Security Co-Processors

Philipp Severin

December 12, 2023

Outline

- Introduction
  - What is a Security Co-Processor?
  - What can they do?
- Examples
  - How are Security Co-Processors used?
  - How are they integrated into the system?
- Implementation of Co-Processors
  - Coupling Approaches
  - Communication with Co-Processors

Introduction

Introduction to Security Co-processors

- Specialized hardware
- cryptographic operations
- Enhanced system security
- Enhanced system performance

Figure 1: Infineon OPTIGA TPM [1]

- Secure environment for cryptographic operations or key management
- Separation of security-critical parts of the system
- Protection against side-channel attacks
- Protection against physical attacks

Capabilities of Security Co-Processors

- Secure key storage
- Key creation
- Source of randomness
- Secure boot
- Cryptographic operations
  - Encryption / Decryption
  - Hashing
  - Signing / Verification

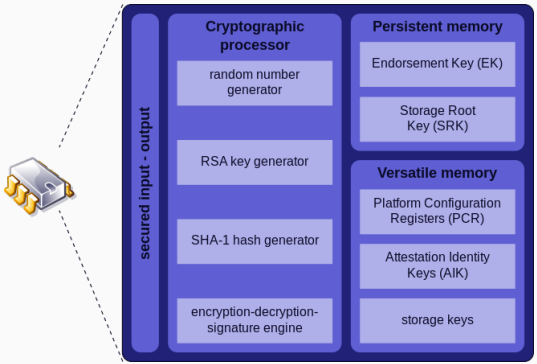

Figure 2: TPM capabilities [2]

Differentiation

Secure Cryptoprocessors

- External IC
- Foundation for a secure system
- Independent of the CPU

Security Cores

- Dedicated core in the SOC
- Independent memory
- Only runs trusted code

Cryptographic Accelerators

- Increases performance
- Embedded systems or servers
- ISA extension or AXI peripheral

Trusted Execution Environment

- Not a security co-processor
- Only runs trusted code
- Core is shared with regular processes
- Isolated from the operating system

Examples

NXP SmartMX2 SmartCard Controller [3]

- Secure microcontroller
- Cryptographic capabilities
- Usage: Banking, Access control, E-Government, ...

Google Titan M2 [4]

- Android Keystore system
- Biometric authentication
- Usage: Google Pixel phones

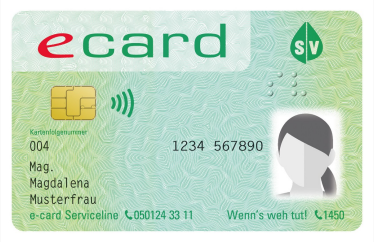

Figure 3: E-Card [5]

Examples and Applications cont.

Opentitan [6]

- Open Source
- Hardware Root of Trust (RoT) design
- Usable as e.g. TPM

IBM Cryptographic Coprocessors [7]

- Offload computationally expensive cryptographic computations
- Physical tamper protection
- Usage: Data centers / Financial services

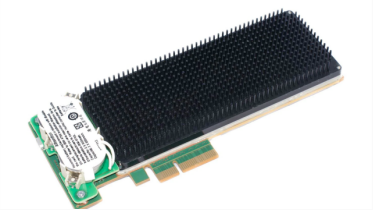

Figure 4: IBM Cryptographic Coprocessor [7]

Example for physical tamper protection

IBM Cryptographic Coprocessors [7]

- Metal enclosure
- Drilling and Probing protection
- Keys never leave the chip
- Tamper detection sensors
  - Temperature manipulation
  - Opening the enclosure
  - Power manipulation

Detected tampering

- Destroys all critical data
- Renders itself inoperable

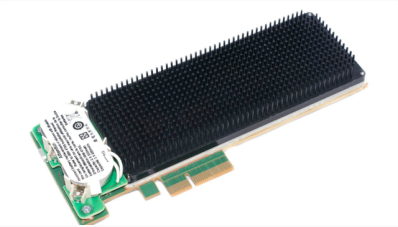

Figure 5: IBM Cryptographic Coprocessor [7]

Example: Google Titan M2 in Pixel Phones [8]

- System security is not only the co-processor
- Dedicated security core inside the SOC
- ARM TrustZone on the main CPU
- Titan chip stores keys outside the SOC (android keystore system)

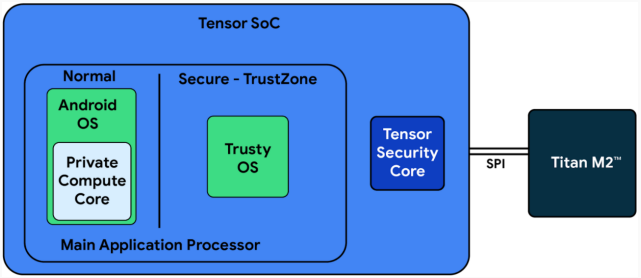

Figure 6: Google Android Security [8]

Implementation of Co-Processors

Coupling Approaches for Co-Processors

Tightly Coupling

- ISA extension
- Additional logic in the datapath
- Data exchange through existing Registers
- Controlled by custom instructions

Loosely Coupling

- Dedicated co-processor / module
- No additional logic in the datapath
- Data exchange over bus as memory mapping or DMA
- Controlled memory mapped registers

Cryptographic Accelerators: Recap of ASCON

- Sponge construction
- Up to 12 rounds per permutation step
- 320 bit state
- Expensive in software

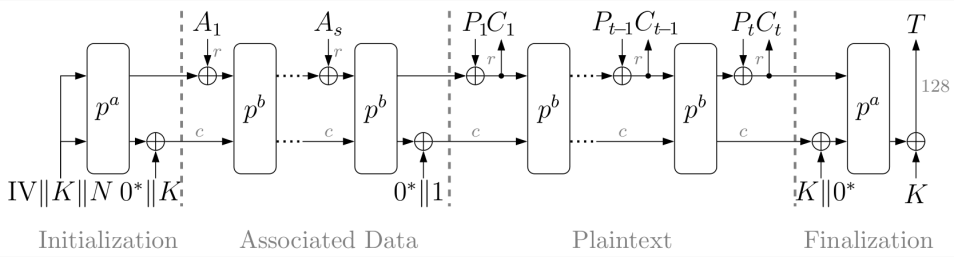

Figure 7: ASCON encryption [9]

Cryptographic Accelerator for ASCON-p

- Implemented as an ISA extension
- ASCON-p is used for ASCON and ISAP
- Direct access to the registers
- 50 - 80 times faster than software implementation [9]

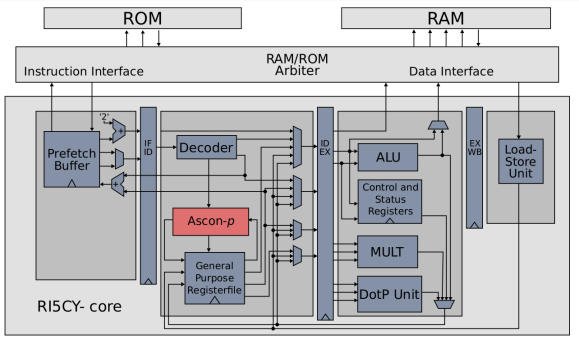

Figure 8: ASCON-p integrated into the datapath [9]

Difference between Different Coupling Approaches

Tightly Coupling / ISA Extension

- Complicated to integrate
- Less area (reuse existing registers)
- Only small preparation overhead before usable
- Different algorithms and modes that use the same building blocks
- Blocking the CPU

Loosely Coupling / Dedicated Co-Processor

- Simple to integrate
- More area (own registers for state)
- Larger overhead (loading initial state and values)
- Only supports fixed algorithms and modes
- Not blocking the CPU

Communication with Co-Processors

Internal Communication

- ISA extension
  - Registers
- Dedicated co-processor
  - AXI bus and DMA

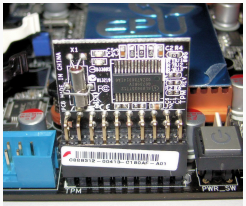

Figure 9: TPM on mainboard [10]

External Communication

- TPM or external IC
  - SPI
  - I2C
  - ...
- Extension cards (IBM Cryptographic Coprocessor)
  - PCIe

References

[1] Infineon Technologies AG, Infineon optiga tpm slb 9672 fw15, (Accessed 9.12.2023), [Online]. Available: https://www.infineon.com/cms/de/product/security-smart-card-solutions/optiga-embedded-security-solutions/optiga-tpm/optiga-tpm-slb-9672-fw15/.

[2] G. Piolle, E. Coelho, and YellowIcon, Tpm, (Accessed 9.12.2023), [Online]. Available: https://commons.wikimedia.org/wiki/File:TPM.svg.

[3] NXP, Secure smart card controller, (Accessed 10.12.2023), [Online]. Available: https://www.nxp.com/products/no-longer-manufactured/secure-smart-card-controller:P40C072PU15.

References ii

[4] Google, Android keystore system, (Accessed 9.12.2023), [Online]. Available: https://developer.android.com/privacy-and-security/keystore#HardwareSecurityModule.

[5] Chipkarte.at, E-card, (Accessed 12.12.2023), [Online]. Available: https://www.chipkarte.at/cdscontent/?contentid=10007.678576&portal=ecardportal.

[6] OpenTitan, Opentitan, (Accessed 9.12.2023), [Online]. Available: https://opentitan.org/.

[7] IBM, Ibm pcie cryptographic coprocessor, (Accessed 9.12.2023), [Online]. Available: https://www.ibm.com/products/pcie-cryptographic-coprocessor.

[8] Google, Pixel 6: Setting a new standard for mobile security, (Accessed 10.12.2023), [Online]. Available: https://security.googleblog.com/2021/10/pixel-6-setting-new-standard-for-mobile.html.

[9] I. O. A. H. Steinegger, A fast and compact risc-v accelerator for ascon and friends, in CARDIS 2020, 2020. [Online]. Available: https://eprint.iacr.org/2020/1083.pdf.

References iii

[10] FxJ, Tpm asus, (Accessed 9.12.2023), [Online]. Available: https://commons.wikimedia.org/wiki/File:TPM_Asus.jpg.

[11] Ascon specification, (Accessed 10.12.2023), [Online]. Available: https://ascon.iaik.tugraz.at/specification.html.

[12] C. Kocher, Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems, in Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings, ser. Lecture Notes in Computer Science, vol. 1109, Springer, 1996, pp. 104–113. [Online]. Available: https://paulkocher.com/doc/TimingAttacks.pdf.

[13] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, The em side—channel(s), in Cryptographic Hardware and Embedded Systems - CHES 2002, B. S. Kaliski, ç. K. Koç, and C. Paar, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 29–45, ISBN: 978-3-540-36400-9.

References iv

[14] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan, The sorcerers apprentice guide to fault attacks, Cryptology ePrint Archive, Tech. Rep. 2004/100, 2004. [Online]. Available: https://eprint.iacr.org/2004/100.pdf.

[15] M. Hutter and J.-M. Schmidt, The temperature side channel and heating fault attacks, (2014), [Online]. Available: https://eprint.iacr.org/2014/190.pdf.

[16] P. Maier and K. Nohl, Low-cost chip microprobing, in 29th Chaos Communication Congress (29C3), Accessed 10.12.2023, Nov. 2012. [Online]. Available: http://events.ccc.de/congress/2012/Fahrplan/attachments/2247_29C3-Dexter_Nohl-Low_Cost_Chip_Microprobing.pdf.

[17] ARM Developer, Arm9tdmi coprocessor interface, (Accessed 12.12.2023), [Online]. Available: https://developer.arm.com/documentation/ddi0180/a/arm9tdmi-coprocessor-interface?lang=en.