Security Module with HW-accelerated Post-Quantum Cryptography and TRNG for Reconfigurable Payload System-On-Chips in Space

SpacE FPGA User Workshop, 6th Edition

daniel.fortun.sanchez@gmv.com

D. Fortún Sánchez
D. González-Arjona
M. Bárez
C. Menéndez
J. Fernández-Gamo
A. Pérez
M. Orza

INNOVATING SOLUTIONS

Space-based security and cryptography

Why is important

- Space is more accessible than ever, but complexity is increasing too.
- Multi-subsystems and reconfigurable devices as SRAM-based FPGAs introduce security challenges
- Attacks can have different consequences, from data loss until loss control over the satellite

Space-based security and cryptography

Security threats

- Different types of attackers can target a satellite: External Attackers, Malicious Payload Users, Malicious Payload Service Hosters, and malicious Operators
- Some of these attacks could come directly from the supply chain and would require an approach different of on-board security
- Main attack vectors are communications with external entities (ground or other satellites) and communication buses within the satellite
- Access control is recommended

Hardware Security Module (HSM)

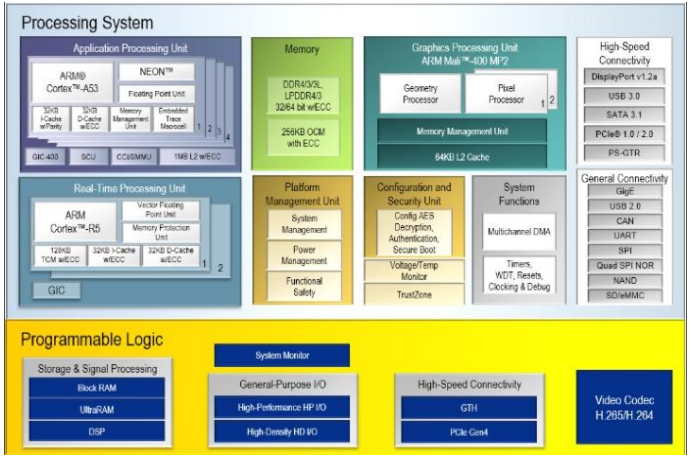
What is it?

- Specialized device designed to perform various cryptographic functions securely
- Frequently used on servers to enhance security of the installation
- Manufactured to avoid physical tampering
- There are also HSM’s available as a cloud service

On-board HSM solution

Baseline

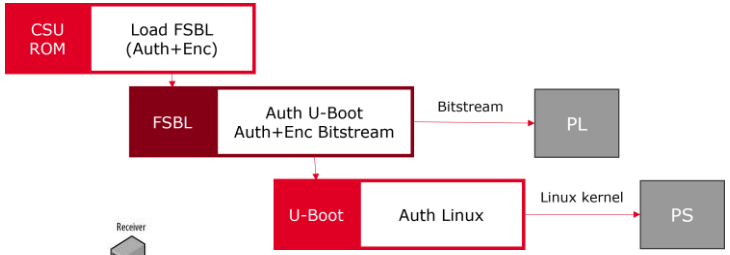
- Based on an Alen Space TREVO SDR
- Zynq UltraScale+ XQZU3EG
- Take advantage of both, Processing System and Programmable Logic
- Use of the FPGA to accelerate cryptographic algorithms
- FPGA partial reconfiguration to separate mission specific design from security features
- FPGA non-modifiable to isolate security features in hardware

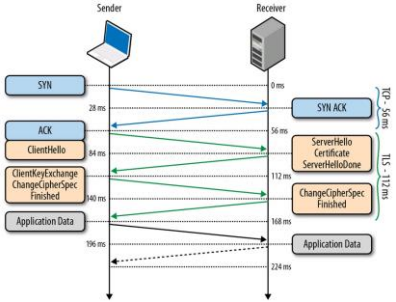


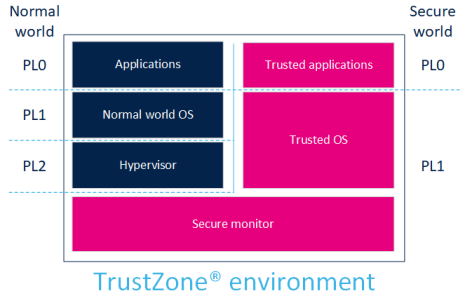
On-board HSM solution

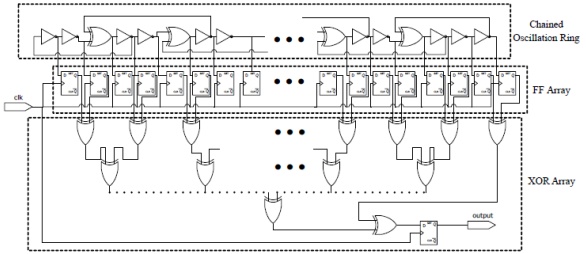
Functionalities

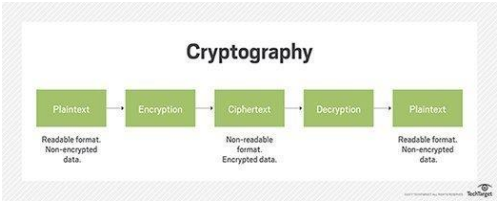
- Secure boot
- Remote attestation
- Post Quantum Cryptography
- True Random Number Generator
- Key management
- Cryptography
- Root of Trust
- Confidential bus
- TEE Hypervisor for Trust Execution Environment in SW





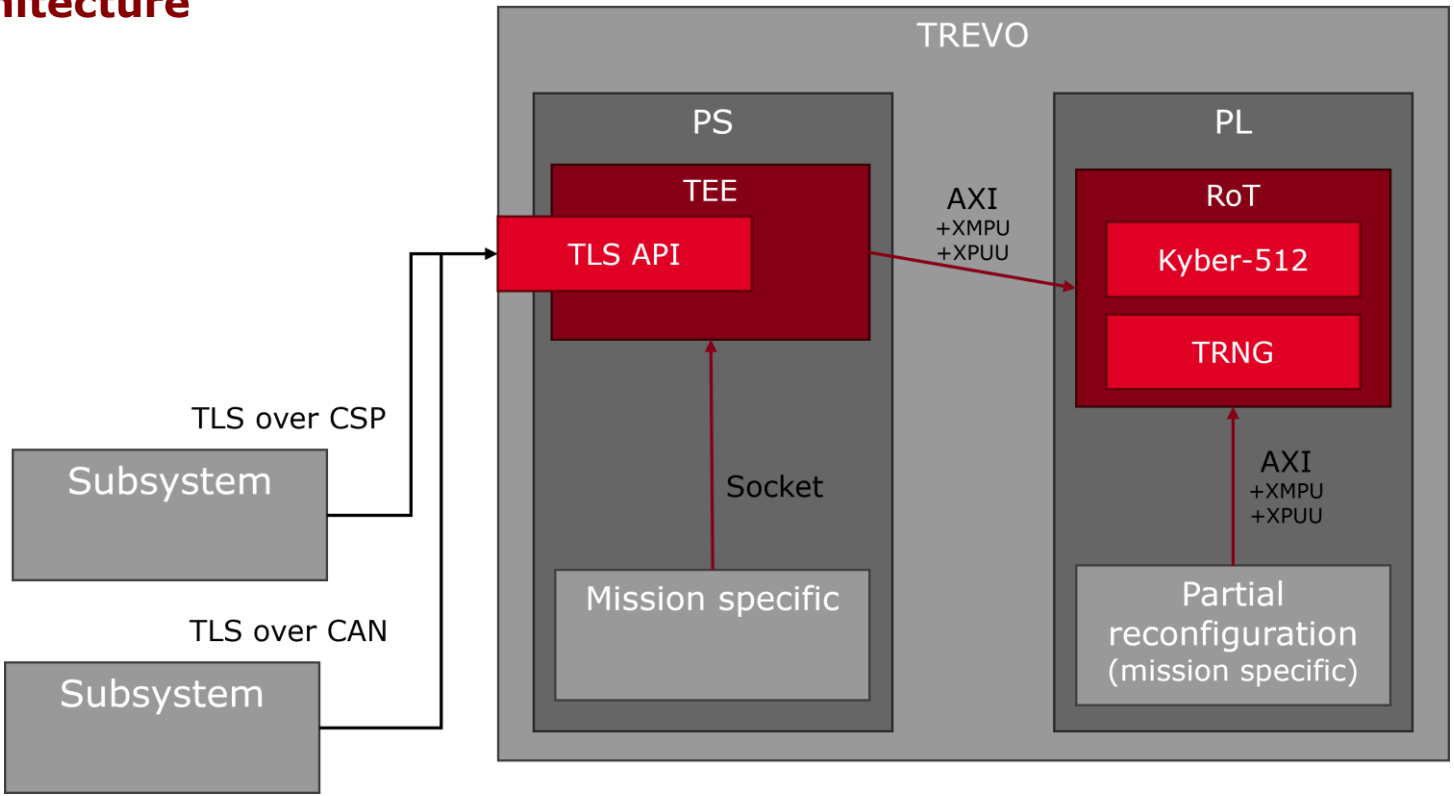






On-board HSM solution

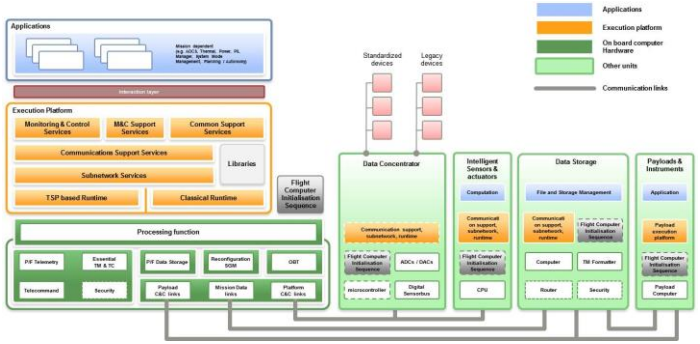
Architecture



Avionics for on-board security

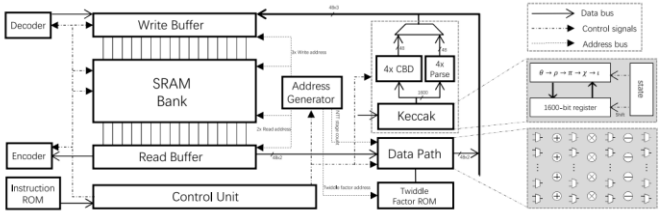
On-board security

- HSM functionalities could be accesible to other subsystems, for that, being compliant with standard avionics architecture, as SAVOIR, gains relevance for an easier integration
- Different levels of access to HSM services are necessary in order to ensure the integrity of satellite in case a subsystem is corrupted
- Secure update of the system allows adaptation to new security protocols



Post Quantum Cryptograhy

Crystal Kyber-512



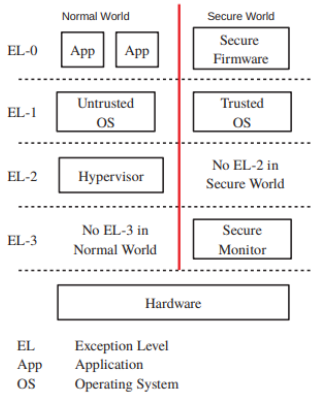
- Quantum computers are a threat against traditional encryption algorithms
- Crystal Kyber is a solution for Public-key Encryption and Key-establishment selected by NIST
- Crystal Kyber-512 benefits of a FPGA implementation from standard C code in terms of performance
- SHA-3 as RNG but there are alternatives
- SRAM organized strategically, to ensure that sampled data and intermediate values can be stored and accessed

Function	Total Luts	Logic Luts	FFs	RamB18	DSP Blocks
Key generator	4003(5.67%)	3995(5.66%)	3599(2.55%)	11(2.55%)	46(12.78%)
Encoder	5690(8.06%)	5690(8.06%)	4867(3.45%)	17(3.94%)	80(22.22%)
Decoder	3248(4.60%)	3248(4.607%)	3013(2.14%)	7(1.62%)	41(11.39%

Trusted Zone Environment (TEE)

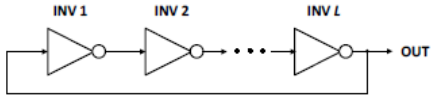
ARM Trustzone

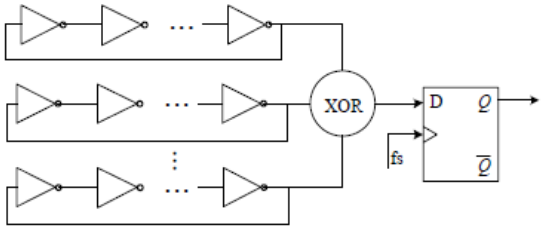
- **Technology designed to provide secure area within a device that ensures the storage, processing, and protection of sensitive data in an isolated and trusted environment, safeguarding it from malicious modifications**
- **ARM TrustZone virtualizes a physical core into two virtual environments: the Secure World, where sensitive applications run, and the Normal World**
- **ARM TrustZone is available in Zynq 7000 SoC and Zynq UltraScale+**
  - eXtended Memory Protection Unit (XMPU)
  - eXtended Peripheral Protection Unit (XPPU)
  - NS control signal to AXI transactions
- **Can be used to deploy Petalinux on a secure environment and add libraries for security purposes**



TRNG

FPGA implementation





- Device that generates random numbers based on unpredictable physical phenomena
- Combination of metastability and jitter noise as source of entropy
- Chained ring oscillator, a flip-flop array, and finally an XOR array to generate the output.
- The Chained Oscillation Ring is constructed using XOR gates and multiple ring oscillators
- Nested ROs = 3·N+1 with N∈ N_0

Resource	Utilization	Available	Utilization (%)
FF	101	141120	0.07
LUT	28	70560	0.03

For N=1, on a ZU3EG (Alen Space TREVO)

Conclusion

- On-board security is a topic that must be addreses with the increase accesibility of space
- A FPGA-based HSM design offers significant advantages in terms of scalability and flexibility, particularly in the context of evolving cryptographic standards
- Subsystems with access to an HSM will see their security improve and will not need to store secrets, making development process easier
- FPGA-based implementation of cryptographic algorithms, including post quantum cryptography, benefits of parallel processing to increase performance
- Functions of the HSM can be extended to include new algorithms and secure communication protocols for inter-satellite links

Thank you

INNOVATING SOLUTIONS