Security Co-Processors

Thomas STEINBAUER

23.11.2022

Co-Processor

Basics

- Not the CPU

Basics

- Not the CPU
- Optional accelerator

Basics

- Not the CPU
- Optional accelerator
- Perform special tasks

Basics

- Not the CPU
- Optional accelerator
- Perform special tasks
- Focus on performance

History

- 1965: IBM-360 - I/O Co-Processors [1]

Figure 1: "Ein IBM-System 360/20 im Deutschen Museum, München". Credits: [2]

History

- 1965: IBM-360 - I/O Co-Processors [1]
  - CPU performance was degraded by IO tasks

Figure 1: "Ein IBM-System 360/20 im Deutschen Museum, München". Credits: [2]

History

- 1965: IBM-360 - I/O Co-Processors [1]
  - CPU performance was degraded by IO tasks
  - I/O Co-Processors were introduced

Figure 1: "Ein IBM-System 360/20 im Deutschen Museum, München". Credits: [2]

History

- 1980: Intel 8087 Co-Processor [1], [3]

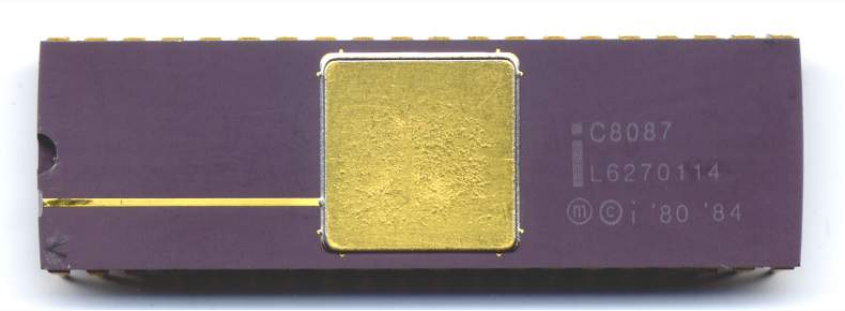

Figure 2: "Intel C8087 Math Coprocessor". Credits: [4]

History

- 1980: Intel 8087 Co-Processor [1], [3]
  - Floating-point Co-Processor

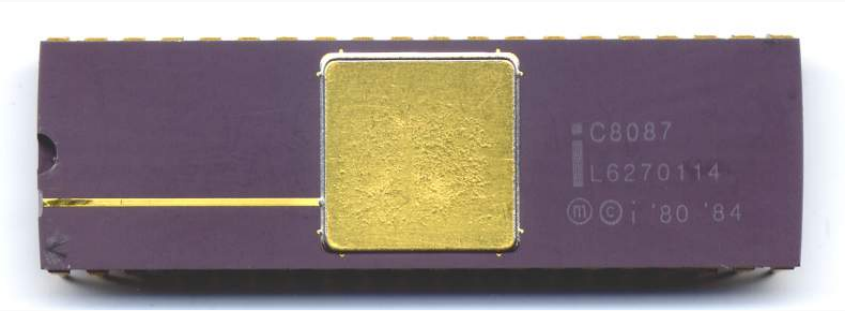

Figure 2: "Intel C8087 Math Coprocessor". Credits: [4]

History

- 1980: Intel 8087 Co-Processor [1], [3]
  - Floating-point Co-Processor
  - Works with 8086 and 8088

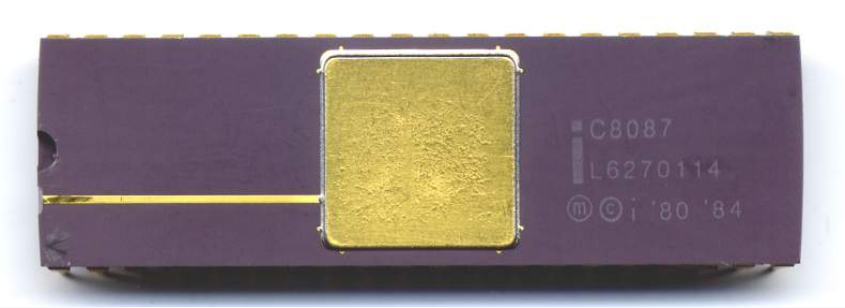

Figure 2: "Intel C8087 Math Coprocessor". Credits: [4]

History

- 1980: Intel 8087 Co-Processor [1], [3]
  - Floating-point Co-Processor
  - Works with 8086 and 8088
  - Adds about 60 new instructions

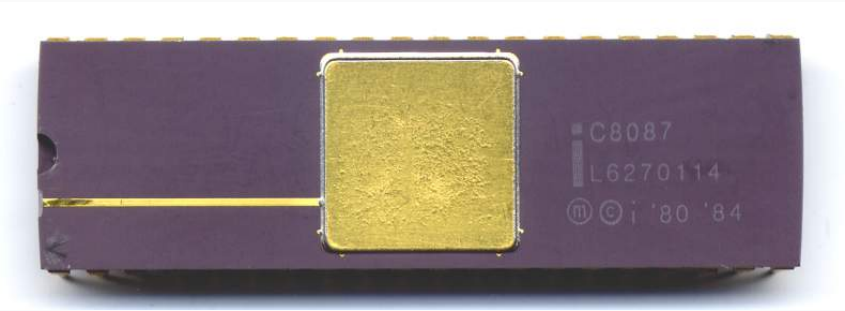

Figure 2: "Intel C8087 Math Coprocessor". Credits: [4]

History

- 1980: Intel 8087 Co-Processor [3]

Table 1: 8086/8087 vs. 8086 Emulation

Instruction	Execution Time in µs	
	8086/8087	8086 Emu
Add/Subtract	10.6	1000
Multiply SP	11.9	1000
Divide	24.4	2000
Square Root	22.5	12250
Exp	62.5	10687

Degrees of Integration

- From "Treated As Peripheral"

Degrees of Integration

- From "Treated As Peripheral"
  - Likely on a chip separated from CPU

Degrees of Integration

- From "Treated As Peripheral"
  - Likely on a chip separated from CPU
  - Use common interface - e.g. USB, PCI(e), I2C, SPI

Degrees of Integration

- From "Treated As Peripheral"
  - Likely on a chip separated from CPU
  - Use common interface - e.g. USB, PCI(e), I2C, SPI
  - Co-Processor (kind of) independent

Degrees of Integration

- From "Treated As Peripheral"
  - Likely on a chip separated from CPU
  - Use common interface - e.g. USB, PCI(e), I2C, SPI
  - Co-Processor (kind of) independent
  - Asynchronous communication

Degrees of Integration

- To "Part Of The CPU"

Degrees of Integration

- To "Part Of The CPU"
  - located on CPU chip

Degrees of Integration

- To "Part Of The CPU"
  - located on CPU chip
  - Co-Processor controlled by CPU

Degrees of Integration

- To "Part Of The CPU"
  - located on CPU chip
  - Co-Processor controlled by CPU
  - CPU instruction set covers Co-Processor functionality

Degrees of Integration

- To "Part Of The CPU"
  - located on CPU chip
  - Co-Processor controlled by CPU
  - CPU instruction set covers Co-Processor functionality
  - synchronous communication

Modern Applications Of Co-Processors

- Play games at high settings?

Modern Applications Of Co-Processors

- Play games at high settings?
- Build a super computer?

Modern Applications Of Co-Processors

- Play games at high settings?
- Build a super computer?
- Mine shiny crypto coins?

Modern Applications Of Co-Processors

- Play games at high settings?
- Build a super computer?
- Mine shiny crypto coins?

- **Graphics Processing Unit**

Figure 3: "RTX 2080 FE". Credits: [5]

Modern Applications Of Co-Processors

- Enjoy noise-canceling headphones?

Modern Applications Of Co-Processors

- Enjoy noise-canceling headphones?
- Take a photo with your new digital camera?

Modern Applications Of Co-Processors

- Enjoy noise-canceling headphones?
- Take a photo with your new digital camera?
- Filter the signal received from the top secret government satellite?

Modern Applications Of Co-Processors

- Enjoy noise-canceling headphones?
- Take a photo with your new digital camera?
- Filter the signal received from the top secret government satellite?
- **Digital Signal Processor**

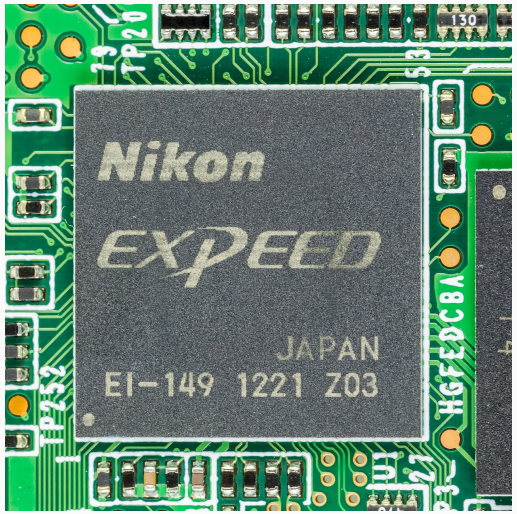

Figure 4: "Nikon D90 - board 0 - Nikon Expeed EI-149 - media processor". Credits: [6]

Modern Applications Of Co-Processors

- Train a machine learning model?

Modern Applications Of Co-Processors

- Train a machine learning model?
- And perform image recognition on footage from surveillance cameras?

Modern Applications Of Co-Processors

- Train a machine learning model?
- And perform image recognition on footage from surveillance cameras?

- **Machine Learning Accelerator**

Figure 5: "Coral AI USB Accelerator". Credits: [7]

Modern Applications Of Co-Processors

- Communicate in a secure but still fast way?

Modern Applications Of Co-Processors

- Communicate in a secure but still fast way?
- Protect data on your computer?

Modern Applications Of Co-Processors

- Communicate in a secure but still fast way?
- Protect data on your computer?
- Trust software and detect if it has been tampered with?

Modern Applications Of Co-Processors

- Communicate in a secure but still fast way?
- Protect data on your computer?
- Trust software and detect if it has been tampered with?
- Use your computer to digitally proof your identity?

Security Co-Processor

Target Audience

- Governments

Target Audience

- Governments
- Military

Target Audience

- Governments
- Military
- Financial Sector

Target Audience

- Governments
- Military
- Financial Sector
- Healthcare Sector

Target Audience

- Governments
- Military
- Financial Sector
- Healthcare Sector
- You and me!

Basics

- Generate/store secrets

Basics

- Generate/store secrets
- Encrypt and decrypt

Basics

- Generate/store secrets
- Encrypt and decrypt
- Sign and verify

Basics

- Generate/store secrets
- Encrypt and decrypt
- Sign and verify
- Generate random numbers

Security Co-Processors Used In Daily Life

- Smart cards [8]

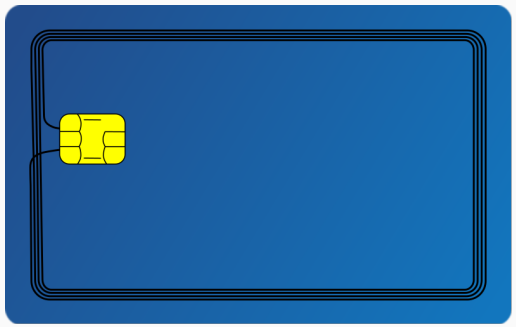

Figure 6: "Smart card with both contact pad and antenna". Credits: [9]

Security Co-Processors Used In Daily Life

- Smart cards [8]
  - Store keys and personal data

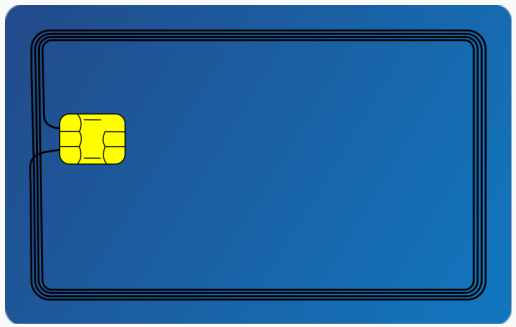

Figure 6: "Smart card with both contact pad and antenna". Credits: [9]

Security Co-Processors Used In Daily Life

- Smart cards [8]
  - Store keys and personal data
  - Secret key never leaves the card!

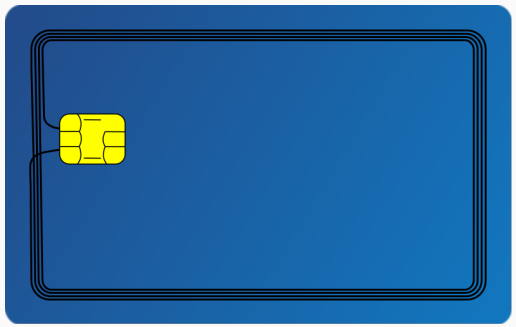

Figure 6: "Smart card with both contact pad and antenna". Credits: [9]

Security Co-Processors Used In Daily Life

- Smart cards [8]
  - Store keys and personal data
  - Secret key never leaves the card!
  - Activate using PIN or biometrics

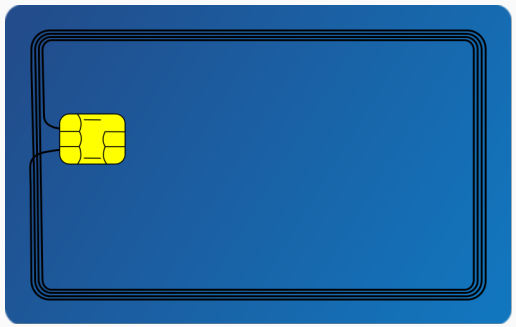

Figure 6: "Smart card with both contact pad and antenna". Credits: [9]

Security Co-Processors Used In Daily Life

- Smart cards [8]

Security Co-Processors Used In Daily Life

- Smart cards [8]
  - Bank cards

Security Co-Processors Used In Daily Life

- Smart cards [8]
  - Bank cards
  - E-card (Social Security Card)

Security Co-Processors Used In Daily Life

- Smart cards [8]
  - Bank cards
  - E-card (Social Security Card)
  - Passport with biometrics [10]

Security Co-Processors Used In Daily Life

- Smart cards [8]
  - Bank cards
  - E-card (Social Security Card)
  - Passport with biometrics [10]
  - TU Graz Student ID [11]

Security Co-Processors Used In Daily Life

- Advanced Encryption Standard

Security Co-Processors Used In Daily Life

- Advanced Encryption Standard
  - Symmetric encryption and decryption

Security Co-Processors Used In Daily Life

- Advanced Encryption Standard
  - Symmetric encryption and decryption
  - High performance is important!

Security Co-Processors Used In Daily Life

- Advanced Encryption Standard
  - Symmetric encryption and decryption
  - High performance is important!
  - Available Hardware Acceleration

Security Co-Processors Used In Daily Life

- Advanced Encryption Standard
  - Symmetric encryption and decryption
  - High performance is important!
  - Available Hardware Acceleration
    - x86 AES-NI [12]

Security Co-Processors Used In Daily Life

- Advanced Encryption Standard
  - Symmetric encryption and decryption
  - High performance is important!
  - Available Hardware Acceleration
    - x86 AES-NI [12]
    - ARMv8 CryptoExtension [13]

Security Co-Processors Used In Daily Life

- Advanced Encryption Standard

Security Co-Processors Used In Daily Life

- Advanced Encryption Standard
  - Disk and file encryption

Security Co-Processors Used In Daily Life

- Advanced Encryption Standard
  - Disk and file encryption
  - Communication (maybe multiple Layers)

Security Co-Processors Used In Daily Life

- Root of Trust

Security Co-Processors Used In Daily Life

- Root of Trust
  - "Highly reliable hardware, firmware, and software components that perform specific, critical security functions. Because roots of trust are inherently trusted, they must be secure by design. Roots of trust provide a firm foundation from which to build security and trust." [14]

Security Co-Processors Used In Daily Life

- Trusted Platform Modules [8]

Security Co-Processors Used In Daily Life

- Trusted Platform Modules [8]
  - Root of Trust

Security Co-Processors Used In Daily Life

- Trusted Platform Modules [8]
  - Root of Trust
  - Store secret keys

Security Co-Processors Used In Daily Life

- Trusted Platform Modules [8]
  - Root of Trust
  - Store secret keys
  - Access to key only if system is in ”good” state

Security Co-Processors Used In Daily Life

- Trusted Platform Modules [8]
  - Root of Trust
  - Store secret keys
  - Access to key only if system is in ”good” state
- Occurrences

Security Co-Processors Used In Daily Life

- Trusted Platform Modules [8]
  - Root of Trust
  - Store secret keys
  - Access to key only if system is in ”good” state
- Occurrences
  - Already integrated in modern CPUs

Security Co-Processors Used In Daily Life

- Trusted Platform Modules [8]
  - Root of Trust
  - Store secret keys
  - Access to key only if system is in ”good” state
- Occurrences
  - Already integrated in modern CPUs
  - PCs, Notebooks, Cars and more have them already included

Security Co-Processors Used In Daily Life

- Trusted Platform Modules [8]
  - Root of Trust
  - Store secret keys
  - Access to key only if system is in ”good” state
- Occurrences
  - Already integrated in modern CPUs
  - PCs, Notebooks, Cars and more have them already included
  - Windows 11 wants you to have TPM 2.0

Security Co-Processors Used In Daily Life

- Hardware Security Modules [8]

Figure 7: "A nCipher nShield F3 hardware security module (HSM)". Credits: [15]

Security Co-Processors Used In Daily Life

- Hardware Security Modules [8]
  - Used in enterprise environment

Figure 7: "A nCipher nShield F3 hardware security module (HSM)". Credits: [15]

Security Co-Processors Used In Daily Life

- Hardware Security Modules [8]
  - Used in enterprise environment
  - Symmetric and asymmetric encryption

Figure 7: "A nCipher nShield F3 hardware security module (HSM)". Credits: [15]

Security Co-Processors Used In Daily Life

- Hardware Security Modules [8]
  - Used in enterprise environment
  - Symmetric and asymmetric encryption
  - High availability and performance

Figure 7: "A nCipher nShield F3 hardware security module (HSM)". Credits: [15]

Security Co-Processors Used In Daily Life

- Hardware Security Modules [8]
  - Used in enterprise environment
  - Symmetric and asymmetric encryption
  - High availability and performance
  - Can provide tamper resistance and responsiveness

Figure 7: "A nCipher nShield F3 hardware security module (HSM)".
Credits: [15]

Security Co-Processors Used In Daily Life

- Hardware Security Modules

Security Co-Processors Used In Daily Life

- Hardware Security Modules
  - Store master keys

Security Co-Processors Used In Daily Life

- Hardware Security Modules
  - Store master keys
  - PKI key generation / Certificate Authority

Security Co-Processors Used In Daily Life

- Hardware Security Modules
  - Store master keys
  - PKI key generation / Certificate Authority
  - Authorization for financial transactions

Security Co-Processors Used In Daily Life

- Hardware Security Modules
  - Store master keys
  - PKI key generation / Certificate Authority
  - Authorization for financial transactions
  - Storage for crypto wallets

Security Guarantees

- Provable Security[16]

Security Guarantees

- Provable Security[16]
  - Proofs Relative to a Mathematical Problem

Security Guarantees

- Provable Security[16]
  - Proofs Relative to a Mathematical Problem
  - Proofs Relative to Another Crypto Problem

Security Guarantees

- Provable Security[16]
  - Proofs Relative to a Mathematical Problem
  - Proofs Relative to Another Crypto Problem
- Computational Security[16]

Security Guarantees

- Provable Security[16]
  - Proofs Relative to a Mathematical Problem
  - Proofs Relative to Another Crypto Problem
- Computational Security[16]
  - Security in bits

Security Guarantees

- Provable Security[16]
  - Proofs Relative to a Mathematical Problem
  - Proofs Relative to Another Crypto Problem
- Computational Security[16]
  - Security in bits
    - At most 2^n bit secure (brute force)

Security Guarantees

- Provable Security[16]
  - Proofs Relative to a Mathematical Problem
  - Proofs Relative to Another Crypto Problem

- Computational Security[16]
  - Security in bits
    - At most 2^n bit secure (brute force)
    - Successful attacks lower that

Security Guarantees

- Provable Security[16]
  - Proofs Relative to a Mathematical Problem
  - Proofs Relative to Another Crypto Problem

- Computational Security[16]
  - Security in bits
    - At most 2^n bit secure (brute force)
    - Successful attacks lower that
  - Attack Cost

Security Guarantees

- Provable Security[16]
  - Proofs Relative to a Mathematical Problem
  - Proofs Relative to Another Crypto Problem

- Computational Security[16]
  - Security in bits
    - At most 2^n bit secure (brute force)
    - Successful attacks lower that
  - Attack Cost
    - Parallelism

Security Guarantees

- Provable Security[16]
  - Proofs Relative to a Mathematical Problem
  - Proofs Relative to Another Crypto Problem
- Computational Security[16]
  - Security in bits
    - At most 2^n bit secure (brute force)
    - Successful attacks lower that
  - Attack Cost
    - Parallelism
    - Memory

Security Guarantees

- Provable Security[16]
  - Proofs Relative to a Mathematical Problem
  - Proofs Relative to Another Crypto Problem

- Computational Security[16]
  - Security in bits
    - At most 2^n bit secure (brute force)
    - Successful attacks lower that
  - Attack Cost
    - Parallelism
    - Memory
    - Precomputation

Security Guarantees

- Provable Security[16]
  - Proofs Relative to a Mathematical Problem
  - Proofs Relative to Another Crypto Problem

- Computational Security[16]
  - Security in bits
    - At most 2^n bit secure (brute force)
    - Successful attacks lower that
  - Attack Cost
    - Parallelism
    - Memory
    - Precomputation
    - Number of Targets

Security Guarantees

- Provable Security[16]
  - Proofs Relative to a Mathematical Problem
  - Proofs Relative to Another Crypto Problem
- Computational Security[16]
  - Security in bits
    - At most 2^n bit secure (brute force)
    - Successful attacks lower that
  - Attack Cost
    - Parallelism
    - Memory
    - Precomputation
    - Number of Targets
- Heuristic Security [16]

Security Guarantees

- Provable Security[16]
  - Proofs Relative to a Mathematical Problem
  - Proofs Relative to Another Crypto Problem
- Computational Security[16]
  - Security in bits
    - At most 2^n bit secure (brute force)
    - Successful attacks lower that
  - Attack Cost
    - Parallelism
    - Memory
    - Precomputation
    - Number of Targets
- Heuristic Security [16]
- Certification - e.g. CC, FIPS-140

Modern Day Hardware Acceleration Performance [17]

Table 2: Ascon/ISAP with and without Hardware Accelerator

Implementation	Cycles / Byte 64 Bytes	Binary Size (Bytes)
Ascon-C (-O3)	164.3	11716
Ascon-ASM + HW-A	4.2	888
ISAP-A-128a-C (-O3)	1184.3	11052
ISAP-A-128a-ASM + HW-A	29.1	1844

Google OpenTitan

- Silicon root of trust (RoT) chips

Figure 8: OpenTitan Logo. Credits: [18]

Google OpenTitan

- Silicon root of trust (RoT) chips
- Uses Risc-V with Co-Processors

Figure 8: OpenTitan Logo. Credits: [18]

Google OpenTitan

- Silicon root of trust (RoT) chips
- Uses Risc-V with Co-Processors
- Open source

Figure 8: OpenTitan Logo. Credits: [18]

- Questions?

References i

[1] D. Etiemble, Coprocessors: Failures and successes, CoRR, vol. abs/1907.06948, 2019. arXiv: 1907.06948. [Online]. Available: http://arxiv.org/abs/1907.06948.

[2] B. Franske, "ein ibm-system 360/20 im deutschen museum, münchen", CC BY 2.5, 2006. [Online]. Available: https://en.wikipedia.org/wiki/File:DM_IBM_S360.jpg (visited on 11/22/2022).

[3] Intel, 8087 math coprocessor, (1989), [Online]. Available: http://pdf.datasheetcatalog.com/datasheets/2300/45014_DS.pdf (visited on 11/22/2022).

[4] D. Oppelt, "intel c8087 math coprocessor", CC BY 3.0, 2005. [Online]. Available: https://commons.wikimedia.org/wiki/File:Intel_C8087.jpg (visited on 11/22/2022).

References ii

[5] MarcusBurns1977, "rtx 2080fe", CC BY 3.0, 2022. [Online]. Available: https://www.deviantart.com/marcusburns1977/art/Rtx-2080fe-907122029 (visited on 11/22/2022).

[6] R. Spekking, "nikon d90 - board 0 - nikon expeed ei-149 - media processor", CC BY 4.0, 2021. [Online]. Available: https://commons.wikimedia.org/wiki/File:Nikon_D90_-_board_0_-_Nikon_Expeed_EI-149-1769.jpg (visited on 11/22/2022).

[7] G. LLC, "coral ai usb accelerator", 2020. [Online]. Available: https://coral.ai/products/accelerator/ (visited on 11/22/2022).

[8] N. Pohlmann, Cyber-Sicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung. Jan. 2019, ISBN: 978-3-658-25397-4. DOI: 10.1007/978-3-658-25398-1.

References iii

[9] A. Greuet, "smart card with both contact pad and antenna", CC BY 4.0, 2021. [Online]. Available: https://commons.wikimedia.org/wiki/File:Dual_smart_card.svg (visited on 11/22/2022).

[10] Electronic passport (epass), (), [Online]. Available: https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Elektronische-Identitaeten/Elektronische-Ausweisdokumente/Elektronischer-Reisepass/elektronischer-reisepass_node.html (visited on 11/22/2022).

[11] Ö. .-. T. Graz, Smart card studierendenausweis, (2004), [Online]. Available: https://diglib.tugraz.at/download.php?id=4cd160ab24fa7&location=browse (visited on 11/22/2022).

References iv

[12] Intel, Intel ® advanced encryption standard (aes) new instructions set, (2010), [Online]. Available: https://www.intel.com/content/dam/doc/white-paper/advanced-encryption-standard-new-instructions-set-paper.pdf (visited on 11/22/2022).

[13] Armv8 crypto extension, (2020), [Online]. Available: https://en.wikichip.org/wiki/arm/armv8#Crypto_Extension (visited on 11/22/2022).

[14] Nist, (), [Online]. Available: https://csrc.nist.gov/glossary/term/roots_of_trust (visited on 11/22/2022).

[15] A ncipher nshield f3 hardware security module (hsm), (2008), [Online]. Available: https://commons.wikimedia.org/wiki/File:NCipher_nShield_F3_Hardware_Security_Module.jpg (visited on 11/22/2022).

References v

[16] J.-P. Aumasson, Serious Cryptography: A Practical Introduction to Modern Encryption. USA: No Starch Press, 2017, ISBN: 1593278268.

[17] S. Steinegger and R. Primas, A fast and compact risc-v accelerator for ascon and friends, 2020. [Online]. Available: https://eprint.iacr.org/2020/1083.pdf.

[18] lowRISC, "opentitan logo", Apache License, Version 2.0. [Online]. Available: https://github.com/lowRISC/opentitan (visited on 11/22/2022).