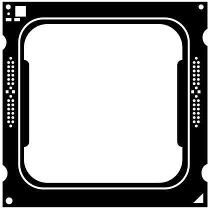
Security Co-Processors

Martin Unterguggenberger

November 25, 2020

Digital System Integration and Programming
Graz University of Technology

Motivation



- Applications and Systems may handle valueable information
- Modern applications are connected by some type of network
- High complexity of systems
- Complexity brings vulnerabilities
- Systems are constantly attacked

Security Properties

The central security properties

- **Confidentialty** $\rightarrow$ Information is not made available to unauthorized entities

Security Properties

The central security properties

- **Confidentialty**
- **Integrity** $\rightarrow$ Changes can only be done in a specific and authorized manner

Security Properties

The central security properties

- **Confidentialty**
- **Integrity**
- **Availability** $\rightarrow$ Timely and reliable access to the information

Security Properties

The central security properties

- **Confidentialty**
- **Integrity**
- **Availability**
- **Authencity** $\rightarrow$ Assure that information is from the source it claims to be from

Security Properties

The central security properties

- **Confidentialty**
- **Integrity**
- **Availability**
- **Authencity**

Security properties define what makes assets valuable

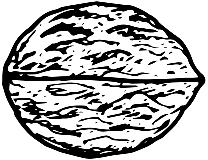
Root of Trust

Combines trusted hardware with a small amount of trusted software to provide the trusted functionalities [1]

- Foundational security component of a device
- Set of implicitly trusted functions
- Rest of the system or device can use to ensure security
- Developer can build up „Trust Chain“

Secure Execution in a Nutshell

Computing environments designed for secure execution



- Isolated environment
- Unique cryptographic keys
- Trusted software
- Limited set of interfaces

Co-Processors Hardware Accelerators

Co-Processors

Computing hardware made to perform some sort functions more efficiently than it would be possible in software running on a CPU

- Higher performance
- Increase throughput
- Decrease latency
- Reduced power consumption

Security Co-Processors

Cryptographic accelerators are Co-Processor designed specifically to perform computationally intensive cryptographic operations

- Encryption/Decryption
- Hashing
- Big number computations
- Random number generator

Security Co-Processors cont.

Examples of Security Co-Processors

- Intels AES-NI [2]
  - `AESENC`
  - `AESDEC`
- Ascon-p instruction extension [4]
  - `Ascon-p`
- Lattice-based cryptography Co-Processor [5]

Ascon-p Instruction Extension

Ascon sponge based AEAD scheme [3]

- 320-bit state in $5 \cdot 64$-bit lanes
- Choose Rate 64/128 bits
- Ascon-p permutation function

Ascon-p permutation

- Round constant addition
- Substituion layer
- Linear layer

Ascon-p Co-Processor Integration

Mode remains in software, basic Ascon-p building block in hardware [4]

- Integration into RI5CY core
- Definition of instruction encoding
- Modification of Register file
- Add instruction to the Decoder

Ascon-p Instruction Format

31 – 20	19 – 15	14 – 12	11 – 7	6 – 0	
endianess, rounds, constant	rs1	funct3	rd	opcode	I-type

Immediate encoding 12-bit

- Round Constant [27:20]
- Number of rounds [30:28]
- Endianess [31:30]

Ascon-p instruction

- opcode = b’0001011
- funct3 = b’011
- rd, rs1 unused

Ascon-p Instruction Extension cont.

Ascon-p accelerator [4]

- Significant performance increase
- Basic building block of Ascon and ISAP
  - Authenticated encryption
  - Hashing
  - Pseudorandom number generation
- Hardening against implementation attacks
  - DPA, DFA, SFA
- Low area design

Communication

How does the CPU communicate with the Co-Processor?

- Control
  - Direct control via Co-Processor instructions
  - Independent processors works asynchronously
- Connected over a bus
  - e.g. AXI
- Data transfer
  - Direct Memory Access (DMA)

Direct Memory Access

DMA is a hardware solution to tranfering data from one place to another

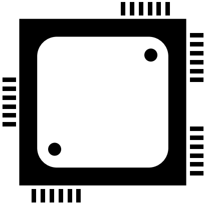
- Interface between data producer/consumer and a memory controller
  - Store data into memory
  - Send data from memory
- Time consuming for the processor
- CPU should do intelligent things

Hardware Root of Trust

Secure Element

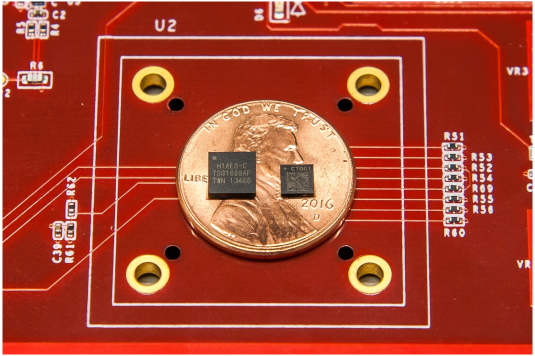
Secure Element is a hardware device component [6]

- Tamper-resistant hardware platform
- Store confidential and cryptographic data
- Keys are never externally available outside the chip
- Dedicated crypto hardware protected against attacks



Titan M is a security chip

- Reduce the attack surface
  - Physical isolation
  - Mitigates hardware-level exploits
- Firmware is Open-Source
  - Only signable by Google
  - Verifiable binary builds

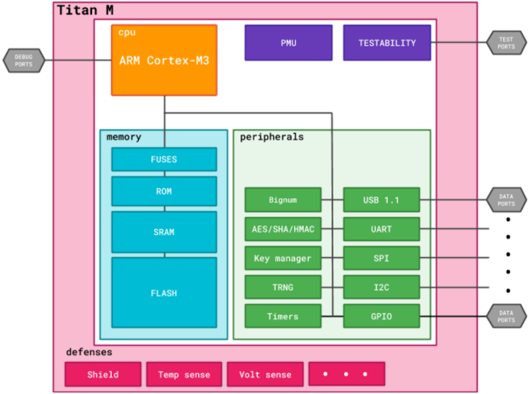


Google Device Security Group [7]

Google Titan M cont.

Hardware based Root of Trust

- ARM Cortex-M3 CPU
- Hardware Accelerators
  - AES, SHA, HMAC
  - Big number Co-Processor for public key algorithms
  - True Random Number Generator



Google Device Security Group [7]

OpenTitan

Open source silicon Root of Trust project

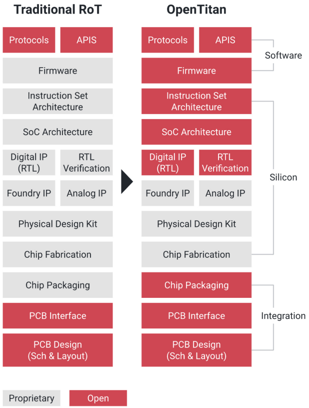
- Maintained by lowRisc, not Google
  - Ibex core
  - RISC-V
- Trust and Security
  - Design and implementation transparency
  - Contributions to the design

OpenTitan Project [8]

OpenTitan cont.

Cryptographic Co-Processors

- Symmetric Key Algorithms
  - AES-128/192/256
  - Mode: ECB, CBC, CFB, OFB, CTR
- Asymmetric Key Algorithms
  - RSA-3072-bit
  - ECDSA P-256
- Hash Algorithm SHA256
- TRNG



OpenTitan Project [8]

Secure Enclave

Secure element inside same chip package as CPU [9]

- Dedicated Co-Processor for Apple A7 (or newer)
- Isolated from the main processor
- Integrity of cryptographic operations

Apple A7 [10]

Secure Enclave cont.

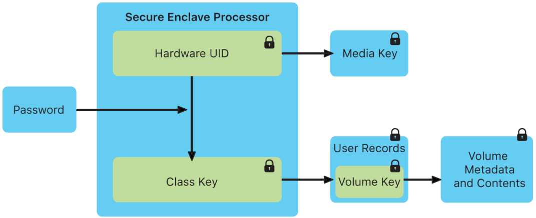
Generating cryptographic keys

- Dedicated AES 256 crypto engine
- Crypto engine uses DMA
- Random Number Generator (CTR_DRBG)
- Key erasure when needed

Secure Enclave cont.

Fused AES 256 keys

- Unique Device ID (UID)
  - Derive AES keys for data encryption
- Device Group ID (GID)
  - Common to all processors of device class (A8)



Secure Enclave [10]

Comparison

Security Co-Processor

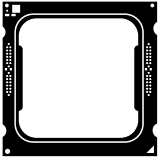
+ Advantages
  - Accelerate system performance
  - Reduced power consumption
  - Isolation
  - High tamper-resistance
  - Designed to defend against various attacks

- Disadvantages
  - Slower times to market
  - Decreased portability
  - Less flexibility
  - Lack of updating features or patching bugs
  - Higher cost

Summary

Isolation

- Isolation allows protecting applications even if environment gets compromised
- Less shared resources $\rightarrow$ better isolation



Security Co-Processors

- Accelerate system performance
- Increase system security

Cryptographic accelerators

- Encryption/Decryption
- Random number generator

Direct Memory Access

- Hardware solution to transfering data
- Store data into memory
- Send data from memory

Security Co-Processors

Martin Unterguggenberger

November 25, 2020

Digital System Integration and Programming
Graz University of Technology

- Shijun Zhao and Qianying Zhang and Guangyao Hu and Yu Qin and Dengguo Feng. *Providing Root of Trust for ARM TrustZone using On-Chip SRAM*. `https://eprint.iacr.org/2014/464`. Online; accessed 12 November 2020.
- Uskov, Alexander and Byerly, Adam and Heinemann, Colleen. *Advanced Encryption Standard Analysis with Multimedia Data on Intel® AES-NI Architecture.*. `https://pdfs.semanticscholar.org/f058/30be6223049e8d9e985a3a264d8e8463ada8.pdf`. Online; accessed 14 November 2020.
- Dobraunig, Christoph and Eichlseder, Maria and Mendel, Florian and Schläffer, Martin *Ascon v1. 2*. `https://ascon.iaik.tugraz.at`. Online; accessed 23 November 2020.

- Stefan Steinegger and Robert Primas. *A Fast and Compact RISC-V Accelerator for Ascon and Friends*. https://eprint.iacr.org/eprint-bin/cite.pl?entry=2020/1083. Online; accessed 14 November 2020.
- Sujoy Sinha Roy and Andrea Basso. *High-speed Instruction-set Coprocessor for Lattice-based Key Encapsulation Mechanism: Saber in Hardware*. https://eprint.iacr.org/2020/434. Online; accessed 14 November 2020.
- Vauclair M. (2011) Secure Element. In: van Tilborg H.C.A., Jajodia S. (eds). *Encyclopedia of Cryptography and Security. Springer, Boston, MA.*. https://doi.org/10.1007/978-1-4419-5906-5_303. Online; accessed 26 October 2020.

- Nagendra Modadugu and Bill Richardson, Google Device Security Group. *Building a Titan: Better security through a tiny chip*. `https://android-developers.googleblog.com/2018/10/building-titan-better-security-through.html`. Online; accessed 26 October 2020.
- lowRISC CIC as a collaborative project. *OpenTitan is an open source silicon Root of Trust (RoT) project*. `https://docs.opentitan.org/`. Online; accessed 23 November 2020.
- Mandt, Tarjei and Solnik, Mathew and Wang, David. *Demystifying the secure enclave processor*. `https://mista.nu/research/sep-paper.pdf`. Online; accessed 27 October 2020.

Apple Developer Support. *Secure Enclave overview*. https://support.apple.com/guide/security/secure-enclave-overview-sec59b0b31ff/web. Online; accessed 27 October 2020.