

PROMETHEUS

PRivacy preserving pOst-quantuM systEmS
from
advanced crypTograpHic mEchanisms Using latticeS



BENOÎT LIBERT

[PORTEUR ADMINISTRATIF]



SÉBASTIEN CANARD

[PORTEUR SCIENTIFIQUE]

DAMIEN STEHLÉ

CONTEXTE H2020 DE PROMETHEUS

Call: H2020-DS-2016-2017 (Digital Security Focus Area)

Topic: DS-06-2017 (Cybersecurity PPP: Cryptography)

Type of action: RIA (Research and Innovation Action)

Montant demandé : 5,496,968.75 EUR

Montant accordé : 5,496,968.75 EUR

Evaluation : 15/15

Durée : 48 mois à partir du 01/01/2018

LE CONSORTIUM

Partenaires académiques

Ecole Normale Supérieure de Lyon .FR

Université de Rennes I .FR

Universitat Politècnica de Catalunya .ES

Centrum voor Wiskunde en Informatica .NL

Royal Holloway .UK

Ruhr Universität Bochum .DE

Weizmann Institute of Science .IL

Partenaires industriels

Orange SA .FR

Thales Communications and Security .FR

Scytl Secure Electronic Voting .ES

Toegepast Natuurwetenschappelijk
Onderzoek (TNO) .NL

IBM Research .CH

CONTEXTE SCIENTIFIQUE

Cryptographie : fondement mathématique / algorithmique de la sécurité digitale

Problèmes calculatoires difficiles
Factorisation de grands nombres,
Logarithmes discrets, etc.



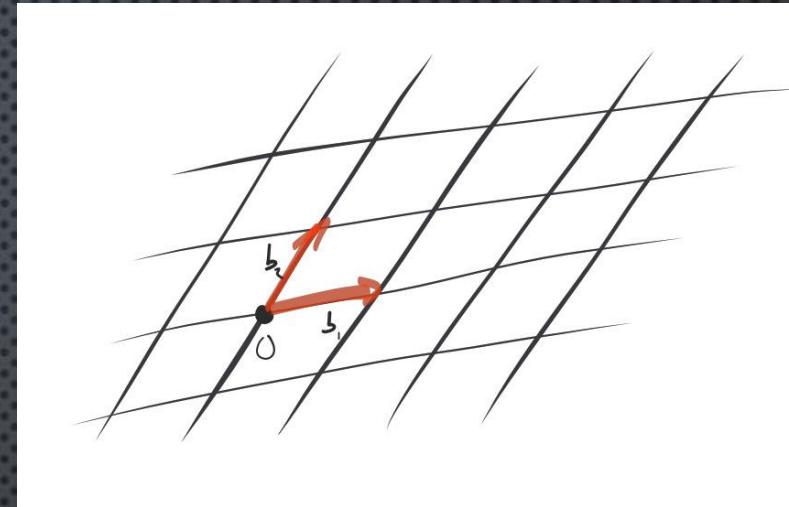
Protocoles cryptographiquement sûrs
Signatures digitales, échange de clés,
chiffrement, etc.

GROS SOUCI EN VUE : Si un ordinateur quantique est construit, alors

- Les problèmes « difficiles » utilisés aujourd'hui deviennent faciles
- La sécurité des protocoles utilisés aujourd'hui est anéantie

PROMETHEUS

- ❖ Cryptographie reposant sur les **réseaux Euclidiens**
 - ❖ Principale alternative post-quantique (cf processus de standardisation NIST)
 - ❖ Plus expressif, plus rapide
 - ❖ Les briques élémentaires (chiffrement, signature) sont déjà bien comprises



PROMETHEUS (informellement) : Consolider cette 1ère étape, et aller au-delà !

- ❖ E-cash
- ❖ E-voting
- ❖ Coopération pour la cyber-intelligence

CONSTRUCTION DU PROJET

Un projet assez en amont, avec un poids académique fort

- Les participants académiques se connaissent depuis longtemps
- Utilisation de collaborations académie – industrie pérennes
 - ENS de Lyon – Orange
 - CWI – TNO
 - CWI – Thales
 - UPC – ScytI

Un impact potentiellement très important

- Un ordinateur quantique anéantirait la sécurité digitale actuelle

Organisation de la soumission

- Un duo de choc (B. Libert et S. Canard)
- Un soutien au montage de projets de grande qualité, à l'ENS de Lyon (Q. Touitou)

LA CRYPTO A L'ENS DE LYON

<http://www.ens-lyon.fr/LIP/AriC/crypto>

Au sein de l'équipe Aric du LIP [UMR CNRS, ENS de Lyon, INRIA, U. Lyon 1, U. Lyon]

3 permanents

6 post-docs, 1 ingénieur CDD, 9 doctorants

=> 11 nationalités

Thèmes de recherche

- Réseaux Euclidiens
- Protocoles et preuves cryptographiques
- Théorie algorithmique des nombres

Financements actuels

- ERC-Starting LattAC [réseaux Euclidiens]
- ANR Alambic [malléabilité en cryptographie]
- BPI-DGE RISQ [regroupement de l'industrie française pour la sécurité post-quantique]
- H2020 PROMETHEUS