Метод снижения вычислительной сложности цифровой подписи для устройств с ограниченными ресурсами

Снижение вычислительной сложности, минимизация использования памяти и уменьшение нагрузки на канал связи в ЭЦП

Программа позволяет применять электронную цифровую подпись (ЭЦП) на маломощных устройствах (например, БТС, в контроллерах беспилотных систем UVS) за счет снижения вычислительной сложности ЭЦП на основе криптографии на эллиптических кривых без снижения криптостойкости.
Программа совмещает математические оптимизации ECPM и архитектурные приёмы для минимизации использования рабочей памяти и процессорных циклов, необходимых для реализации цифровой подписи.

ЦЕННОСТНОЕ ПРЕДЛОЖЕНИЕ

Построение эффективных и безопасных криптографических протоколов для систем с ограниченными ресурсами

ОБЛАСТИ ПРИМЕНЕНИЯ

Платежные устройства, бортовые системы автономного транспорта, устройства IoT, блокчейн-системы, документооборот

КОНКУРЕНТНЫЕ ПРЕИМУЩЕСТВА

- Производительность: прирост до 82% (для алгоритмов на эллиптических кривых)
- Скорость: сокращение времени выполнения до 71%
- Память: снижение потребления оперативной памяти (SRAM) до 80%

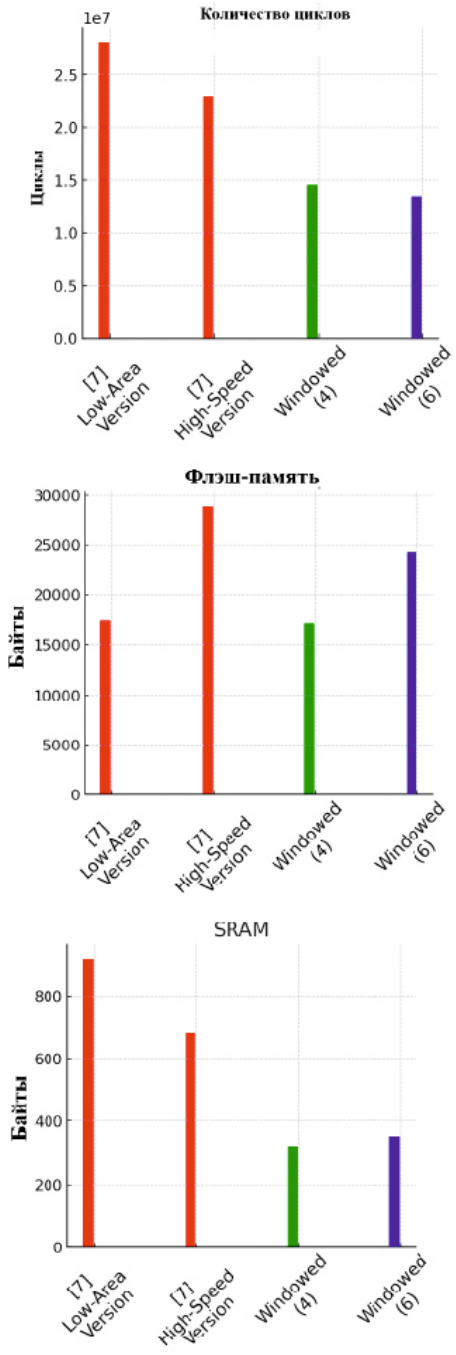
СТАДИЯ РАЗРАБОТКИ

Выполнена программная реализация и экспериментальная верификация разработанных методов на платформе Atmega2560

ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Поддерживаемые протоколы и стандарты:
- SSH-подключения
- SSL/TLS-сертификаты (совместимость с Let's Encrypt, Cloudflare)
- API-аутентификация

Поддерживаемые криптографические алгоритмы: эллиптические кривые



Сравнение результатов скалярного умножения между предложенным методом и существующими

ПРАВОВАЯ ОХРАНА

- Свидетельство о государственной регистрации программы для ЭВМ № 2025681382 «Программа для оптимизации умножения точек эллиптической кривой устройств с ограниченными ресурсами»
- Свидетельство о государственной регистрации программы для ЭВМ № 2025681064 «Программа для оптимизации алгоритмов электронной подписи устройств с ограниченными ресурсами»