Sécurité et Cryptographie dans le Monde Quantique, et présentation du ETSI WG QSC

Presented by: **Mark Pecen, Président passé**
ETSI TC Cyber WG QSC

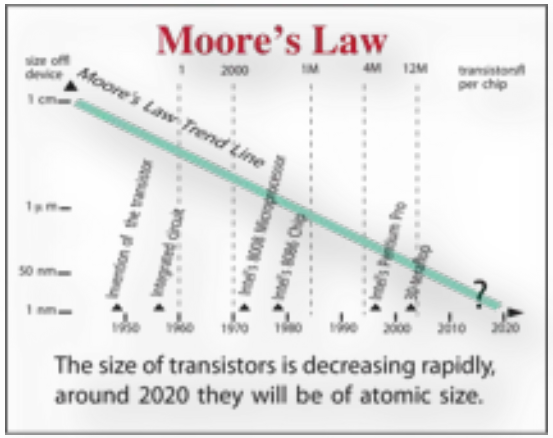
For: **ETSI Webcast**

Mise à jour
15/2/2023

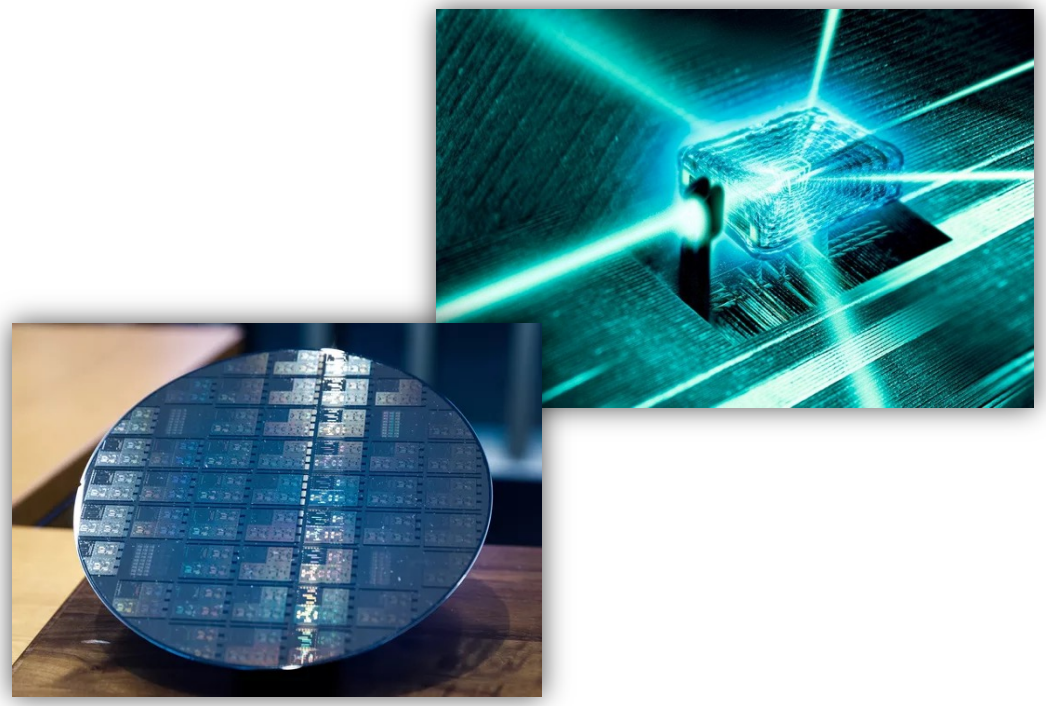
Ordre du jour

- Un aperçu du calcul quantique
- Les impacts de l’ordinateur quantique sur la sécurité de l’information
- La réponse par l'industrie aux problèmes de sécurité
- Paysage des techniques de sécurité « quantum-safe »
- À propos du ETSI WG for Quantum-Safe Cryptography

L'informatique quantique c'est un mélange de...



Théorie d'information



Mécanique quantique

Avec les deux domaines, on peut calculer avec certitude, en utilsant des effets d'incertitude !

Un bit classique peut être soit 1 ou 0

- C'est comme une ampoule qui est activée ou désactivée
- Dans un processeur Von Neumann standard, on obtient un ensemble d’états pour chaque pulsation d'horloge

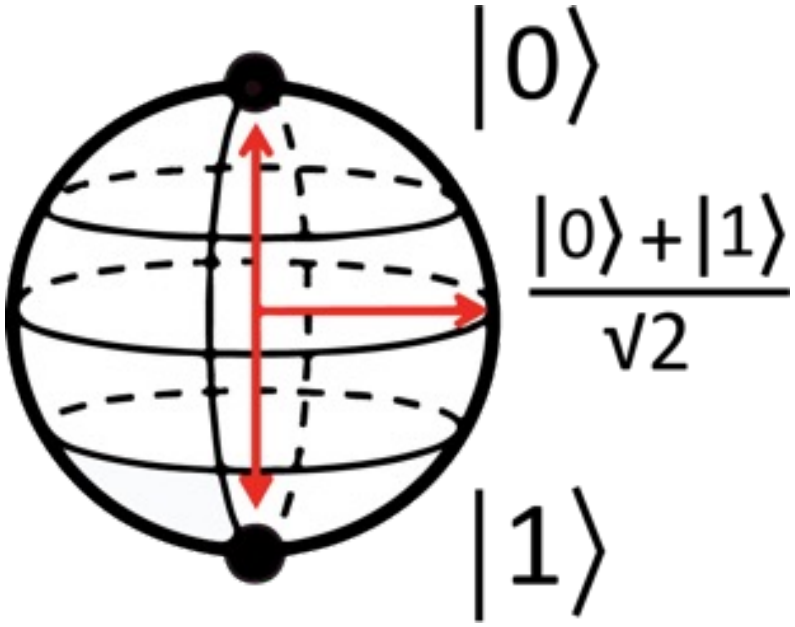
or

0
“Éteinte”

1
“Allumée”

Un bit quantique (qubit) est extrêmement différent

- Un bit quantique peut exister dans les **multiples états simultanément**, comme une lampe qui est allumée et non allumée à la même fois
- Nombre d'états = 2^N, où N = nombre de qubits
- Exemple: Un système ayant 16 qubits peut être dans 2^{16} = 65,536 états simultanément!

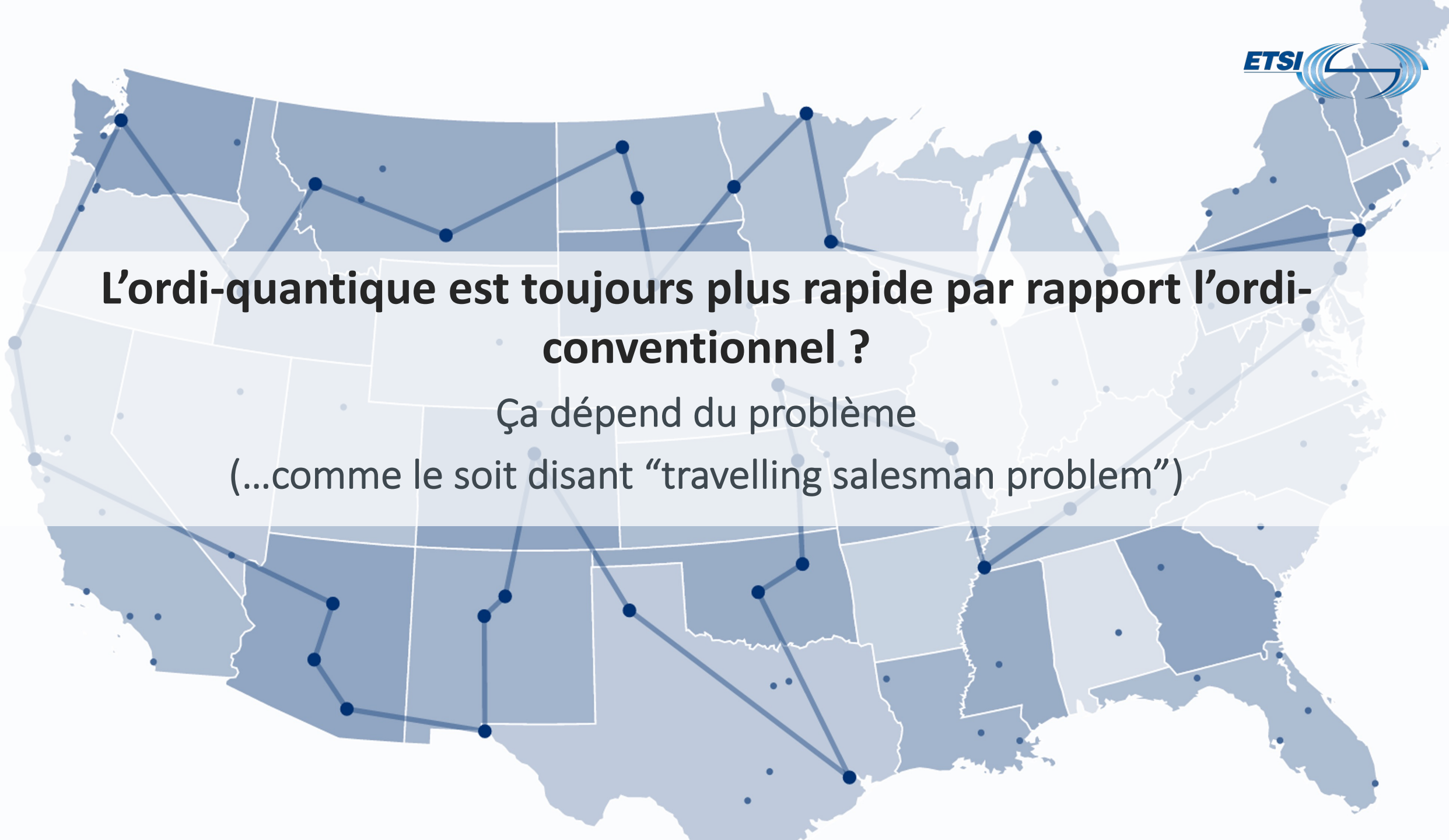


Comment C’est Possible?

Il y a une meilleure question…

Comment peut-on utiliser cette caractéristique pour trouver des solutions aux problèmes difficiles et très importants ?

L'ordinateur quantique rend possible la résolution de certains problèmes trop difficiles pour les ordinateurs conventionnels

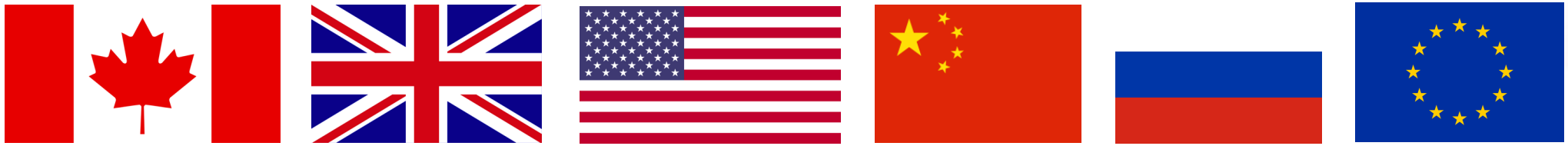


L’ordi-quantique est toujours plus rapide par rapport l’ordi-conventionnel ?

Ça dépend du problème

(…comme le soit disant “travelling salesman problem”)

La course à la technologie quantique est déja lancée



Microsoft Google rigetti EeroQ QUANTUM HARDWARE

IBM

Forte croissance des investissements !

D-Wave The Quantum Computing Company™

aws Braket

QCi Ready-to-Run Quantum Systems

intel

AQT

XANADU

diraq

ATLANTIC QUANTUM

Atos

ColdQuanta

ZAPATA

Baidu 百度

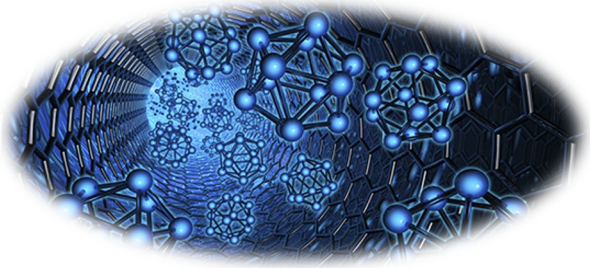
atom computing

QCWARE

bleximo

Un nouveau domaine de possibilités

L'informatique quantique résoudra les problèmes insolubles d'aujourd'hui et révolutionnera de nombreux secteurs



Conception des matériaux

Cryptographie

“Big data”

Prévisions météorologiques

Chimie

Intelligence artificielle

Un grand défi après l'adoption des ordinateurs quantiques à grande échelle :

La sécurité

Les ordinateurs quantiques vont briser les normes actuelles de chiffrement à clé publique

Type	Algorithme	Force clé classique(bits)	Force clé quantique(bits)	Attaque quantique
Asymétrique	RSA 2048	112	0	Shor's Algorithme
	RSA 3072	128		
	ECC 256	128		
	ECC 521	256		
Symétrique	AES 128	128	64	Grover's Algorithme
	AES 256	256	128	

Impact sur la communication sécurisée

Protocole de communication sécurisée

Authentification | **L'échange de données**

L'algorithme de Shor rompt l'authentification par clé publique

Authentification Brisée

Chiffrement symétrique

AES 256 → AES 128

L'algorithme de Grover **réduit** l'efficacité par 50%

Impact sur les mises à jour logicielles

Embed a Root of Trust at Manufacture

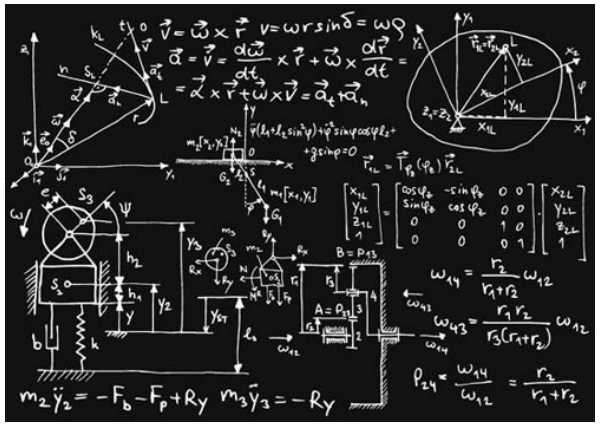
Digital Signature | Software Update

- Reçoit la demande pour mise à jour logiciel
- Vérifier la signature ECDSA or RSA
- Applique la mise à jour de logiciel

→ **brisée par l'algorithme de Shor**

Les Pistes vers résistance aux attaques quantiques

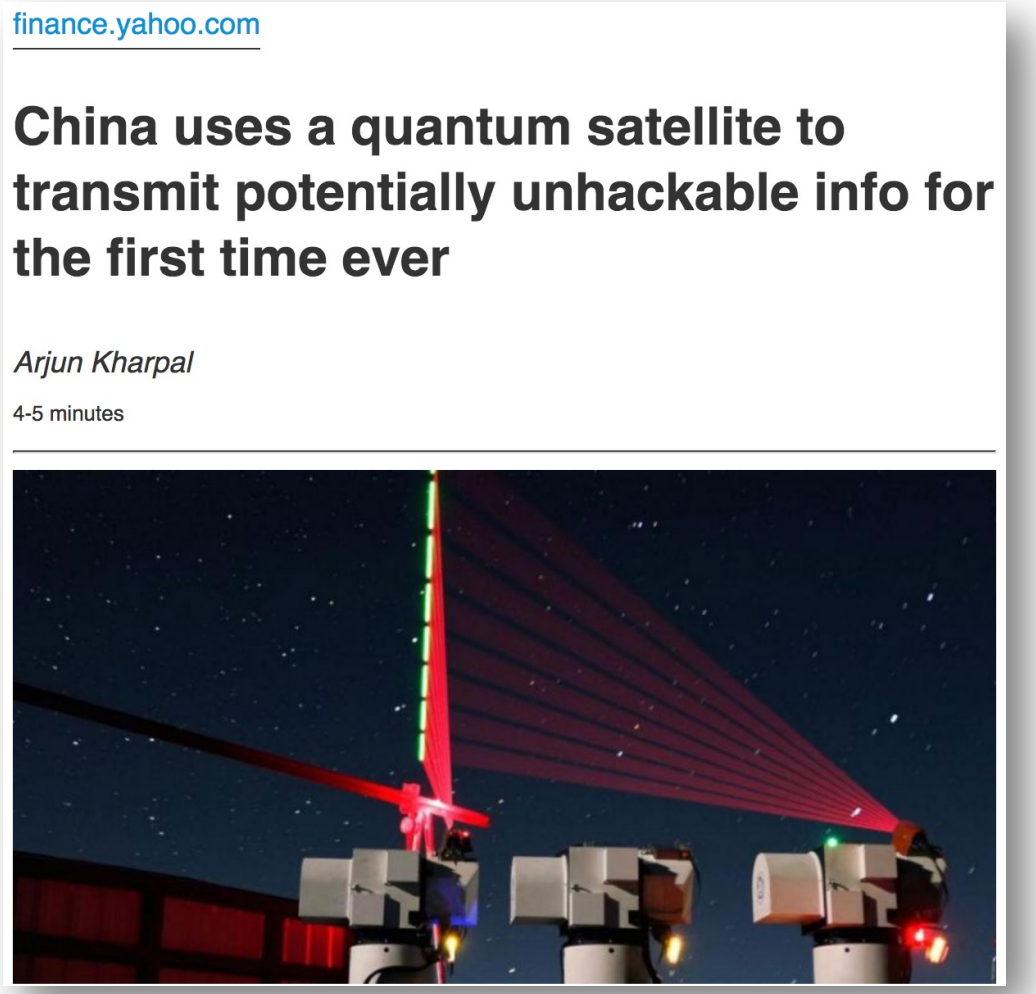
Quantum Key Distribution (QKD)



Quantum-Safe Cryptography (QSC)

Quantum Key Distribution (QKD)

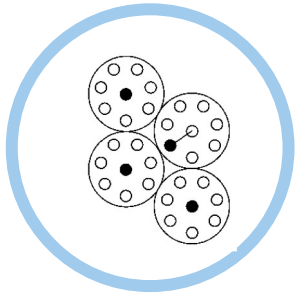
- Utiliser les propriétés à base de physique pour protection des données
- Exiger les connexions optiques à fibre ou directe lignes de vision
- Portée limitée par la distance
- Risques des attaques “indirectes”
- Exigeant d’un chaîne protégée pour authentification bout à bout



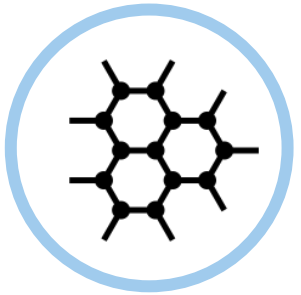
“Quantum Safe Cryptography” (QSC): Les Nouveau Mathes

QSC: Les Nouveau Mathes

Basée sur les hachages

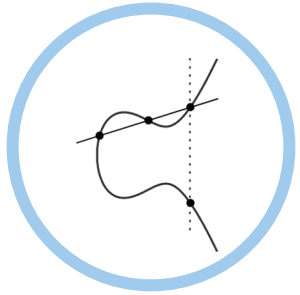


Basée sur les codes



Basée sur les treillises

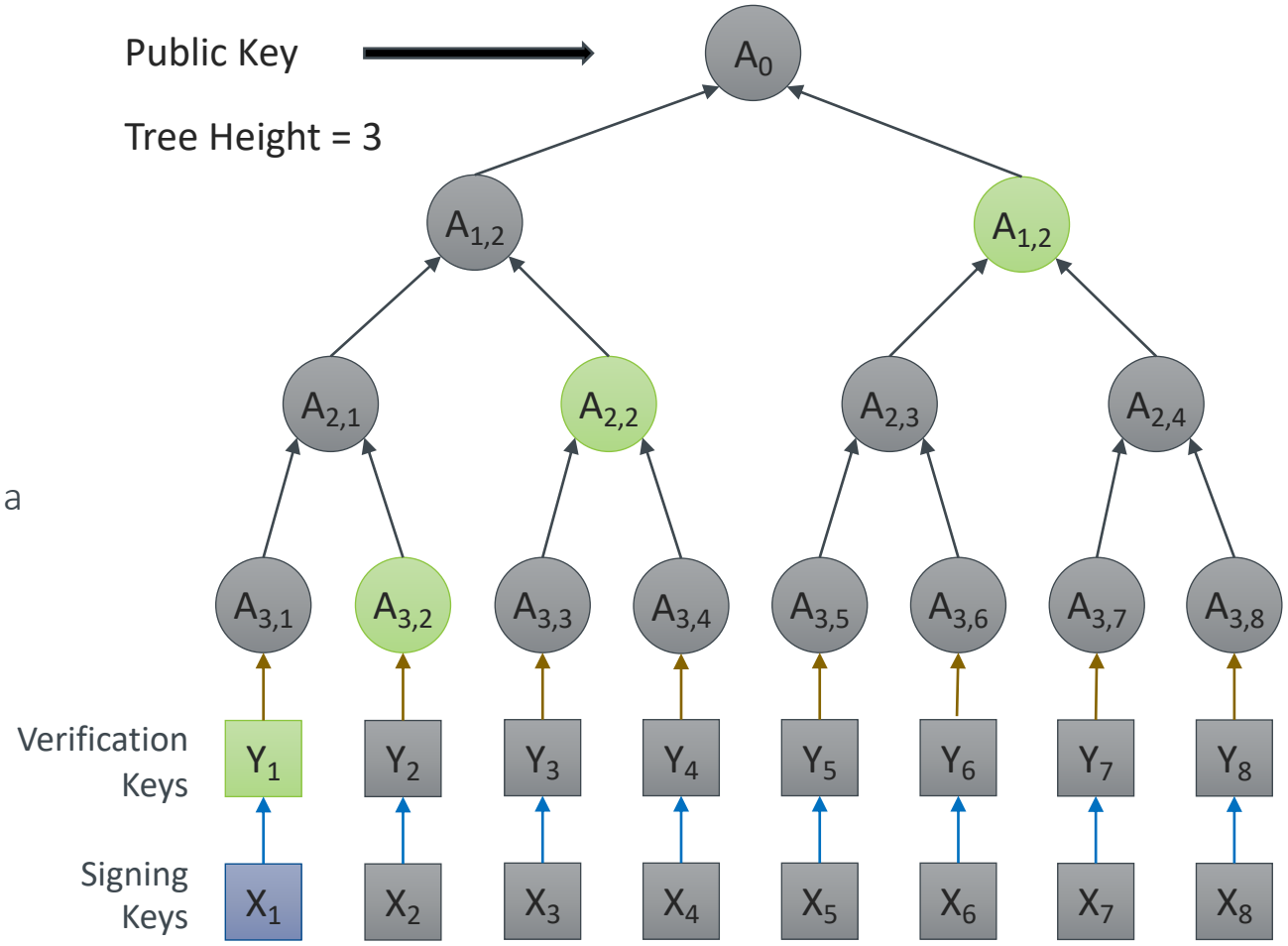
Basée sur les variables multiples



Basée sur les Isogenies

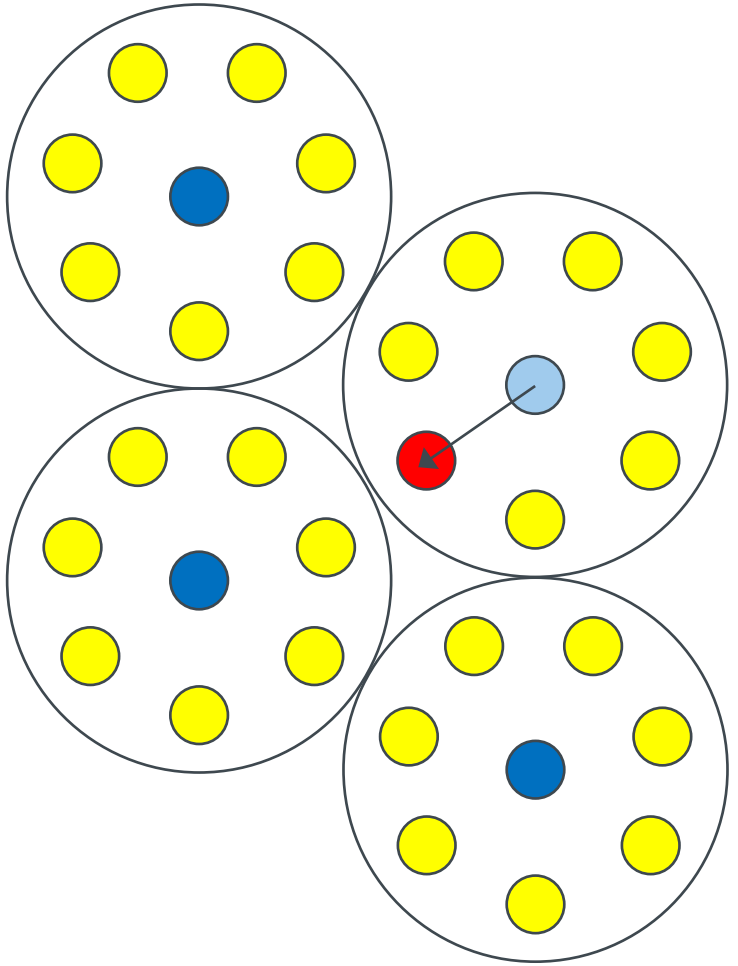
Cryptographie basée sur les hachages

- Créé par Merkle depuis 1979
- “One-Time Signatures” – utilisation une seule fois
- Petite clef publique, mais clef privée très large
- Rapide signatures et vérification
- Exigent le stockage des états de réseau
- La technique devenue pratique par combiner les clefs de la vérification – résultant une seule clef publique
- En plus, c’est naturellement résistant aux attaques quantique
- Candidates
  - Leighton-Micali Signatures (LMS)
  - eXtended Merkle Signature Scheme (XMSS)
  - SPHINCS



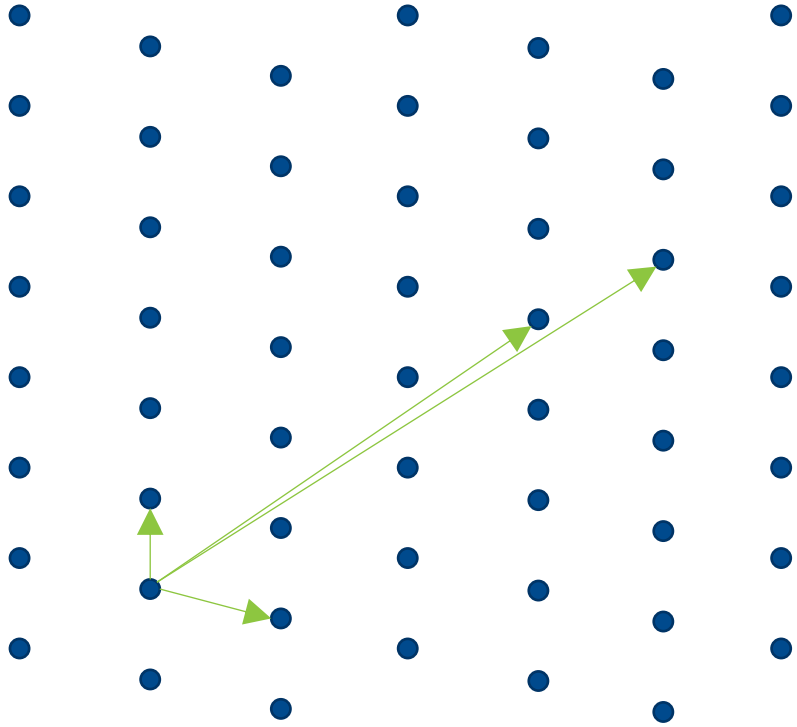
Cryptographie basée sur les codes

- Développé par McEilece à 1978
- Basée sur la difficulté de déchiffrer les codes pas connus
- Extrêmement grosse clef publique
- Chiffrement et déchiffrement rapide
- Variations plus petites – QC-MDPC, McBits, etc.
- Attaques récemment arrêtées par l'usage des clefs éphémères



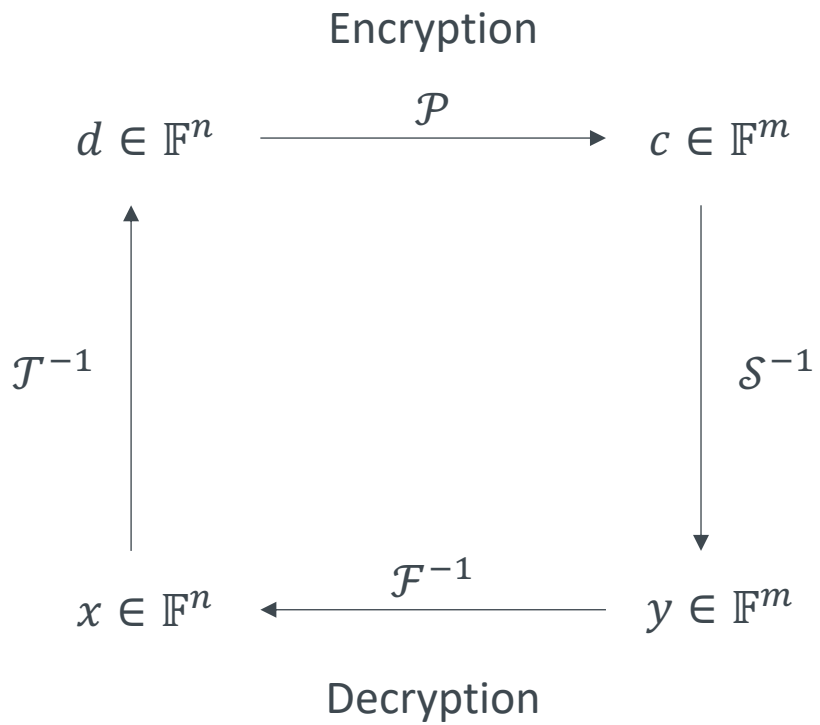
Cryptographie basée sur les treillis

- Première version commercial était NTRU (1996)
- Problèmes difficiles mathématiques:
  - Solution des plus cours nombres entiers (SIS)
  - Apprentissage avec les erreurs (LWE)
- Tailles des clefs raisonnables, et opérations très rapides
- Il reste quelques questions autour des “réductions”
- Quelques risques en utilisant les clefs statiques
- Expérimentation par Google avec NewHope dans le Chrome Canary



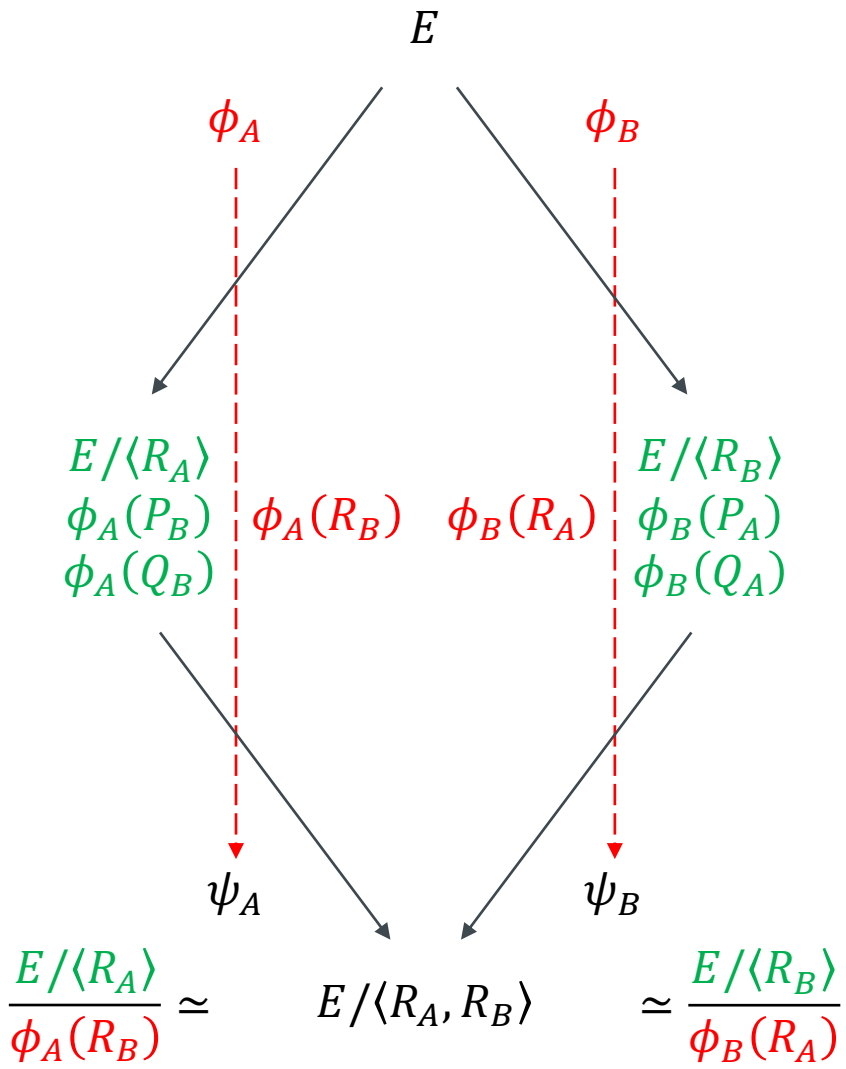
Cryptographie Multivariate

- Développée par Matsumoto and Imai (1988)
- Trouver la solution des “N” équations non-linéaires
- C’est possible d’utiliser pour les signatures, échange de clefs et transport des clefs
- Souvent, il y a un échange de taille de clef et la vitesse d’opération



Cryptographie basées sur les isogénies

- Développée par David Jao (2009)
- Basée sur la difficulté de trouver les ”isogénies” (correspondances) entre deux courbes elliptiques
- Taille de clefs assez raisonnable
- Opérations un peu lentes
- Quelques risques avec les clefs statiques
- Exemples, SIKE, qui était brisée 2022 pendant la compétition NIST (cassé à cause d'un petit jeu de paramètres)



Les Normes Exigent le succès

Corps de normalisation de la Cryptographie Quantum-Safe

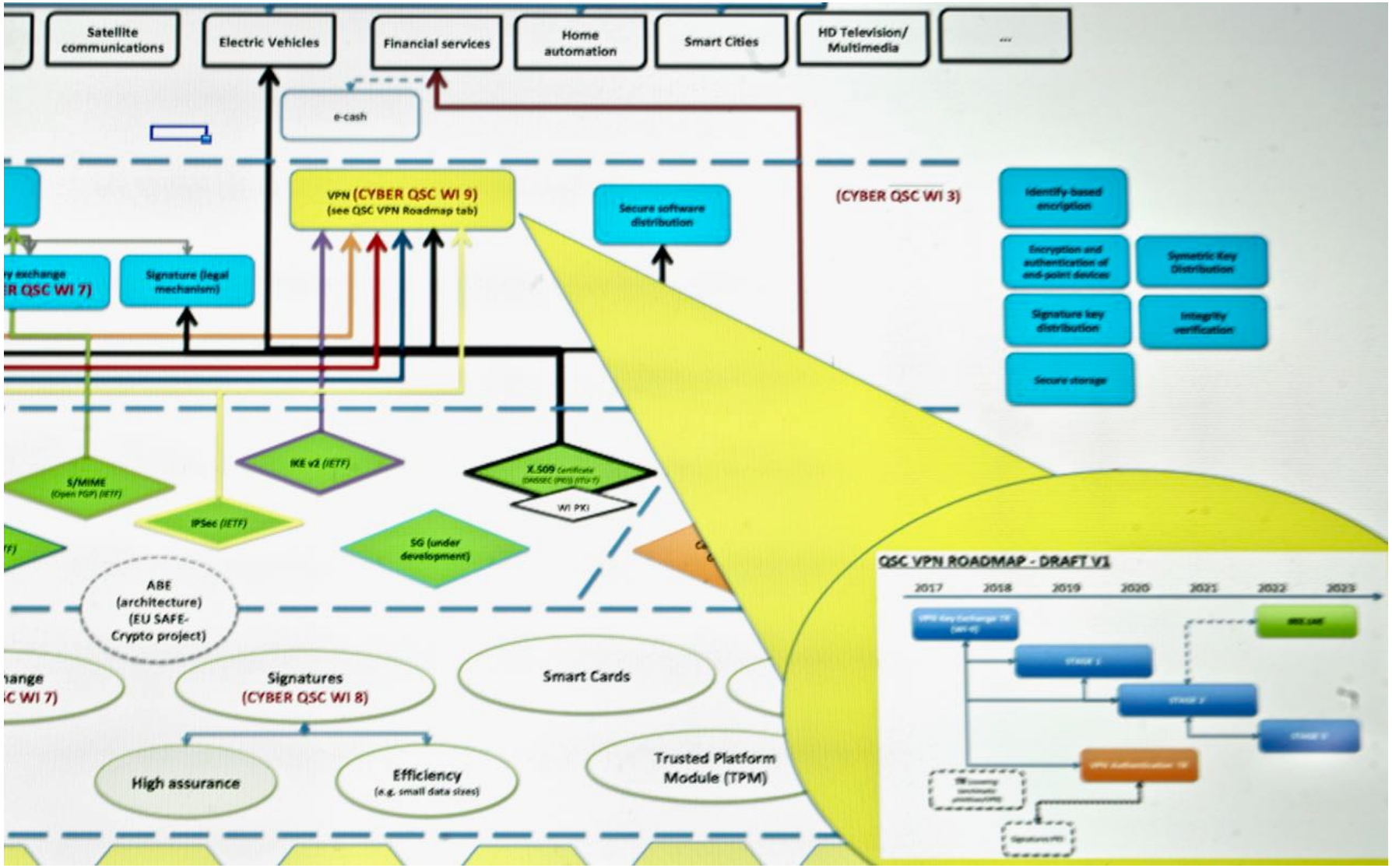
Concernant le Technical Committee Cyber (TC Cyber) Groupe de Travail pour Quantum-Safe Cryptography (QSC)

- Créé en mars 2015 comme ETSI Groupe d'Industrie Spécification puis changé en groupe de travail de TC Cyber en mars 2017
- L'objectif primaire est l'ingénierie pratique des algorithmes QSC, incluant les aspects de performance, capacités, architecture et protocoles pour les applications spécifiques.
- Les travaux résultant peuvent cibler d'autres groupes ETSI et projets par ex. 3GPP et aussi les autres corps de normalisation par ex. Union Internationale des Télécommunications (UIT)
- Les objectifs n'incluent PAS le développement des primitives cryptographiques elles mêmes
  - C'est la fonction des autres groupes plus spécialisées pour cela

Feuille de route à long terme de Cyber QSC était fait

- C’est un document à l’intérieur du group, incluant
  - Une charte qui montre les éléments de technologies et leur relation les uns aux autres
  - Les feuilles de routes dérives des composants technologiques de cette charte
  - Il s’agit d’un mécanisme pour guider les membres avec leurs activités de normalisation, dépendant de leur intérêts commerciaux
  - La feuille de route montre des possibilités, pas les certitudes !
- Première feuille de route était complète depuis mai 2017
- Chaque réunion, la feuille de route est revue rapidement et mise à jour quand il est nécessaire

Une partie de la feuille de route qui montre les relations entre les éléments avec quelques détails plus fins



Questions ?

Vous pouvez me contacter:

mpecen@approachinfinity.ca