RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

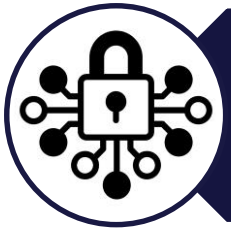
RISC-V SUMMIT 2025

RISC-V open designs and contributions to hardware security research and development activities

Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

Technical challenges

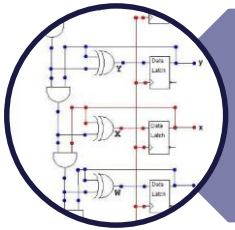
Secure Hardware Foundation



Implement hardware-based security functions

- Performances optimization, SWaP and security balancing (mobility, sustainability)
- Early stages, protection of the cores, techno specific properties

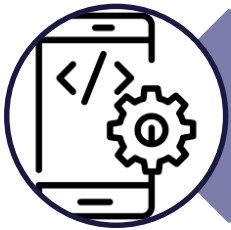
Secure by design



Improve the level of assurance

- Improvement of tools for security proof verification
- Control the design and the configuration of the security functions

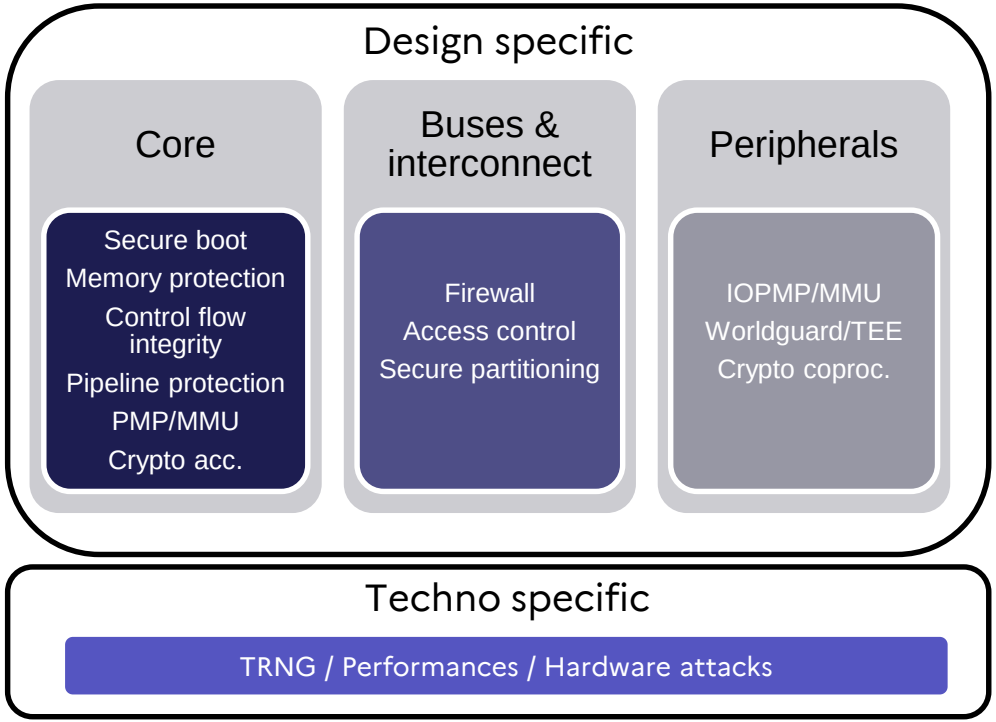
Tightly coupling of hardware and software security

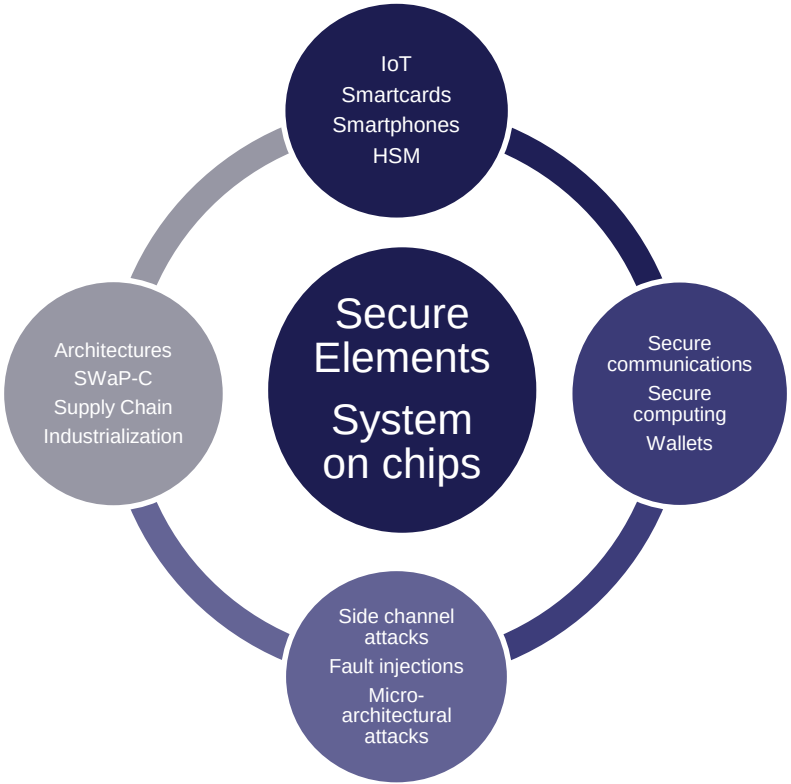


Securing the software

- Mechanisms securing the software implementation
- Support the increase in the size and complexity of systems

Security features





Some current activities or topics of interest

… but there are many other project to which ANSSI does not contribute directly

❑ Survey and technical analysis

- ➢ Core security functions : CVA6, CV32E40S, Ibex (Secure and CherIoT), Caliptra
- ➢ Secure SoC design : OpenTitan, Caliptra
- ➢ Tools : µArchiFI

❑ Collaborations

- ➢ Hardware accelerator with the IP ECC
- ➢ Hardware resources sharing for crypto-agility in PQC

❑ Contributions to funded projects

- ➢ ARSENE Project - funded under PEPR Cyber - 2022 / 2027
- ➢ FORWARD project - funded under PTCC – 2025 / 2029

Hardware acceleration for Elliptic Curves Crypto (ECC)

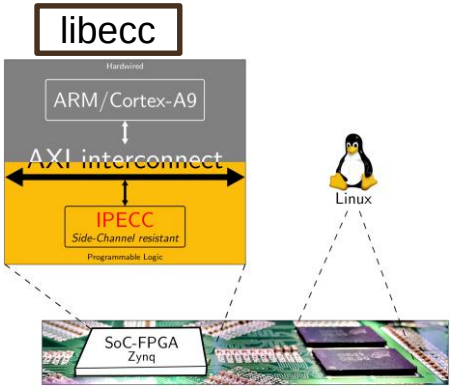
… for side channel & physical-attacks countermeasures analysis and testing

- Use case models: hardware root of trust (e.g secure enclave) or authentication
- IP Features:
  - Embedded TRNG
  - Two static exclusive modes :
    - ✓ unsecure
    - ☞ In this mode, every synthesized countermeasure (CM) can be engaged or disengaged
    - ✓ secure
    - ☞ In this mode, no synthesized countermeasure can be disengaged
  - SCA countermeasures : «defense-in-depth» rationale:
    - ✓ Built-in CMs : Constant time, Initial coordinates randomization, Anti-address bit DPA (including anti-collisions), Check that input and output points belong to the curve
    - ✓ Optional CMs : Blinding, Sensitive points address shuffling, Large Numbers memory address shuffling, Periodic coordinates randomization
- IP Design: 100% technology agnostic (except for TRNG) both for FPGA & ASIC

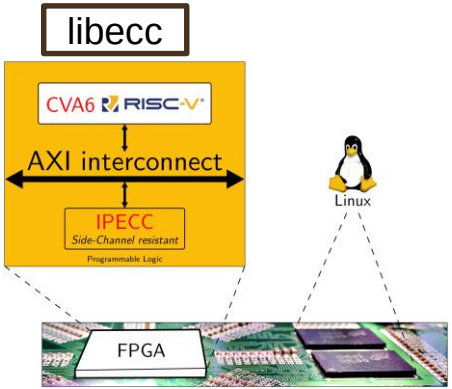
Hardware acceleration for Elliptic Curves Crypto (ECC)

From FPGA designs to full ASIC implementation

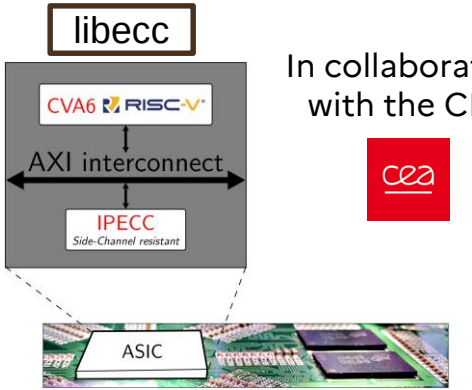
- Can be used with libecc* project running on ARM / RISC-V processor



1st Step :
SoC / FPGA



2nd Step :
Full FPGA



3rd Step :
Full ASIC
ongoing

In collaboration with the CEA

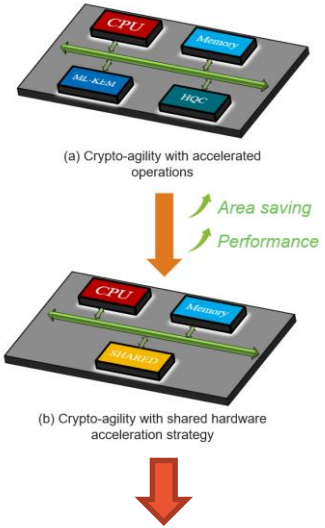
cea

* Library for elliptic curves cryptography

Hardware sharing for ML-KEM and HQC

Switching between different PQC cryptosystems... based on a same hardware

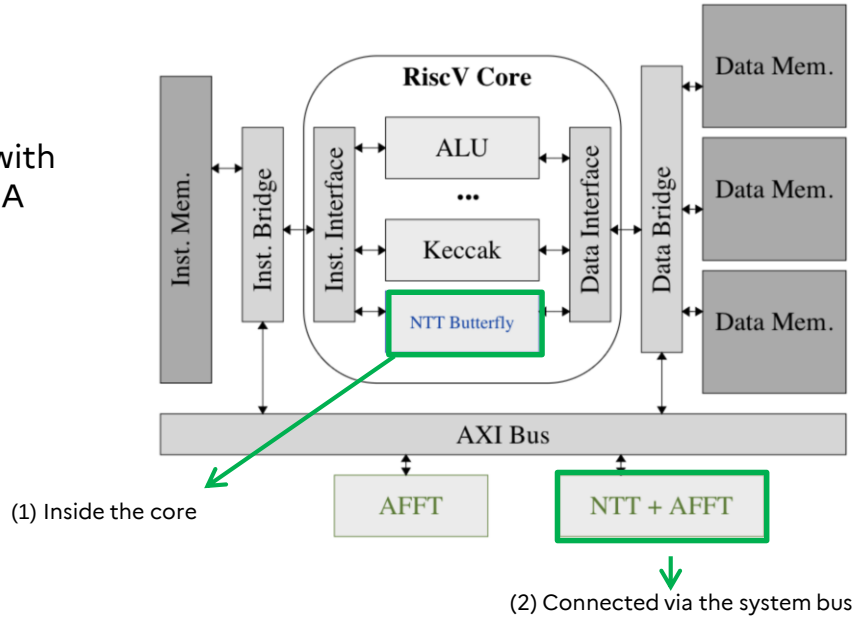
- **Our targeted agility + Hardware : ML-KEM (lattice-based) + HQC (code-based)**
  - Identification and share common operations in a single implementation



PHOENIX design based on Super-Butterfly

In collaboration with the CEA & INRIA

- **Application-specific accelerators integration strategy**
  - Tightly-coupling (1) : Few flexibility but low latency
  - Loosely-coupling (2) : More flexible but higher latency



ARSENE project

ANSSI is part of the consortium

- **Part of the Priority Research Programs and Equipment – France 2030**
  - Program overseen by the CEA, CNRS, and Inria, divided in ten challenges (among which ARSENE)
  - Partners: CEA, CNRS, Inria, IMT, Grenoble INP, ENSTA Bretagne, ANSSI, and several universities (Grenoble Alpes, Saint-Etienne, Montpellier, Bretagne Sud, Bretagne Occidentale, Rennes 1)
- **Challenge: hardware and software security of embedded systems**
  - Securing the reference implementations of two ranges of RISC-V processors:
    - ✓ 32-bit RISC-V, for constrained IoT applications, intrinsically secure against physical attacks
    - ✓ 64-bit RISC-V for richer applications, particularly secure against software attacks exploiting hardware vulnerabilities
  - Secure integration of these processors within systems-on-chip (SoCs)
    - ✓ research and development of critical building blocks (random number generators, secure memories, agile cryptographic accelerators for so-called "pre- and post-quantum" algorithms, etc.)
  - Study of software tools for secure codes, secure kernels, dynamic supervision techniques
  - Demonstration and validation on FPGA and ASIC type components

ARSENE project: ANSSI's perspectives

❑ Contributions

- ➢ Security analysis of 32-bit RISC-V based secure elements (SCA and FI)
- ➢ Securing 64-bit RISC-V based applicative SoC (micro-architectural attacks, lifecycle, boot management)
- ➢ Work on the RISC-V ISA to improve performance and security of cryptographic algorithms

❑ Interests

- ➢ Availability of open-hardware secure elements, protected against high level attackers,…
- ➢ A step towards applicative processors with security features, suitable for mobile secure applications
- ➢ Contribution to the test chip produced during the project and practical analysis of it

FORWARD project

ANSSI is part of the consortium

- **Part of the Cyber Campus Transfert Program – France 2030**
  - Relies on the dynamics of the Cyber Campus and its network to promote joint projects between academic, industrial and government players
  - Partners: CEA, Inria, Sorbonne university, Mines Saint-Etienne, ANSSI, Thales DIS, Safran
- **Challenge: formal verification and physical attacks resilience of HW countermeasures**
  - Formal analysis applied to countermeasures verification
  - Designing countermeasures and characterizing their robustness
    - ✓ Sophisticated attacker models
    - ✓ Multiple faults
  - Quantifying the gap between experimental characterizations and formal verification
    - ✓ Experimentation platforms : Fault injection platforms (laser or EM)
    - ✓ Formal verification platforms : e.g. µArchiFI, SAMVA (software centric)

FORWARD project: ANSSI's perspectives

❑ Interests

- ➢ Interest in applying formal verification methods to the hardware domain
  - ✓ Better threat coverage
- ➢ Dissemination of open-source tools to industry
- ➢ Having a proven methodology to validate the security benefits of hardware countermeasures
  - ✓ Being able to use characterization results during the design step
  - ✓ Being able to compare several countermeasure proposals available in the state of the art
- ➢ Need for formal methods that are as close as possible to experimental analysis results
  - ✓ Interesting to measure the gap between the two approaches

References

- **IPECC project : https://github.com/ANSSI-FR/IPECC**
  - Libecc projet : https://github.com/ANSSI-FR/libecc
- **PHOENIX paper (eprint) : https://eprint.iacr.org/2025/601.pdf**
- **ARSENE project (for French readers…) :**
  - Project overview : https://www.pepr-cybersecurite.fr/projet/arsene/
  - Some details : https://www.pepr-cyber-arsene.fr/details/
- **FORWARD project (for French readers too…) :**
  - Project summary : https://ptcc.fr/projets/forward/
- **µArchiFI project : https://github.com/CEA-LIST/uArchiFI**
- **SAMVA paper (JAIF 2023) : https://jaif.io/2023/media/JAIF2023-slides-Gicquel.pdf**

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Thank you for your attention

Any questions ?