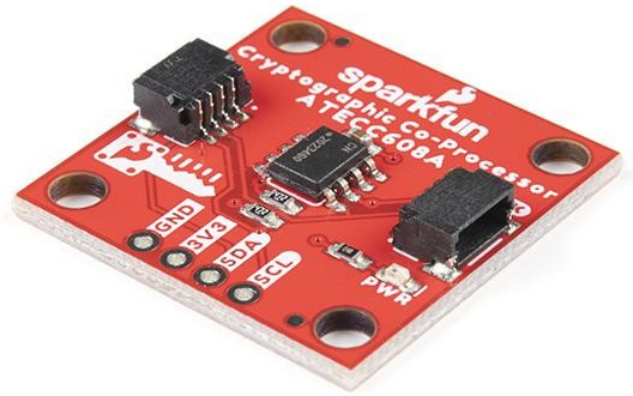
Datenblatt

SparkFun Qwiic Kryptographischer Co-Prozessor Breakout, ATECC608A



Artikel-Nr.:	DEV-18077
Hersteller:	SparkFun
Herkunftsland:	USA
Zolltarifnummer:	85423911
Gewicht:	0.002 kg

Mit dem SparkFun ATECC608A Cryptographic Co-processor Breakout können Sie Ihrem IoT-Knoten, Edge-Device oder Embedded-System starke Sicherheit hinzufügen. Dazu gehören **asymmetrische** Authentifizierung, **symmetrische** AES-128-Verschlüsselung/Entschlüsselung und vieles mehr. Wie bereits erwähnt, hat der ATECC608A eine begrenzte Arduino-Unterstützung und das vollständige Datenblatt steht unter NDA mit Microchip.

Dieses Breakout-Board enthält zwei Qwiic-Ports für Plug-and-Play-Funktionalität. Durch die Verwendung unseres praktischen Qwiic-Systems ist kein Löten erforderlich, um es mit dem Rest Ihres Systems zu verbinden. Dennoch haben wir die Pins im 0,1"-Abstand herausgebrochen, falls Sie lieber ein Breadboard verwenden möchten. Der ATECC608A-Chip ist zu vielen kryptographischen Prozessen fähig, einschließlich, aber nicht beschränkt auf:

- Erzeugen und sicheres Speichern einzigartiger asymmetrischer Schlüsselpaare basierend auf Elliptic Curve Cryptography (FIPS186-3).
- AES-128: Verschlüsseln/Entschlüsseln, Galoisfeld-Multiplikation für GCM
- Erstellen und Verifizieren von 64-Byte-Digitalsignaturen (aus 32-Byte-Nachrichtendaten).
- Erstellung eines gemeinsamen geheimen Schlüssels auf einem öffentlichen Kanal mittels Elliptic Curve Diffie-Hellman Algorithmus
- SHA-256 & HMAC Hash einschließlich Off-Chip-Kontextspeicherung/Wiederherstellung
- Interner hochqualitativer FIPS-Zufallszahlengenerator.

In den Chip eingebettet ist ein 10 KB großes EEPROM-Array, das für die Speicherung von Schlüsseln, Zertifikaten, Daten, Verbrauchsprotokollen und Sicherheitskonfigurationen verwendet werden kann. Der Zugriff auf die Speicherbereiche kann dann eingeschränkt und die Konfiguration gesperrt werden, um Änderungen zu verhindern. Jeder ATECC608A Breakout wird mit einer garantiert eindeutigen 72-Bit-Seriennummer ausgeliefert und enthält mehrere Sicherheitsfunktionen, um physische Angriffe auf das Gerät selbst oder logische Angriffe auf die zwischen dem Gerät übertragenen Daten zu verhindern.

Ein zusammenfassendes Datenblatt für den ATECC608A ist hier verfügbar. Das vollständige Datenblatt steht unter NDA mit Microchip. Sie müssen sich an Microchip wenden, um Zugriff auf das gesamte Datenblatt zu erhalten. In der Zwischenzeit unterstützt die ArduinoATECCX08 Library derzeit nur den ATECC608A mit SAMD21 Arduino-Boards.

Wir haben viel mehr Unterstützung für die ATECC508A Version dieses Chips. Bitte schauen Sie sich unsere ATECC508A Hookup Guide und Arduino Library (die sechs Beispiele enthält) an. Damit werden Sie mit den Grundlagen der elliptischen Kurvenkryptographie und dem Signieren/Verifizieren von Daten mit der ATECC508A-Version des Chips vertraut gemacht.

Hinweis: Die I2C-Adresse des ATECC608A ist 0x60 und kann per Software auf eine beliebige Adresse eingestellt werden. Ein Multiplexer/Mux ist erforderlich, um mit mehreren ATECC608A-Sensoren unter der Standardadresse zu kommunizieren, wenn sie sich auf einem einzigen Bus befinden. Wenn Sie mehr als einen ATECC608A-Sensor an der Standardadresse verwenden möchten, sollten Sie das Qwiic Mux Breakout in Betracht ziehen. **Hinweis:** Der ATECC608A kann nur einmal konfiguriert werden, bevor er **PERMANENT** gesperrt wird. Es ist ratsam, dass Benutzer mehrere Boards kaufen, um andere Konfigurationen zu verwenden und die erweiterten Funktionen des ATECC608A zu erkunden.

Darüber hinaus **ist** dieses Board in der Lage, Daten zu verschlüsseln und zu entschlüsseln. Um Zugang zu diesen zusätzlichen Funktionen zu erhalten, müssen Sie sich jedoch an Microchip wenden und einen NDA-Vertrag unterzeichnen, um das vollständige Datenblatt zu erhalten.

Es wird empfohlen, ein SparkFun RedBoard Turbo - SAMD21 Development Board mit diesem Produkt zu verwenden, da die Puffergröße auf dem I2C-Bus erforderlich ist.

Merkmale:

- Betriebsspannung: 2.0V-5.5V (**Standard bei Qwiic System: 3.3V**)
- Aktive Stromaufnahme (für ATECC608A): 16 mA
- Sleep-Strom (für ATECC608A): <150 nA
- Garantiert eindeutige 72-Bit-Seriennummer
- 10 Kb EEPROM-Speicher für Schlüssel, Zertifikate und Daten
    - Speicherplatz für bis zu 16 Schlüssel
    - 256-Bit Schlüssellänge
- Interner hochqualitativer FIPS-Zufallszahlengenerator (RNG)
- Konfigurierbare I2C-Adresse (7-Bit): 0x60 (**Standard**)

Dokumente:

- Schaltplan
- Eagle-Dateien
- Platinenabmessungen
- Datenblatt Zusammenfassung (ATECC608A)
- CryptoAuthLib - Microchip CryptoAuthentication Library (mit Python-Unterstützung)
- Microchip ATECC608A Produktseite
- ArduinoECCX08 Arduino Bibliothek
- Github Hardware Repo

Hinweis: Das auf dieser Seite aufgeführte Datenblatt ist *nicht* das vollständige Dokument, das unter NDA mit Microchip steht.

Weitere Bilder: