СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПОТОКОВЫХ ШИФРОВ TRIVIUM, GRAIN-128A И MICKEY 2.0: ВЫБОР РЕШЕНИЙ ДЛЯ УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ

Худайкулов Зариф Туракулович
PhD, доцент, заведующий кафедрой «Криптология» Ташкентского университета информационных технологий имени Мухаммада ал-Хоразми
E-mail: zarif.khudoykulov@tuit.uz , Тел.: +998 (97) 729-60-47
Хамраев Ахрор Кушбой угли
магистр 1-го курса, факультет Магистратуры, специальность Криптография и криптоанализ», Ташкентского университета информационных технологий имени Мухаммада ал-Хоразми
E-mail: 1810010ak001@gmail.com, Тел.: +998 (99) 919-51-73

Qabul qilindi: 11.12.2025
Ko‘rib chiqildi: 12.12.2025
Tasdiqlandi: 13.12.2025

Актуальность. Рост числа IoT-устройств и объёмов передаваемых ими данных повышает требования к защите конфиденциальности и целостности. Ограниченные ресурсы большинства IoT-платформ (память, процессор, энергия) требуют применения лёгких криптографических примитивов. Потоковые шифры остаются одним из наиболее подходящих подходов для таких устройств, однако выбор конкретного алгоритма должен базироваться на сопоставлении безопасности, затрат ресурсов и удобства реализации в реальных условиях.

Степень научной разработанности проблемы. Проблема лёгкой криптографии активно исследуется в рамках проектов eSTREAM и NIST (lightweight crypto). Trivium, Grain-128a и MICKEY 2.0 получили широкую поддержку в литературе как образцы лёгких потоковых шифров; имеются публикации по их аппаратной реализации, энергоэффективности и криптоанализу. Тем не менее сравнительные исследования, ориентированные конкретно на практические ограничения IoT-плат, остаются востребованными.

(Ключевые источники: eSTREAM, спецификация Trivium, описание Grain-128a, исследования по MICKEY 2.0.)

Цель исследования. Определить сильные и слабые стороны Trivium, Grain-128a и MICKEY 2.0 с позиции применимости в типичных сценариях IoT и предложить рекомендации для выбора алгоритма при разработке потокового шифра для магистерского проекта.

Источниковая (эмпирическая) база исследования. Аналитический обзор официальной документации eSTREAM и публикаций (2006–2023), отчётов по аппаратным реализациям (FPGA/MCU), результаты экспериментальных оценок производительности и требования к памяти из открытых исследований.

Основные тезисы

1. **Потоковые шифры остаются предпочтительным выбором** для передачи коротких и частых сообщений в IoT благодаря низкой задержке и простоте потоковой обработки.

2. **Trivium** демонстрирует оптимальный баланс скорости и простоты реализации: низкие аппаратные затраты и хорошая криптостойкость, что делает его универсальным кандидатом для магнитных и бытовых IoT-плат.

3. **Grain-128a** выгодно отличается поддержкой встроенной аутентификации (MAC), что повышает защищённость протоколов передачи, но требует немного больших вычислительных и памятных ресурсов.

4. **MICKEY 2.0** ориентирован на минимизацию памяти и энергорасхода; подходит для «ультра-лёгких» устройств, но требует аккуратной инициализации и контроля реализации.

5. **Выбор алгоритма должен определяться сценариями использования**: при ограниченной памяти — MICKEY, при необходимости аутентификации и повышенной безопасности — Grain-128a, при универсальной скорости и простоте — Trivium.

6. **Аппаратная оптимизация и валидация на реальных платах** критически важны: показатели теоретической эффективности часто отличаются от результатов на конкретных MCU/FPGA.

7. **Криптостойкость всех трёх шифров соответствует современным требованиям**, но реализация и защита от боковых каналов накладывают дополнительные проектные ограничения.

Краткое описание методики. Сопоставление алгоритмов проводилось по формализованным критериям: структура внутреннего состояния, длина ключа/IV, требования к памяти и времени, сложность аппаратной реализации, устойчивость к известным видам атак. Данные были собраны из технических спецификаций и результатов экспериментальных работ в литературе.

Выводы. Проведённый сравнительный анализ подтверждает применимость всех трёх шифров в средах IoT, однако для магистерского проекта автора оптимальным выбором является **Trivium** как наиболее сбалансированное решение для дальнейших модификаций и аппаратной реализации. Grain-128a рекомендуется при строгих требованиях к аутентификации, а MICKEY 2.0 — в условиях крайней экономии памяти и

энергии. Для окончательного выбора необходима прототипная реализация и измерения на целевых платах.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. eSTREAM Project: The eSTREAM Portfolio. (2008).
2. Canniere C. Trivium Specification. eSTREAM, 2006.
3. Hell M., Johansson T., Meier W. Grain-128a Specification. eSTREAM, 2006.
4. Jakobsson M., et al. Analysis of MICKEY 2.0. Journal of Cryptographic Engineering, 2019.
5. NIST Lightweight Cryptography Report, 2021.
6. Saarinen M.-J. Lightweight Cryptography for Embedded Systems. Springer, 2020.