A.D. 1308
unipg
DIPARTIMENTO
DI INGEGNERIA
DIPARTIMENTO DI ECCELLENZA
MUR 2023/2027

Progetto: BLOCKCHAIN4FOODCHAIN

Sensoristica Tamper-proof e blockchain

GIANLUCA REALI

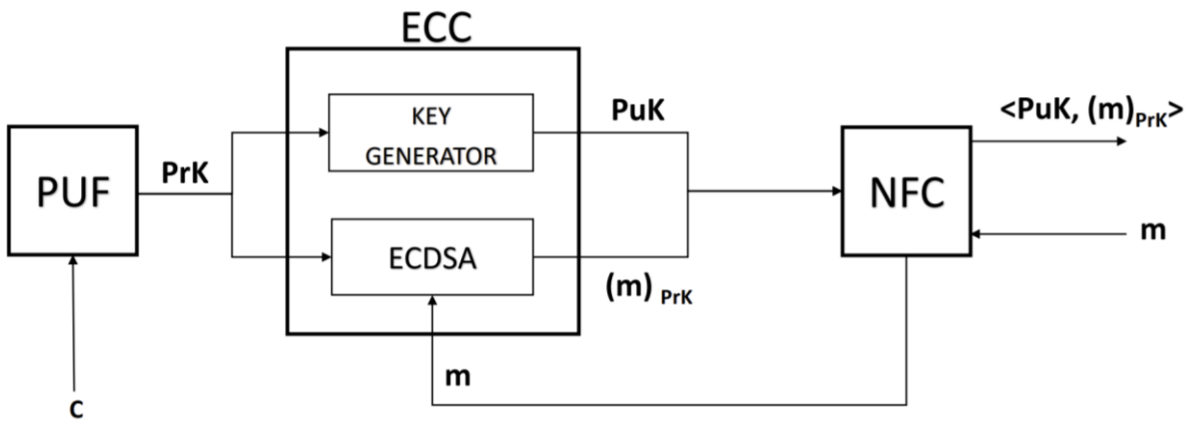
Ref: Alberto Falcone, Carmelo Felicetti, Alfredo Garro, Antonino Rullo, Domenico Saccà
PUF-based Smart Tags for Supply Chain Management
ARES 21: Proceedings of the 16th International Conference on Availability, Reliability and Security
August 2021

Physically Unclonable Function (PUF)
Una funzione PUF è una primitiva hardware che per un dato **input** e condizioni **(sfida)** produce un'**impronta digitale** basata su hardware (risposta) che funge da **identificatore univoco** per un dispositivo, che non può essere replicato (**non clonabile**).

Un PUF è basato su variazioni fisiche uniche che si verificano naturalmente durante il processo di fabbricazione dei dispositivi a semiconduttore, se piccolo variazioni e imperfezioni nei materiali presentano casualità modifiche ai parametri di funzionamento dei circuiti.

Ref: Alberto Falcone, Carmelo Felicetti, Alfredo Garro, Antonino Rullo, Domenico Saccà
PUF-based Smart Tags for Supply Chain Management
ARES 21: Proceedings of the 16th International Conference on Availability, Reliability and Security
August 2021

SMART TAG

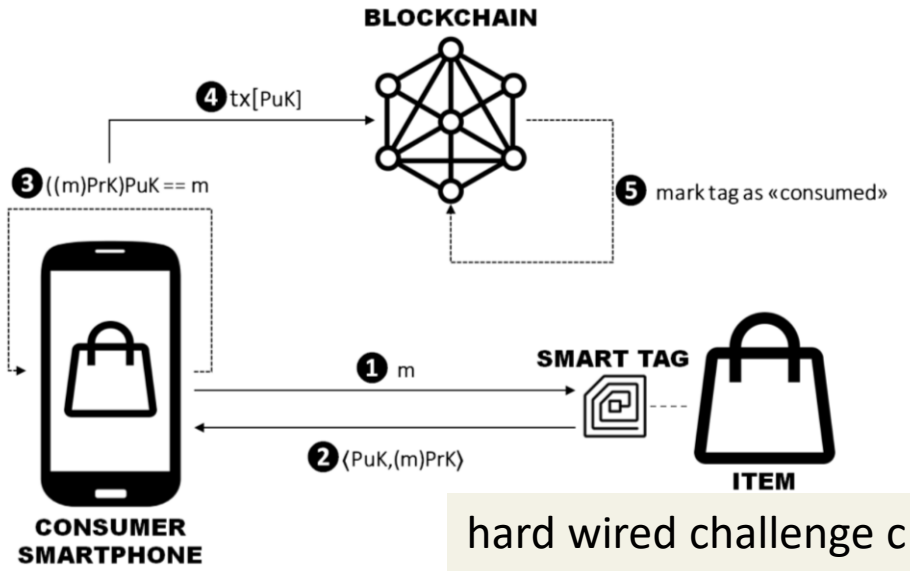


PUF è usato per generare un'impronta digitale per lo smart tag sotto forma di una stringa di bit;

ECC utilizza l'impronta digitale come chiave privata per generare una chiave pubblica, e per firmare i messaggi in arrivo;

NFC (Near Field Communication) interfaccia lo smart tag con il mondo esterno. NFC è disponibile nei telefoni cellulari per operare come lettori RFID

Ref: Alberto Falcone, Carmelo Felicetti, Alfredo Garro, Antonino Rullo, Domenico Saccà
PUF-based Smart Tags for Supply Chain Management
ARES 21: Proceedings of the 16th International Conference on Availability, Reliability and Security
August 2021



hard wired challenge c

1- il cliente invia un messaggio m al tag;

il tag sfida il PUF per rigenerare la sua coppia di chiavi pubblica-privata ⟨PuK, PrK⟩, e le restituisce al cliente;

Il il cliente controlla se ((m)PrK)PuK è uguale a m, e in caso di successo, può completare il processo di autenticazione verificando sulla blockchain che la chiave pubblica del tag sia stata registrata.

Questo viene fatto emettendo una transazione sulla blockchain che contiene la chiave pubblica PuK: se il tag non è già stato utilizzato in passato, quindi la chiave pubblica del tag viene contrassegnata come "consumata", rendendo il tag inutilizzabile per un utilizzo futuro, altrimenti il consumatore riceve una notifica.

In questo modo, se lo stesso tag viene riutilizzato per articoli non originali, questi saranno rilevati come contraffatti.

A. Maiti, P. Schaumont, **Improved Ring Oscillator PUF: An FPGA-friendly Secure Primitive,** April 2011
Journal of Cryptology

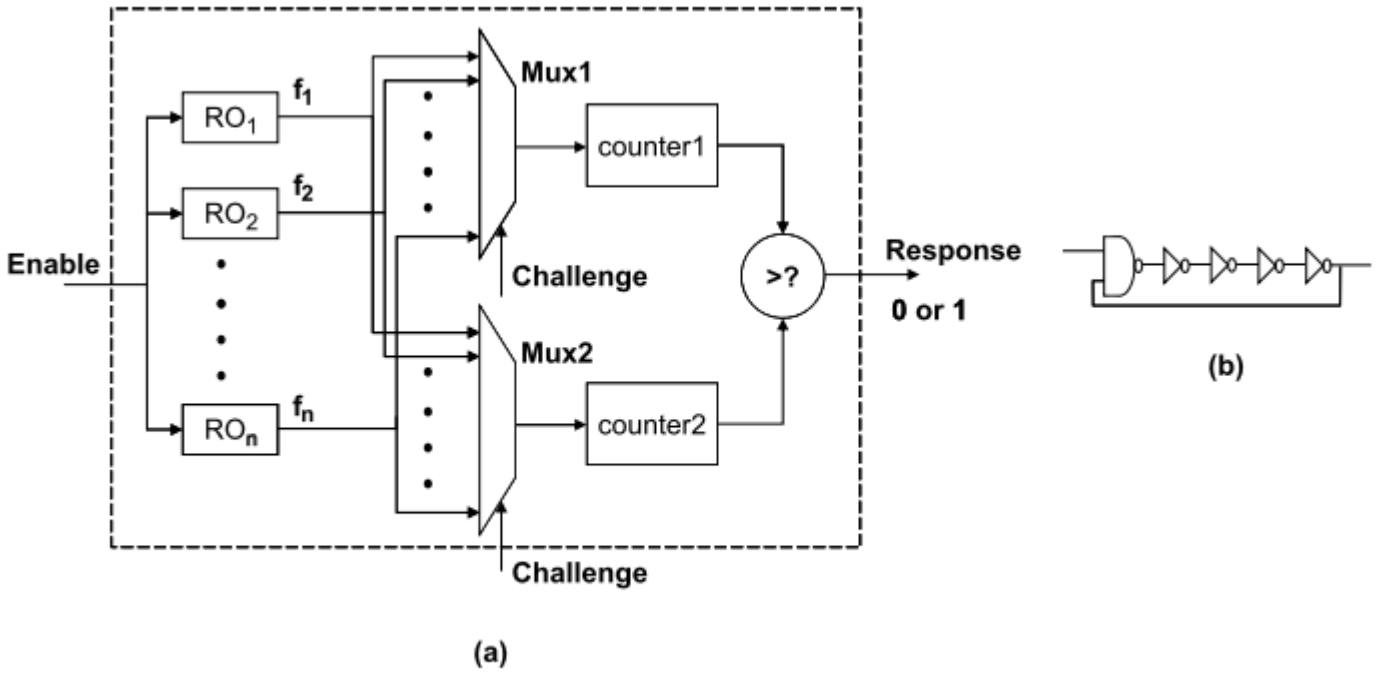


Fig. 1. (**a**) Ring oscillator PUF scheme. (**b**) A basic five-stage ring oscillator loop.

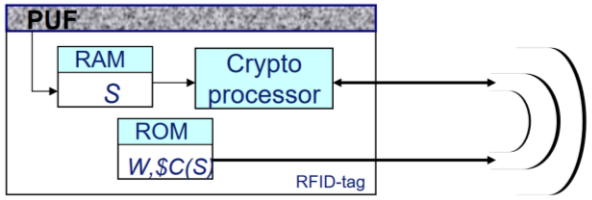
Per ogni *k* bit di challenge, genera 2*k* bit di risposta

Altre soluzioni

PHILIPS

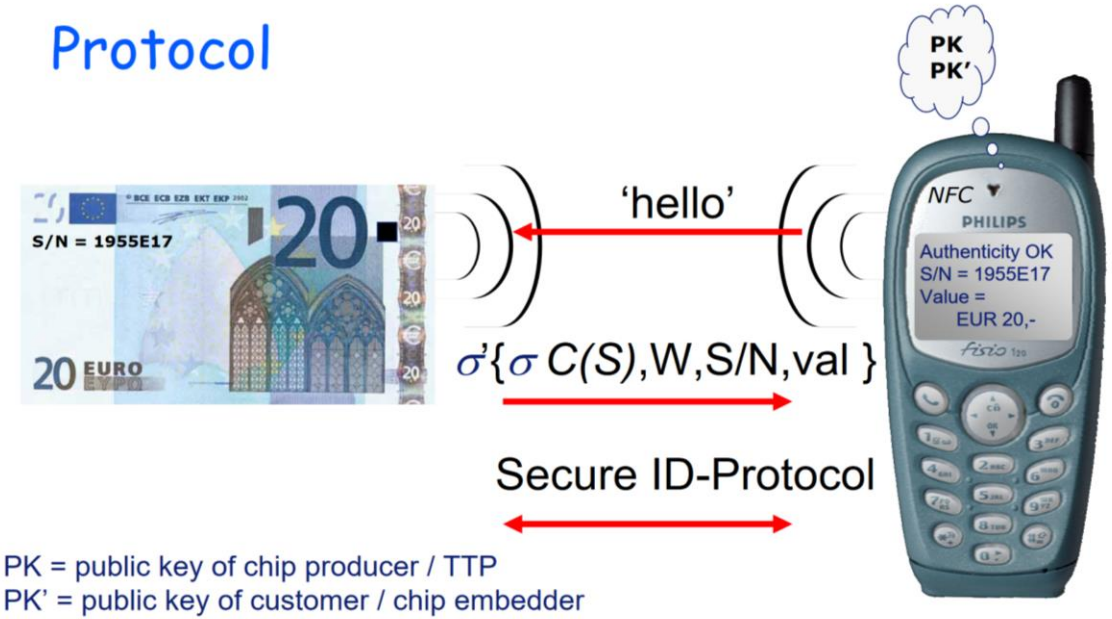
Unclonable RFID tag

- RFID-tag equipped with a coating PUF
  - Removing the PUF leads to destruction
  - Attacker can not tamper with the communication between PUF and tag
  - PUF-output is inaccessible to an attacker
- A unique, secret bit-string *S* is derived from the Coating PUF.
  - (helper data/Fuzzy Extractor)
- *S* is only temporarily in volatile memory
- Reference information $\sigma(C(S))$: *commitment* to *S*, *signed* by TTP and stored in ROM.
- *Aux data: produced by the Fuzzy Extractor*: W



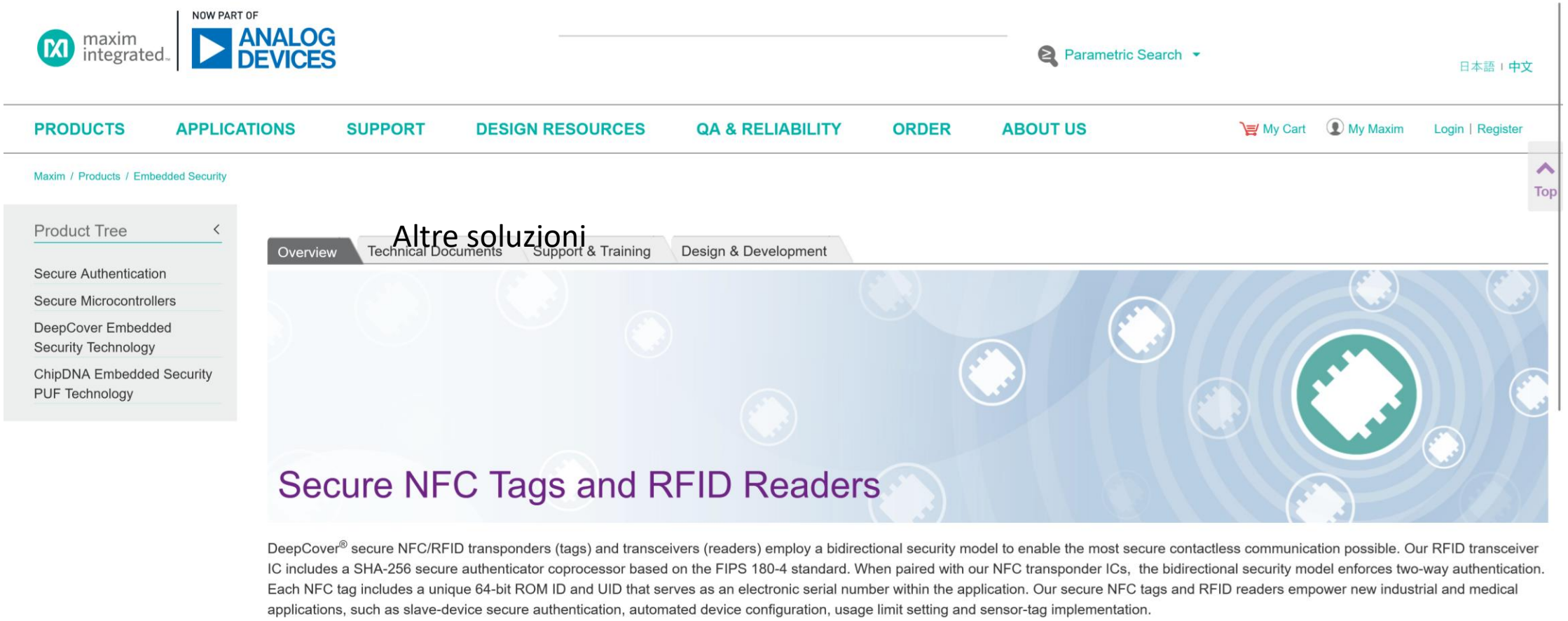
PHILIPS

Protocol

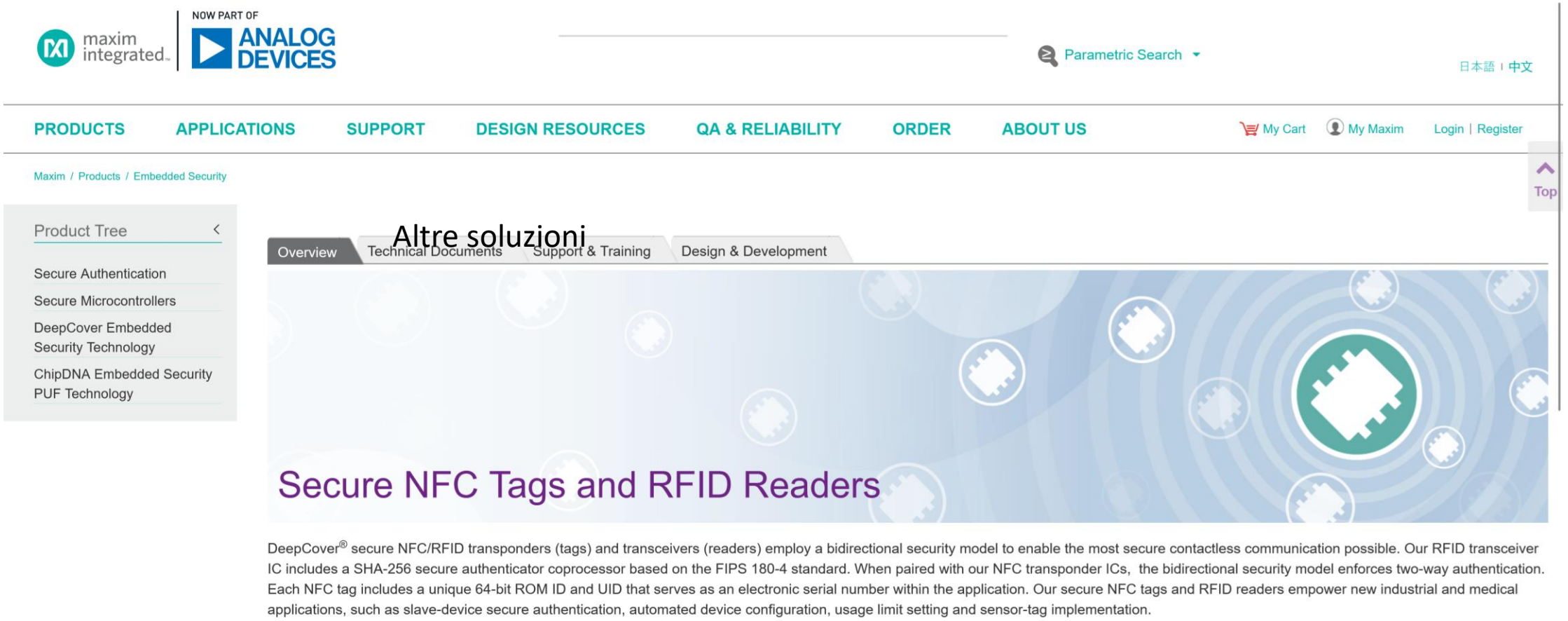


PK = public key of chip producer / TTP
PK' = public key of customer / chip embedder
S/N = serial number

Altre soluzioni



Altre soluzioni



https://para.stg-maximintegrated.com/results.mvp?fam=ibutton_rfid&sel=no&295=Tag|Reader

Importa segnalibri... | Come iniziare | Descrivere le funzional... | Microsoft Certified: Se... | Avviso n. 341 del 15-0... | BIOMARKER IDENTIFI... | Networking in Compo... | OWASP Top 10 Securit... | Explore Azure

PARAMETRIC SEARCH

Bookmark Download Email

Parametric Produ

NFC/RFID Products

Show Controls — Total Parts: 3 — Matching Parts: 2	Protocol	Functions	End Equipment	Memory Type	Memory Size	Security Features	Features	EV Kit	Oper. Temp. (°C)	Package/Pins	Smallest Available Pckg. (mm^2) (max w/pins)	Budgetary Price (See Notes)
Current Selections:	-	= Tag	-	-	-	-	-	-	-	-	-	-
Hidden Columns: 0	Hide	Hide	Hide	Hide	Hide	Hide	Hide	Hide	Hide	Hide	Hide	Hide
Compare — Sort by: Part Number: ▲▼ Default = Newest First — All None	▲▼	▲▼	▲▼	▲▼	▲▼	▲▼	▲▼	▲▼	▲▼	▲▼	▲▼	▲▼
MAX66242 Secure Authenticator with ISO 15693, I2C, SHA-256, and 4Kb User EEPROM	ISO15693	Tag	Access Control Asset Tracking Electronic Access Control IP Protection Medical Sensor Authentication and Calibration Printer Cartridge Configuration and Monitoring System Intellectual Property Protection	EEPROM	4K bits 4K x 1	SHA-256 Write-Only Secrets	I^2C Interface Memory Protection Programmable IO SHA Authentication Serial Number	Yes	-20 to +85	SOIC (N)/8 TDFN/10	12.7	0
MAX66240 Secure Authenticator with ISO 15693, SHA-256, and 4Kb User EEPROM	ISO15693	Tag	Access Control Asset Tracking Electronic Access Control IP Protection Medical Sensor Authentication and Calibration Printer Cartridge Configuration and Monitoring System Intellectual Property Protection eCash	EEPROM	4K bits 4K x 1	SHA-256 Write-Only Secrets	Memory Protection SHA Authentication Serial Number	Yes	-20 to +85	SOIC (N)/8 TDFN/10	12.7	0

Notes: *This pricing is BUDGETARY, for comparing similar parts. Prices are in U.S. dollars and subject to change. Quantity pricing may vary substantially and international prices may differ due to local duties, taxes, fees, and exchange rates. For volume-specific and version-spec
and availability page or contact an authorized distributor.

NXP LPC55S16 MCU Awarded PSA Level 2 and SESIP Assurance Level 2 Certifications

November 17, 2020 9:00 AM by NXP Semiconductors News Brief

The LPC55S16 MCU integrated security features include:

- Arm TrustZone® technology, which enables system-wide software protection with the ability to securely isolate peripherals to reduce the risk of attack on critical components.
- AES-256 accelerator provides confidentiality and secure hash algorithm (SHA2) accelerator provides integrity of secure communications and secure boot.
- PRINCE module offers real-time encryption and decryption of the on-chip flash to provide both secure storage of data and asset protection of software intellectual property (IP).
- CASPER Crypto co-processor enables hardware acceleration of various asymmetric cryptographic algorithms to establish secure connections.
- Physical Unclonable Function (PUF) uses dedicated on-chip SRAM to construct unique device root keys (64 to 4096 bits) for secure storage.
- 128-bit unique device serial number for identification (UUID).
- True Random Number Generator (TRNG).
- Code watchdog enables integrity checking of execution flow of the firmware.
- Debug authentication protocol for secure debugging.

Product Availability

The LPC55S16 MCU family is available now with a suggested resale price starting at $1.54 (USD) for 10,000-unit quantities.

Visit the LPC55S16 MCU for more information.

Also see EdgeLock Assurance, PSA Certified and Security Evaluation Standard for IoT Platforms (SESIP) published by GlobalPlatform web pages for further details.

About NXP Semiconductors

NXP Semiconductors N.V. enables secure connections for a smarter world, advancing solutions that make lives easier, better and safer. As the world leader in secure connectivity solutions for embedded applications, NXP is driving innovation in the automotive, industrial & IoT, mobile and communication infrastructure markets. Built on more than 60 years of combined experience and expertise, the company has approximately 29,000 employees in more than 30 countries and posted revenue of $8.88 billion in 2019. Find out more at NXP Semiconductors.