КРИПТОНИТ

Физически неклонируемые функции в криптографии

Чичаева Анастасия

Физически неклонируемые функции

Физически неклонируемые функции (ФНФ)
от англ. Physical Unclonable Functions, PUF

Интернет вещей

ПЛИС

Датчики, микроконтроллеры

Определение физически неклонируемой функции

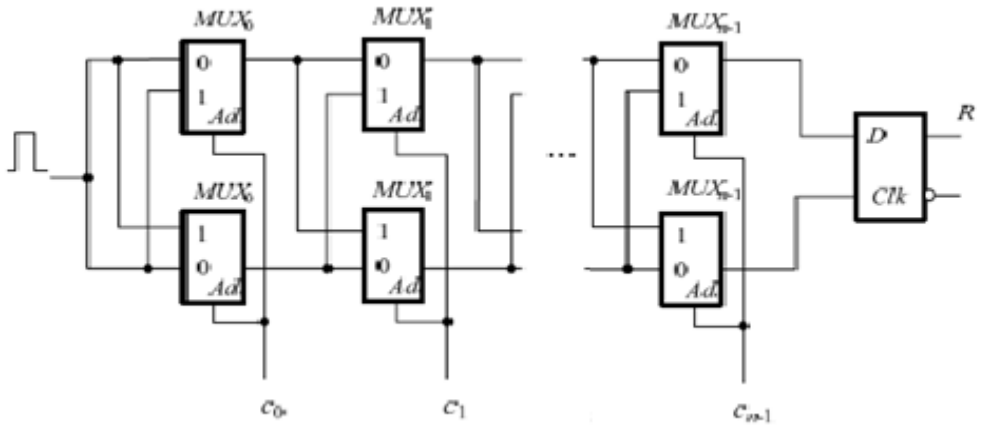
- $\boldsymbol{P}$ – класс ФНФ
- $\boldsymbol{P}.Create$ – алгоритм создания экземпляров класса $\boldsymbol{P}$
- puf_i – экземпляр ФНФ
- $puf_i(x)$ – состояние экземпляра ФНФ, соответствующее запросу x
- $puf_i(x).Eval$ – процедура оценки состояния экземпляра ФНФ
- $Y_i\ (x)$ – ответ экземпляра ФНФ puf_i на запрос x.

Свойства классов физически неклонируемых функций:

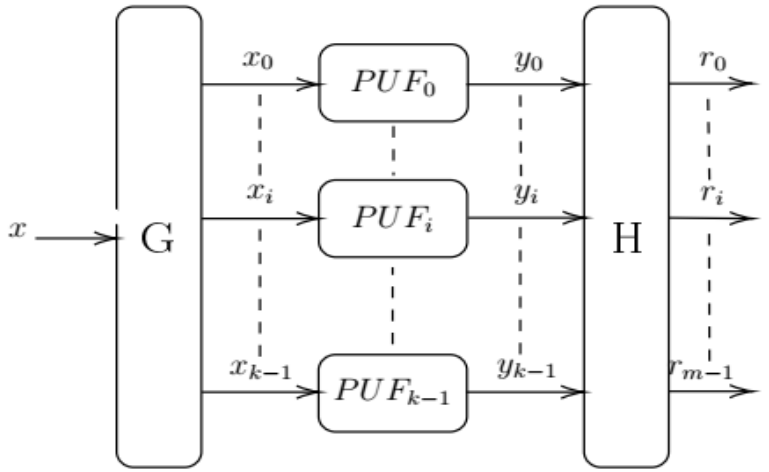
- Конструируемость
- Оцениваемость
- Воспроизводимость
- Уникальность
- **Идентифицируемость**
- **Физическая неклонируемость**

Классы ФНФ, реализуемые в цифровых устройствах

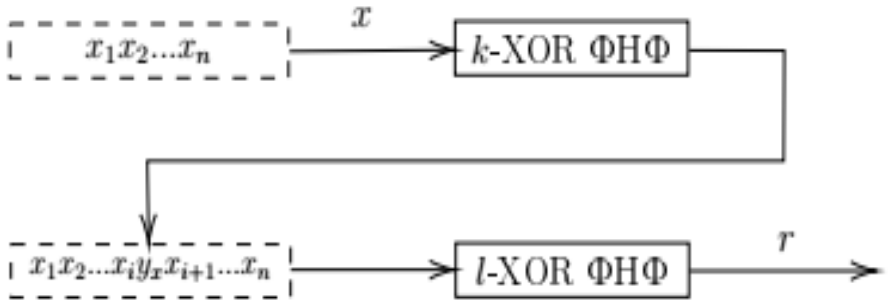
- ФНФ по типу арбитр
- ФНФ на базе кольцевых генераторов
- ФНФ на основе элементов памяти
- Комбинации ответов экземпляров ФНФ



ФНФ-арбитр

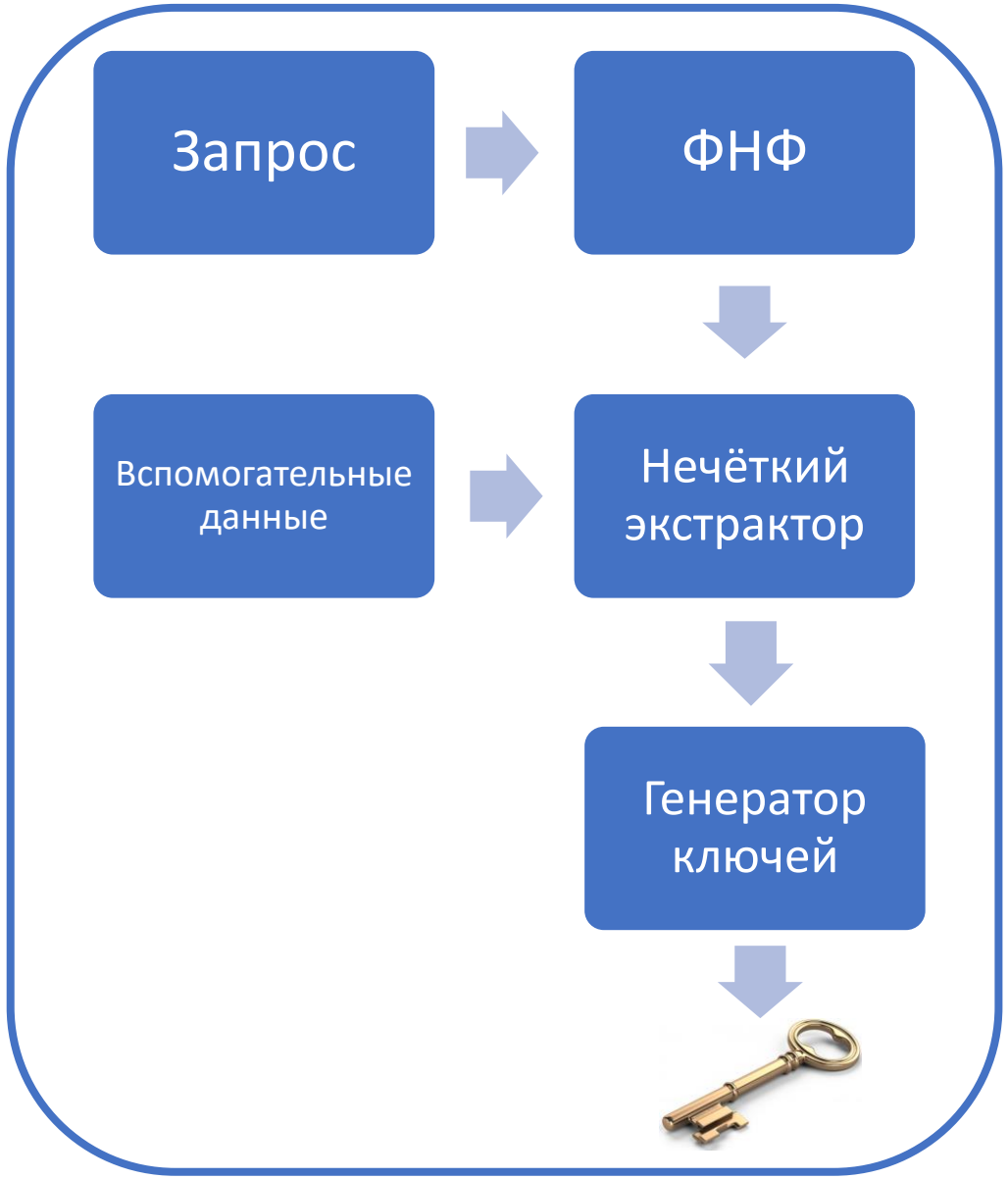


Лёгкая ФНФ



Промежуточная ФНФ

Генерация случайных параметров на основе ФНФ



Нечёткий экстрактор

- $Gen(y) = (h, k)$
- $Rep(y', h) = k$

Защищенный эскиз

- $SS(y) = h$
- $Rec(y', h) = y$

Протоколы аутентификации на основе ФНФ. Парольная аутентификация

	Клиент	аутентифицирует ⟵	Сервер
1	$y \leftarrow PUF()$		
		$y \longrightarrow$	
			$(k, h) \leftarrow Gen(y)$
∞			$n \leftarrow TRNG()$
		$\longleftarrow n, h$	
	$y' \leftarrow PUF()$		
	$k' \leftarrow Rep(y', h)$		
	$a \leftarrow I_{k'}(n)$		
		$a \longrightarrow$	
			Ошибка, если $a \neq I_k(n)$

- Протокол Садэги А.Р. и др [1]
- Протокол с перевернутым нечётким экстрактором [2]

[1] Sadeghi A. R., Visconti I., Wachsmann C. Enhancing RFID security and privacy by physically unclonable functions

[2] Maes R. Physically Unclonable Functions: Constructions, Properties and Applications (Fysisch onkloonbare functies: constructies, eigenschappen en toepassingen)

Протоколы аутентификации на основе запросов и ответов ФНФ

	Клиент А	аутентифицирует ⟵	Сервер
1 g			$c_i \leftarrow TRNG()$
		$\xleftarrow{c_i}$	
	$y_i \leftarrow PUF(c_i)$		
		$\xrightarrow{y_i}$	
			$g_A \leftarrow g$
g			$i \leftarrow g_A$
			$(c, y) \leftarrow (c_i, y_i)$
			$g_A \leftarrow g_A - 1$
		$\xleftarrow{c}$	
	$y' \leftarrow PUF(c)$		
		$\xrightarrow{y'}$	
			Ошибка, если $HD(y, y') > \epsilon$

- Контролируемые протоколы на основе ФНФ [3]
- Низкоресурсный протокол на основе ФНФ [4]
- Протоколы блокировки на основе ФНФ [5]

[3] Gassend B. et al. Controlled physical random functions and applications .
[4] Majzoobi M. et al. Slender PUF protocol: A lightweight, robust, and secure authentication by substring matching.
[5] Yu M. D. et al. A lockdown technique to prevent machine learning on PUFs for lightweight authentication.

Атаки, моделирующие ФНФ на основе машинного обучения

Тип конструкции	Число пар запрос-ответ для обучения	Успешность атаки (%)	Время обучения
Лёгкая ФНФ-арбитр (5-XOR)	1 200 000	96.22	3 часа 11 мин
(4,4)-промежуточная ФНФ-арбитр	647 000	97.68	32 мин 17 с
5-XOR ФНФ-арбитр	655 000	97.87	29 мин 21 с
Лёгкая ФНФ-арбитр (6-XOR)	800 000	97.42	33 мин 24 с
6-XOR ФНФ-арбитр	680 000	97.68	20 мин 52 с
(4,4)-промежуточная ФНФ-арбитр	320 000	97.44	5 мин 23 сек

Выводы

- В настоящее время ФНФ используются в программируемых логических интегральных схемах (ПЛИС) и в устройствах Интернета вещей в качестве встроенного неклонируемого идентификатора устройства и для генерации ключей.

- Физически неклонируемые функции являются перспективными для использования в устройствах с ограниченными ресурсами в отношении **выработки случайных значений**, не сохраняющихся в памяти.

- Большинство предложенных на данный момент физически неклонируемых функций имеют ряд эксплуатационных недостатков и уязвимы к атакам на основе методов машинного обучения.

КРИПТОНИТ

Спасибо за внимание!

Чичаева Анастасия,

Электронная почта: a.chichaeva@kryptonite.ru