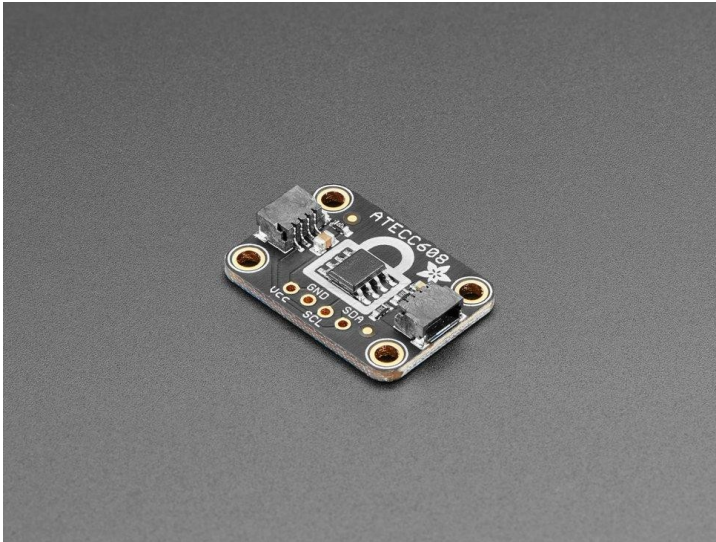




Adafruit ATECC608 Breakout Board - STEMMA QT / Qwiic



N.º artículo:	ADA4314
Hersteller:	Adafruit
Herkunftsland:	USA
Zolltarifnummer:	85423911
Gewicht:	0.003 kg

Sie haben Geheimnisse und wollen sie sicher verwahren? Die meisten Mikrocontroller sind nicht für den Schutz vor Schnüfflern ausgelegt, aber mit einem Krypto-Authentifizierungs-Chip lassen sich private Schlüssel sicher wegschließen. Sobald der private Schlüssel darin gespeichert ist, kann er nicht mehr ausgelesen werden, sondern nur noch Challenge-Response-Abfragen gesendet werden. Das heißt, selbst wenn jemand Ihre Hardware in die Hände bekommt und die Firmware zurücklesen kann, wird er nicht in der Lage sein, das Geheimnis zu extrahieren!

Der ATECC608 ist der neueste Krypto-Auth-Chip von Microchip, und er verwendet I2C, um Befehle zu senden/empfangen. Sobald Sie den Chip mit Ihren Daten "verriegelt" haben, können Sie ihn für ECDH und AES-128 Verschlüsselung/Entschlüsselung/Signierung verwenden. Es gibt auch Hardware-Unterstützung für die Erzeugung von Zufallszahlen und SHA-256/HMAC-Hash-Funktionen, um die Kryptographie-Befehle eines langsameren Chips erheblich zu beschleunigen.

Wir fangen an, diese kostengünstigen Secure-Element-Chips in verschiedenen Produkten zu sehen, so dass ein weniger teurer Chip verwendet werden kann, um Peripheriegeräte anzusteuern, ohne sich um die Sicherheit zu kümmern. Dieser Chip hat kein öffentliches Datenblatt, aber er ist kompatibel mit der früheren Version ATECC508, die ein solches hat. Bitte lesen Sie daher das [vollständige Datenblatt](#) sowie [das ATECC608-Übersichtsblatt](#). Die gute Nachricht ist, dass es trotz der nicht vollständigen Dokumentation *eine* Software-Unterstützung gibt. Für die Verwendung mit Arduino gibt es die [Arduino ATECCx08 Bibliothek](#). Für Python und C/C++ gibt es die [Microchips Cryptoauthlib](#) (ja, wir finden es auch seltsam, dass es kein Datenblatt gibt, aber veröffentlichten Code).

Um die Arbeit mit dem ATECC608 so einfach wie möglich zu machen, haben wir ihn auf eine Breakout-Platine mit der erforderlichen Support-Schaltung und SparkFun qwiic-kompatiblen [STEMMA QT](#)-Anschlüssen gesetzt. Dies ermöglicht es Ihnen, ihn mit anderen ähnlich ausgestatteten Boards zu verwenden, **ohne dass Sie löten müssen**. Dieser Chip funktioniert mit 3,3V oder 5V Power/Logic Micros, so dass er bereit ist, mit einer Reihe von Entwicklungsboards zu arbeiten.

Bitte beachten Sie, dass die I2C-Adresse auf 0x60 festgelegt ist und laut Microchip sollten Sie diesen Chip bei höheren I2C-Geschwindigkeiten wie 400KHz verwenden, wenn andere Geräte auf dem I2C-Bus sind, um eine I2C-Bus-Konkurrenz zu vermeiden (Wie auch ein Datenblatt fehlt, ist dies noch nirgends dokumentiert)

Durchsichtiges Vorhängeschloss und STEMMA QT-Kabel nicht im Lieferumfang enthalten

Weitere Bilder:

