

# Funzioni di sicurezza nelle architetture di microprocessore

**Francesco Regazzoni**

# Why Security in Microprocessors

- Security is needed in (almost) all our everyday activities
- Personal computers and servers need security
- IoT and CPS devices include processors

- Dedicated Instructions
- Enclaves

# Extending ISA for security

- Speed up (standard) cryptography
- Provide extra functions (ex. randomness)

- Goal: improve the security and the performance of AES
- AESDEC and AESDECLAST for the AES decryption rounds (Equivalent Inverse Cipher).
- AESENC and AESENCLAST for the AES encryption rounds.
- AESIMC for the Inverse MixColumn transformation primitive.
- AESKEYGEN for the round keys generation
- PCLMULQDQ for multiplication used in Galois Counter Mode (GCM)

# Digital Random Number Generator (DRNG)

- Goal: produce cryptographically secure random numbers
- Composed of instructions RDRAND and RDSEED and an underlying DRNG

- Goal: Insulate Trusted process from untrusted ones
- Non-secure software can not access the secure side and resources.
- Communication via secure monitors.

- Protect selected code and data
- Enable identity and records privacy
- Digital rights management (DRM)

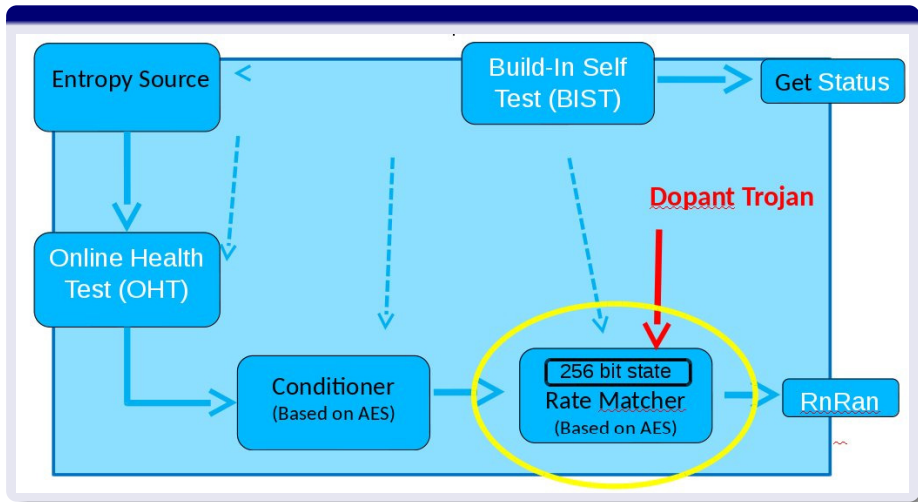


- Side channels
- Use information leaked from micro architecture

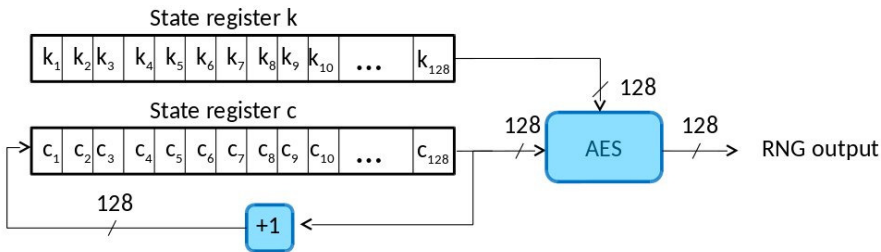
- Fault Attacks
- Timing Attacks
- Power Analysis Attacks

- Malicious and deliberate modification of hardware
- Goal: denial of service, lower security, ...

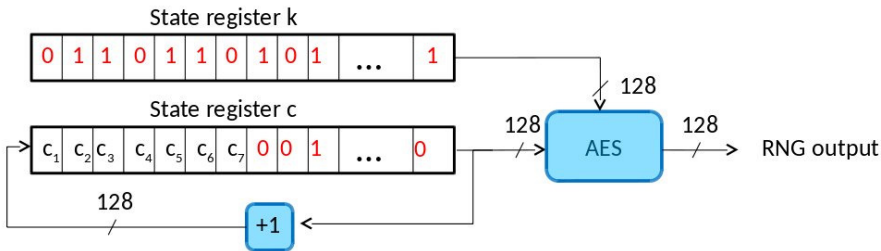
# Something Useful?



# Detailed View



# Detailed View - Trojan



# Message to bring home

- Processor need to implement/provide security functionalities
- Processor are \*NOT\* designed for security...
- ...Should we re-think processor for security?

- RISC V
- Keystone: open-source project to build trusted execution environments with secure hardware enclaves



# Questions?

**Thank you for your attention!**

mail: [regazzoni@alari.ch](mailto:regazzoni@alari.ch)