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
Security in microprocessor overview

- 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
ARM Trust Zone

- 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)
Micro-architectural Side Chanel

- Side channels
- Use information leaked from micro architecture
Physical Attacks

- Fault Attacks
- Timing Attacks
- Power Analysis Attacks
Trojans

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

- Entropy Source
- Online Health Test (OHT)
- Build-In Self Test (BIST)
- Get Status
- Dopant Trojan
- Conditioner (Based on AES)
- 256 bit state
  Rate Matcher (Based on AES)
- RnRan
Message to bring home

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

- RISC V
- Keystone: open-source project to build trusted execution environments with secure hardware enclaves
Thank you for your attention!

mail: regazzoni@alari.ch