MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE
*Liberté Égalité Fraternité*

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE
*Liberté Égalité Fraternité*

FILIÈRE INFRASTRUCTURES NUMÉRIQUES

Systematic
Paris Region Deep Tech Ecosystem

# CRYPTOEXPERTS

- **Overview** – Independent French SME (Paris, 2009); strong technical focus on cryptography (several PhDs, senior engineers and researchers); alumni of Gemalto, Idemia, Thales, ANSSI. 200+ scientific publications in applied cryptography; active in standardization.

- **Business segment: cryptography expertise and solutions**
  - **Expertise –** research, consulting and outsourced R&D, audits, custom cryptographic designs, PQC transition, training – for telecom, banking, healthcare, defence, embedded systems & IoT.
  - **Solutions – PQLib**: portable PQC library for embedded systems (ML-KEM, ML-DSA, hybrid); built-in security countermeasures (SCA/FIA-protected version); certification readiness (CC AVA_VAN.5 target, preliminary side-channel evaluation by ITSEF)
    **White-Box Engine**: white-box cryptography technology (protecting keys in software, without secure hardware, for mobile apps and IoT).

➔ Contact : Matthieu Rivain, CEO – matthieu.rivain@cryptoexperts.com

CRYPTOEXPERTS
WE INNOVATE TO SECURE YOUR BUSINESS

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE
*Liberté Égalité Fraternité*

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE
*Liberté Égalité Fraternité*

FILIÈRE INFRASTRUCTURES NUMÉRIQUES

Systematic
Paris Region Deep Tech Ecosystem

- **Key challenges addressed**
  - **Post-quantum cryptography (PQC): design, migration and crypto-agility** – design of PQC algorithms and protocols (8 schemes submitted to NIST), expertise in the NIST standards (ML-KEM, ML-DSA, SLH-DSA, FN-DSA, HQC); optimised low-level implementations; hybridization, crypto-agile protocol integration and key management; migration strategies aligned with ANSSI and EU roadmaps.
  - **Secure cryptographic implementations** – resistance to side-channel attacks (SCA) and fault-injection attacks (FIA) on constrained devices, masking, formal verification, evaluation and certification.
  - **Zero-knowledge proofs (ZKP) and privacy-enhancing technologies (PET)** – post-quantum ZKP system (response to the NIST MPTC call); PoC of post-quantum anonymous credentials for ML-DSA. Also working on FHE and MPC.

➔ Contact : Matthieu Rivain, CEO – matthieu.rivain@cryptoexperts.com

CRYPTOEXPERTS
WE INNOVATE TO SECURE YOUR BUSINESS

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE
*Liberté Égalité Fraternité*

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE
*Liberté Égalité Fraternité*

FILIÈRE INFRASTRUCTURES NUMÉRIQUES

Systematic
Paris Region Deep Tech Ecosystem

- **Links to 6G / SNS JU** – Relevant assets for 6G: **PQLib** (IoT devices, secure elements, edge nodes); **consulting, audit and co-design** of PQC protocols, architectures and key management, hardware roots of trust, security evaluation and certification support; post-quantum ZK proofs for **identity and attestation**.
- **National projects** – **RESQUE** (Bpifrance, France 2030; 2023-2026; with ANSSI, Inria, CryptoNext, Thales, TheGreenBow): side-channel-secure PQC implementations for embedded systems; funded PQLib. **RELATE** (ANR, 2026-2029; with PQShield, LIRMM): research on PQC and ZKP.
- **European projects** – **AMAskZONE** (Horizon Europe ERC; 2023-2028): secure cryptographic implementations & formal verification. **PQCSA** (Horizon Europe CSA; 2025-2027; with KU Leuven, TU/e, TCD, Bundesdruckerei): European PQC standardisation agenda and migration roadmap. **EQUIP** (Horizon Europe RIA, 2026-2029; Technikon, KU Leuven, PQShiled, Tampereen AU, TY Graz): secure PQC implementations.

➔ Contact : Matthieu Rivain, CEO – matthieu.rivain@cryptoexperts.com

CRYPTOEXPERTS
WE INNOVATE TO SECURE YOUR BUSINESS

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE
*Liberté Égalité Fraternité*

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE
*Liberté Égalité Fraternité*

FILIÈRE INFRASTRUCTURES NUMÉRIQUES

Systematic
Paris Region Deep Tech Ecosystem

- **SNS JU WP 2027 topics of interest**
  - **Stream D "Quantum Safe Security" (IA)** – PQC-based authentication, key exchange and data protection across the stack; crypto-agile frameworks; secure devices with hardware roots of trust; PQC benchmarks on constrained devices; standardisation and open source.
  - **Stream B "Security and Resilience by Design for Sovereign 6G" (RIA)** – dynamic trust, identity and attestation; privacy-preserving verification (ZKP) of identities, AI agents and network functions; quantum-era risks; security-overhead metrics.
  - **Also** – Stream B Flagship (PQC at a critical level of the infrastructure); Stream D AI-native topics (post-quantum integrity of models and data); Stream B Optical Connectivity for Massive AI (crypto-agile, post-quantum-resistant frameworks) Stream C Quantum Enhanced Connectivity (hybrid configurations with PQC)
- **Our role in a consortium** – cryptography technology provider and WP leader (SME)

➔ Contact : Matthieu Rivain, CEO – matthieu.rivain@cryptoexperts.com

CRYPTOEXPERTS
WE INNOVATE TO SECURE YOUR BUSINESS