XinaBox Datasheet AH01 - SHA-256 Hardware Encryption

Contents

Overview

This xCHIP is a core encryption module which forms part of the Crypto module range, running a security algorithm based on SHA-256.

This xCHIP includes the ATECC508A from Atmel, which is a secure CryptoAuthentication device, which is equipped with an EEPROM array that can be used for storing of up to 16 key, certificates, consumption logging, security configurations and other types of secure data. Access to the various sections of memory can be restricted in several different ways and then the configuration can be locked permanently, to prevent changes.

The ATECC508A features a wide array of defense mechanisms specifically designed to prevent physical attacks on the device itself, or logical attacks on the data transmitted between the device and the system. Hardware restrictions on the ways in which keys are used or generated provide further defense against certain styles of attack.

Access to the device is made through a standard I^2C interface at speeds of up to 1 Mb/s.

Product Highlights

- Cryptographic co-processor with secure hardware-based key storage
- SHA-256 hash algorithm with HMAC option
- 256-bit key length
- Storage for up to 16 keys
- Guaranteed unique 72-bit serial number

Applications

- IoT node security and ID
- Secure download and boot
- Ecosystem control
- Message security
- Anti-cloning

Specifications

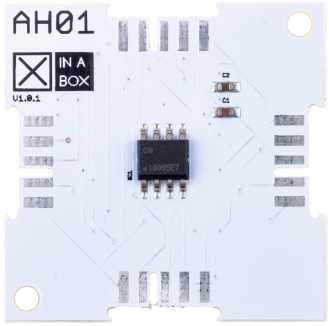
- Performs high-speed Public Key (PKI) algorithms:
    1. ECDSA: FIPS186-3 Elliptic Curve Digital Signature Algorithm
    2. ECDH: FIPS SP800-56A Elliptic Curve Diffie-Hellman Algorithm
- NIST standard P256 elliptic curve support
- Host and client operations
- Two high-endurance monotonic counters
- Internal high-quality FIPS Random Number Generator (RNG)
- 10 Kb EEPROM memory for keys, certificates, and data
- Operating temperature range: -40ºC to 85ºC
- <150 nA sleep current

External Links

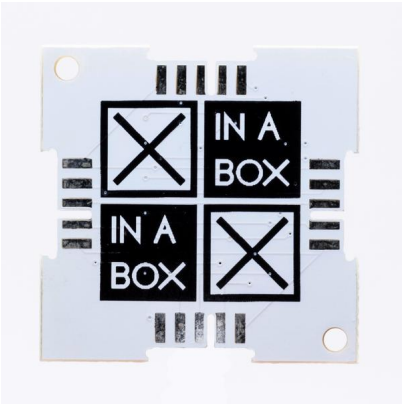
GitHub

- AH01 on GitHub (https://github.com/xinabox/xCH01)

AH01 - SHA-256 Hardware Encryption (ATECC508A/ATECC508)



Front



Back

☒CHIP	
Main Category	Core
Sub Category	Encryption
Introduced	1 January 2017
Current version	1.0.1
Current version date	1 January 2017
Dimensions	
Size	2x2U (32x32 mm)
Weight	2.9 g
Height	3.2/1.6/0 mm
Main Chip Set	
Main Chip	ATECC508A
EEPROM Memory Size	10 Kb
I^2C Speed	1 MHz
I²C Configuration	
Default Address	0x60