Тип устройства: цифровой шифратор речи (кодек + шифратор + модем) в режиме точка-точка для HF/VHF/UHF радиостанций и других речевых аналоговых каналов связи.

Ближайший аналог: RT1- In-Line Voice & Position Encryptor *https://at-communication.com/en/print/hf-encryption/na/rt1-encryptor.html*

Тип проекта: полностью открытый исходный код на C и частично ASM в среде Keil uVision 5

Платформа: Cortex M4 Nuvoton M481LIDAE (192MHz CPU, 512K ROM, 160K RAM, ADC, DAC, DMA):

Новый (2018) контроллер от Nuvoton, доступный в Украине по цене ниже $4 в розницу, корпус QFP48, QFN33.

Режимы работы: прозрачный режим/шифрование, симплекс (PTT)/полудуплекс/полный дуплекс

Интерейсы: два аналоговых 12 битных 8 КГц PCM устройства записи + воспроизведения

Управление: кнопка передачи без шифрования, кнопка передачи с шифрованием

Индикация: индикатор обнаружение несущей (автоматическое переключение в режим шифрования), индикатор питания и разряда батареи.

Код аутентификации: до 16 цифр, хранение в энергонезависимой памяти, защита от считывания (клонирования).

Ввод кода: оперативный, с помощью DTMF через микрофон или линейный вход, опционно через UART с конфигуратора или консоли или с помощью 3*4 клавиатуры

Уровень защиты: 128 бит

Свойства защиты: уникальный сессионный ключ, совершенная обратная секретность (PFS) для сессии, аутентификация общим секретом с нулевым разглашением

Криптографические примитивы (реализованы програмно): волатильный код на ассемблере специально для архитектуры Cortex M4, строго постоянны по времени выполнения, оптимизированы с учетом минимизации утечек по побочным каналам ЭМ-излучения и флуктуаций потребляемого тока .

Симметричное шифрование: потоковый шифр NIST Shake-128 на базе преобразования Keccak-800 (мы категорически не доверяем AES из-за «непрозрачного» формирования S-блоков).

Ассиметричное шифрование: Diffie-Hellmann на эллиптической кривой X25519

Аутентификация (анти-MitM): протокол с нулевым разглашением SPEKE с использованием алгоритма Elligator2 для хеширования на кривую.

Генератор случайных чисел: сидирование от младшего бита шума на резисторе при включении устройства, оценка накопленной энтропии с помощью блочного частотного теста, PRNG на базе PRF Keccak-800.

Аудио кодек: NATO STANAG 4591 MELPe +NPP7 1200bps, адаптированный к архитектуре Cortex M4.

Модем: авторский потоковый самосинхронизирующийся модем, специально разработанный для HF/VHF/UHF, полезный битрейт 1200bps.

Модуляция: BPSK, несущий сигнал 1333Гц, 1 период/бит

Спектр: не шире 200-2000 Гц

Время синхронизации: 150-300 мс с любого места потока

Предельный уровень ошибок для синхронизации: BER=3%

Встроенная коррекция ошибок: 9/10, «мягкая», усиление +1.5-2.5dB, избыточность совмещена с синхровставкой

Особенности модема:

- низкий пик-фактор гарантирует высокую устойчивость к нелинейным искажениям канала и паразитной амплитудной модуляции (замираниям в условиях многолучевости).

- петля подстройки частоты и фазы сэмплирования гарантирует высокую устойчивость к доплеру (при ионосферных связях на HW).

Девелоперская версия проекта: https://github.com/gegel/jackpair

для отладочной платы Nucleo STM32F446RE с целью облегчения инсталляции разработчиками.

Цель: разработка модемов для различных каналов связи, в т.ч. сотовой связи и VOIP. Битрейт кодека снижен до 800bps. В наличии два 800 bps модема:

- BPSK, несущая 1333Гц, 1.5 периода/бит, лучше подходит для HF BLoS связи.
- Pulse (Kondoz, Katugampala), 1 импульс на каждые 24 сэмпла в 4-х возможных позициях, позитивной или негативной полярности, кодирует 3 бита данных, подходит для речевых каналов, сжатых AMR кодеком (GSM, UMTS).