CRYPTONEXT SECURITY

CRYPTONEXT Security

Protection numérique : y-sommes-nous vraiment préparé·e·s

L. Perret, perret@cryptonext-security.com
J.C. Faugère, jcf@cryptonext-security.com

SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

Inria

afnic

Agoranov

WILCO

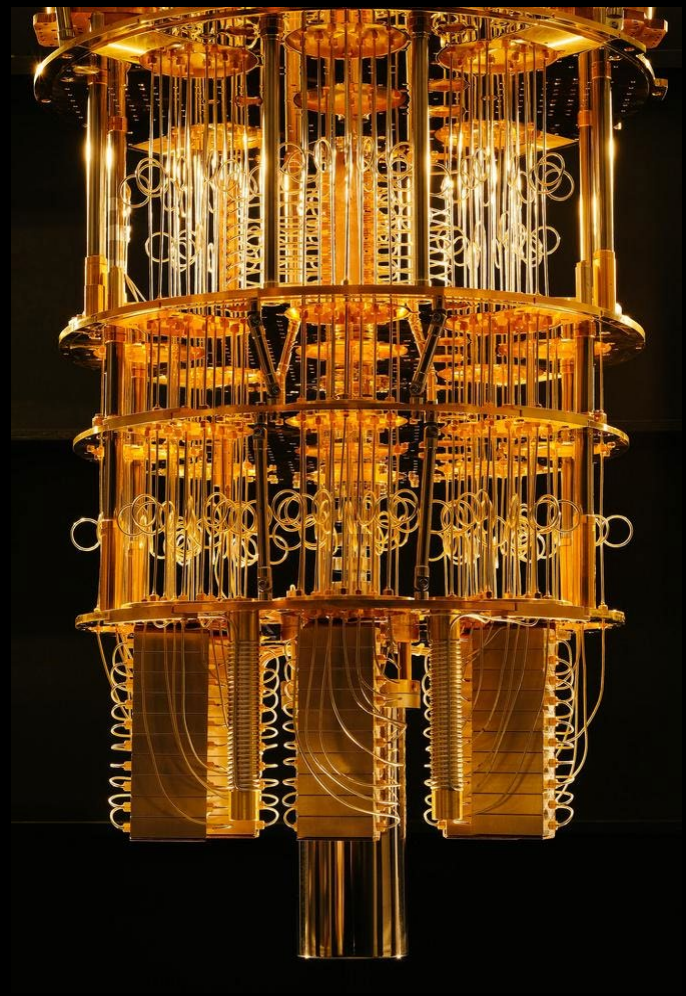
CYBER@ STATION F

AGENDA

Menace quantique

Standardisation

Exemple d’intégration



BAROMÈTRE ALLIANZ 2019 SUR LES RISQUES D'ENTREPRISES

"En France, les incidents cyber sont pour la première fois en tête des risques."

Enquête mondiale sur les risques d'entreprise, Allianz Global Corporate & Specialty (AGCS), 2019.

DES CYBER-ATTAQUES DE PLUS EN PLUS SOPHISTIQUÉES

"Les cyber-attaques sont de plus en plus sophistiquées. Les entreprises doivent se préparer à la prochaine menace : l'ordinateur quantique."

D. Mercier, ancien commandement suprême transformation de l'OTAN, Janvier 2019.

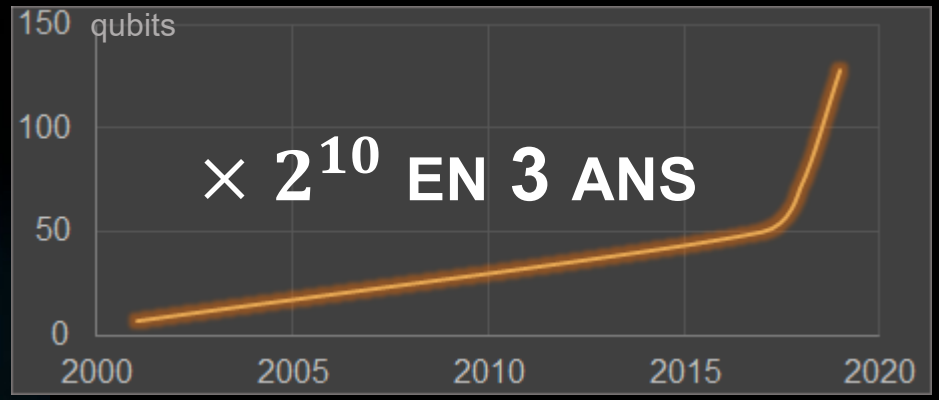
L'ORDINATEUR QUANTIQUE : UN CHANGEMENT DE PARADIGME

EN "vente libre":

ATOS QLM (2017)

IBM Q System One (2019)

Puissance de l'ordinateur quantique

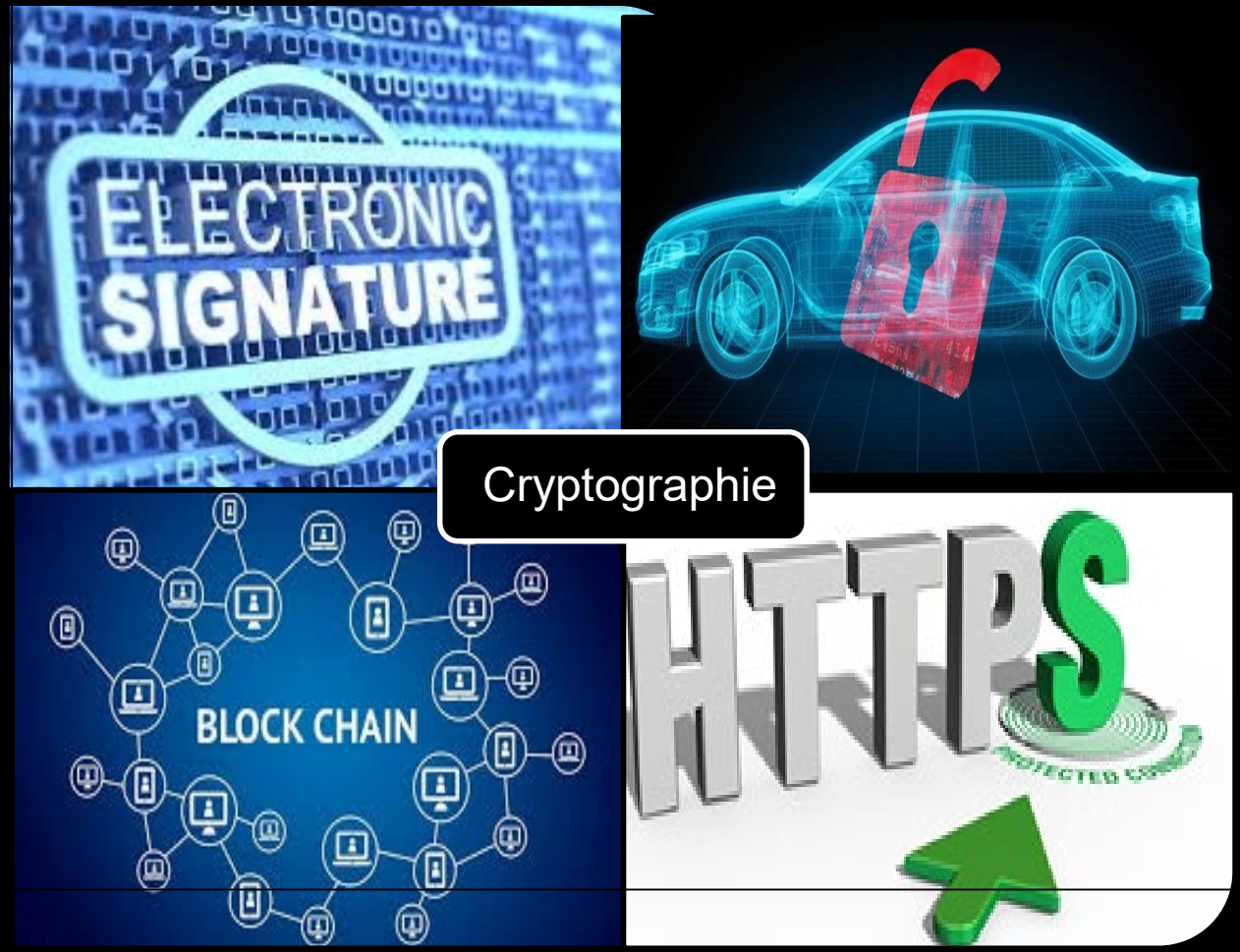


http://www.qubitcounter.com/

ORDINATEUR	Durée pour casser le standard actuel (RSA-1024)
Classique	~ 400 ans
Quantique	**1.2 h**

"*How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits*", C. Gidney, and Ma. Eker, 2019.

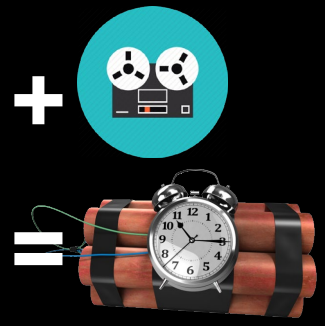
A TIME BOMB



Cryptographie

Objets/données avec une longue durée de vie

Enregistrer les données aujourd'hui pour les déchiffrer plus tard



PERCEPTION DU RISQUE

"IAD will initiate a transition to quantum resistant algorithms in the not too distant future. Based on experience in deploying Suite B, we have determined to start planning and communicating early about the upcoming transition to quantum resistant algorithms. [….]

For those partners and vendors that have not yet made the transition to Suite B elliptic curve algorithms, we recommend not making a significant expenditure to do so at this point but instead to prepare for the upcoming quantum resistant algorithm transition".
NSA, 2015.

PERCEPTION DU RISQUE

“Quantum risk is now simply too high and can no longer be ignored”.
D. Moody, NIST, 2016.

“L’ordinateur quantique menaçant la cryptographie n’existera peut-être jamais, mais le risque est au dessus du niveau acceptable pour Airbus”,
L. Granboulan, 2018.

“My customers are already asking about my transition plan to a quantum-safe cryptography.”
M. Campagna, Amazon Web Service, 2017.

PERCEPTION DU RISQUE

“Quantum risk is now simply too high and can no longer be ignored”.
D. Moody, NIST, 2016.

“L’ordinateur quantique menaçant la cryptographie n’existera peut-être jamais, mais le risque est au dessus du niveau acceptable pour Airbus”,
L. Granboulan, 2018.

“My customers are already asking about my transition plan to a quantum-safe cryptography.”
M. Campagna, Amazon Web Service, 2017.

STANDARDISATION

Impact sur Cryptographie

Cryptographie à clé secrète

Cryptographie à clé publique

Inverser la fonction (k est la taille de la sortie)

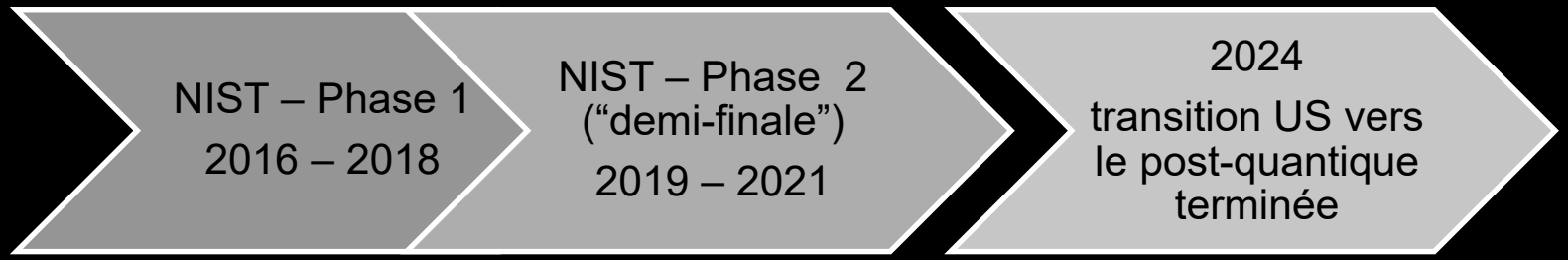
Classique $O(2^k)$ Recherche exhaustive

Quantique $O(2^{\frac{k}{2}})$ Algorithme de Grover

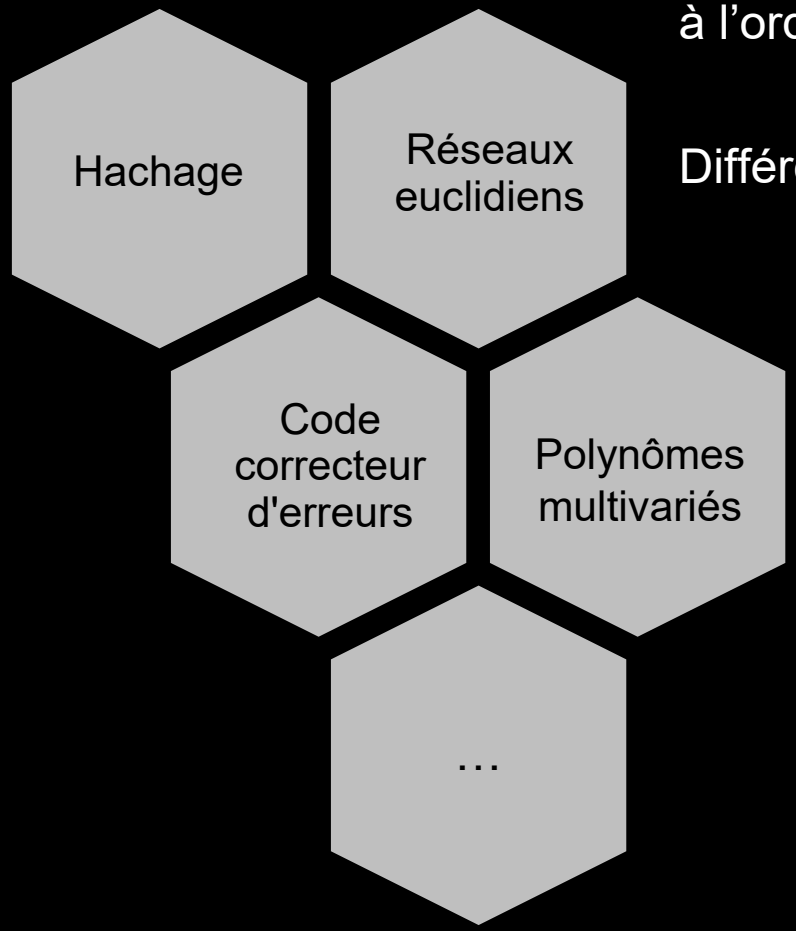
Algorithme polynomial (Shor) pour la factorisation (RSA) et le problème du log. discret (Diffie-Hellman, ECDSA, …)

NOUVEAUX STANDARDS RÉSISTANTS À L'ORDINATEUR QUANTIQUE EXIGÉS POUR 2021

*" …. transition of US IT government infrastructure to a post-quantum cryptography will be completed by **2024**".*
M. Scholl, NIST, 2017.



La cryptographie au cœur de l'enjeu



Il est nécessaire d'exploiter de nouveaux problèmes mathématiques résistants à l'ordinateur quantique pour imposer de nouveaux standards.

Différentes méthodes mathématiques sont en lice pour la standardisation

Exemple: résoudre des **équations non linéaires (44% des candidats à la seconde phase en signature)**:

$$\begin{cases} x_1x_4 + x_1x_5 + x_2x_3 + x_2x_4 + x_3x_4 + x_4 + x_5 + 1 = 0 \\ x_1x_3 + x_1x_5 + x_2x_4 + x_3x_4 + x_3x_5 + x_2 + x_5 + 1 = 0 \\ x_1x_3 + x_1x_4 + x_1x_5 + x_2x_5 + x_3 + x_4 = 0 \\ x_1x_3 + x_1x_5 + x_2x_3 + x_2x_4 + x_2x_5 + x_3x_5 + x_4x_5 + x_1 + x_5 + 1 = 0 \\ x_1x_2 + x_1x_4 + x_1x_5 + x_2x_3 + x_2x_5 + x_3x_4 + x_4x_5 + x_1 = 0 \end{cases}$$

GeMSS: A Great Multivariate Short Signature

Jacques Patarin. *Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms*. EUROCRYPT 1996: 33-48

Clé publique

$$\begin{cases} x_1x_4 + x_1x_5 + x_2x_3 + x_2x_4 + x_3x_4 + x_4 + x_5 + 1 = 0 \\ x_1x_3 + x_1x_5 + x_2x_4 + x_3x_4 + x_3x_5 + x_2 + x_5 + 1 = 0 \\ x_1x_3 + x_1x_4 + x_1x_5 + x_2x_5 + x_3 + x_4 = 0 \\ x_1x_3 + x_1x_5 + x_2x_3 + x_2x_4 + x_2x_5 + x_3x_5 + x_4x_5 + x_1 + x_5 + 1 = 0 \\ x_1x_2 + x_1x_4 + x_1x_5 + x_2x_3 + x_2x_5 + x_3x_4 + x_4x_5 + x_1 = 0 \end{cases}$$

Clé secrète

$$Fs(X) = \sum_{\substack{0 \le i \le j \le n-1 \\ 2^{i+j} \le D}} A_{i,j} X^{2^{i+j}} + \sum_{\substack{0 \le i \le n-1 \\ 2^i \le D}} B_i X^{2^i} + C \in \mathbb{F}_{2^n}[X],$$

GeMSS: A Great Multivariate Short Signature

A. Casanova, CS
J.-C. Faugère, INRIA, Sorbonne Université, CNRS
G. Macario-Rat, Orange
J. Patarin, University of Versailles
L. Perret, Sorbonne Université, CNRS, INRIA
J. Ryckeghem, Sorbonne Université, CNRS, INRIA

Level	Parameter set	Secret-key	Public-key	Signature	Keypair Generation	Signature	Verification
1	GeMSS128	13.44 Bytes	352.19 KB	258 Bits	38.5 MC	750 MC	82 KC
	BlueGeMSS128	13.7 Bytes	363.61 KB	270 Bits	39.3 MC	106 MC	111 KC
	RedGeMSS128	13.1 Bytes	375.21 KB	282 Bits	39.2 MC	2.79 MC	109 KC

J.-C. Faugère, L. Perret, J. Ryckeghem.
"***Software Toolkit for HFE-based Multivariate Schemes***". IACR Trans. CHES 2019.

PROCESSUS CONCURRENT

Phase 1
03/2019

Phase 2
11/19

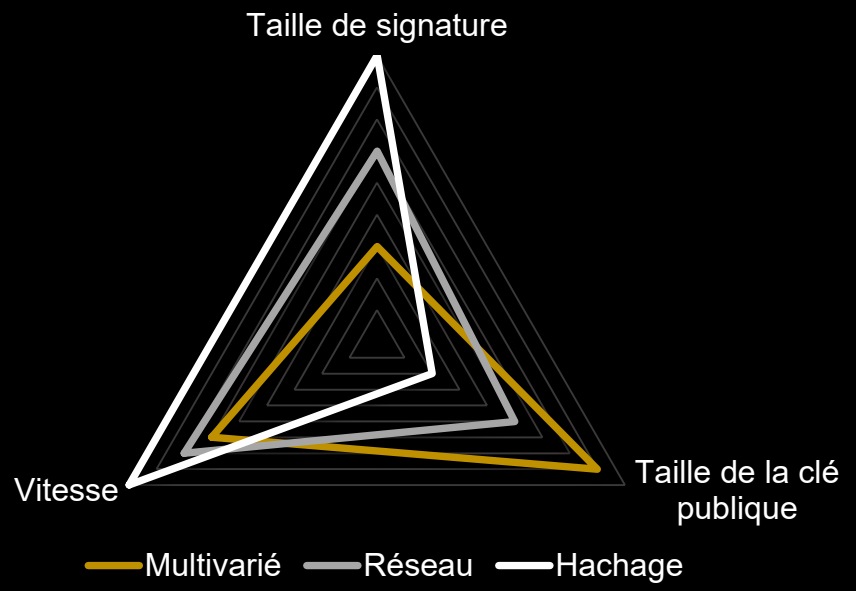
Nouveaux standards
12/19

J.-C. Faugère, E. Koussa, D. Lin, G. Macario-Rat, J. Patarin, L. Perret. "*PKP-Based Signature Scheme*". 2018.

#PK : 73 Bytes
#Sig : 16.37 Kbytes

PLUSIEURS STANDARDS EN FONCTION DES USAGES

Chaque méthode en lice pour la standardisation possède ses avantages et ses inconvénients en fonction des domaines d'application. Plusieurs standards seront retenus.



L'optimisation est la clé du déploiement de ces nouveaux protocoles.

UN PROCESSUS MONDIALISÉ

- ISO (international)
- ITU (international)
- IETF (internet)
- ETSI (EU)
- …….

ETSI TC CYBER QSC

Industry Specification Group (2015), et sous-groupe de TC Cyber (2017)
Chair : M. Pecen (Canada)

"*Analysis of Quantum-Safe Primitives*"
"*Quantum-Safe Case Studies & Use Cases*"
"*Quantum-Safe Threat Analysis*"
"*Limits of Quantum Computing on Symmetric Key Cryptography*"
"*Quantum-Safe Key Exchanges, Implementation Analysis*"
"*Quantum-Safe Virtual Private Networks*"

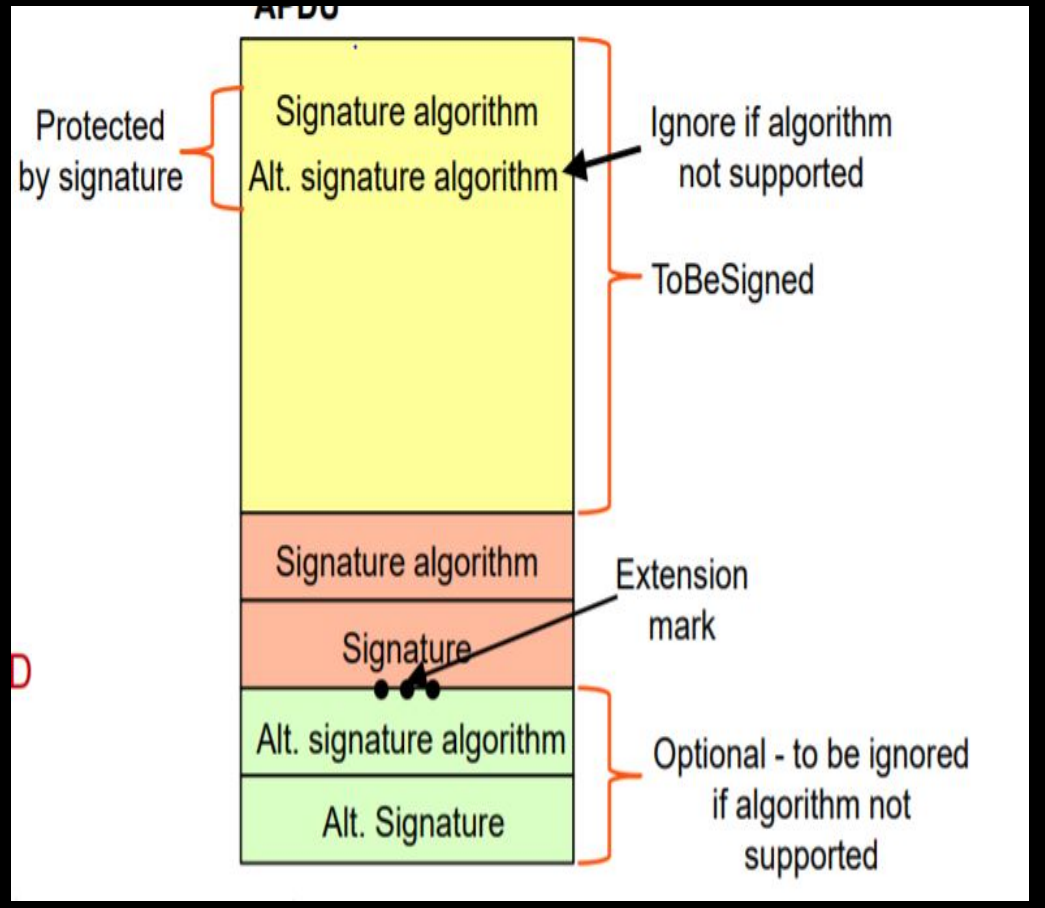
En cours
"*Quantum-Safe Cryptographic Signature assessment*"
"*Quantum-Safe Identity-Based Encryption (IBE)*"
"*Migration Techniques to Quantum-Safe Systems*"
"*Technical Specification for Hybrid Key Exchange Subsystem*", (Rapporteur, Amazon)

ITU

Migration strategy for X509
Chair : E. Andersen (Danemark)

"*Specification of extensions with procedures, e.g., for public-key certificates, is in Rec. ITU-T X.509 | ISO/IEC 9594-8 to be finally approved later this year for publication early 2020*"

Quantum-safe for 5G ?



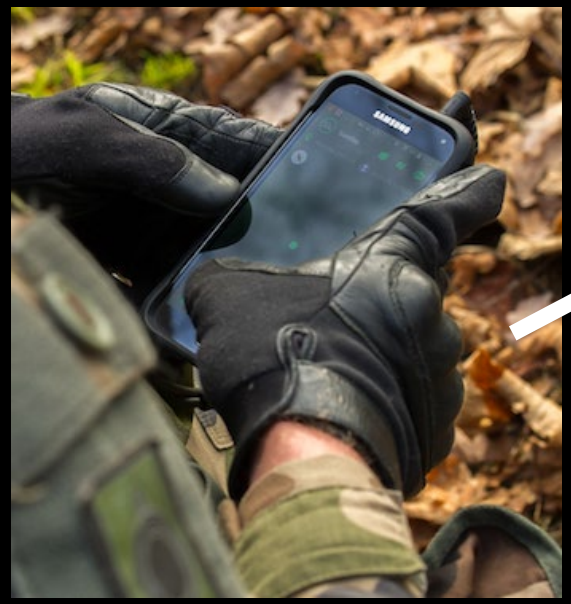
INTÉGRATION

DÉPLOIEMENT

Prototypage et validation terrain avec l'Armée de Terre d'une messagerie sécurisée contre les ordinateurs quantiques.

Photos issues du test terrain Base de Saint-Germain-en-Laye (150 participants)

DÉMONSTRATION



Utilisateur 3

Message

Utilisateur 1

Message

Document

Utilisateur 2

Echange de clé post-quantique
+ AES

DÉMONSTRATION

https://crypt

CONCLUSION

PROJET RISQ (2017-2020)

DIRECTION GÉNÉRALE DES ENTREPRISES

INVESTISSEMENTS D'AVENIR

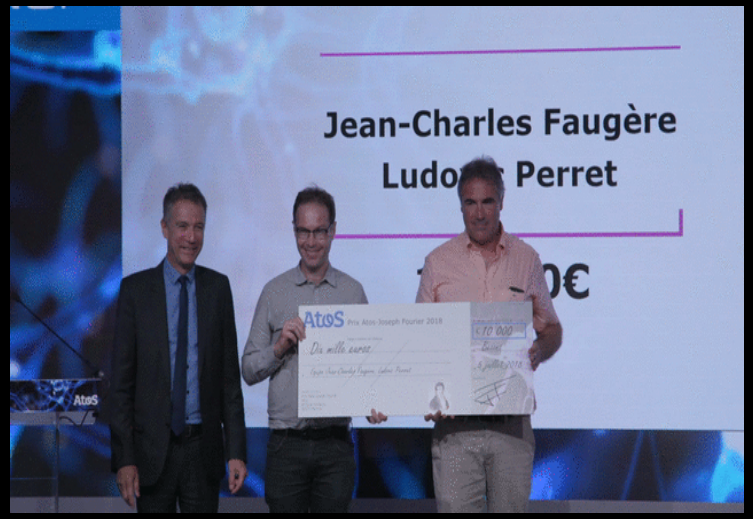
TABLE RONDE (10 OCTOBRE 2019)

Menace quantique sur la sécurité

J.-C. Gougeon - Bpifrance
C. Jurczak (Quantonation)
D. Mercier (ex. commandant suprême de la transformation à l'OTAN)
P. Forteza (députée LREM, responsable mission quantique)
L. Perret
O. Senot (Docapost)

SE PRÉPARER À LA TRANSITION POST-QUANTIQUE

1er prix Atos- Fourier 2018
calcul quantique



www.cryptonext-security.com

contact@cryptonext-security.com