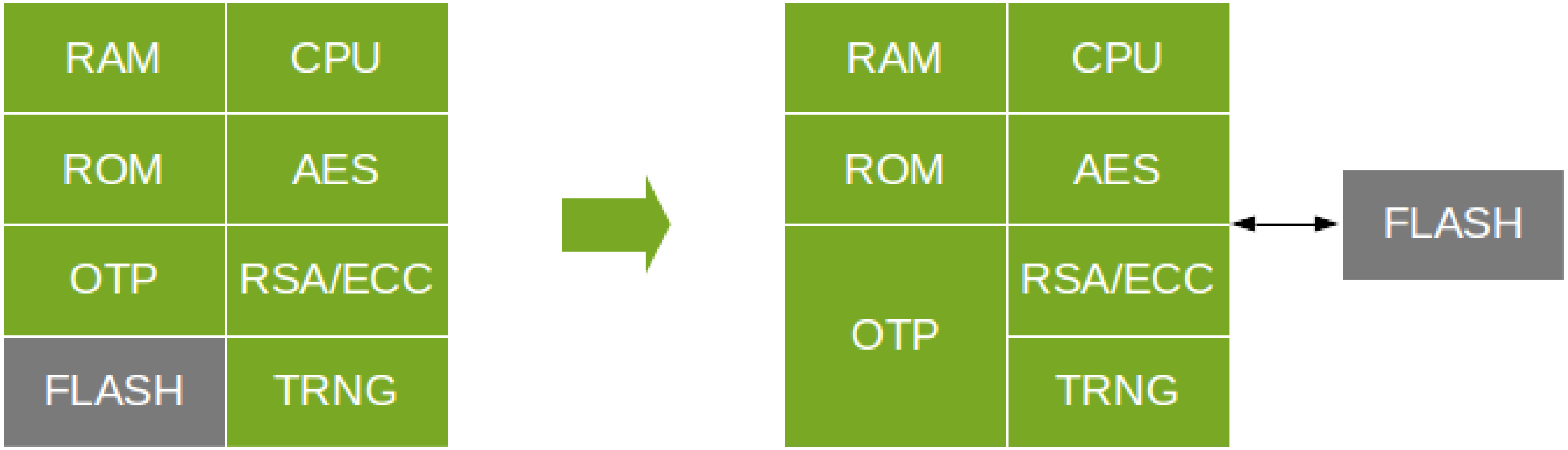
LWC use cases

External memory encryption

September 13, 2020

Secure IC with external NVM memory

- Typical secure element/smart card: internal flash memory (everything on single chip)
- Our goals:
  - Use external (flash) memory
  - Achieve same security level



RAM CPU
ROM AES
OTP RSA/ECC
FLASH TRNG

RAM CPU
ROM AES
OTP RSA/ECC
TRNG

FLASH

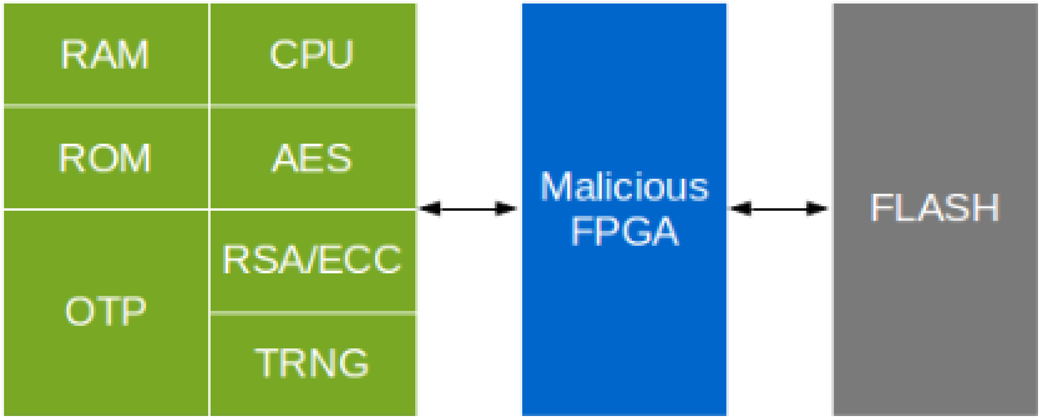
What’s wrong with embedded NVM* ?

- IC is more expensive
  - Embedded NVM requires additional process steps and test time
  - Additional yield loss
- No flexibility on memory size
  - Supporting several memory size means designing several ICs
  - It takes about 1 year to support a new memory size
- Not available on latest technology nodes

* Embedded NVM: here we mean “Multiple Time Programmable NVMs” such as EEPROM, flash and MRAM. Strictly speaking ROM and OTP are “NVMs”. In this document we use “NVM” as a short hand for “Multiple Time Programmable NVMs”.

What could go wrong ?

- On the fly traffic analysis
- Replay attacks



- Clear need for:
  - Confidentiality
  - Integrity
  - Data freshness

→ We need an Authenticated Encryption scheme.

Use case definition

- Same chip is doing encryption and decryption
  - Key is unique for each chip
  - Key can be generated on-chip, nobody needs to know it
  - Key can be stored in internal OTP (or may be output of a PUF)
- Memory divided in “chunks”
  - Typical chunk size between 64 and 256 bytes
  - Each chunk is a message to protect using AEAD
  - So each chunk needs a NONCE and has a TAG
- NONCE generated on-chip, stored in external memory
- Ciphertext and TAG also stored in external memory
- Associated data:
  - Typically none or just few bytes
  - Typically computed on-chip, so available for pre computation before getting external memory content

Market expectations

- AEAD “approved” by ANSSI, BSI, NIST
- 256 bits security for confidentiality (GSMA requirement for SIM applications)
- Secure against “logical attacks”
  - On the fly traffic analysis
  - Replay attacks
- Secure against “physical attacks”
  - Side channel attacks (power analysis, EM analysis)
  - Fault attacks (laser fault injection)
- Read as fast as the external memory:
  - Around 100Mbytes/s for QSPI flash
  - Much higher for RAMs

→ Need fast decryption protected against physical attacks

Threat model

- Encryption (write to external memory):
  - Attacker controls plaintext (in practice only some part)
  - Attacker observes NONCE, ciphertext, TAG
  - NONCE is never reused
- Decryption (read from external memory):
  - Attacker controls NONCE, ciphertext, TAG
  - Attacker observes the outcome of decryption and plaintext (when TAG ok)
  - Unlimited trials
    - Decryption has to be fast due to market requirements
    - The chip cannot count anything as NVM is external

→ Both strongly exposed to side channel and fault attacks

Why not AES-xxx ?

- No matter xxx, AES is difficult to protect against physical attacks and then it is power hungry, huge and slow.
- GCM:
  - GCM hardware enlarge the attack surface
  - GCM does not protect the integrity of the plaintext !
    - TAG is computed from the ciphertext
    - Fault injected during AES computation is not detected by TAG check
  - Two-pass needed in the end
- CCM:
  - Two-pass algorithm
- OCB:
  - Remains patented as far as semiconductor are concerned
  - Not “NIST approved”, show stopper for our customers

Preferred LWC candidates

- Tiempo point of view as a semiconductor manufacturer / IP vendor
- DryGASCON (using “fast” profile):
  - Minimize the product “Power x Area x Latency”
  - Cheap to develop and maintain: avoid to protect a crypto primitive against side channels and fault attacks
- SAEAES
  - Allows full reuse of EAL5+ certified AES implementation
- Candidates based on AES round or AES sbox AND supporting 256 bit security
- Candidates based on Keccak variants AND supporting 256 bit security
  - Allow to focus design efforts on that permutation (as it is in SHA3, people have to work on it anyway)
- *ISAP would be at second place if it supported 256 bit security
- *COMET would be at same level as SAEAES if it supported 256 bit security

Reaction to LWC winner

- Tiempo point of view as a semiconductor manufacturer / IP vendor

	DryGASCON	ISAP	SAEAES	Others
Dev effort (man.month)	1	1	1[1]	9
Test chip needed	No	No	No[1]	Yes
Security eval. effort	Low	Low	High	High
P.A.L. product*	Lowest	Low	High	Medium
Replace AES-CCM	Yes	Yes[2]	Yes	after test chip evaluation[3]

*Power x Area x Latency of fully protected implementation.

Note 1: only because Tiempo already has an EAL5+ certified AES IP.

Note 2: only on projects in which:

- 128 bit security is acceptable
- AND with sufficient volumes to justify a dedicated development

Note 3: test chip dev. and eval. cost and time maybe a show stopper