Cryptographie fondée sur les codes

CBCTYPT

Appel : Défi 9

Année : 2017

Instrument : PRC

Contact : jean-pierre.tillich@inria.fr

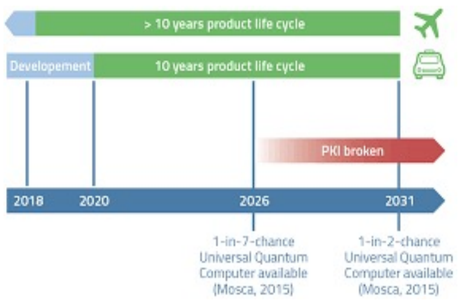
COORDINATEUR : **Jean-Pierre Tillich**

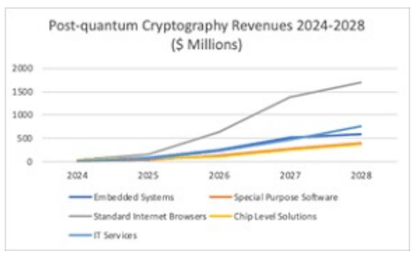
PARTENAIRES : **Inria de Paris**
Univ. Bordeaux, Limoges, Rouen

Résumé (3 lignes max) :
Compétition du NIST → besoin de primitives cryptographiques résistant à l'ordinateur quantique
Solution proposée : cryptographie à base de codes
Sécurité: repose sur le problème du décodage (NP complet) qui a de très bonnes chances d'être résistant à l'ordinateur quantique

CONTEXTE ET OBJECTIFS

Compétition du NIST: va changer toute la cryptographie à clé publique dans les années à venir.





Ordinateur quantique: casserait tous les schémas à clé publique utilisés en pratique (RSA, DSS, Diffie-Hellman..)

Solution proposée: cryptographie à base de codes, sécurité repose sur le problème NP complet de décodage

COMPETITION DU NIST

1er Tour (fin 2017)

1. 7 soumissions faites dans le cadre de ce projet
2. **26** soumissions au total en cryptographie basée sur les codes
3. **69** soumissions au NIST au niveau mondial

2ème Tour (Janvier 2019)

1. 5 soumissions restantes dans le cadre de ce projet
2. **7** soumissions restantes au totalen cryptographie basée sur les codes
3. **26** soumissions restantes au NIST au niveau Mondial

3ème Tour (Juillet 2020)

1. **1 finaliste et 2 finalistes alternatifs** dans le cadre de ce projet
= totalité des soumissions restantes en cryptographie basée sur les codes
3. **15** soumissions restantes au NIST au niveau Mondial

LE PROBLEME DU DECODAGE

- Résoudre un système linéaire avec plus d'inconnues que d'équations
- Contrainte de poids sur la solution

$$A x = b$$
$$|x| = w$$

Hamming $|x| = \#\{i : x_i \neq 0\}$
95% des cryptosystèmes jusqu'à présent
Rang $|x|$ = rang de la matrice x
50% de nos cryptosystèmes

AUTRES PRIMITIVES

Problème difficile : trouver une solution pour les signatures numériques, toutes les soumissions à base de codes au NIST ont été cassées

Solution 1 (métrique de Hamming) : Wave, best paper ASIACRYPT 2019, adaptation de GPV (réseaux) à la métrique de Hamming

Solution 2 (métrique rang) : DURANDAL, EUROCRYPT 2019

PUBLICATIONS

1. Soumissions au NIST: 1 monopartenaire,
6 multipartenaires
2. Articles dans des conférences internationales :
30 monopartenaires,
7 multipartenaires (ASIACRYPT, EUROCRYPT, ISIT, PQCrypto)
3. 11 thèses soutenues