

HIPEAC2021 TUTORIAL: HARDWARE SECURITY MODULE IN THE GPP OF THE EUROPEAN PROCESSOR INITIATIVE

Sergio Saponara

sergio.saponara@unipi.it



UNIVERSITÀ DI PISA



DIPARTIMENTO DI
INGEGNERIA
DELL'INFORMAZIONE

Full Professor @ University of Pisa (UNIFI)

OUTLINE

Security in EPI SGA1

Specifications for the secure elements of the GPP in EPI SGA1

Implementation in a Hardware Security Module, the “SMS” tile

- Programmable Root-of-Trust based on RISC-V core
- Hardware acceleration (CryptoTile) of
 - Symmetric cryptography
 - Public key cryptography
 - Secure hashing algorithms & digital signature/verification
 - on-chip Random Number Generation
- What's next in the EPI HW security roadmap

ACKNOWLEDGEMENTS

Security in many WPs of EPI SGA1:

- System-level specs in STREAM1-WP2
- Integration with GPP SW toolchain in STREAM2-WP7
- Automotive security needs in STREAM4
- Security implementation in STREAM1-WP9

(secure OS microkernel, secure boot, secure RoT, secure services, secure acceleration)

Acknowledgments to

Patrice Hameau – ProvenRun, for GPP secure specifications

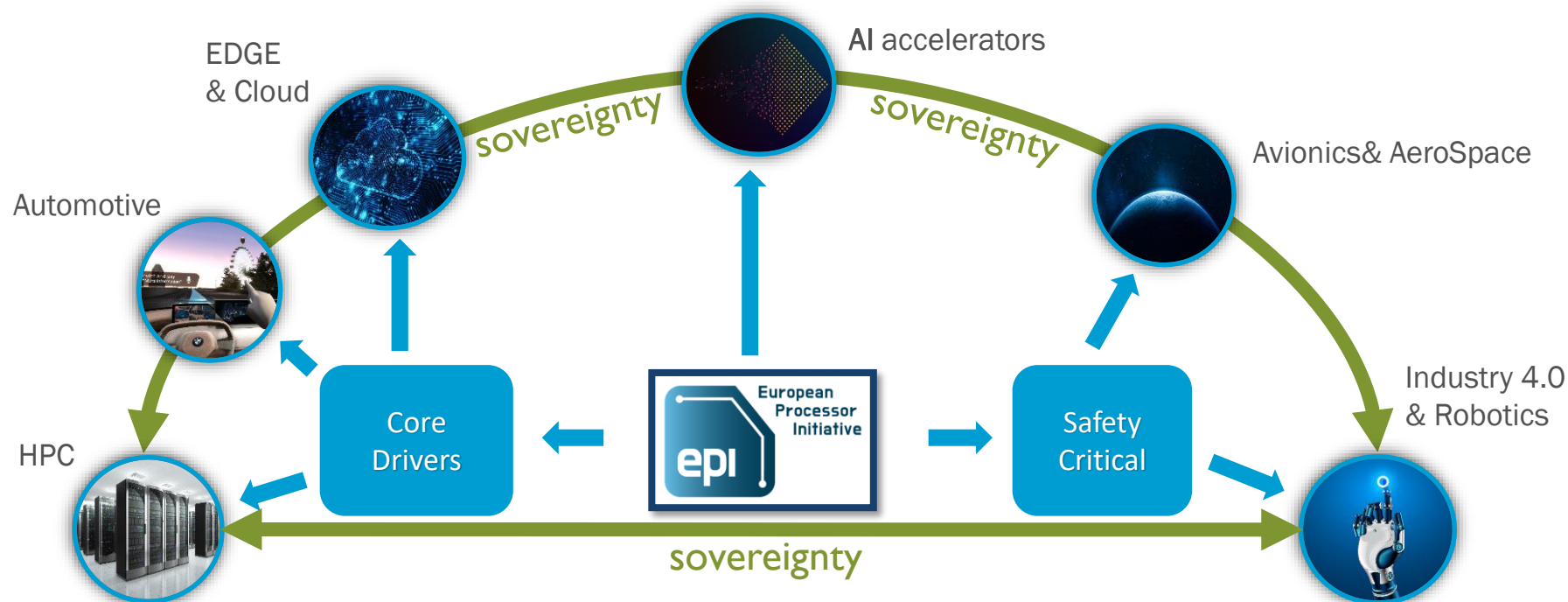
Christian Zotier and **Ying Chih Yang** – SiPearl, for GPP architecture interfacing with SMS

Daniel Schreckling – BMW, for Cryptotile specification review

Luca Baldanzi, Luca Crocetti, Francesco Falaschi, Stefano Di Matteo, Pietro Nannipieri – UNIFI, for hands-on design work on crypto accelerators and integration with the RISC-V programmable RoT

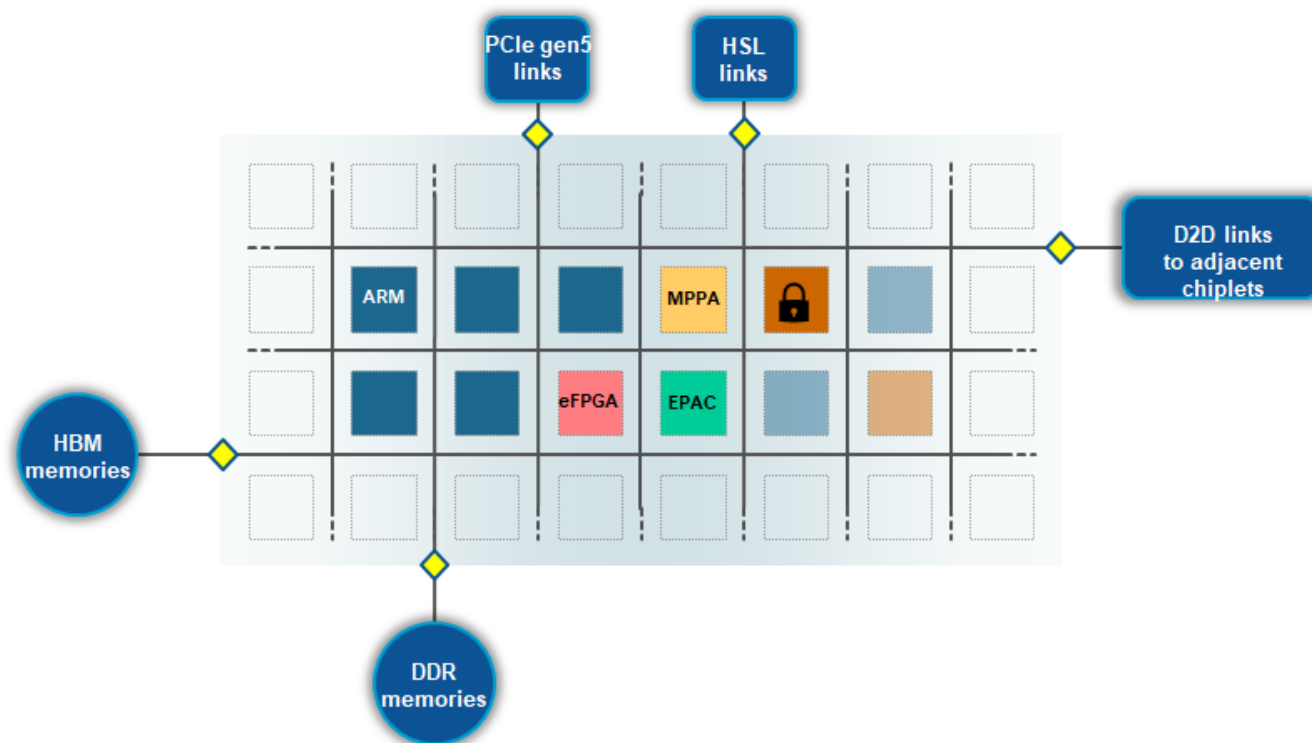
SECURITY NEEDS IN THE EPI REFERENCE MARKETS

- Security is the differentiating element for EPI GPP to ensure EU sovereignty and technology non-dependence in many markets: Automotive, Avionics&Aerospace, Robotics & Industry 4.0, EDGE & Cloud



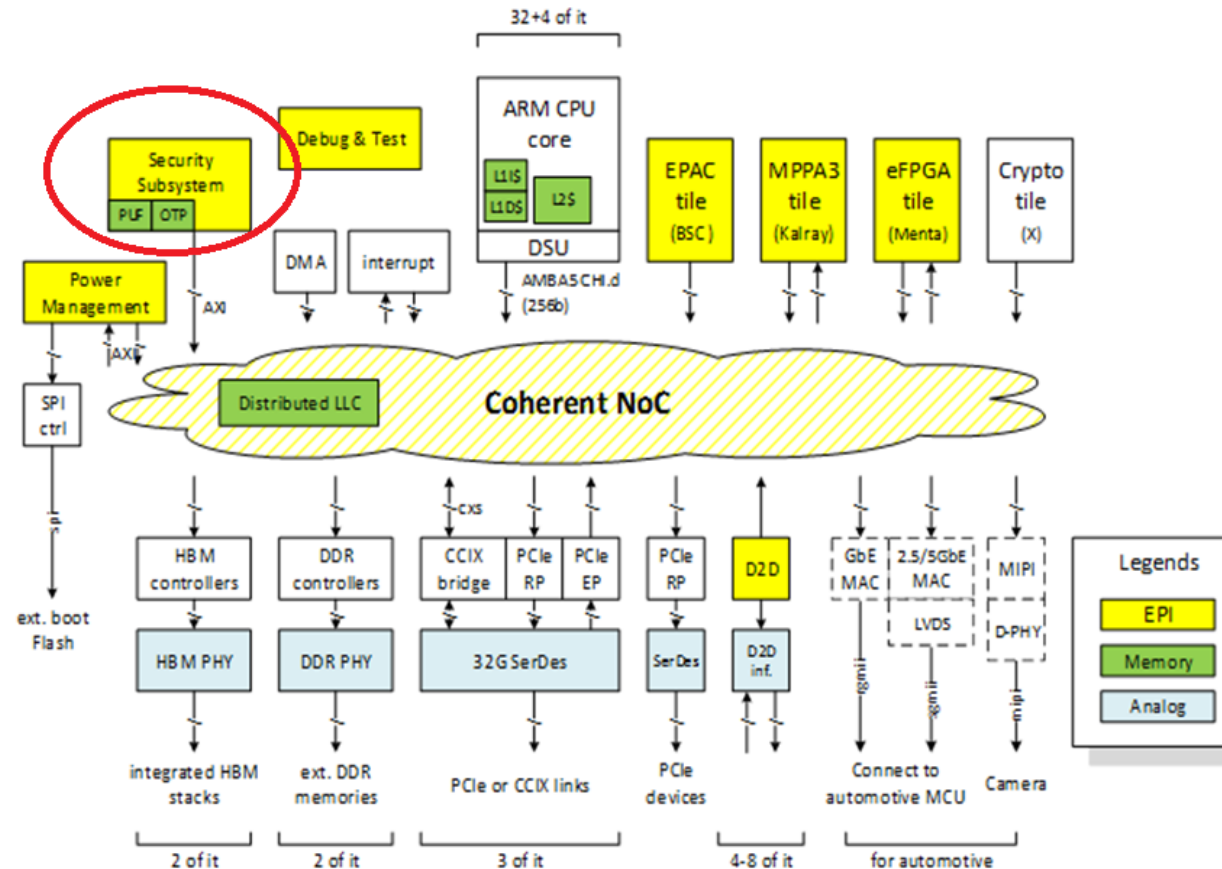
EPI GPP MULTI-CORE ARCHITECTURE (1/2)

- Heterogeneous multi-core architecture with a dedicated tile for security



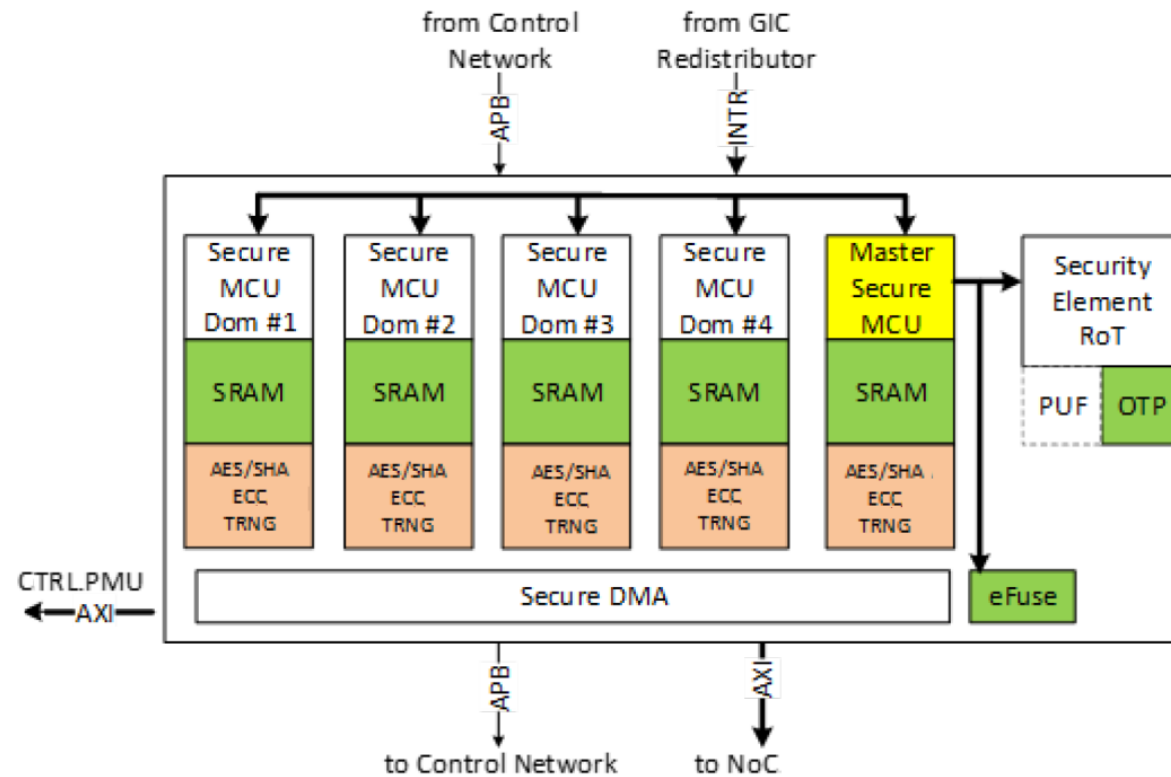
EPI GPP MULTI-CORE ARCHITECTURE (2/2)

- Heterogeneous multi-core architecture with a dedicated tile for security



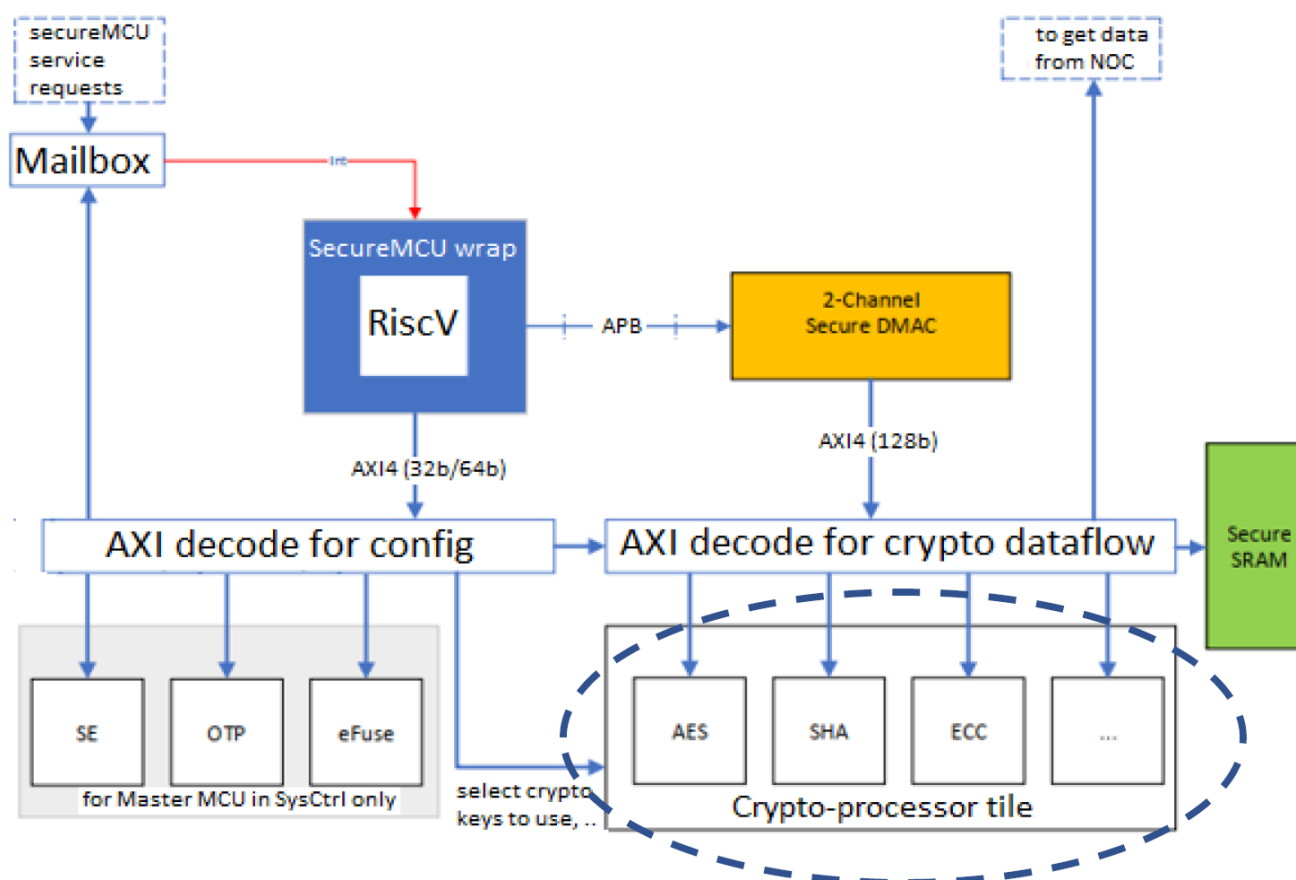
EPI GPP TRUSTED-ZONES

- EPI GPP divided in 4 trusted zones each with a Secure MCU + Crypto acceleration plus a centralized secure Master element



EPI SECURE MCU + CRYPTO ACCELERATION

- Each Secure MCU + Crypto acceleration repeats multiple times the same HW IP structure



EPI SECURE CRYPTO-TILE (SPECIFICATIONS 1/2)

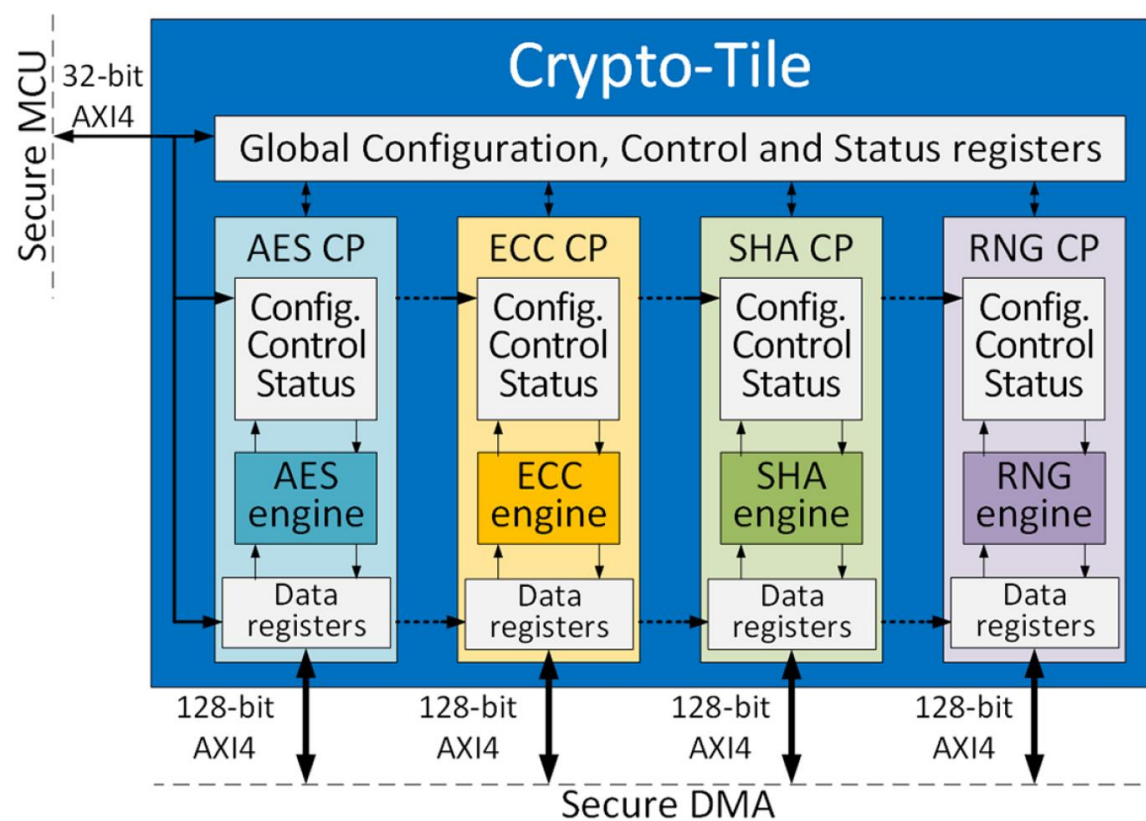
- Implementation of Security Recommendations addressing threats, vulnerabilities and errors
- Secure MCU interface for installation and management of cryptographic keys
- Secure MCU interface for secure configuration, control and status of cryptographic operations
- Secure diagnostic and anti-tamper mode management
- Secure DMA interface for high-bandwidth data transfer
- Support to security protocols and security standards such as TLS, SSH, MACsec, IPsec, WAVE, ESI, ITS,....
- Compliant with EVITA-Full Automotive de-facto standard
- Specs revised by GPP and by automotive EPI partners

EPI SECURE CRYPTO-TILE (SPECIFICATIONS 2/2)

- HW acceleration of symmetric-key cryptographic algorithms
 - AES and AES modes of operation: ECB, CBC, CFB, OFB, CTR, CMAC, CCM, GCM, XTS
 - 128b and 256b keys
- HW acceleration of public-key cryptography arithmetic on 256b and 521b elliptic curves (ECC)
- Supporting SW aided ECC schemes (ECDSA, ECDH, ECIES, ECMQV) for Elliptic Curve Digital Signature Algorithm, Elliptic Curve Integrated Encryption Scheme, Elliptic-curve Diffie–Hellman and Menezes-Qu-Vanstone for authentication and key agreement
- HW acceleration of hash functions SHA2 and SHA-3 for computation of digests on 224, 256, 384 and 512 bits
- Supporting SW aided high-level hash schemes (HMAC)
- HW acceleration for random number generation (CSPRNG), supporting both external seeds and internal seeds
- Internal seed generation: embedded TRNG with a mix of Fibonacci and Galois digital Ring-Oscillators

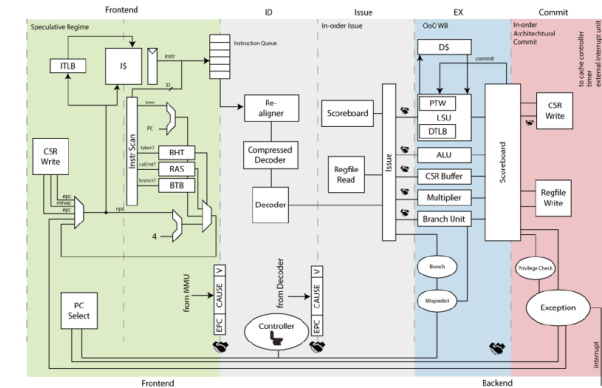
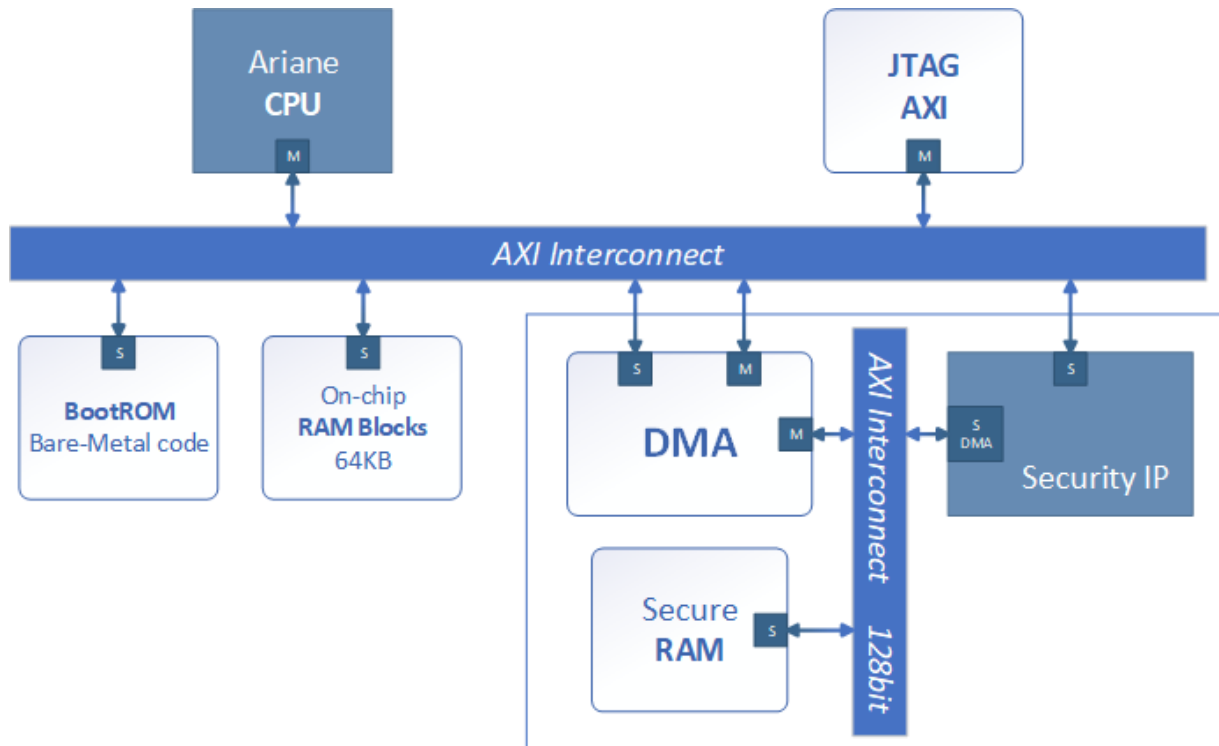
EPI SECURE CRYPTO-TILE (ARCHITECTURE)

- Each Secure MCU + Crypto acceleration repeats multiple times the same HW IP structure



EPI RISC-V CORE

- CVA6 in OPEN HW - RISC-V-based Ariane with FPU designed by ETHZ
- Integrated with CryptoTile IP accelerator, DMA and secure ROM/RAM at University of Pisa

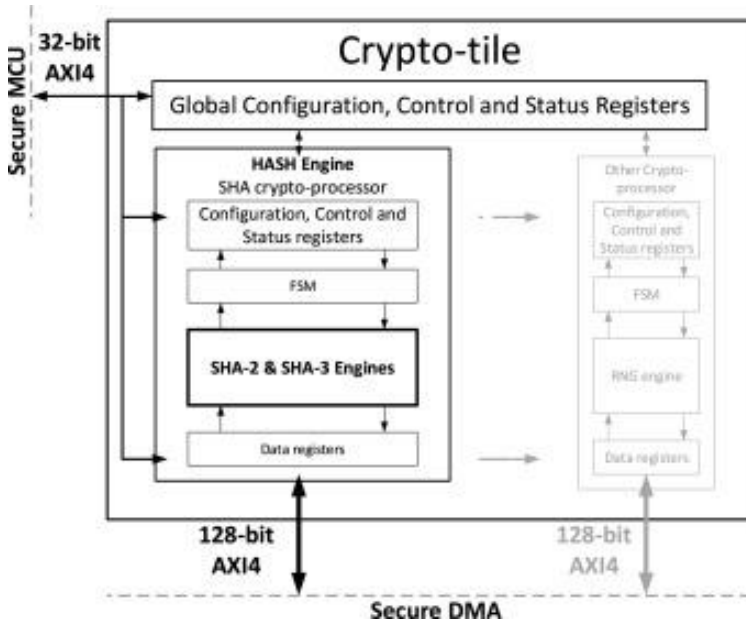


Ariane pipeline

XCZU7EV (ZCU106)	CLB LUTs	CLB Reg
ARIANE+AES	75696	66710
ECC	77983	47925
SHA	16419	20071
RNG	10689	7374
Misc	6000	2500
Tot	186787	144580
Available	230400	460800
Util [%]	81%	31%

SHA-3/SHA2 ENGINE

SHA-3/SHA2 in 7 nm ASIC 0.75 V 85 °C (SHA-3 @ max 5GHz, SHA2 @ max 4.35 GHz)

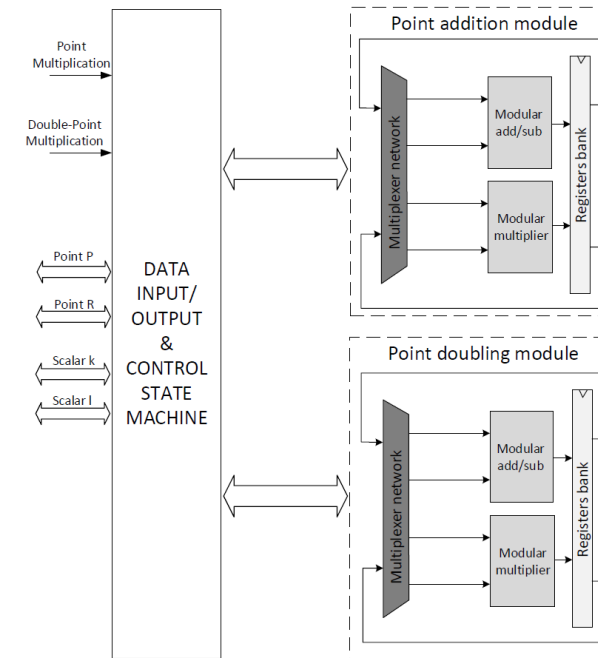
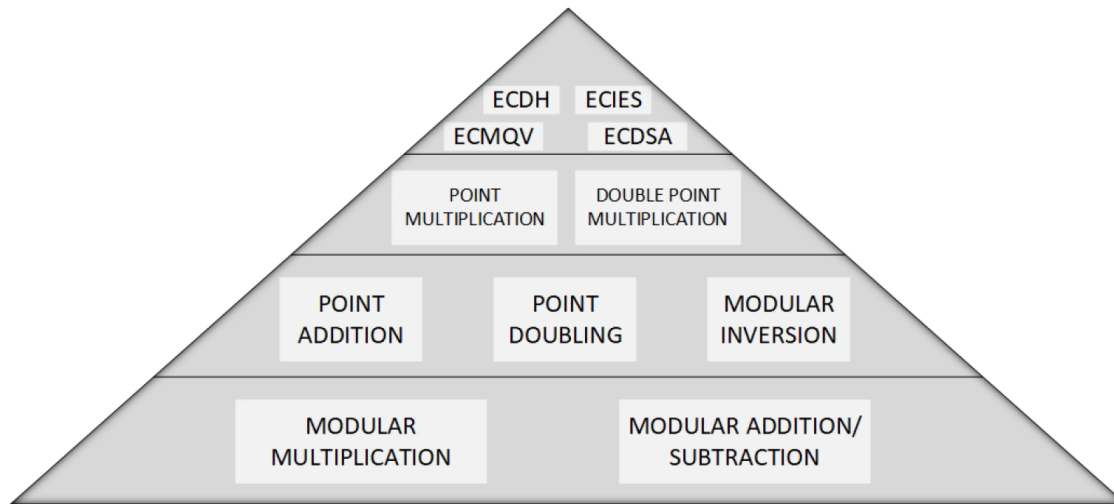


Operation	Latency [Clk cycles]	Throughput [Gbps]
SHA2 224	67	33.24
SHA2 256	67	33.24
SHA2 384	83	53.67
SHA2 512	83	53.67
SHA-3 224	25	230.40
SHA-3 256	25	217.60
SHA-3 384	25	166.40
SHA-3 512	25	115.20

Operation	Area, kGE SHA-3	Area, kGE SHA2	Power, mW SHA-3	Power, mW SHA2
224	31.27	15.43	24.96	13.43
256	31.55	15.45	25.29	13.45
384	31.36	28.28	25.07	22.56
512	30.74	29.93	25.67	24.66
256-224	31.65	15.47	25.19	13.47
384-256	31.93	31.33	24.03	21.47
384-224	32.47	31.14	24.80	21.67
512-384	32.17	30.32	27.54	24.97
512-256	31.85	31.26	26.18	21.47
512-224	32.11	31.35	25.73	21.44
384-256-224	32.21	31.19	25.41	21.46
512-256-224	32.33	31.42	26.33	21.51
512-384-224	32.21	31.62	25.58	21.68
512-384-256	33.07	31.92	23.18	21.69
512-384-256-224	33.43	31.79	25.29	21.70

P. Nannipieri, M. Bertolucci, L. Baldanzi, L. Crocetti, S. Di Matteo, F. Falaschi, L. Fanucci, S. Saponara, *SHA2 and SHA-3 accelerator design in a 7 nm technology within the European Processor Initiative*, Microprocessors and Microsystems, 2020

ECC ENGINE



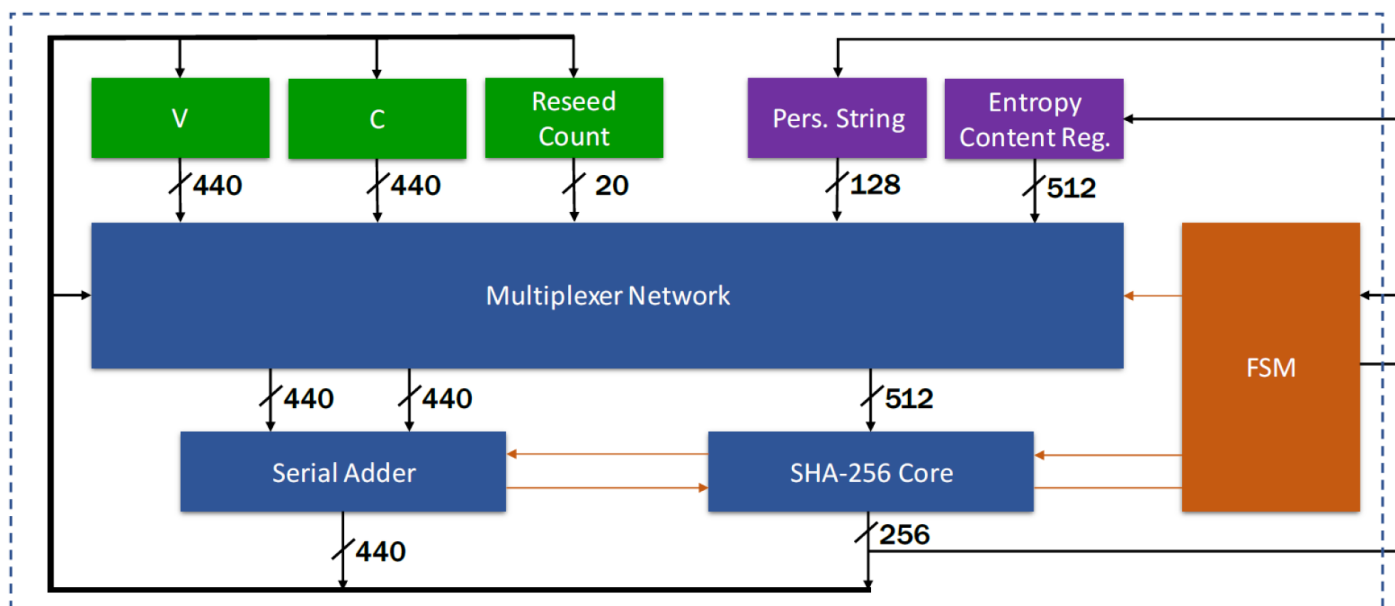
S. Di Matteo, L. Baldanzi, L. Crocetti, P. Nannipieri, L. Fanucci, S. Saponara, *SHA2 and Fats and configurable elliptic curve crypto-processor on 7 nm technology*, Microprocessors and Microsystems, 2020

7 nm ASIC at 0.75 V 85 °C

Configuration	Technology	Gate counts (kGE)	Kcycles	Freq. (MHz)	T(us)
P-256 only	45 nm	281	36.390	400	90.975
P-521 only	45 nm	407	254.456	375	686.54
P-256/-521	45 nm	447	36.390/257.456	375	97.04/686.54
P-256 only	7 nm	279	36.390	1820	19.99
P-521 only	7 nm	405	257.456	1650	156.03
P-256/-521	7 nm	445	36.39/257.456	1650	22.05/156.03

CSPRNG ENGINE

the 7 nm Artisan ASIC standard-cell reaches a throughput value of 19.67 Gbps, given a maximum clock frequency of 5.15 GHz, requiring an overall complexity of 46.56 kGE.



Two Entropy seed options:

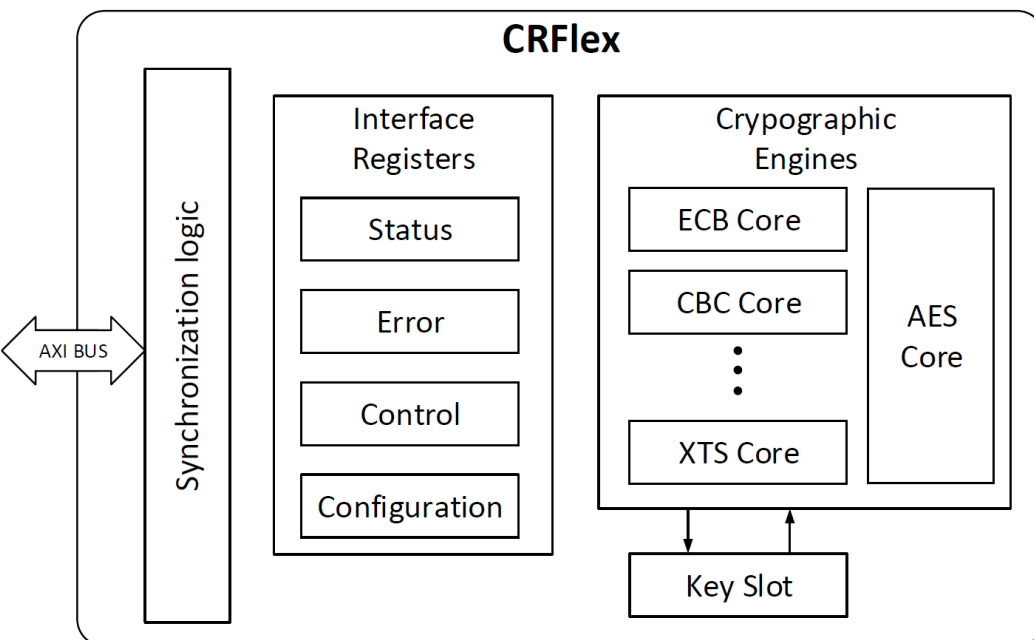
- external seed
- on-chip TRNG made of a mix of Fibonacci and Galois digital Ring-Oscillators

NIST Statistical Test Suite parameters and results

Test	Block/Template Length	Pass Rate
Frequency (Monobit)	-	0.9924
Frequency Within a Block	256	0.9876
Runs	-	0.9901
Longest-Run-of-Ones in a Block	-	0.9878
Binary Matrix Rank	-	0.9901
Discrete Fourier Transform (Spectral)	-	0.9874
Non-overlapping Template Matching	10	[0.9801–0.9974]
Overlapping Template Matching	10	0.9848
Maurer's Universal Statistical	-	0.9901
Linear Complexity	1024	0.9900
Serial	16	0.9825, 0.9876
Approximate Entropy	10	0.9901
Cumulative Sums (Cusums)	-	0.9901
Random Excursions	-	[0.9826–0.9947]
Random Excursions Variant	-	[0.9875–0.9975]

L. Baldanzi, L. Crocetti, F. Falaschi, M. Bertolucci, J. Belli, L. Fanucci,
S. Saponara, Cryptographically Secure Pseudo-Random Number
Generator IP-Core Based on SHA2 Algorithm, Sensors 2020

AES 128/256 ENGINE



Cipher Mode	Confidentiality	Integrity	Authenticity
AES-ECB	✓	✗	✗
AES-CBC	✓	✗	✗
AES-OFB	✓	✗	✗
AES-CFB	✓	✗	✗
AES-CTR	✓	✗	✗
AES-CMAC	✗	✓	✗
AES-GCM	✓	✓	✓
AES-CCM	✓	✓	✓
AES-XTS	✓	✗	✗

CRFlex module	Slice LUT usage	Slice Register usage
AES Core	23 %	17 %
ECB Core	0.2 %	0.4 %
CBC Core	0.3 %	7 %
CFB Core	1 %	7 %
OFB Core	0.3 %	0.6 %
CTR Core	0.2 %	4 %
CMAC Core	2 %	4 %
GCM Core	43 %	17 %
CCM Core	10 %	8 %
XTS Core	3 %	2 %
Interface registers	9 %	8 %
Synchronization logic	8 %	25 %

Slice LUTs and Registers occupation for each CRFlex sub-module on Xilinx Zynq-7000.

7 nm ASIC at 0.75 V 85 °C

AES-ECB-256		
# Stage(s)	Logic Usage	Throughput
1 Stage	28 kGE	27.4 Gbps
2 Stages	55.7 kGE	55 Gbps
7 Stages	195 kGE	192 Gbps
14 Stages	370 kGE	384 Gbps

WHAT'S NEXT IN EPI SECURE HW ROADMAP

- High-throughput (above 300 Gbps) AES XTS for memory and I/O encryption
- Post Quantum Cryptography (PQC)-ready HW acceleration of:
 - public-key cryptography based on Lattice-techniques (under NIST standardization)
 - key generation & encapsulation based on Lattice-techniques (under NIST standardization)
- HW acceleration of new generation PQC-ready SHA techniques, like SHAKE
- Cross-optimization of PMS and SMS tiles in EPI for new services:
 - enhanced robustness to power viruses,
 - power management policies to increase robustness against side channel attacks and increase entropy level during key generation
- Enhancing robustness to side channel attacks (power, EM analysis) and entropy for secure key generation

CONCLUSION

- The HSM in EPI provides programmable root-of-trust with acceleration support for symmetric and asymmetric encryption, digital hashing, signature and verifications services, key generation and encapsulation
- Already compliant with EVITA-full Automotive standard as well as support of TLS, SSH, MACsec, IPsec, WAVE, ESI, ITS standards/services
- Roadmap already traced for PQC support
- HW compliant with any OS and Hypervisor support



sergio.saponara@unipi.it

Full Professor @ University of Pisa (UNIPi)



**DIPARTIMENTO DI
INGEGNERIA
DELL'INFORMAZIONE**

UNIVERSITÀ DI PISA

