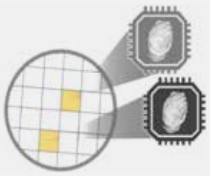
IL005 (G1)

VIA PUF Authenticator

Introduction

IL005, VIA PUF Authenticator, is the world's first VIA PUF technology-based cryptographic encryption/ decryption and authentication device using SHA-256 hash algorithm. IL005 provides H/W based robust security solution that physically generates unclonable unique PUF keys in the IC. Therefore it is not necessary to save the keys in the memory, because they can be regenerated if needed. This is the innovative solution that fundamentally eliminates the limitations and vulnerabilities of conventional security solutions



Description

The IL005 is able to prevent the counterfeiting of ink cartridges, toners for printers or rechargeable batteries of e-tobacco. It is also suitable for IoT M2M authentication and firmware protection of IoT devices. Protecting firmware is achieved by authenticating if the firmware is genuine and has not been compromised by an attacker's firmware code when the device boots up or updates firmware. Authenticating a user verifies, that the user has a legitimate cryptographic key in an IL005 device. Lastly, secure storage functions using cryptographic features of the IL005 can also be achieved so that a secure storage area may be made in a non-secure memory area by encrypting data with a PUF key. Without the key inside of the IL005, the encrypted data can be kept confidential. PUF-based encryption and authentication functions are provided and can be used to authenticate a remote device without exposing the PUF key.

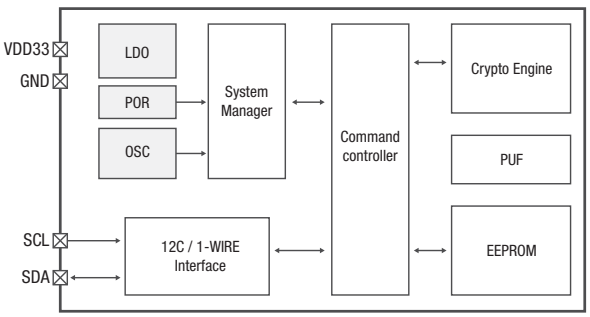
Advantages

- PUF provides the 'Root of Trust' on your system
- Unique IDs for each of your devices
- Specificity and competitiveness for your solution
- High-security authentication at the lowest total system cost
- Secure storage on your system
- Low current, compact size and longtime stability for IoT
- Various package options
- Protect firmware and IPs

Key features

- PUF (Physically Unclonable Function) value(key) generation
- SHA256/HMAC based symmetric authentication
- Authentication and data encryption / decryption with PUF
- Secure Storage (Encrypted EEPROM data with PUF)
- Store up to 16 keys (256 bit key lengths)
- 5Kbit EEPROM for data and key storage
- Hardware crypto engines : SHA256 / HMAC
- TRNG (True random number generator)
- Operating voltage range : VDD33 : 3.0~3.6 V
- Interface: I2C / 1-Wire (OWI)
- <150nA sleep current
- Security countermeasure: Fault injection & Side channel attack
- Physical attack protection

Block Diagram



Package options

- 8-pin SOIC (SOP)
- 3-pin SOT 23-3L
- 8-pin DFN

Application

IL005 (G1)

Secure ID

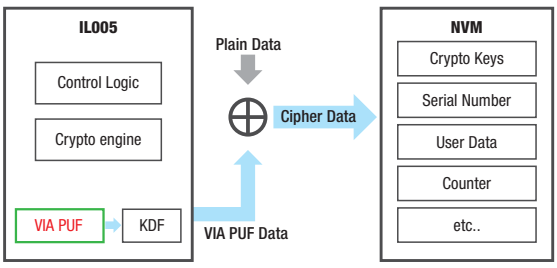
- Direct ID : Use VIA PUF itself as unique ID
- Indirect ID : Inject ID & store by “Secure Memory” concept
- No risk of cloning
- ID card, passport, Driver license, Drone ID etc..

2nd factor authentication

- Secure FINTECH
- Smart door/ Smart card/ IoT sensor & gateway

Secure memory

- Stores data in NVM after encryption by VIA PUF key
- Once use, Do not store VIA PUF Key
- Regenerate the VIA PUF key if necessary

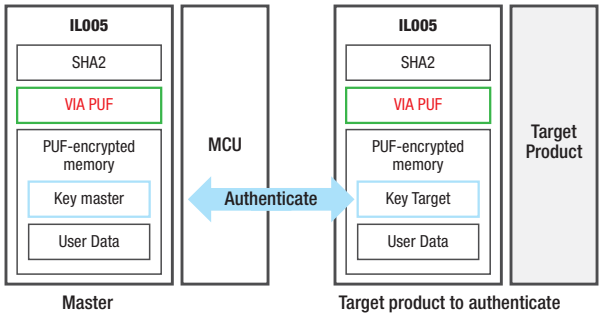


Firmware protection

- Secure boot
- Secure update
- IP protection
- License management

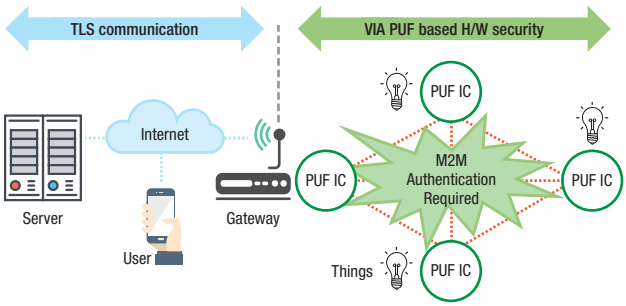
Anti-Counterfeit (off-line)

- Utilize “Secure memory” concept
- Install IL005 in the “Target Product” to authenticate & “Master”
- Enroll “Target Product” before shipping out
- In the field, “Master” and “Target Products” authenticate each other
  - Example : Smart phone accessary, Smart phone battery, Printer ink cartridge, E-Cigarette cartridge, Drone, etc..



IoT security

- Server↔HUB: TLS standards
- HUB↔Thing/ Thing↔Thing : PUF IC security(H/W)



www.ictk.com

ICTK holdings co., ltd

Headquarters

323, Pangyo-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea

+82-31-739-9459 +82-31-739-7891 puf@ictk.com

China Office

6F06-07 Wan Jun Trade Building, No.21 Baoxing Road, Baoan District, Shenzhen P.R.C

+86-0755-2322-0007 +86-0755-2307-8557

info@ictk-china.com