Cryptops

主権的なポスト量子暗号化。

AllEyes Resilient — 重要インフラ事業者と共に、そのために設計されたフランス発のポスト量子暗号プラットフォーム。

ポスト量子 · フランス主権 · HPC から Edge まで

cryptops.fr

量子の課題に真面目に向き合う。

課題

量子コンピュータは 2030〜2035 年頃に RSA と ECDH を脅かします。今日僞受されたデータは将来復号されます（harvest now, decrypt later）。重要インフラは今すぐ移行すべきです。

アプローチ

すべてのリンクがポスト量子な主権プラットフォーム：NIST 標準プリミティブ、AMD FPGA でのハードウェア分離、ホストに決して鍵を漏らさない。フランスで設計・運用。

ML-KEM-1024

FIPS 203

ML-DSA-87 ⊕ SLH-DSA

FIPS 204

製品。

AllEyes Resilient

FPGA 暗号装置 · 4U / 2U

ラインレート暗号化、AMD FPGA 上の CPU-Blind アーキテクチャ。AES 鍵はシリコン内にあり、ホストから到達できません。

GARANCE PKI

信頼機関 · 100% RUST

主権的ポスト量子 PKI。複合署名 ML-DSA-87 ⊕ SLH-DSA、管理された鍵生成儀式、検証可能な信頼連鎖。

GLUON

PQC-WAN エージェント · 1U NEBS〜EDGE

FPGA 不要のポスト量子トンネル。自社開発の IKEv2 スタックが回線を保護します。

主権 HPC

CONFIDENTIAL COMPUTING · CPU/GPU/FPGA

HPC・AI ワークロードを加速・端から端まで暗号化し、REDSHIFT がオーケストレーションします。

REDSHIFT — 主権的オーケストレーション。

チェーン全体がポスト量子で主権的なプラットフォーム：端から端までのセキュリティ、フランスでの運用・ホスティング。鍵を漏らさず HPC・AI をオーケストレーション。

- 端から端までのポスト量子セキュリティ
- 主権的な信頼 PKI
- HPC の中核から Edge まで

サービス。

FPGA エンジニアリング

AMD ポートフォリオ全体の開発—Versal、Alveo、RFSoC、UltraScale+、Kria。

ポスト量子統合

ML-KEM-1024、ML-DSA-87 ⊕ SLH-DSA、AES-256-GCM-XPN—公開 NIST ベクトルに基づく。

主権的セキュリティ

CPU-Blind アーキテクチャ、堅牢化、CSPN / EUCC 評価準備。

暗号。

鍵交換	ML-KEM-1024 (FIPS 203)
署名	複合 ML-DSA-87 ⊕ SLH-DSA (FIPS 204)
共通鍵暗号	AES-256-GCM-XPN
KEM ハイブリッド	ML-KEM-1024 · FrodoKEM-1344 · P-384 · PSK

認証。

CSPN ANSSI	2027 年目標
EUCC / CC EAL4+	2029 年ターゲット
NIS2 · DORA	規制枠組み
主権	フランスで設計・運用

> 現時点で取得した認証はありません。取組中のものと取得済みを常に区別します。

Cryptops

ポスト量子アーキテクチャについてお話ししましょう。

機密デモ。暗号領域の評価。エンジニアが対応。

contact@cryptops.fr · cryptops.fr

FLDG Holding SASU · SIREN 987 561 263 · 19 rue du Colisée, 75008 Paris