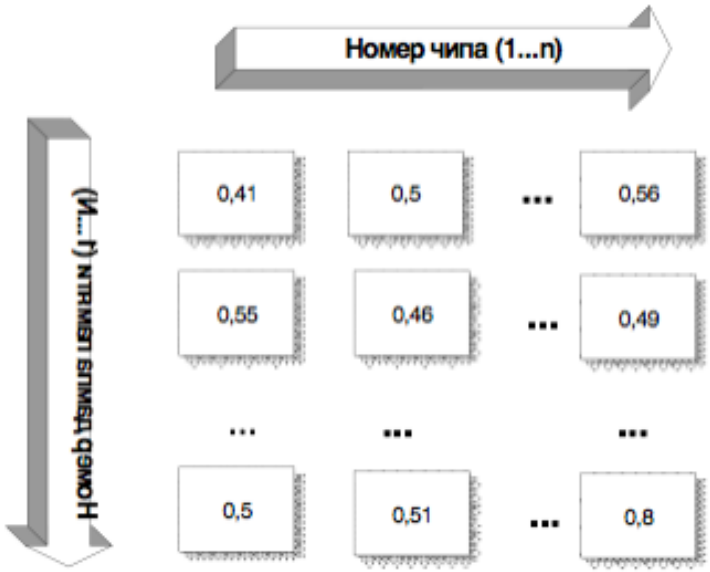
# Эксперимент

- Количество чипов – $n = 20$
- размер дампа памяти – $l = 262144$ бита
- температура окружающей среды – +20; +85
- входное напряжение – 2.7, 3.3, 3.6 V
- общее количество дампов памяти для каждого устройства и на каждый набор условий – $N = 500$



# Среднее арифметическое значение ячеек памяти среди набора дампов памяти одной ФНФ (случайность)

- Для каждого дампа вычислить среднее значение $w(k,j) = \frac{1}{l}\sum_{i=1}^{l} x_i^{k,j}, k = 1,...,n, j = 1,...,N$
- Вычислить среднее для каждого столбца $w(k) = \frac{1}{N}\sum_{i=1}^{N} w(k,j)$
- В предположении о случайности и равновероятности битов в дампах проверить принадлежность значения интервалу, определяемом правилом «3-х сигм»



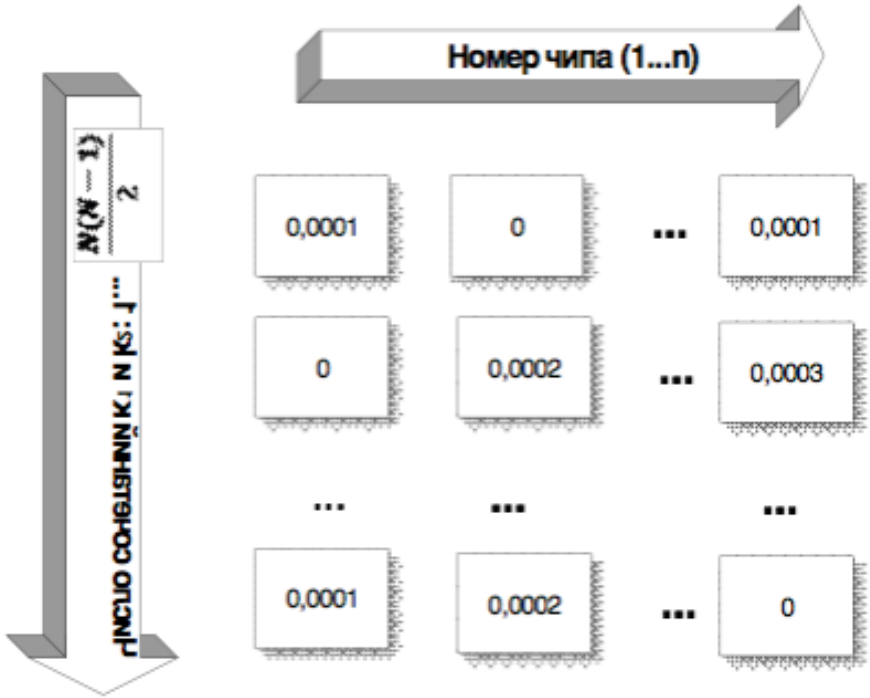
# Внутреннее расстояние между ячейками памяти среди набора дампов памяти одной ФНФ (случайность)

| Номер чипа | Выборочное среднее и выборочная дисперсия | | |
|---|---|---|---|
| | V=2,7В | V=3,3В | V=3,6В |
| 1 | 0.50146072<br>0.000000092118 | 0.50150923<br>0.000000087895 | 0.50137165<br>0.000000084968 |
| 2 | 0.50071073<br>0.000000060286 | 0.50064802<br>0.000000056856 | 0.50061232<br>0.000000055518 |
| 3 | 0.49884998<br>0.000000066712 | 0.49884940<br>0.000000066384 | 0.49874670<br>0.000000063403 |
| 4 | 0.49560645<br>0.000000074413 | 0.49564218<br>0.000000081667 | 0.49584036<br>0.000000065499 |

Результат слабо зависит от напряжения и температуры (стабильность)

# Внутреннее расстояние между ячейками памяти среди набора дампов памяти одной ФНФ (уникальность)

- Для каждого чипа вычислить значения $v(k, j_1, j_2) = \frac{||x_i^{k,j_1} \oplus x_i^{k,j_2}||}{l}, k = 1, ..., n, j_1, j_2 = 1, ..., N$ и записать их в таблицу
- Вычислить среднее для каждого столбца $w_v(k) = \frac{2}{N(N-1)} \sum_{i=1}^{N(N-1)/2} v(k, j_1, j_2)$
- Проверить по правилу «3-х сигм»



# Внутреннее расстояние между ячейками памяти среди набора дампов памяти одной ФНФ (уникальность)

| Номер чипа | Внутренние расстояния: выборочное среднее и выборочная дисперсия | | |
|---|---|---|---|
| | V=2,7B | V=3,3B | V=3,6B |
| 1 | 0.05906259<br>0.000002281870 | 0.05447963<br>0.000003854626 | 0.06518235<br>0.000003293177 |
| 2 | 0.05918106<br>0.000001566328 | 0.05741587<br>0.000002626647 | 0.04953285<br>0.000007457934 |
| 3 | 0.04879665<br>0.000006580269 | 0.05643666<br>0.000003256706 | 0.06154798<br>0.000002290288 |

Рис.: $t = 20$

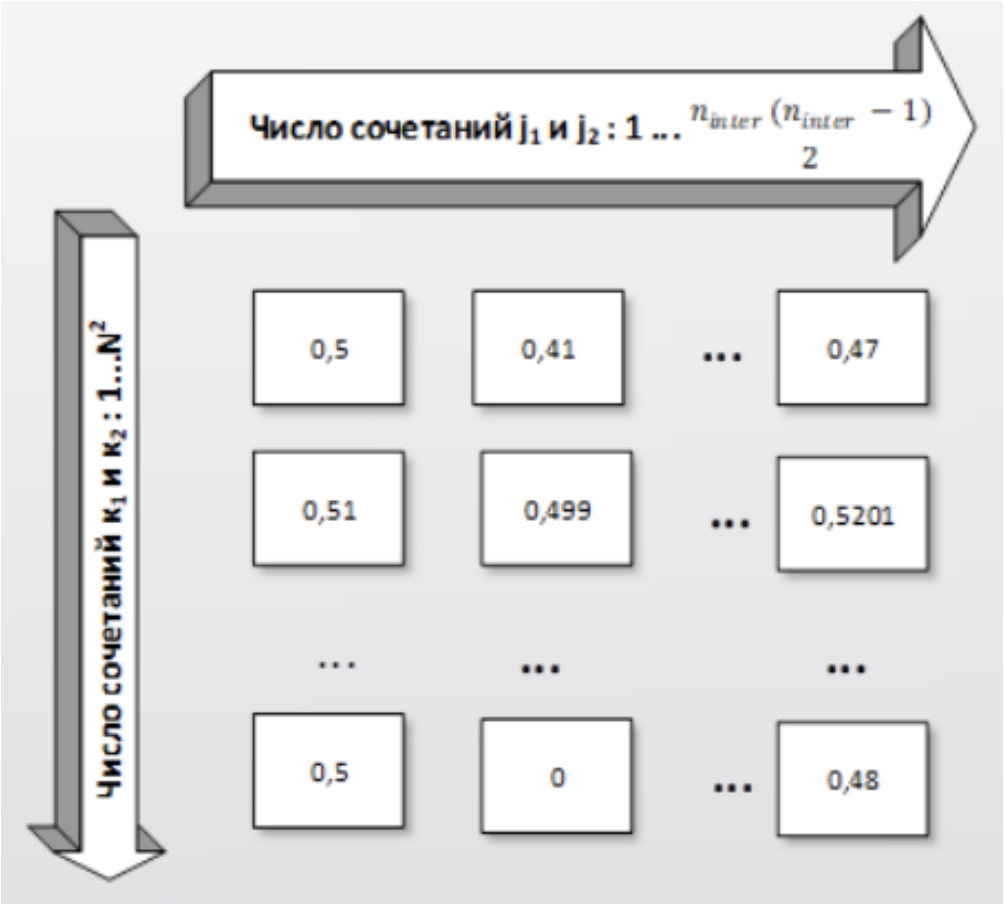
| Номер чипа | Внутренние расстояния: выборочное среднее и выборочная дисперсия | | |
|---|---|---|---|
| | V=2,7B | V=3,3B | V=3,6B |
| 1 | 0.04627226<br>0.000000808308 | 0.04688653<br>0.000001419718 | 0.04549836<br>0.000000622746 |
| 2 | 0.03043424<br>0.000000495024 | 0.03034042<br>0.000000690844 | 0.03081065<br>0.000000546972 |
| 3 | 0.03260373<br>0.000000508577 | 0.03302181<br>0.000000845546 | 0.03350127<br>0.000000506031 |
| 4 | 0.03778450<br>0.000000963293 | 0.03803549<br>0.000001376060 | 0.03872527<br>0.000000923761 |

Рис.: $t = 85$

Результат значимо зависит от внешних условий (нестабильность)

# Внешнее расстояние между ячейками дампов памяти различных ФНФ (уникальность)

- Для каждого чипа вычислить значения $ex(k_1, k_2, j_1, j_2) = \frac{||x_i^{k_1,j_1} \oplus x_i^{k_2,j_2}||}{l}, k_1, k_2 = 1, ..., n, j_1, j_2 = 1, ..., N$ и записать их в таблицу
- Вычислить среднее для каждого столбца $w_{ex}(j_1, j_2) = \frac{1}{N^2} \sum_{i=1}^{N^2} ex(k_1, k_2, j_1, j_2)$
- Проверить по правилу «3-х сигм»



# Внешнее расстояние между ячейками дампов памяти различных ФНФ (уникальность)

| Номера чипов | Внешнее расстояние: выборочное среднее и выборочная дисперсия | | |
|---|---|---|---|
| | V=2,7B | V=3,3B | V=3,6B |
| 1,2 | 0.4633703075<br>0.000000152145 | 0.4631401058<br>0.000000137501 | 0.4635545975<br>0.000000142796 |
| 1,3 | 0.4577461754<br>0.000000133674 | 0.4577085335<br>0.000000155281 | 0.4578909628<br>0.000000146274 |
| 1,4 | 0.4670000881<br>0.000000138238 | 0.4670570770<br>0.000000152303 | 0.4670326313<br>0.000000141687 |
| 2,3 | 0.3785835445<br>0.000000111257 | 0.3786007230<br>0.000000120847 | 0.3782223327<br>0.000000129675 |
| 2,4 | 0.4859901595<br>0.000000128478 | 0.4860412492<br>0.000000124481 | 0.4862277456<br>0.000000128079 |
| 3,4 | 0.4764103460<br>0.000000133213 | 0.4764334323<br>0.000000146427 | 0.4767964090<br>0.000000141825 |

Рис.: $t = 20$

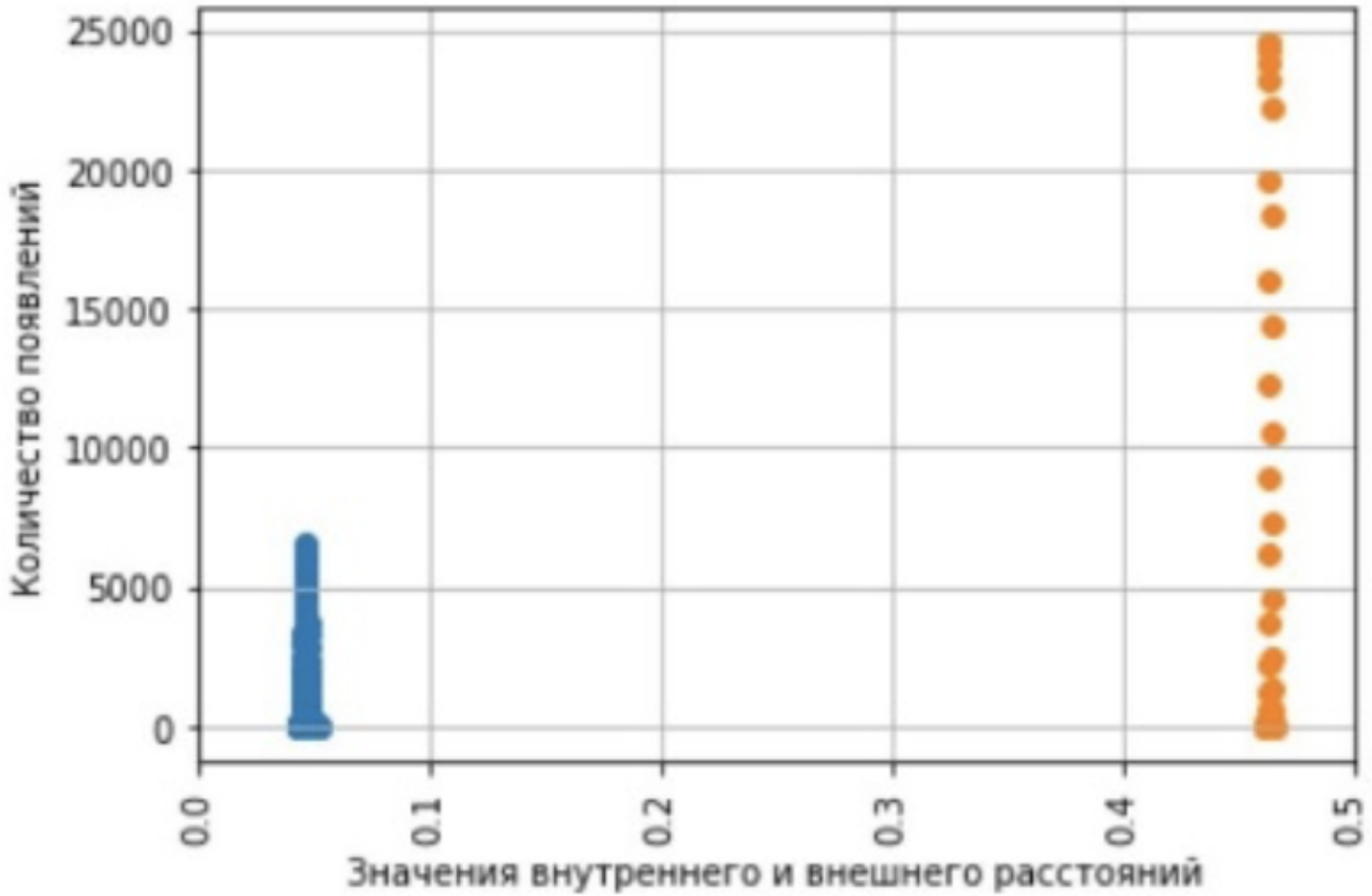
| Номера чипов | Внешнее расстояние: выборочное среднее и выборочная дисперсия | | |
|---|---|---|---|
| | V=2,7B | V=3,3B | V=3,6B |
| 1,2 | 0.4545829845<br>0.000000206244 | 0.4547041212<br>0.000000213804 | 0.4542667564<br>0.000000207752 |
| 1,3 | 0.4508166418<br>0.000000212451 | 0.4513289223<br>0.000000198740 | 0.4513080935<br>0.000000234680 |
| 2,3 | 0.4170767057<br>0.000000321377 | 0.4176572246<br>0.000000348043 | 0.4169089552<br>0.000000467793 |

Рис.: $t = 85$

Результат значимо зависит от внешних условий (нестабильность)

# Уникальность

Внешнее и внутреннее расстояние позволяет эффективно различать последовательности, полученные от одного и разных чипов (даже при изменяющихся условиях – вске-таки стабильность)



# Стабильность/случайность подробнее

- в исходной матрице $w$ ищем биты (почти) константные – это стабильные биты (такие есть)
- удаляем стабильные биты
- для каждого набора параметров анализируем последовательности с помощью критериев согласия из набора статистических критериев

# Случайность

- пересекающиеся 3,4,5-граммы
- ранг матриц
- серий
- случайное блуждание
- непопадания в заданный диапазон (6 вариантов)
- стопка книг
- монотонности

| Чип | Напряжение | Тест 1 | Тест 2 | Тест 3 | Тест 4 | Тест 5 | Тест 6 | Тест 7 | Тест 8 | Тест 9 | Тест 10 | Тест 11 | Тест 12 | Тест 13 | Тест 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 27 | 0.84 | 0.97 | 0.70 | 0.96 | 1.00 | 0.00 | 0.65 | 0.36 | 0.88 | 0.92 | 0.94 | 0.98 | 0.96 | 0.93 |
| | 33 | 0.98 | 0.83 | 0.83 | 0.95 | 1.00 | 0.00 | 0.31 | 0.67 | 0.43 | 0.85 | 0.98 | 1.00 | 0.94 | 0.93 |
| | 36 | 0.97 | 0.93 | 0.50 | 0.96 | 1.00 | 0.00 | 0.36 | 0.64 | 0.89 | 0.75 | 0.97 | 1.00 | 0.92 | 0.94 |
| 2 | 27 | 0.92 | 0.97 | 0.91 | 0.97 | 1.00 | 1.00 | 0.94 | 0.94 | 0.97 | 0.98 | 0.99 | 1.00 | 0.96 | 0.90 |
| | 33 | 0.96 | 0.93 | 0.94 | 0.96 | 1.00 | 0.99 | 0.97 | 0.98 | 0.97 | 0.96 | 0.98 | 1.00 | 0.97 | 0.96 |
| | 36 | 0.61 | 0.98 | 0.90 | 0.95 | 1.00 | 1.00 | 0.97 | 0.93 | 0.99 | 0.92 | 0.96 | 1.00 | 0.97 | 0.92 |
| 3 | 27 | 0.96 | 0.97 | 0.90 | 0.97 | 1.00 | 1.00 | 0.97 | 0.97 | 0.98 | 0.99 | 0.99 | 1.00 | 0.93 | 0.95 |
| | 33 | 0.99 | 0.87 | 0.95 | 0.96 | 1.00 | 0.99 | 0.98 | 0.95 | 0.98 | 0.88 | 0.98 | 0.99 | 0.97 | 0.94 |
| | 36 | 0.92 | 0.98 | 0.70 | 0.97 | 1.00 | 0.99 | 0.90 | 0.73 | 0.98 | 0.97 | 0.99 | 1.00 | 0.98 | 0.96 |
| 4 | 27 | 0.89 | 0.94 | 0.83 | 0.93 | 1.00 | 1.00 | 0.91 | 0.97 | 0.99 | 0.91 | 0.98 | 1.00 | 0.98 | 0.95 |
| | 33 | 0.96 | 0.93 | 0.95 | 0.96 | 1.00 | 0.99 | 0.93 | 0.94 | 0.99 | 0.97 | 0.99 | 1.00 | 0.97 | 0.95 |
| | 36 | 0.96 | 0.99 | 0.72 | 0.97 | 1.00 | 1.00 | 0.92 | 0.98 | 0.99 | 0.96 | 1.00 | 1.00 | 0.96 | 0.98 |

Задача проверки случайности требует более глубокого исследования

# Выводы

- Предложена теоретико-вероятностная формализация задачи оценки характеристик ФНФ
- Предложен статистический эксперимент по оценке характеристик ФНФ
- Для ФНФ типа SRAM данный эксперимент позволил
  - Подтвердить гипотезу об уникальности
  - Показать зависимость значений некоторых характеристик от внешних параметров
  - Позволил выявить стабильные биты
  - Не позволил подтвердить гипотезу о случайности оставшихся битов