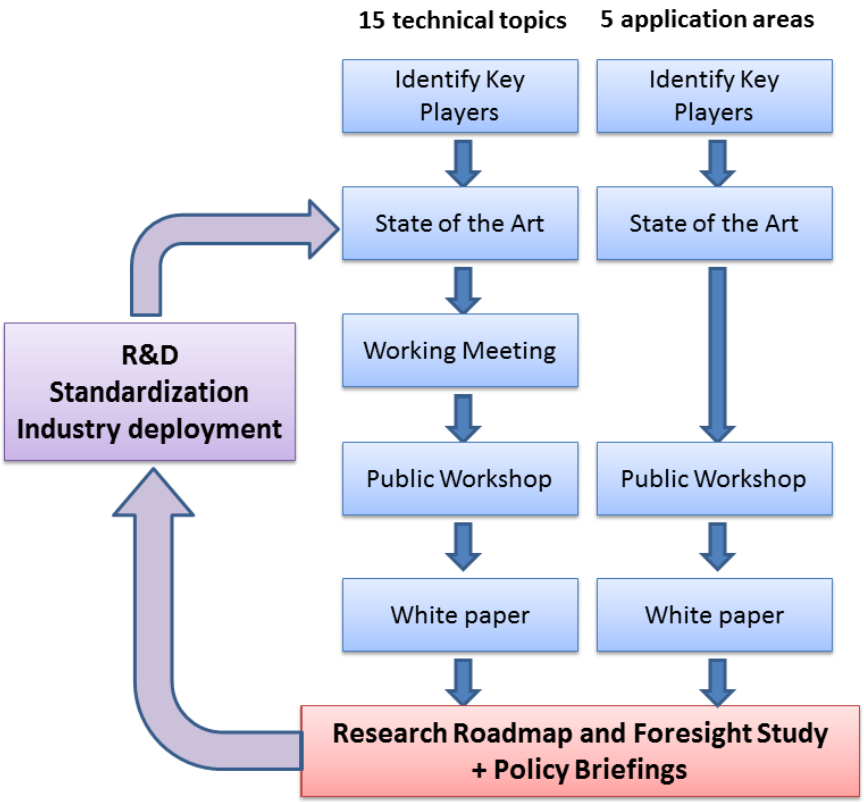
Current activities in cryptology and the DS-06-2017 call

Dr. Florent Frederix
Trust and Security Unit
DG Communications Networks, Content and Technology
European Commission

Content

- Current activities
  - **H2020 LEIT Encryption Projects**
  - **H2020 SC7 Research Executive Agency projects**
- Next H2020 Encryption call
  - **H2020 SC7 in WP 2017**
  - **DS-07-2017 Cryptography call**

H2020 LEIT: ECRYPT_CSA



Workshops and summer schools on encryption covering

- Authentication
- Low energy and small devices
- Symmetric standards
- Asymmetric cryptanalysis
- Random number generation
- Side channel fault resistance
- Modelling tools and proofs
- Cryptocurrencies
- Quantum cryptography
- PETs

H2020-ICT-645421

European Commission

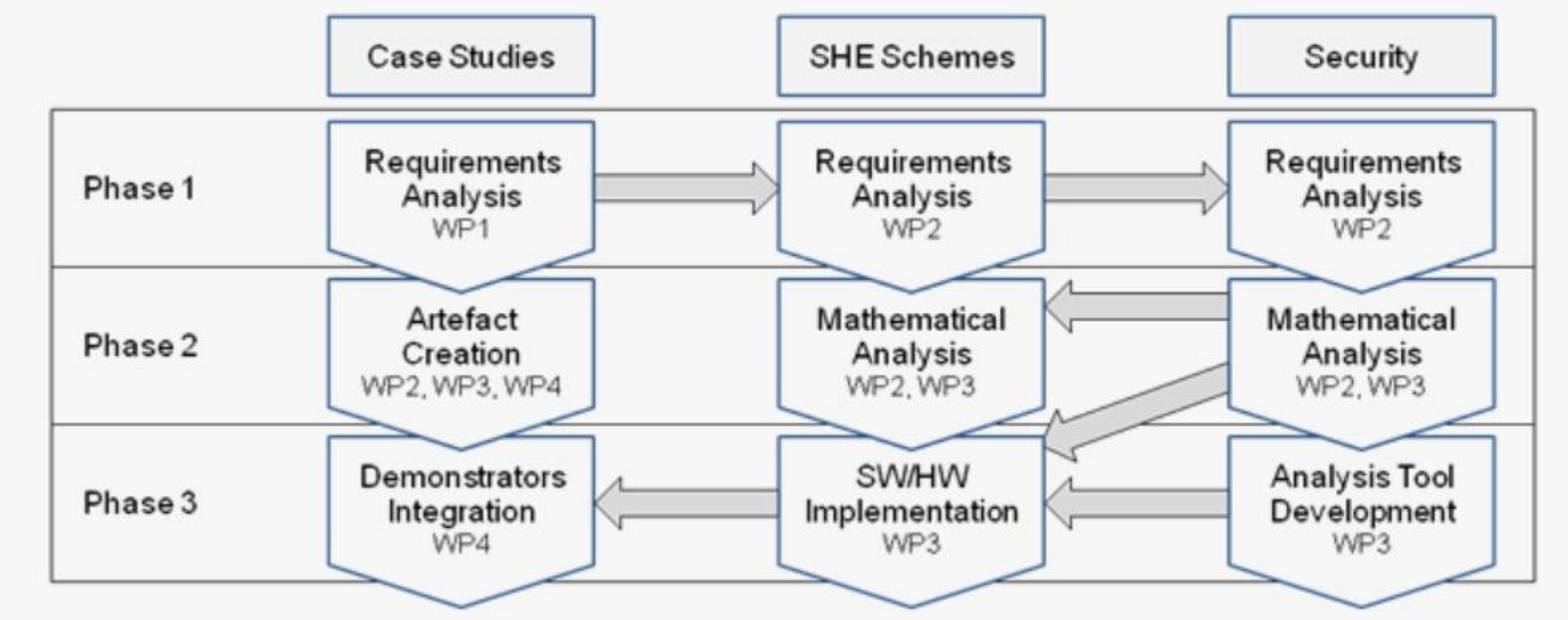
H2020 LEIT: HEAT

HEAT

Homomorphic Encryption Applications and Technology

H2020-ICT-644209

Objective: An **open source software library** to support applications that wish to use **homomorphic cryptography**



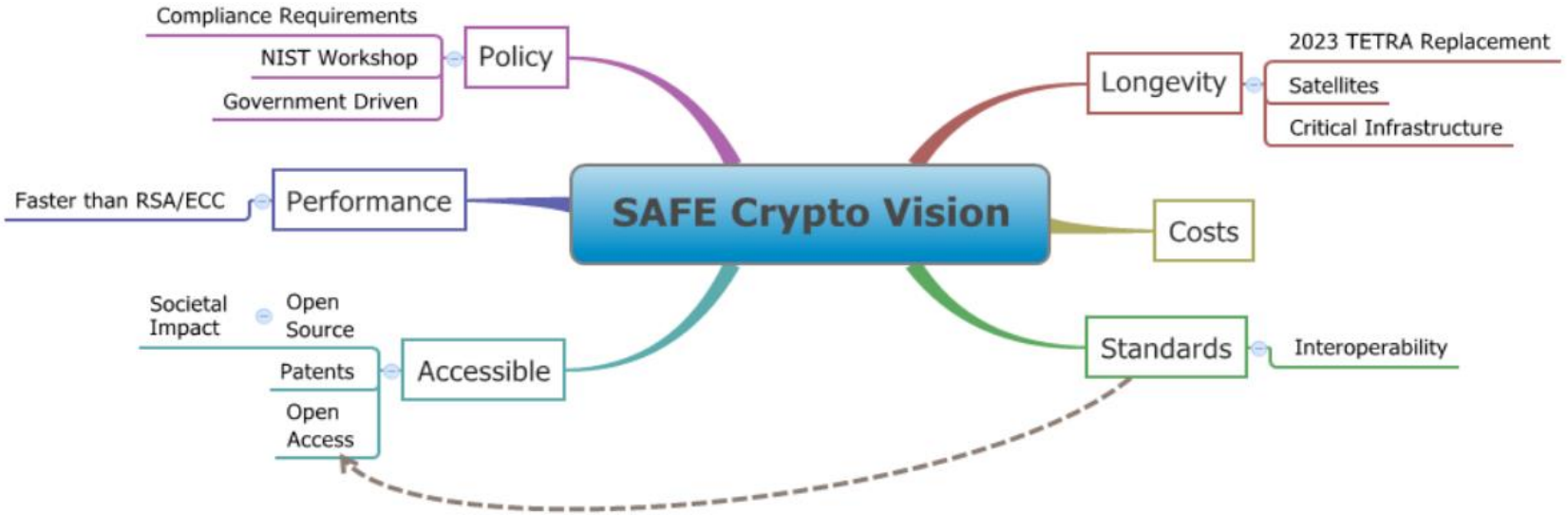
European Commission

H2020 LEIT: SAFEcrypto

Secure Architectures of Future Emerging cryptograpny

H2020-ICT-644729

Objective: a new generation of practical, robust and physically secure **post-quantum cryptographic solutions**



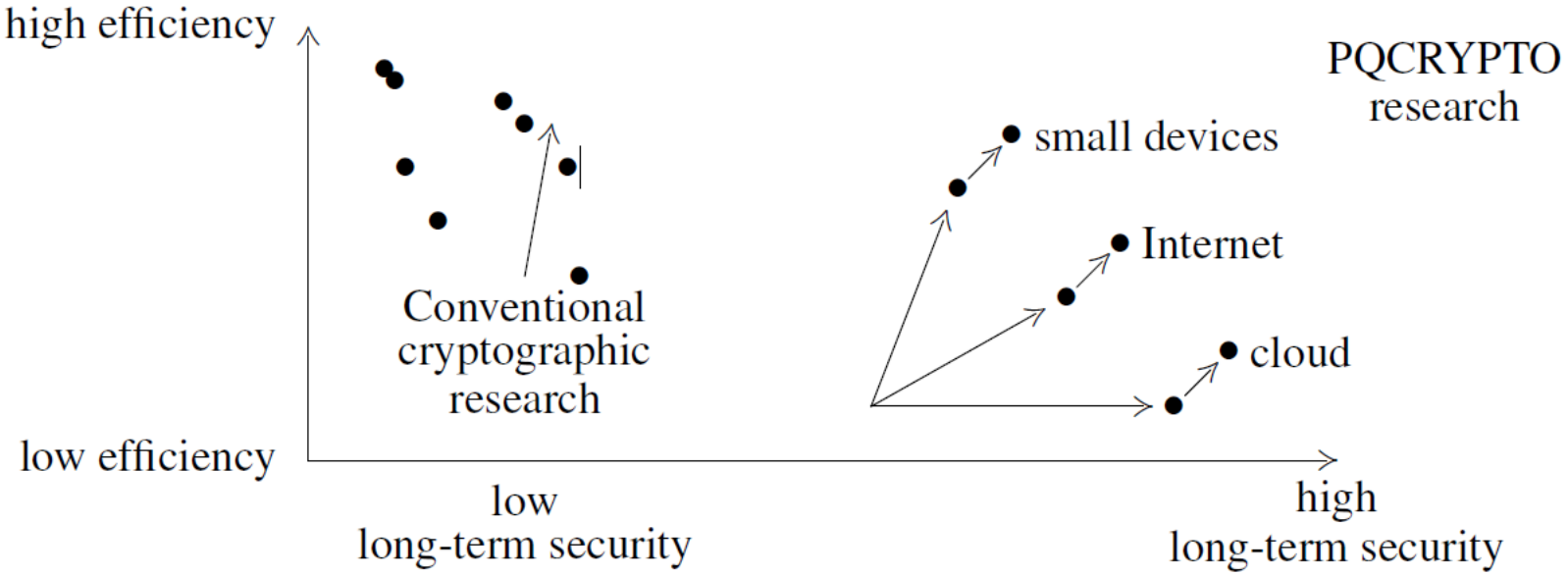
European Commission

H2020 LEIT: PQcrypto

Secure Architectures of Future Emerging cryptography

H2020-ICT-645622

The primary objective of the PQCRYPTO project is **to switch real-world applications to postquantum cryptography**



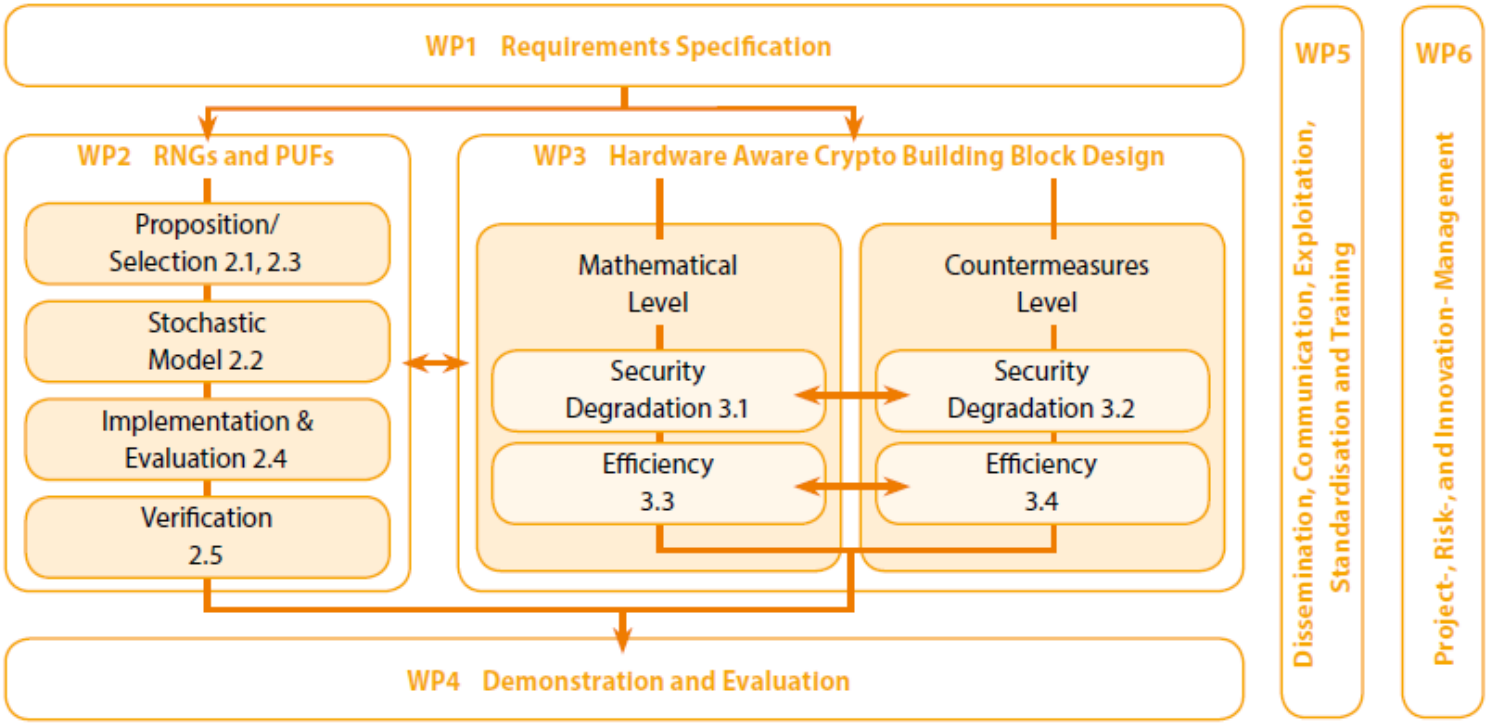
European Commission

H2020 LEIT: Hector

HARDWARE ENABLED CRYPTO AND RANDOMNESS

H2020-ICT-644052

The mission is to close the gap between the mathematical heaven of cryptographic algorithms and their secure hardware implementations.



H2020 SC7 REA call projects

RIA IA CSA

European Commission

Current Activities

Resilience, Secure Network Infrastructures, Critical Infrastructures, Threat Detection/CyberSecurity

MITIGATE (1)
DOGANA (1)
WISER (1)
RECRED
CREDENTIAL
PROTECTIVE
SISSDEN
CIPSEC
CISP
SHIELD
DISIEM
CANVAS
ATENA
CITADEL (1)

Privacy, Biometrics, Identity management, Authentication

OCTAVE (1)
RECRED (1)
PRIVACY FLAG (1)
TYPES (1)
LIGHTest
FutureTrust
CREDENTIAL (1)
PANORAMIX (1)
Speech XRays (1)
VISION (1)
SAFECLOUD (1)
OPERANDO (1)

Trustworthy Service Infrastructure, Secure Software Engineering, Cryptography

CREDENTIAL https://credential.eu/
LIGHTest (1)
FutureTrust(www.futuretrust.eu)

Certification, Cloud Computing

PRIVACY FLAG
MITIGATE
SAFECLOUD
CITADEL

(1) Shows the main category where the project belongs

2014 — Research Executive Agency — 2015

European Commission

Digital Security Focus Area in H2020 SC7 WP 2016-2017

- **Situation:** ICT-driven transformations bring opportunities across many important sectors.
- **Complication**: "Smart", "Connected", "Digital" also introduce vulnerabilities...
- **R&D&I challenge:** Innovative and multidisciplinary actions addressing cyber security, data protection and privacy across individual H2020 pillars and calls.

European Commission

Call – Digital Security Focus Area – Topics

- **DS-01-2016**: Assurance and Certification for Trustworthy and Secure ICT systems, services and components;
- **DS-02-2016**: Cyber Security for SMEs, local public administration and Individuals;
- **DS-03-2016**: Increasing digital security of health related data on a systemic level;
- **DS-04-2016**: Economics of Cybersecurity;
- **DS-05-2016**: EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation;
- **DS-06-2017**: Cryptography;
- **DS-07-2017**: Addressing Advanced Cyber Security Threats and Threat Actors;
- **DS-08-2017**: Privacy, Data Protection, Digital Identities;

European Commission

DS-06-2017: Cryptography (1)

- Research beyond the partial homomorphic encryption algorithms under development. Additionally, means to reduce data leakage
- IoT ultra-lightweight cryptology and means to protect privacy in these applications
- Ultra-high-speed cryptographic algorithms that are fully parallelizable and energy efficient
- Physical cryptanalysis, including tampering, side channel- and faults injection attacks
- Automated proof techniques for cryptographic protocols

DS-06-2017: Cryptography (2)

- Toolkits that seamless integrate encryption
- Authenticated encrypted token research. The proposals should aim to create a real e-currency without compromising security.
- Innovative cryptographic and complementary non-cryptographic privacy-preserving mechanisms.
- Quantum computer safe cryptography
- Improved quantum key distribution schemes with validation by end-users in realistic and relevant scenarios

DS-06-2017: Cryptography - Impact

- Proposals should lead to Technology Readiness Level 3 to 5 prototyping
- Increase the competitiveness of the European ICT, cryptography and smart card industry.
- Increased trust in ICT and online services.
- Protect European Rights of Privacy and Data Protection.
- Improvement in performance and efficiency of cryptography beyond state of the art.
- Protection against emerging threats such as quantum computation

References

Draft work programmes 2016-17

http://europa.eu/!Dh67Gk

CNECT-H4@ec.europa.eu
@EU_TrustSec