The User Manual for KAP-USP0 MiniEVB Board

Rev 1.0

28th February 2025

Table of Contents

1. Introduction

The PQC chip, model KAP-USP0-FB196, is a cryptographic application processor that offers hardware-based cryptographic services. It incorporates post-quantum cryptography (PQC) algorithms directly within the chip. Additionally, the chip features a powerful ARM core capable of operating at up to 240 MHz speeds. The chip also includes a variety of versatile hardware interfaces such as USB 3.0, PCIe, SPI, QSPI, UART, I2C, and GPIO. As a result, the KAP-USP0-FB196 chip can support a wide range of cryptographic applications while maintaining a simple hardware architecture.

1.1. The Potential Applications

With proper firmware and PCB design, KAP chip can be used to create:

- Standalone USB HSM
- Standalone USB authentication dongle (ex: FIDO2, PIV)
- USB3 thumb-drive composed of NVMe SSD
- Crypto coprocessor for the power SoC/CPU through SPI, QSPI, and PCIe interfaces

1.2. The Supporting Cryptographic Algorithms

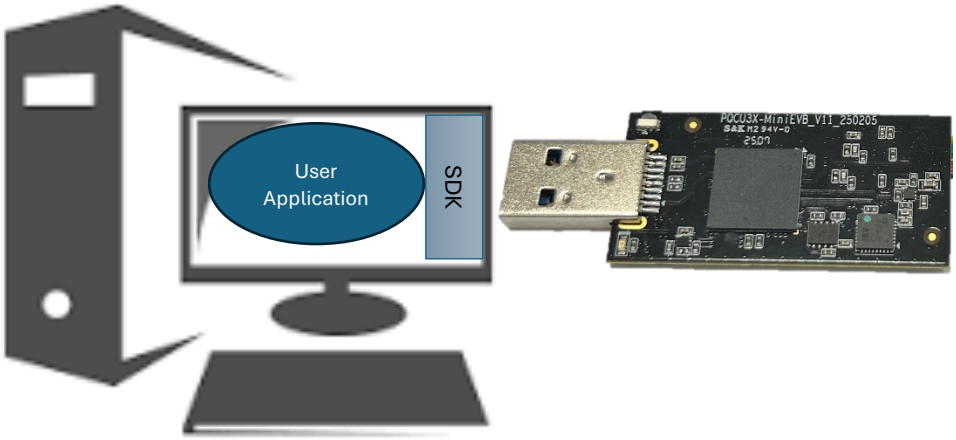
The supporting cryptographic algorithms include:

- PQC: FIPS 203 (ML-KEM) Kyber, FIPS 204 (ML-DSA) Dilithium
- ECC-family: ECDH, ECDSA and their derived ECC-based protocols (e.g., Ed25519 and ECMQV)
- Symmetric Algorithms: AES-128/192/256
- Hash Algorithms: SHA3

- SP 800-90B compliant TRNG entropy source and DRBG services
- Other firmware-implemented cryptographic services and protocols

2. MiniEVB Hardware Details

2.1 MiniEVB Board



The KAP-USP0 MiniEVB enables designers to quickly develop PC-side cryptographic applications through a USB 3.0 interface. In addition, it allows developers to download customized firmware into the chip and validate its functionality.

This kit features a KAP-USP0-FB196 chip, supports USB 3.0 interfaces, and includes 4MB of Flash memory, a secure chip, and three colored LEDs. The EVB also has test-points for various interfaces to facilitate application development, including JTAG, UART, I2C, SPI, and GPIOs.

Flash memory can be used to store firmware binary and retain application data. The application can also use the secure chip on the board to save the keys or sensitive parameters securely.

The following schematic diagram shows the components and their inter-

connections on the board:

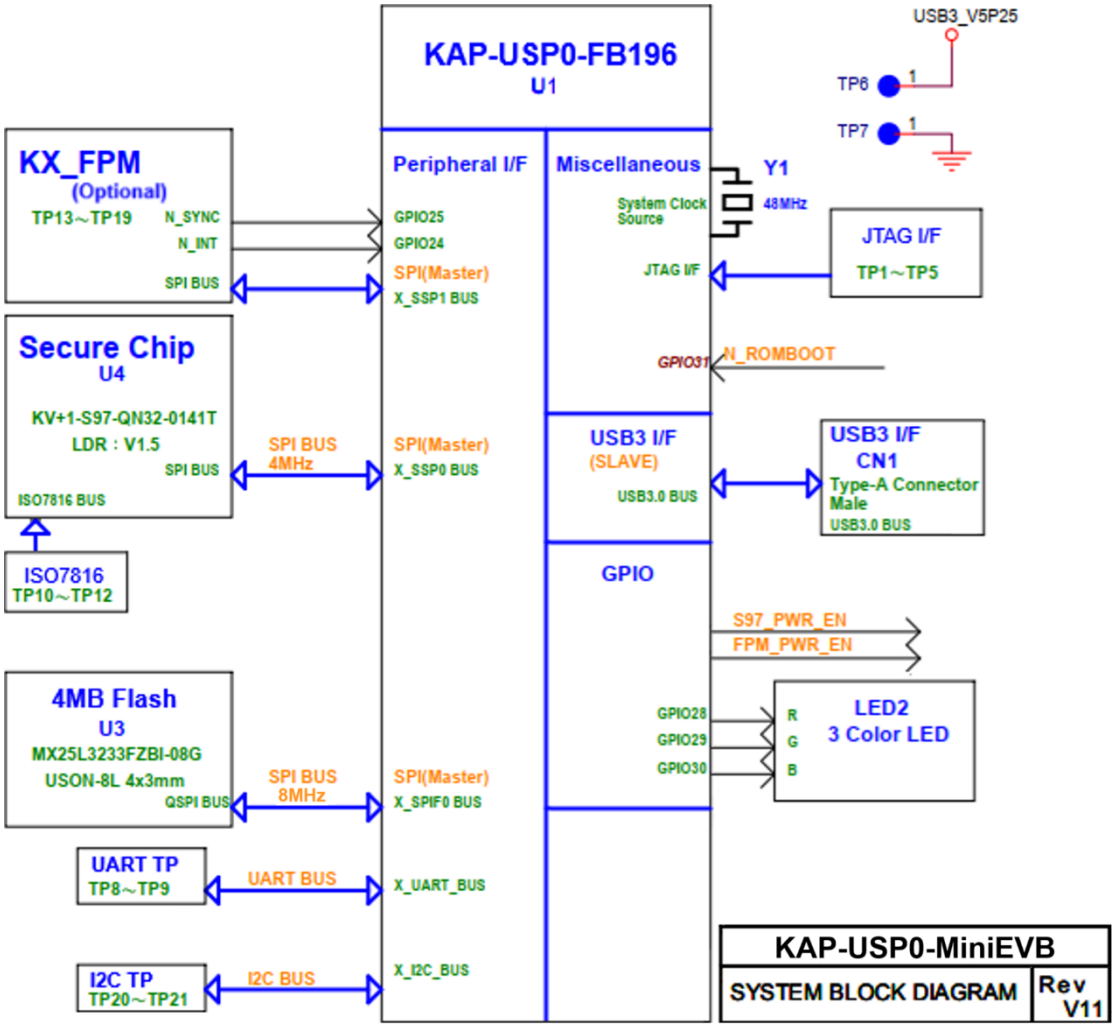
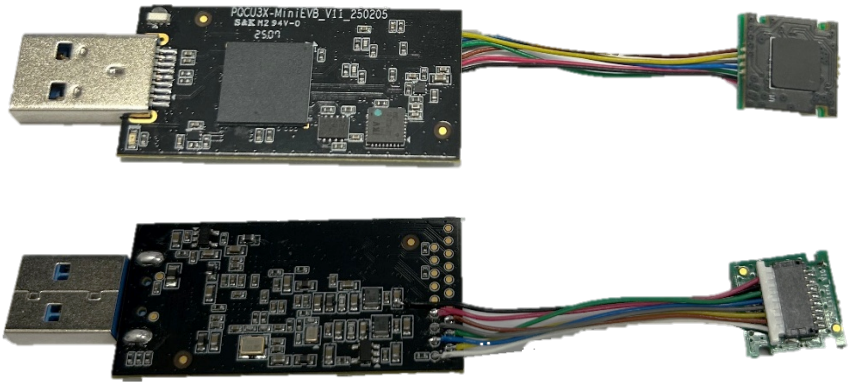


Figure 1. KAP-USP0-MiniEVB System block diagram

Primary components and Test points

Position	Name	Description
U1	KAP-USP0-196	Primary processor ARM Core, support USB3 Interface, cryptographic operation includes AES, ECC, Digest and PQC.
U2	RESET IC	Trigger the Power ON Reset
U3	4MB Flash	QSPI flash for code and data stored
U4	Secure Chip	CC EAL5+ secure element
TP1~TP5	JTAG I/F	Jtag interface for debugger connection
TP6, TP7	---	5V and GND
TP8~TP9	UART TP	Test points for UART
TP10~TP12	ISO 7816	The ISO 7816 Interface of Secure Chip
TP13~TP19	KX_FPM	SPI Interface (CS, CLK, MISO, MOSI) with two additional GPIOs, it can integrate the Fingerprint Module
TP20~TP21	I2C TP	Test points for I2C

- Integrated with Fingerprint Module



- Performance of Peripherals

  The USB is compliant with USB 3.2 Gen1 (5Gbps).

  The SPI clock is up to 4MHz. (Connect with Secure Chip)

  The QSPI clock is up to 8MHz. (Connect with Nor Flash)

2.2 MiniEVB SDK (Evaluation Version)

The miniEVB SDK (Evaluator Version) allows users to evaluate both Classic cryptographic and PQC operations, which are:

- AES (128, 192, 256):
  - SP 800-38A: ECB, CBC, OFB, CFB, CTR
  - SP 800-38D: GCM
  - SP 800-38E: XTS
- Classic cryptographic operations
  - ECDSA (P256, P384, P521)
  - ECDH (P256, P384, P521)
- Post Quantum cryptographic operations
  - FIPS 203 ML-KEM: Key Generation / Encaps / Decaps
  - FIPS 204 ML-DSA: Key Generation / Sign / Verify
- Other cryptographic algorithms inside the chip can be provided on-demand
  - (Once the algorithms are provided in the chip, SDK API and command line tools will also be included.)

2.3 Cryptographic Performance

- AES Encryption/Decryption (via USB 3):
  - Pipeline: 120 MB/s (CTR, ECB, CFB)
  - Non-Pipeline: 40 MB/s (CBC, OFB)
- PQC/ECC (via USB 3):
  - 30-150 TPS (operational Transactions-Per-Second)

3. Revision History

Revision	Date	Author	Description
1.0	2025/02/28	Chris	Initial Version