

ПРОЕКТИРОВАНИЕ КОМПАКТНОГО РЕКОНФИГУРИРУЕМОГО RUF-КОНТРОЛЛЕРА

Трубач К.И., Иванюк А.А.

Минск, 2026

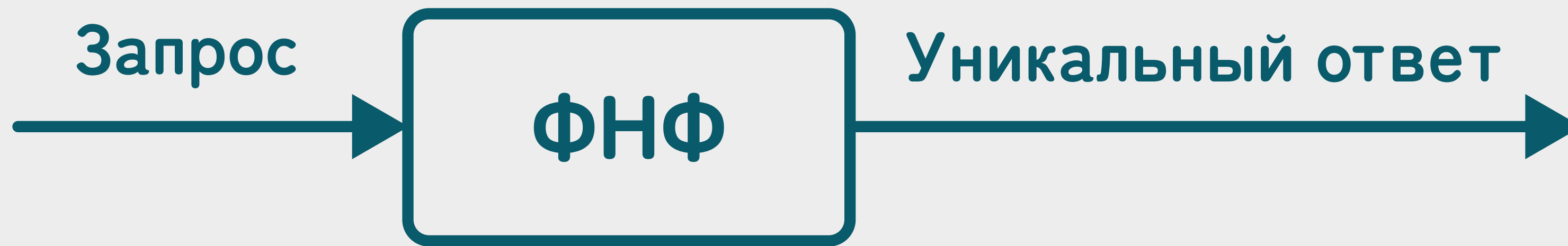
Работа выполнена в совместной
учебной лаборатории БГУИР-YADRO

EDA
Conference



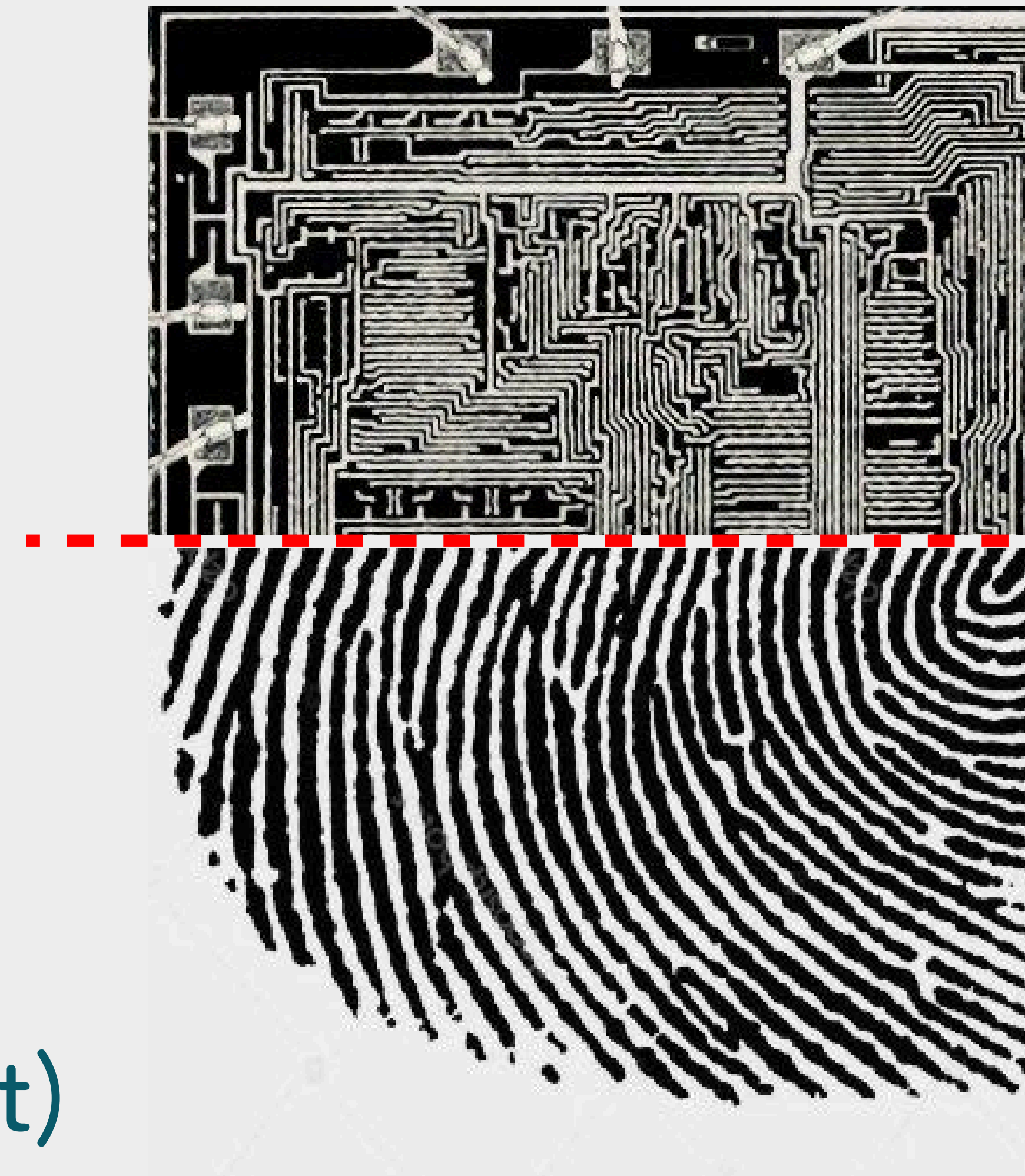
ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫЕ ФУНКЦИИ В IOT

ФНФ – цифровые схемы, чувствительные к неизбежным технологическим разбросам при производстве кристаллов.

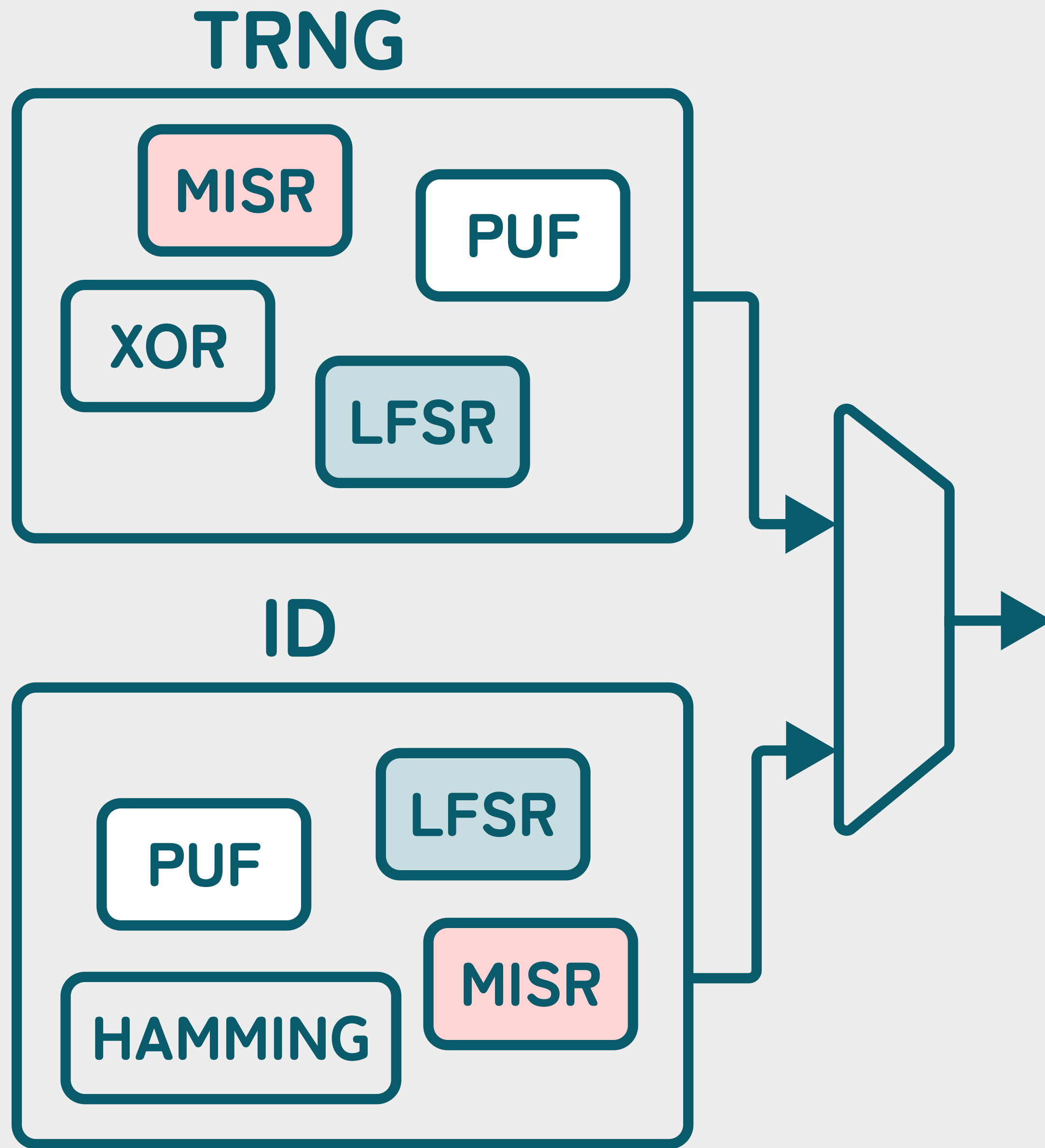


Применение в IoT:

- + аутентификация устройств
- + генерация криптографических ключей
- + создание корней доверия (Root of Trust)
- + генерация случайных чисел



ПРОБЛЕМА АППАРАТНОЙ ИЗБЫТОЧНОСТИ ФНФ-СИСТЕМ

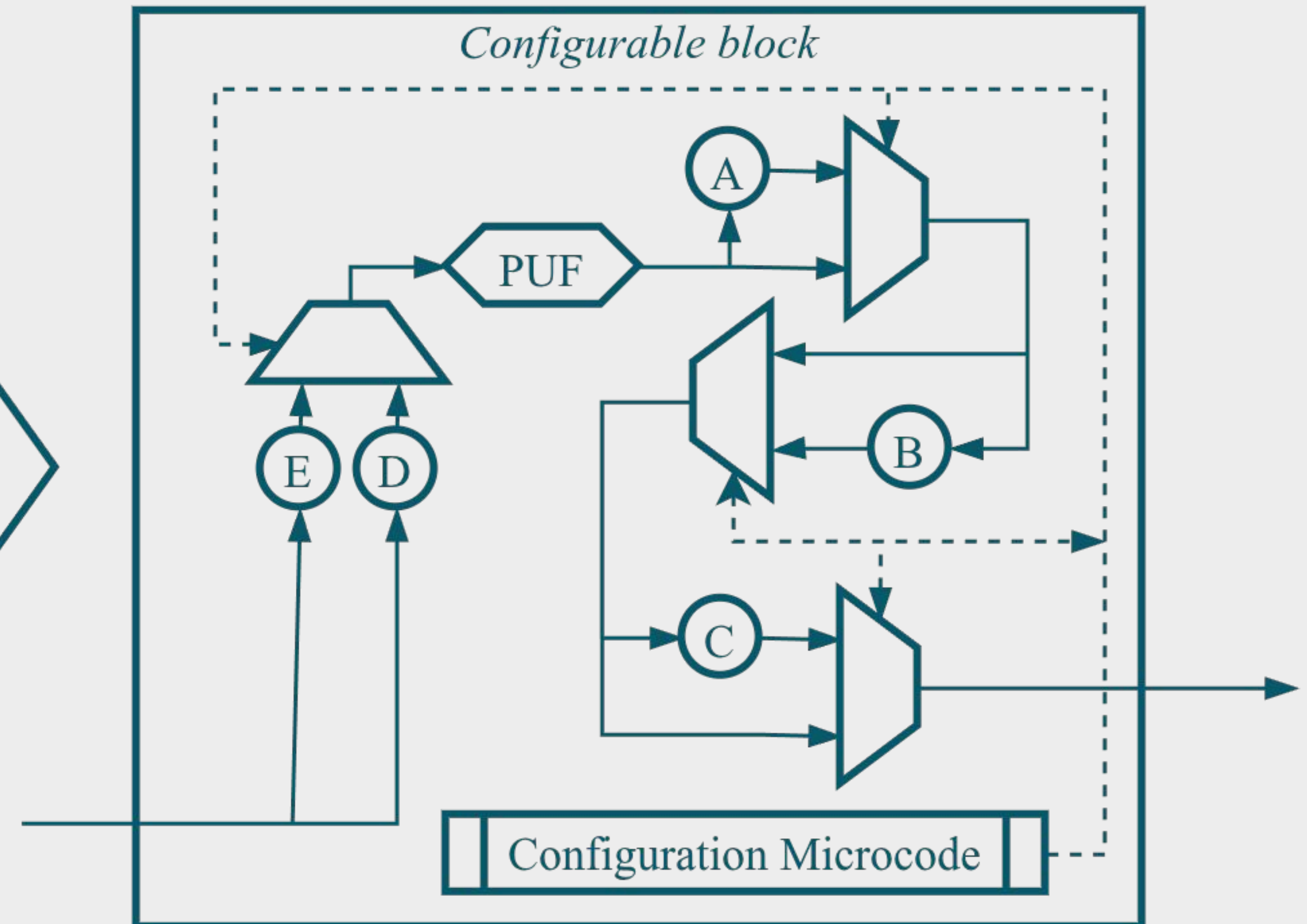
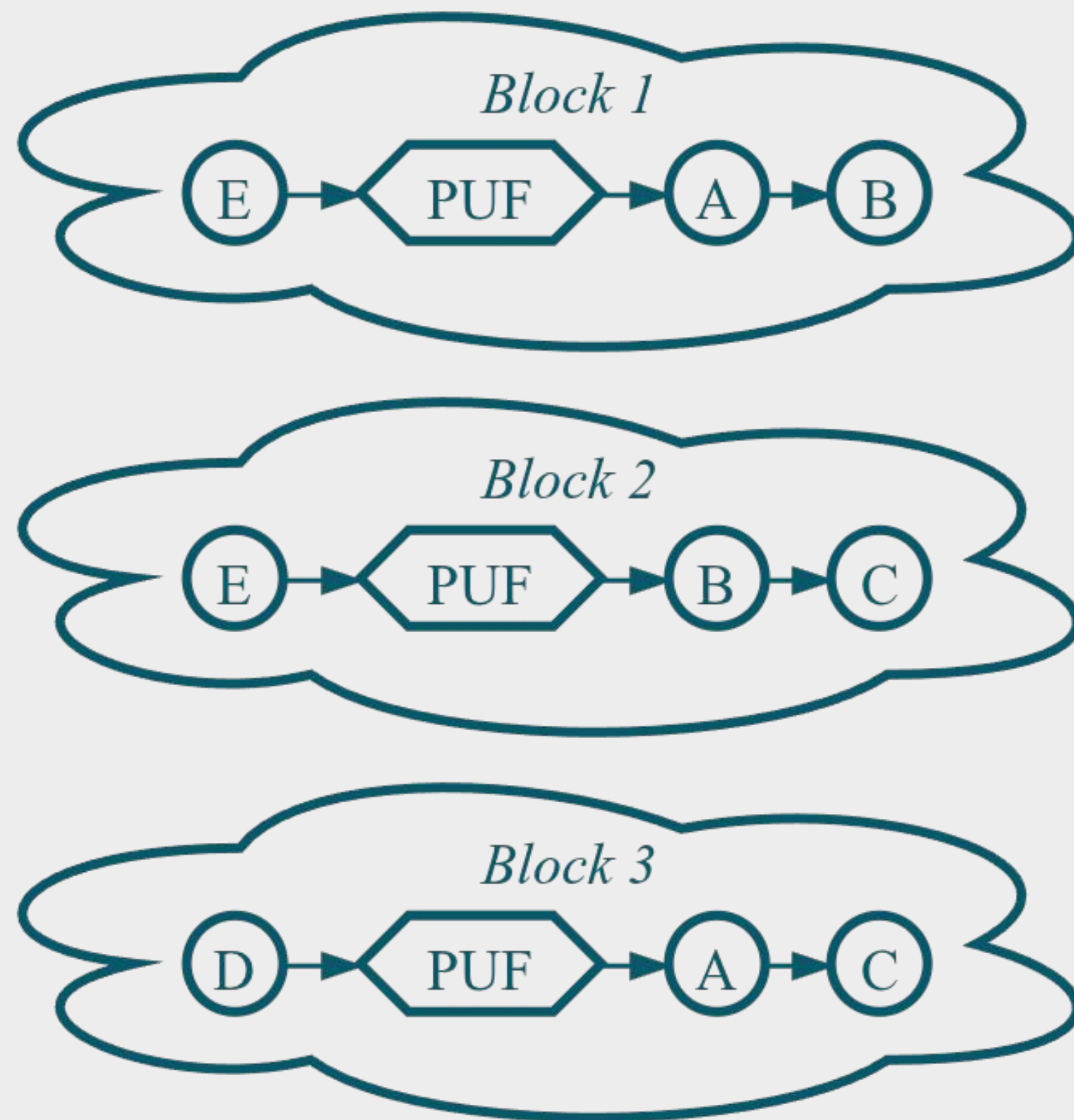


Мультиплексирование полных блоков:

- + простое решение
- рост площади кристалла
- невозможность модификации алгоритмов без полного перепроектирования аппаратуры

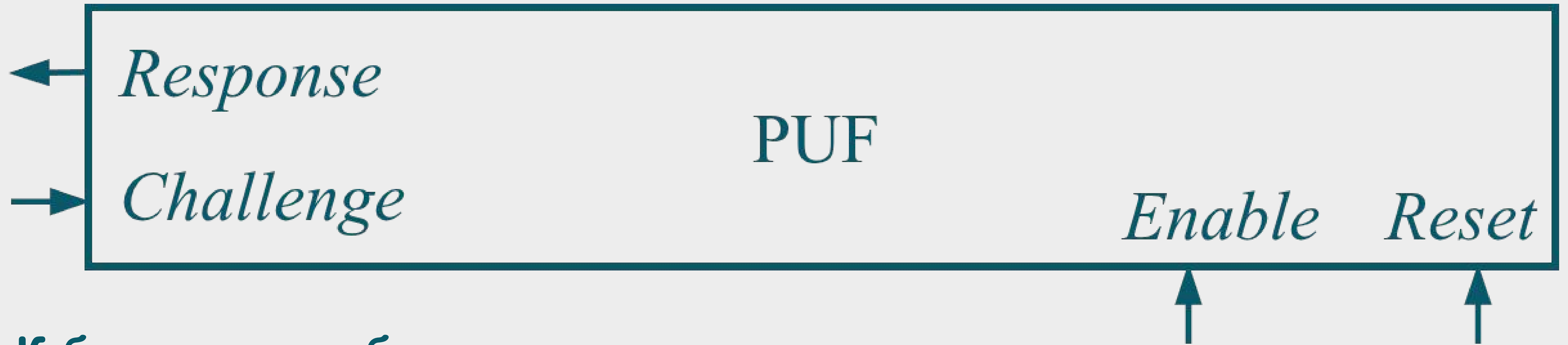
ЦЕЛЬ РАБОТЫ И ПРЕДЛАГАЕМЫЙ ПОДХОД

Цель – снизить аппаратные затраты на управление PUF в IoT-устройствах, сохранив функциональную гибкость.



Решение – выделение общих вычислительных примитивов в единый микропрограммируемый реконфигурируемый блок АЛУ.

МОДЕЛЬ ИНТЕРФЕЙСА И ТРЕБОВАНИЯ К КОНТРОЛЛЕРУ



К базовым требованиям относятся:

- + общий интерфейс к ФНФ для простой интеграции любого типа ФНФ
- + реализация приложения идентификации
- + реализация приложения генерации случайных чисел
- + сокращение площади по сравнению с отдельной реализацией

АЛГОРИТМИЧЕСКИЙ АНАЛИЗ ПРИЛОЖЕНИЙ

Функции охватывают оба этапа жизненного цикла PUF: обучение (формирование Helper Data) и использование.

Постобработка Response:

- + восстановление данных (мажоритарное декодирование, коды Хэмминга, коды BCH)
- + сжатие в сигнатуру (одно- и многовходовые анализаторы SISR/MISR)
- + скремблирование бит через LFSR

Формирование Challenge:

- + линейный перебор с заданным шагом
- + псевдослучайная генерация (M-последовательности, некриптографический хэш djb2)

АНАЛИЗ СТРУКТУРНОЙ ОБЩНОСТИ АЛГОРИТМОВ

ФУНКЦИЯ	LFSR	СУММАТОРЫ	ХОР-ДЕРЕВО	ЭЛЕМЕНТЫ ПАМЯТИ
ГЕНЕРАЦИЯ ЧИСЛА ЛИНЕЙНО С ШАГОМ		+		+
ХЭШ-ФУНКЦИЯ	+	+	+	+
МАЖОРИТАРНОЕ ДЕКОДИРОВАНИЕ				
СЖАТИЕ СИГНАТУРНЫМ АНАЛИЗАТОРОМ	+		+	
ПЕРЕСТАНОВКА БИТ	+			+
КОДЫ ВСН	+			
КОДЫ ХЭММИНГА			+	

ОЦЕНКА ЭФФЕКТИВНОСТИ НА ЭТАПЕ МОДЕЛИРОВАНИЯ



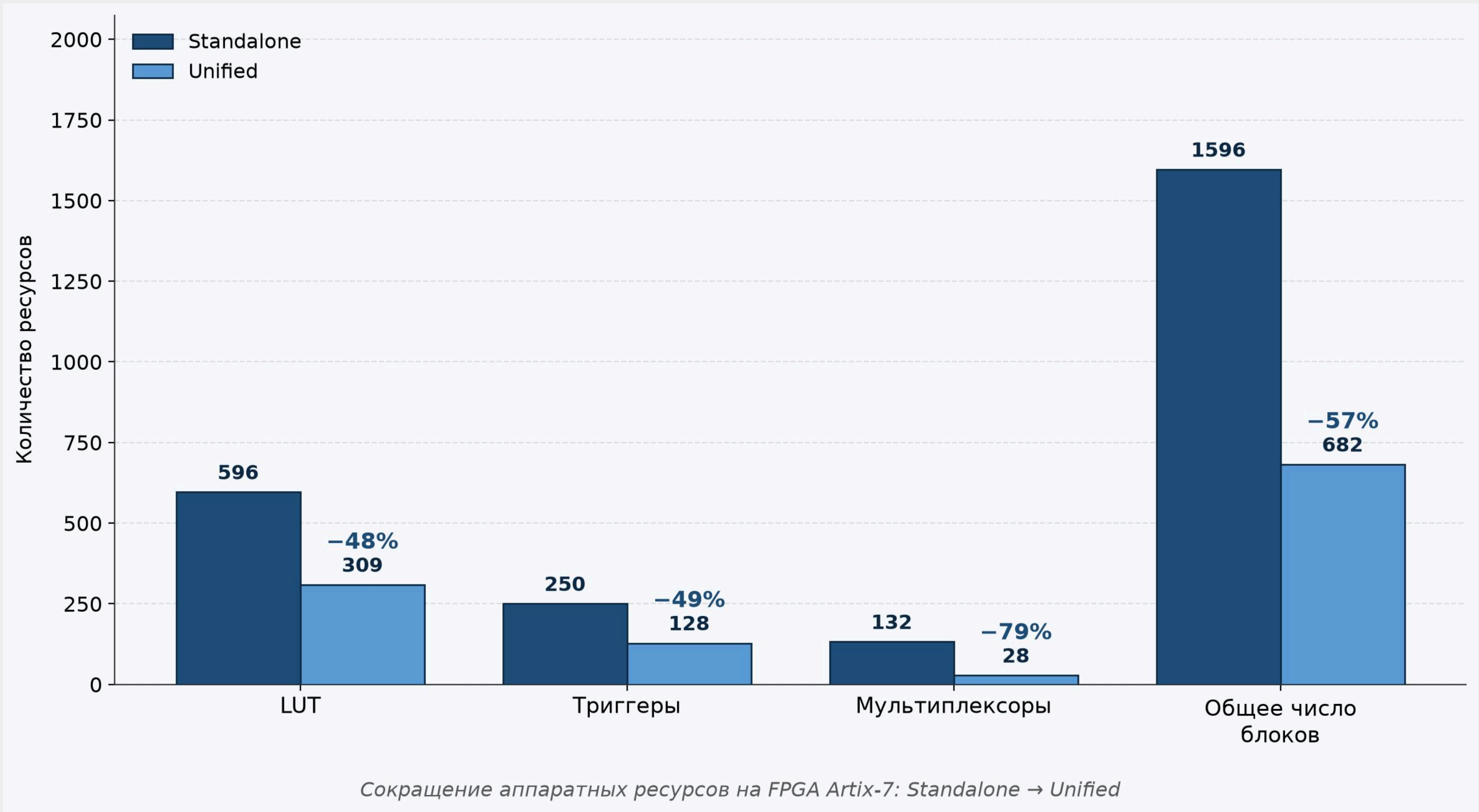
СРАВНЕНИЕ АППАРАТНЫХ ЗАТРАТ НА FPGA ARTIX-7

На FPGA Artix-7 синтезированы два варианта системы:

1. Standalone: независимое инстанцирование всех специализированных модулей (традиционный подход).
2. Unified (предложенный): унифицированный микропрограммируемый блок АЛУ с единым управляемым трактом данных.

Ресурс	Standalone	Unified	Сокращение ресурсов
LUT	596	309	48%
Триггеры	250	128	49%
Мультиплексоры	132	28	79%
Общее число блоков	1596	682	57%

АНАЛИЗ РЕЗУЛЬТАТОВ ЭКСПЕРИМЕНТА



ИТОГИ РАБОТЫ И ДАЛЬНЕЙШИЕ ИССЛЕДОВАНИЯ

Основные результаты:

- доказана состоятельность идеи микропрограммируемого PUF-контроллера;
- обеспечено масштабируемое добавление функций через обновление прошивки микрокода без перепроектирования и верификации аппаратуры.

Направления дальнейших исследований:

- интеграция реального физического PUF-ядра и внешних интерфейсов в единый контроллер;
- синтез в ASIC для точной оценки статического и динамического энергопотребления на низкопотребляющих библиотеках;
- оценка производительности решения;
- поиск оптимального разбиения функций на более простые.

СПАСИБО ЗА ВНИМАНИЕ