Ключник

Генератор истинно случайных паролей (ГИСП) на основе физической энтропии.

Тип проекта:
исследовательский/инженерный

Трек:
Цифровая Схемотехника

Команда проекта

Нехлебов Артём Владимирович

- Беларусь
- Project manager, конструктор

Ильченко Кирилл Александрович

- Беларусь
- Hardware engineer, Схемотехник

Диа Даниэль Мустафа

- Ливан
- UI/UX Разработчик, Разработчик ПО

Детцель Артём Андреевич

- Венгрия
- Технолог, Тестировщик

Янковец Александр Сергеевич

- Беларусь
- Разработчик ПО, Схемотехник

Бодров Лев Андреевич

- Франция
- Разработчик ПО, Сетевой инженер

02

Цель и задачи проекта

Цель

К концу проекта создать полностью функциональный прототип портативного ГИСП, способного генерировать 128-битный ключ за 5 секунд, шифровать его с помощью AES и безопасно передавать по TCP на десктопное приложение.

Задачи

1. Анализ уязвимостей генераторов псевдослучайных паролей и принципов работы ГИСП.
2. Создание схемы электрической-принципиальной и изготовление печатной платы.
3. Сборка и отладка физического устройства.
4. Написание ПО и создание десктопного приложения.

Проблема и актуальность

01. **Проблема:** Программные генераторы паролей предсказуемы

02. **Актуальность:** потребность в источниках истинной случайности становится критически важной для защиты данных

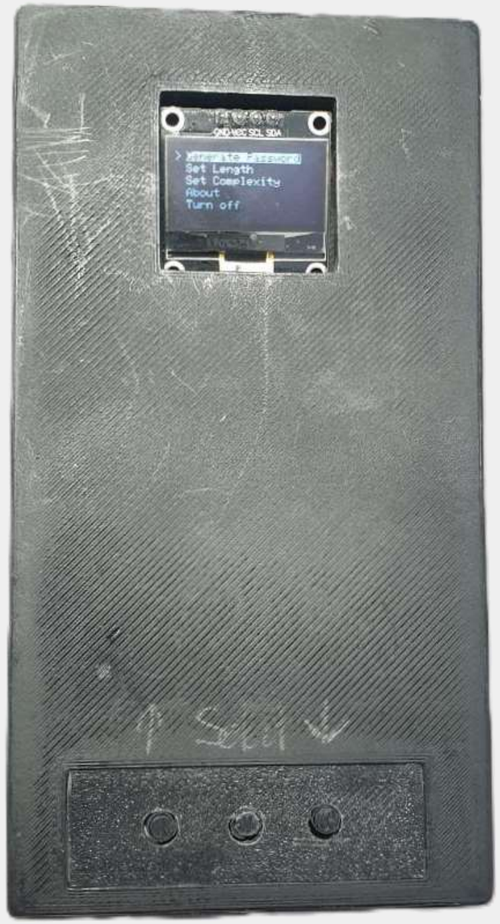
03. Безопасность зависит от случайных чисел, но текущие программные методы уязвимы. Мы предлагаем решение этой проблемы.

70,63%

серверов используют повторяющиеся либо ненадежные пароли

	Our TLS Scan		Our SSH Scans	
Number of live hosts	12,828,613	(100.00%)	10,216,363	(100.00%)
. . . using repeated keys	7,770,232	(60.50%)	6,642,222	(65.00%)
. . . using vulnerable repeated keys	714,243	(5.57%)	981,166	(9.60%)
. . . using default certificates or default keys	670,391	(5.23%)		
. . . using low-entropy repeated keys	43,852	(0.34%)		
. . . using RSA keys we could factor	64,081	(0.50%)	2,459	(0.03%)
. . . using DSA keys we could compromise			105,728	(1.03%)
. . . using Debian weak keys	4,147	(0.03%)	53,141	(0.52%)
. . . using 512-bit RSA keys	123,038	(0.96%)	8,459	(0.08%)
. . . identified as a vulnerable device model	985,031	(7.68%)	1,070,522	(10.48%)
. . . model using low-entropy repeated keys	314,640	(2.45%)		

Ключник



Мы создали аппаратное устройство, которое генерирует истинно случайные числа, улавливая хаотическую энергию физического движения. Эти данные шифруются и отправляются на ПК для создания непредсказуемых паролей

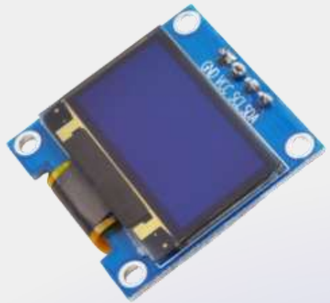
04

Технологии и оборудование

ESP32 NODE MCU
(микроконтроллер)

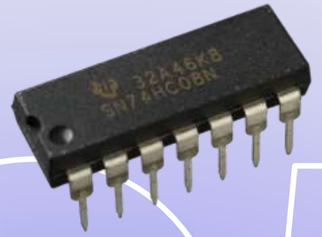
MPU-6050
(акселерометр)

- **Программное обеспечение (ПО):**
  - **Встроенное ПО:** C/C++, фреймворк Arduino, библиотеки I2Cdev, AESLib.
  - **Десктоп:** Rust, tokio для асинхронной работы с сетью, aes для криптографии.
- **Протокол:** TCP/IP для передачи данных.



OLED-дисплей SSD1306

8-битный счётчик
74HC590



логический
вентиль 74HC08

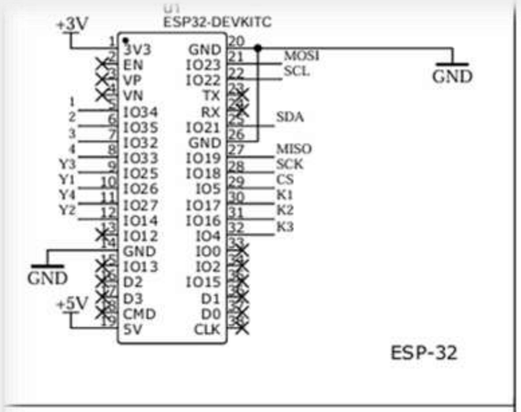
05

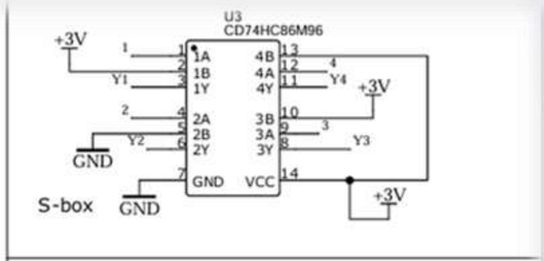
Продукт / Решение

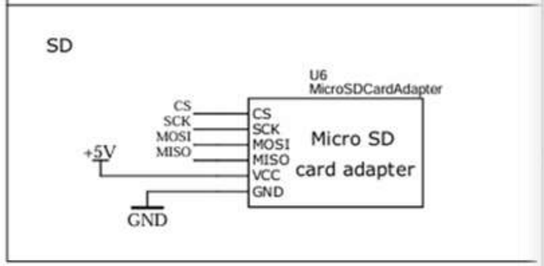
06

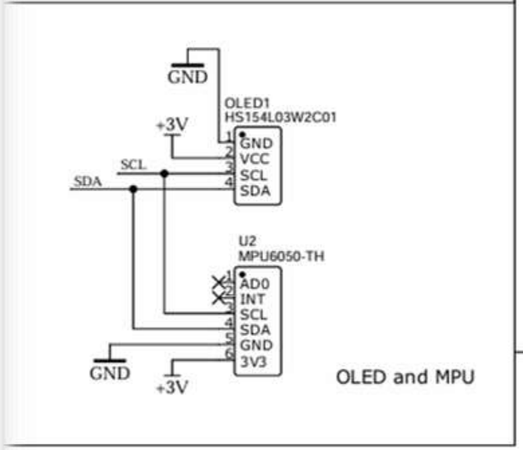
Основные результаты

07

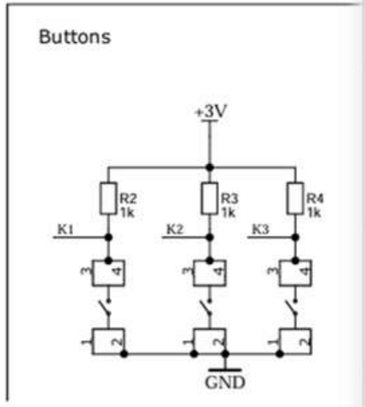


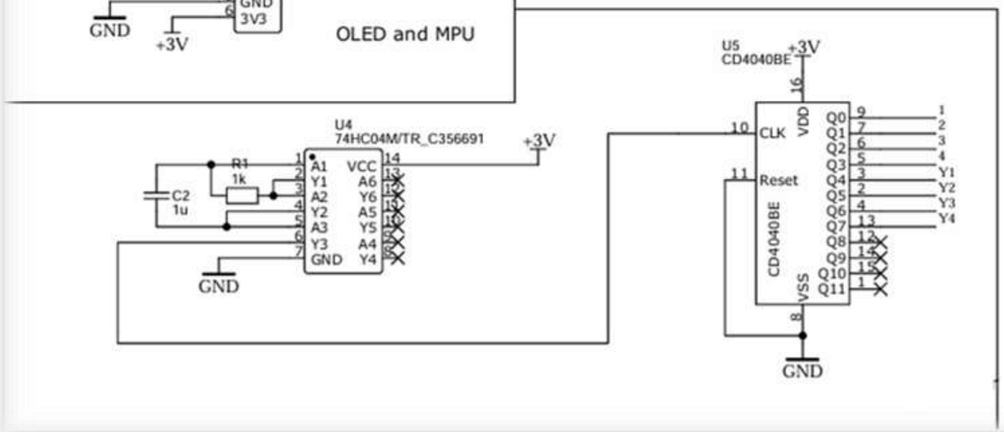






1. РАЗРАБОТАНА СХЕМА ЭЛЕКТРИЧЕСКАЯ-ПРИНЦИПИАЛЬНАЯ

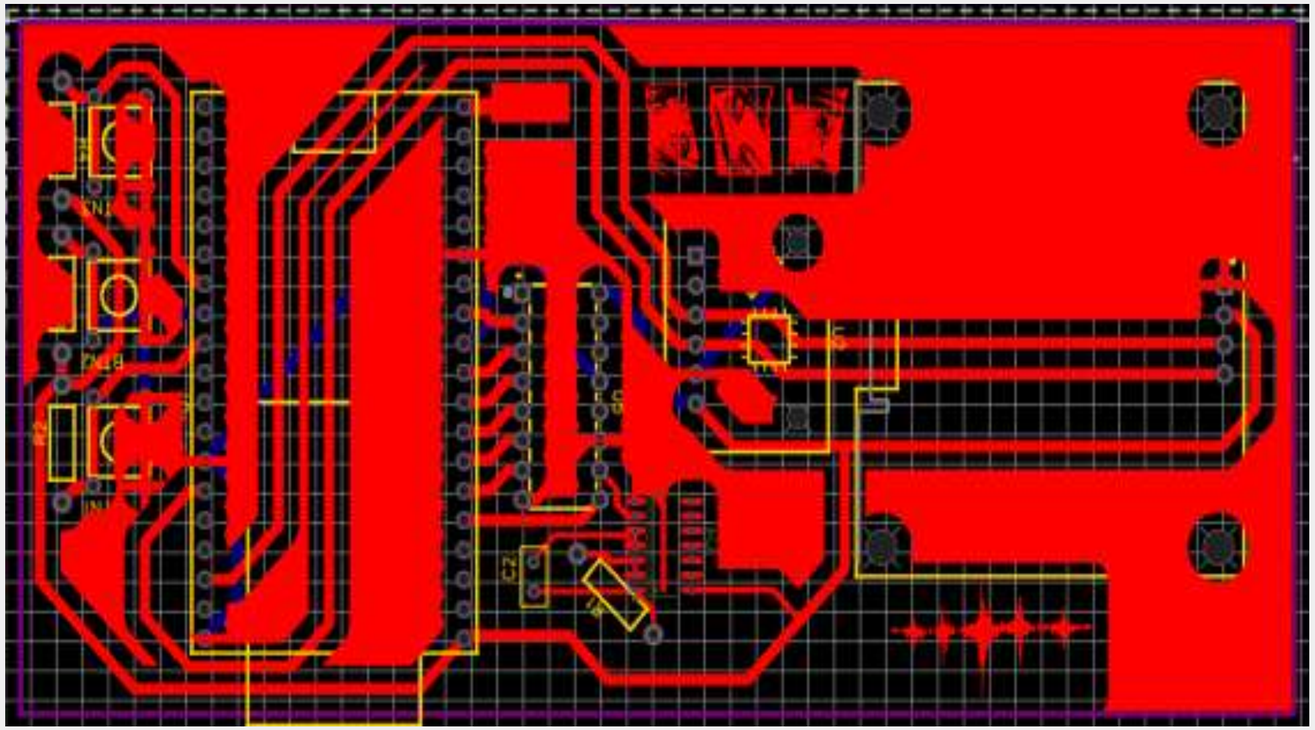




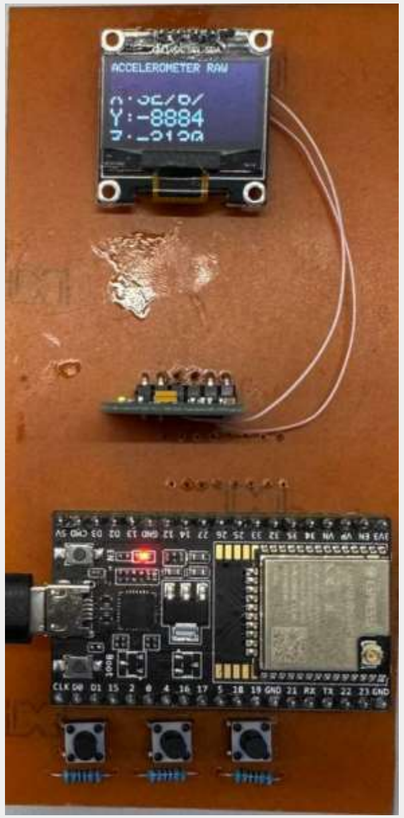
Основные результаты

08

2. Разработана печатная плата



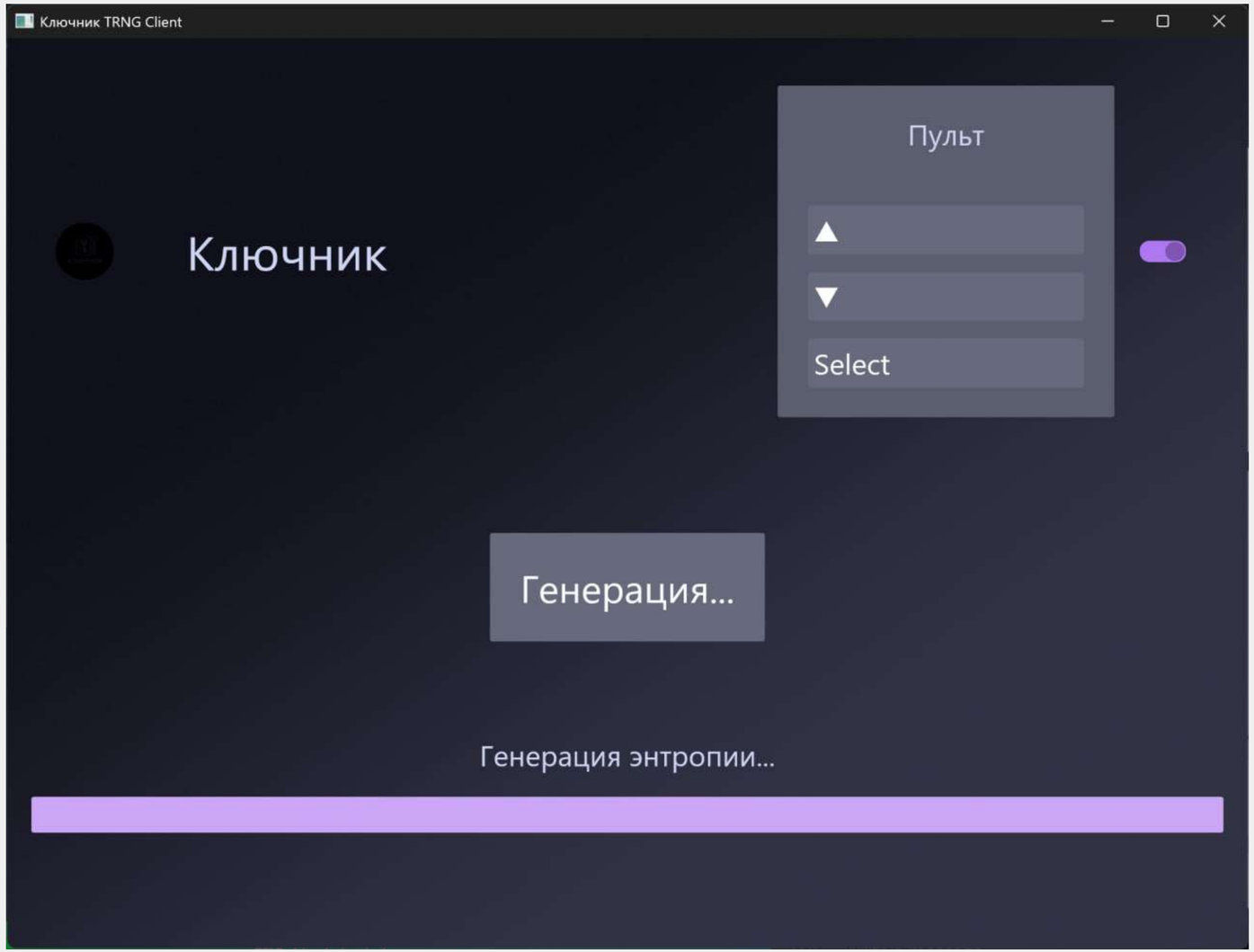
3. Смонтировали на нее все компоненты



Основные результаты

09

4. Сделали Rust-приложение



10

Перспективы развития

01. Создание компактной версии устройства.

02. Добавление других источников энтропии.

03. Мы планируем развивать проект, создавая клиенты для Linux и macOS

Спасибо за внимание!