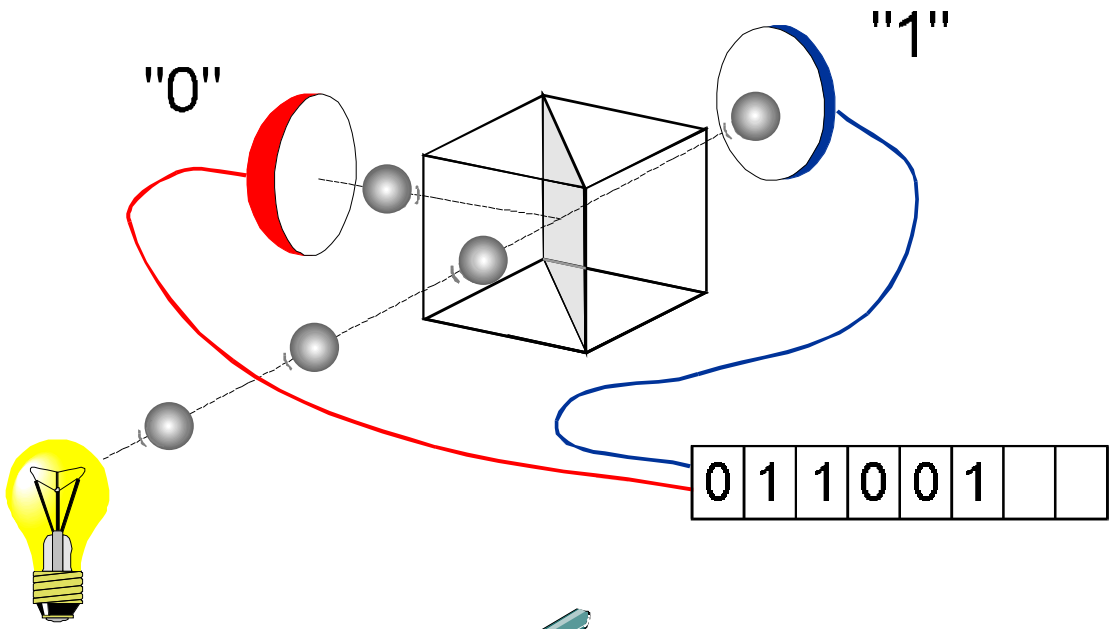
Comment la cryptographie quantique peut contribuer à la cybersécurité

Nicolas Gisin, Hugo Zbinden,
Mikael Afzelius et Rob Thew
GAP-Optique, Université de Genève

- **L'ère de la technologie quantique a commencé**
- **Des générateurs quantiques de nombres aléatoires**
- **Des calculateurs quantiques et le besoin d'avancer vers une cryptographie quantique sûre**
- **La distribution quantique de clés existe aujourd'hui**
- **Que doit-on faire?**

GAP quantique

Principe physique du séparateur de rayons

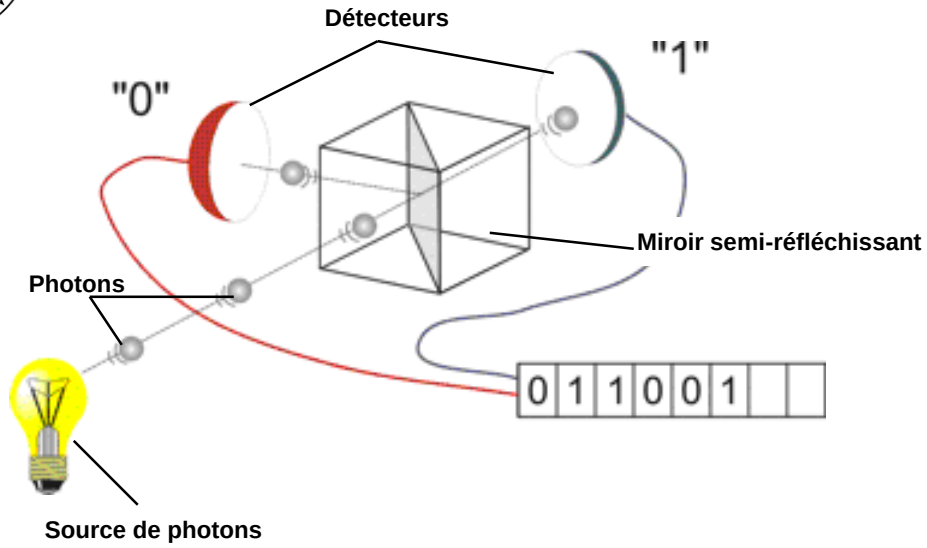


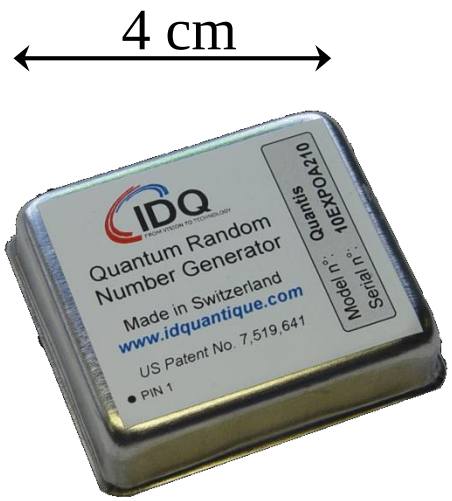
Génération de clés

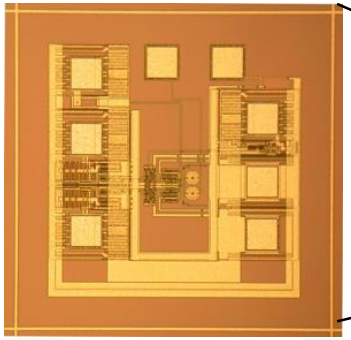
- Une source d'entropie d'une conception simple
- Seule la physique quantique offre un caractère aléatoire fondamental
- Une compréhension aisée de l'origine de l'aléatoire
- Un générateur fonctionnel de nombres aléatoires

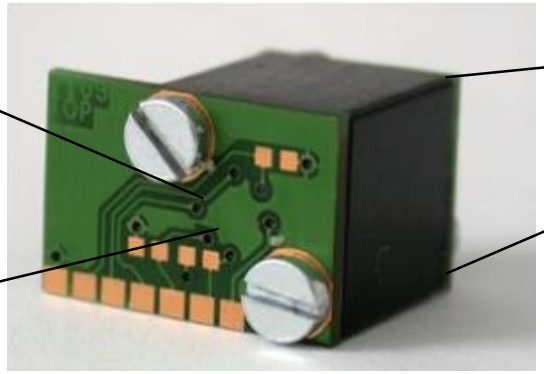
GAP quantique

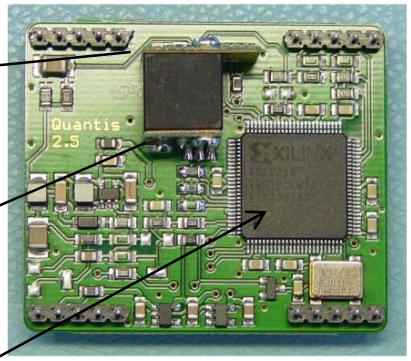
Générateur quantique de nombres aléatoires (GQNA)











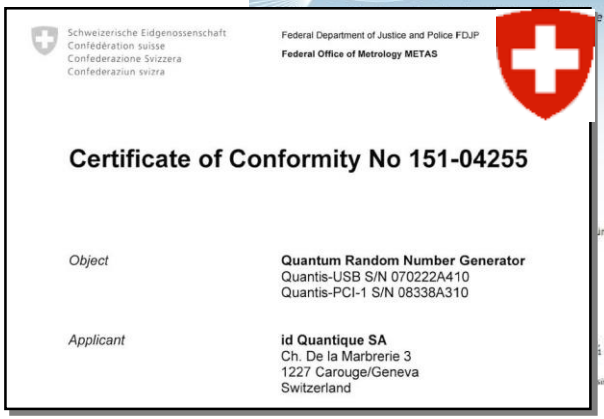
4 Mo par seconde de bits aléatoires uniformément distribués

GAP quantique

Evaluation et certification

GNA (physique) non déterministe

Bundesamt für Sicherheit in der Informationstechnik



- PTG.1

GNA physique avec des tests internes détectant une défaillance totale de la source d'entropie et les erreurs statistiques non tolérables des nombres aléatoires internes

- PTG.2

PTG.2 = PTG.1 + un modèle stochastique de la source d'entropie et des tests statistiques des nombres aléatoires bruts

- PTG.3

PTG.3 = PTG.2 + un post-traitement cryptographique (hybride PTGNA)

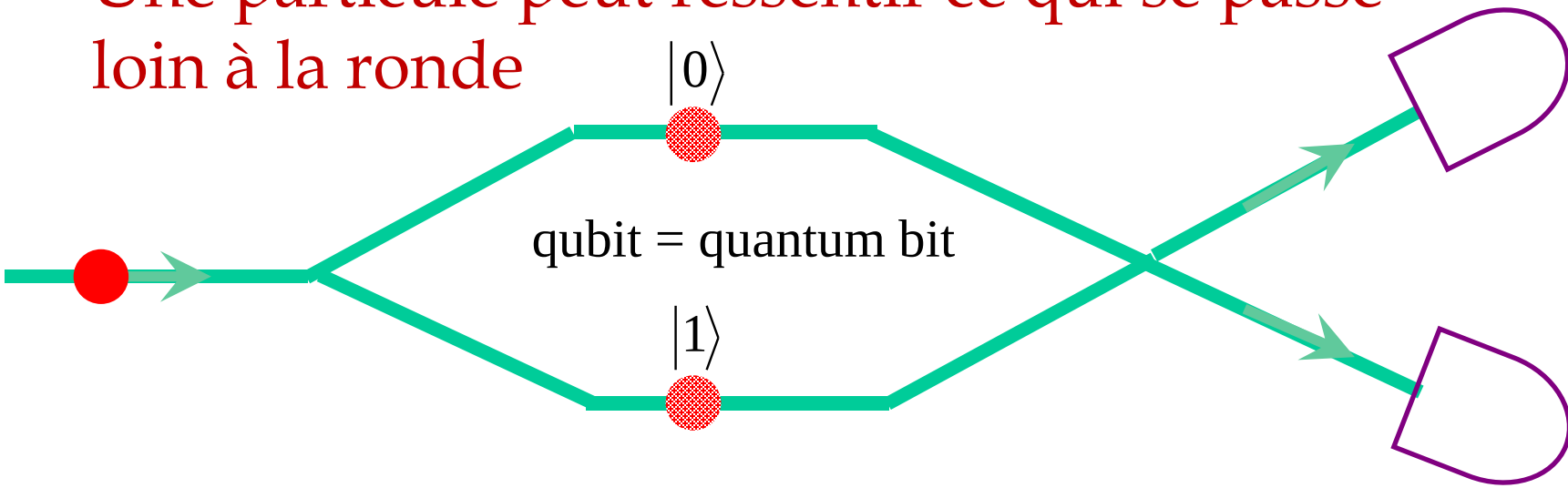
GAP quantique

GNA = générateur de nombres aléatoires
PTG = probabilistic tractography (tractographie probabiliste)

Mécanique quantique

(ce que vous devez savoir sur la physique)

- Une particule peut ressentir ce qui se passe loin à la ronde



- Pareillement, on peut avoir $|0\rangle+|1\rangle+|2\rangle+|3\rangle+...+|n\rangle$
- 100 qubits peuvent comprendre toutes les particules présentes dans l'Univers
- Il s'ensuit qu'avec une mesure, on obtient un seul résultat

GAP quantique

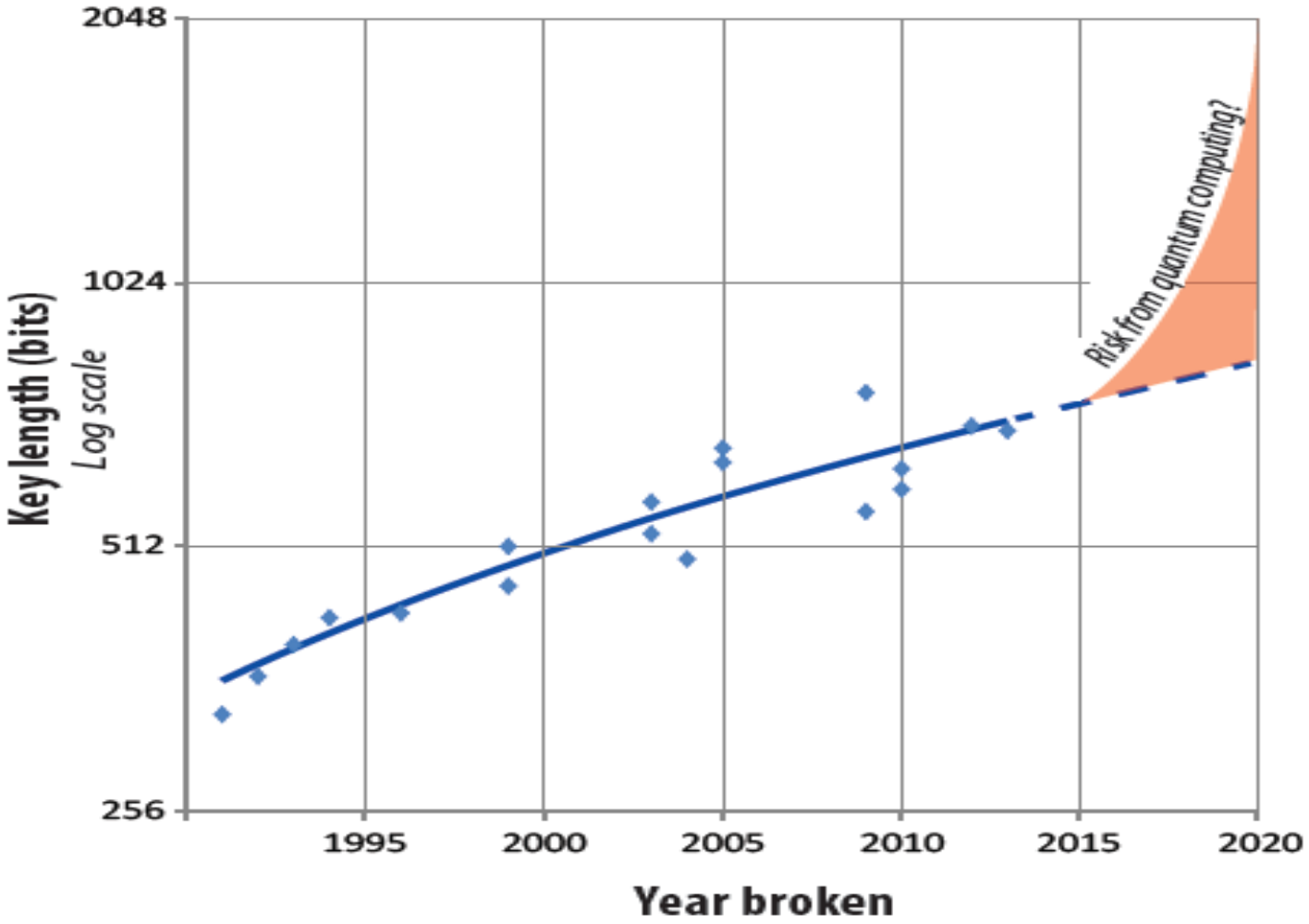
Calculs quantiques

- Traiter l'information: input x $\Rightarrow$ output fct(x)
- Calculateur quantique:
  traitement quantique d'informations classiques,
  input $|0\rangle+|1\rangle+|2\rangle+\ldots+|n\rangle \Rightarrow |fct(0)\rangle+|fct(1)\rangle+|fct(2)\rangle+\ldots+|fct(n)\rangle$
- Une mesure ne peut fournir qu'un seul résultat
- Ce résultat unique peut fournir des informations sur une propriété globale de la fonction fct
- Par exemple, la valeur maximale de la fonction, sa valeur moyenne ou des informations sur sa périodicité

Faits

- Avec la période d'une fonction et un zeste de théorie des nombres
- $\Rightarrow$ on peut casser toutes les clés cryptographiques publiques actuelles
- En clair, on peut donc déchiffrer tous les messages cryptés
- En conséquence, un calculateur quantique rend obsolètes les clés publiques cryptographiques utilisées de nos jours

Effet des calculateurs quantiques sur le chiffrement RSA*

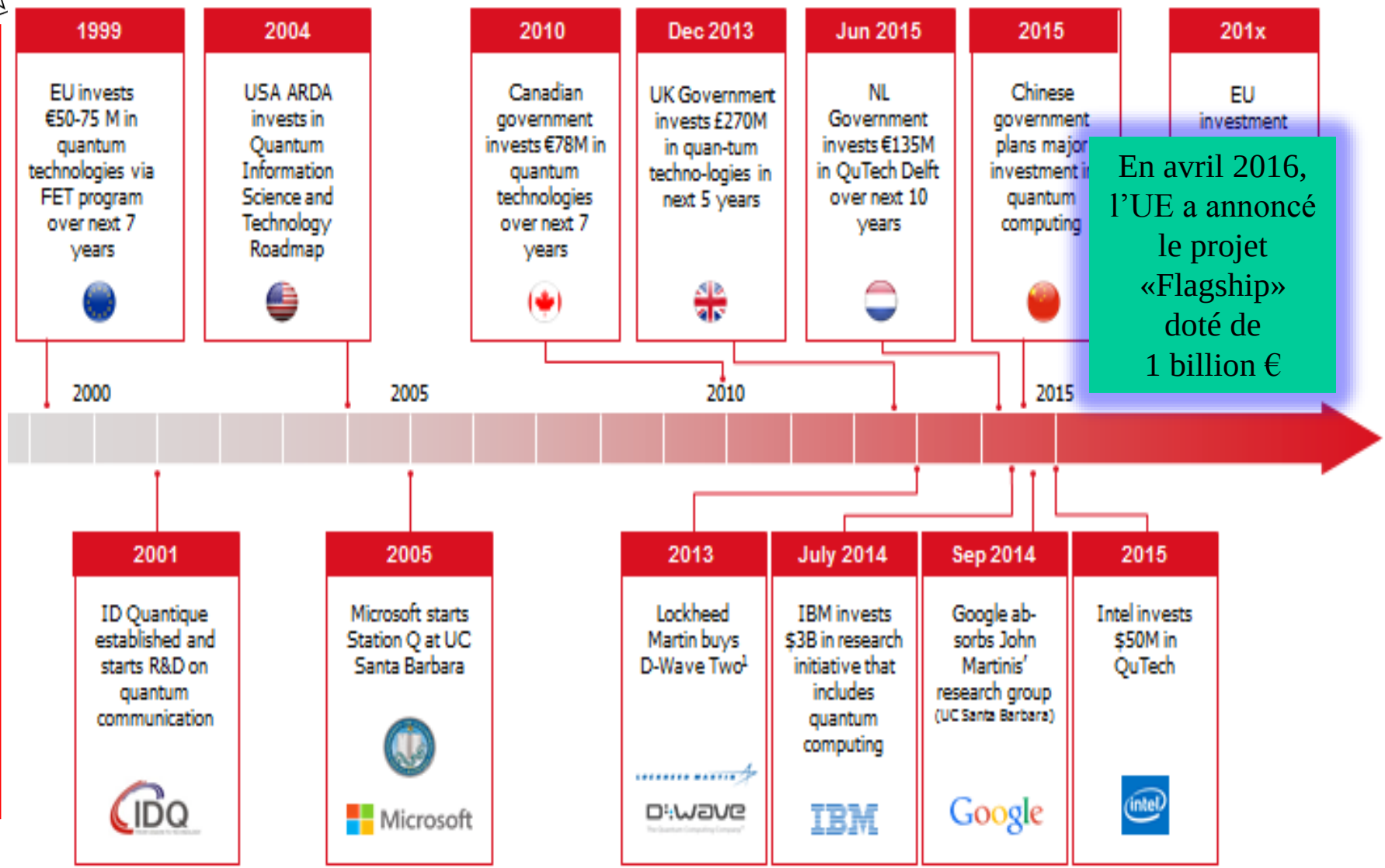


https://downloads.cloudsecurityalliance.org/initiatives/qss/What_is_Quantum_Safe_Security_position_paper.pdf

* chiffrement RSA: système de chiffrement inventé par R. Rivest, A. Shamir et L. Adleman

GAP quantique

Quand disposerons-nous de calculateurs quantiques?



En avril 2016, l'UE a annoncé le projet «Flagship» doté de 1 billion €

GAP quantique

Changements technologiques

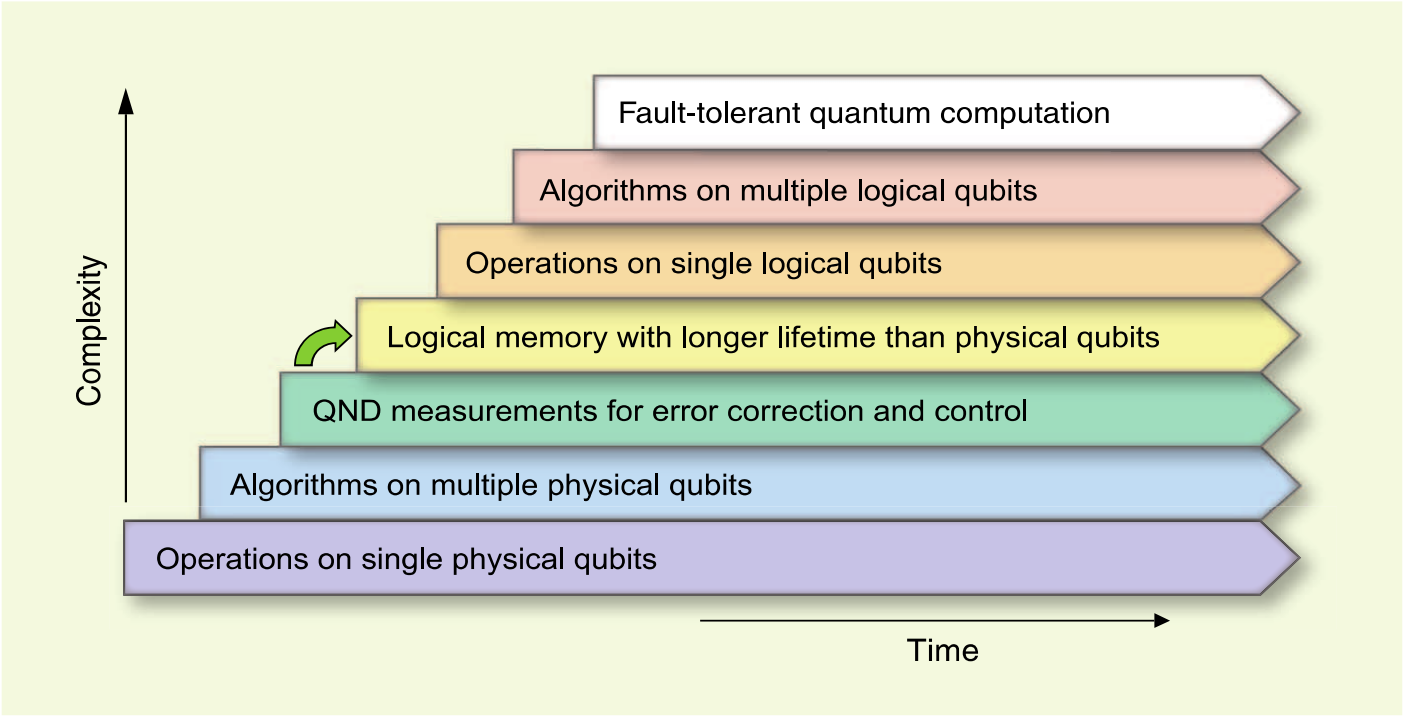


Fig. 1. Seven stages in the development of quantum information processing. Each advancement requires mastery of the preceding stages, but each also represents a continuing task that must be perfected in parallel with the others. Superconducting qubits are the only solid-state implementation at the third stage, and they now aim at reaching the fourth stage (green arrow). In the domain of atomic physics and quantum optics, the third stage had been previously attained by trapped ions and by Rydberg atoms. No implementation has yet reached the fourth stage, where a logical qubit can be stored, via error correction, for a time substantially longer than the decoherence time of its physical qubit components.

Changement de perception

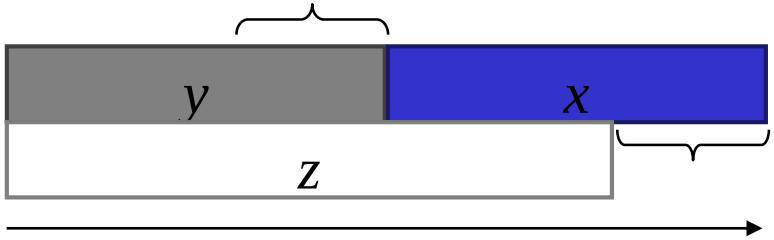
Quand devrons-nous commencer à nous faire du souci?

Cela dépend des réponses aux questions suivantes:

- Pendant combien de temps le cryptage doit-il rester sûr? (*x* années)
- Combien de temps faut-il pour réorganiser l'infrastructure existante avec des solutions quantiques sécurisées à grande échelle? (*y* années)
- Combien de temps faut-il pour construire des calculateurs quantiques à grande échelle (ou toute autre avancée majeure)? (*z* années)

Théorème 1: si $x + y > z$, alors, il y a du souci à se faire.

Que faire dans ce cas??



GAP quantique

Cryptographie quantique sûre

- Cryptographie post-quantique (PQC)
  = *algorithmes classiques basés sur la complexité et résistants à des attaques quantiques connues*

+ peu de changements pour les experts en sécurité

- là encore, pari osé sur l'inconnu

- vulnérabilité en amont

- Distribution quantique des clés cryptographiques (DQC)
  = *distribution basée sur la physique, résistance prouvée aux attaques quantiques*

+ sécurité prouvable

+ sécurité en amont

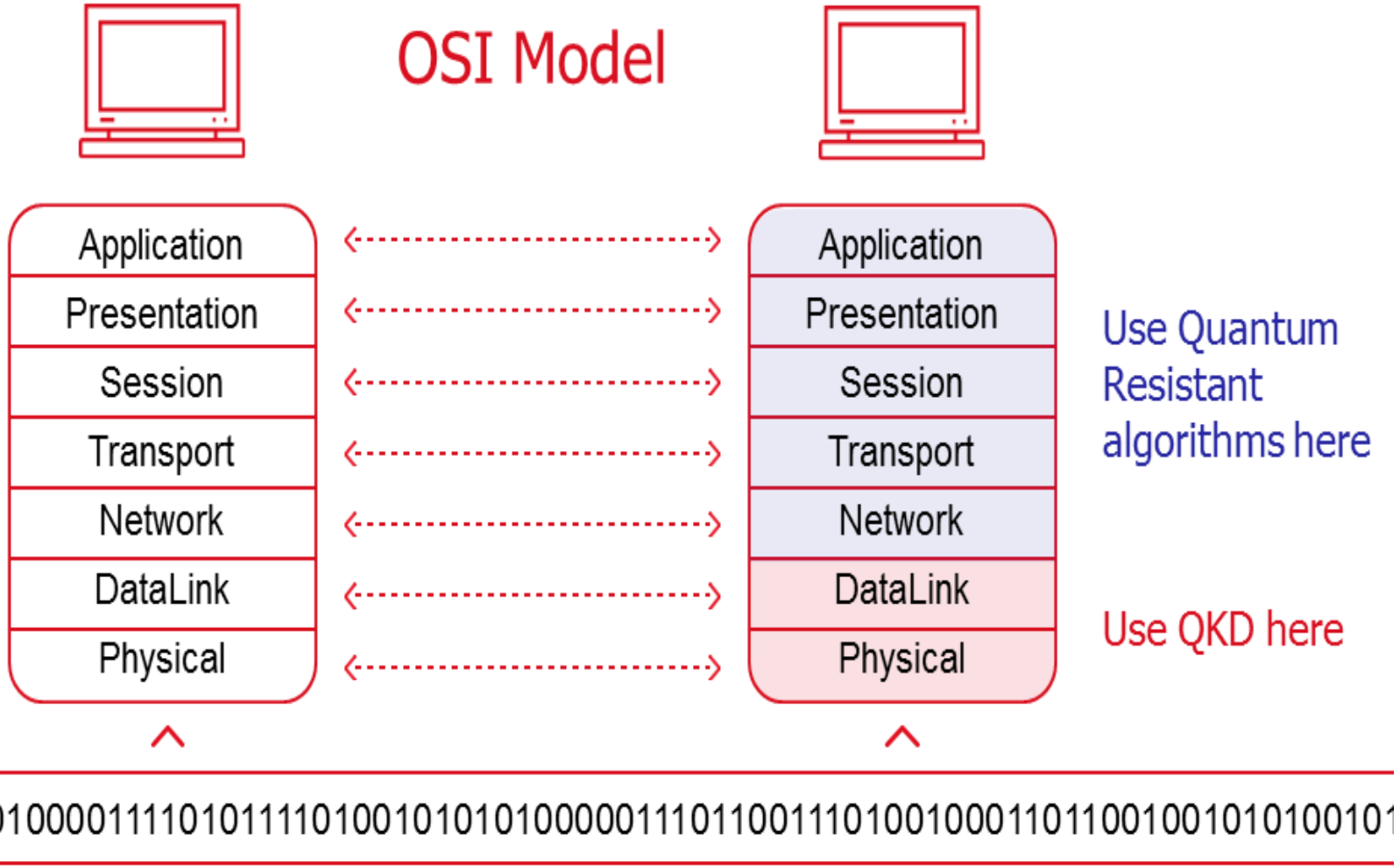
- technologie onéreuse

- chamboulement des infrastructures et des mentalités

- Comme il est probable que chacune des technologies va trouver des applications, la vraie question est la taille de chaque marché.
- Chacune des technologies se fonde sur des bits véritablement aléatoires.

GAP quantique

Exemple de cryptographie quantique sûre



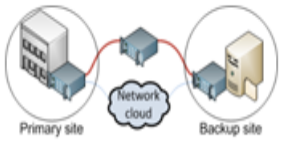
GAP quantique

OSI = Open System Interconnection
QKD = Quantum Key Distribution (DQC, Distribution quantique des clés cryptographiques)

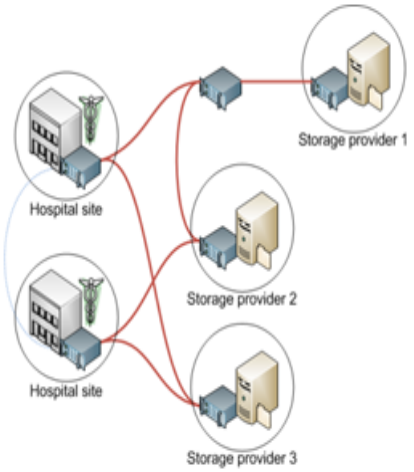
Exemples de cas pratiques

GAP quantique

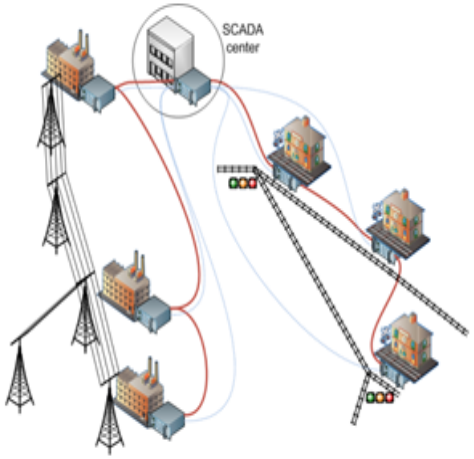
Off-site backup



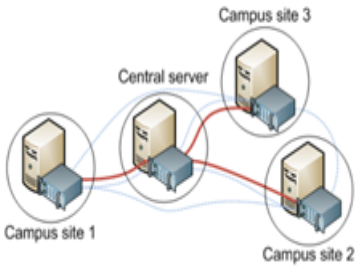
High security cloud storage



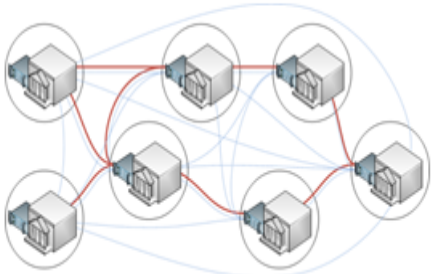
Critical infrastructure protection



Key and signature server



High security private networks

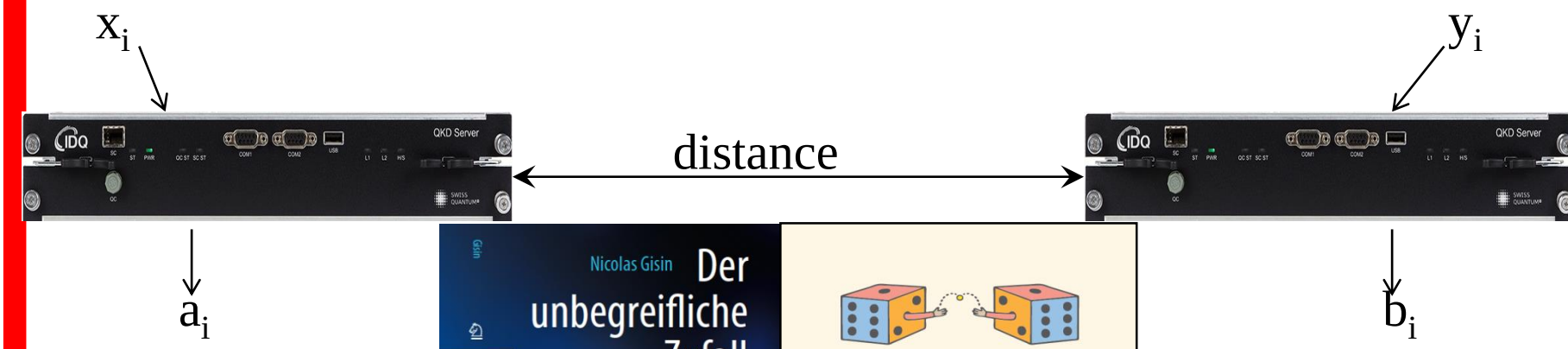


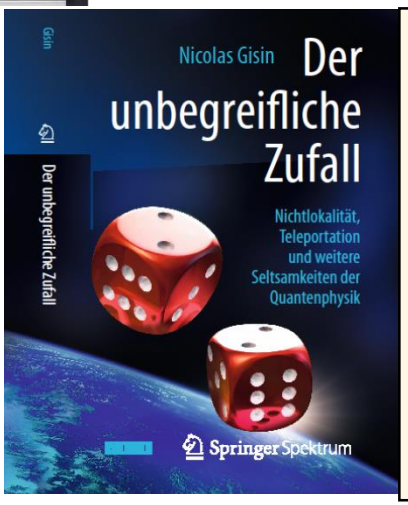
Backbone link protection

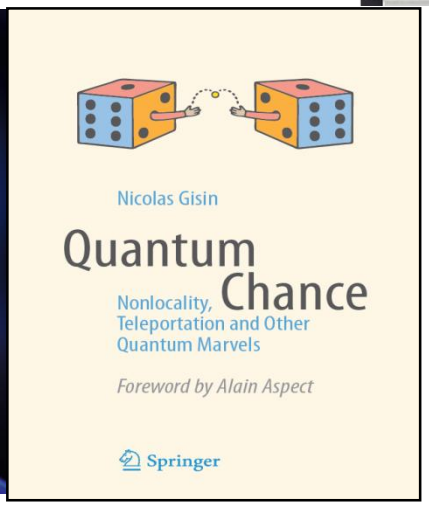
SCADA = Supervisory Control And Data Acquisition (système de contrôle et d'acquisition de données)
ISP = Internet Service Provider (FAI, Fournisseur d'accès à internet)

Le hasard, par nature, est présent partout

- Admettre que les distances sont une réalité.
- Admettre que Alice & Bob peuvent garantir qu'aucune information ne fuitera vers le monde extérieur.
- Admettre que a⊕b=x·y est hautement probable.
  (Noter que cela peut être vérifié.)

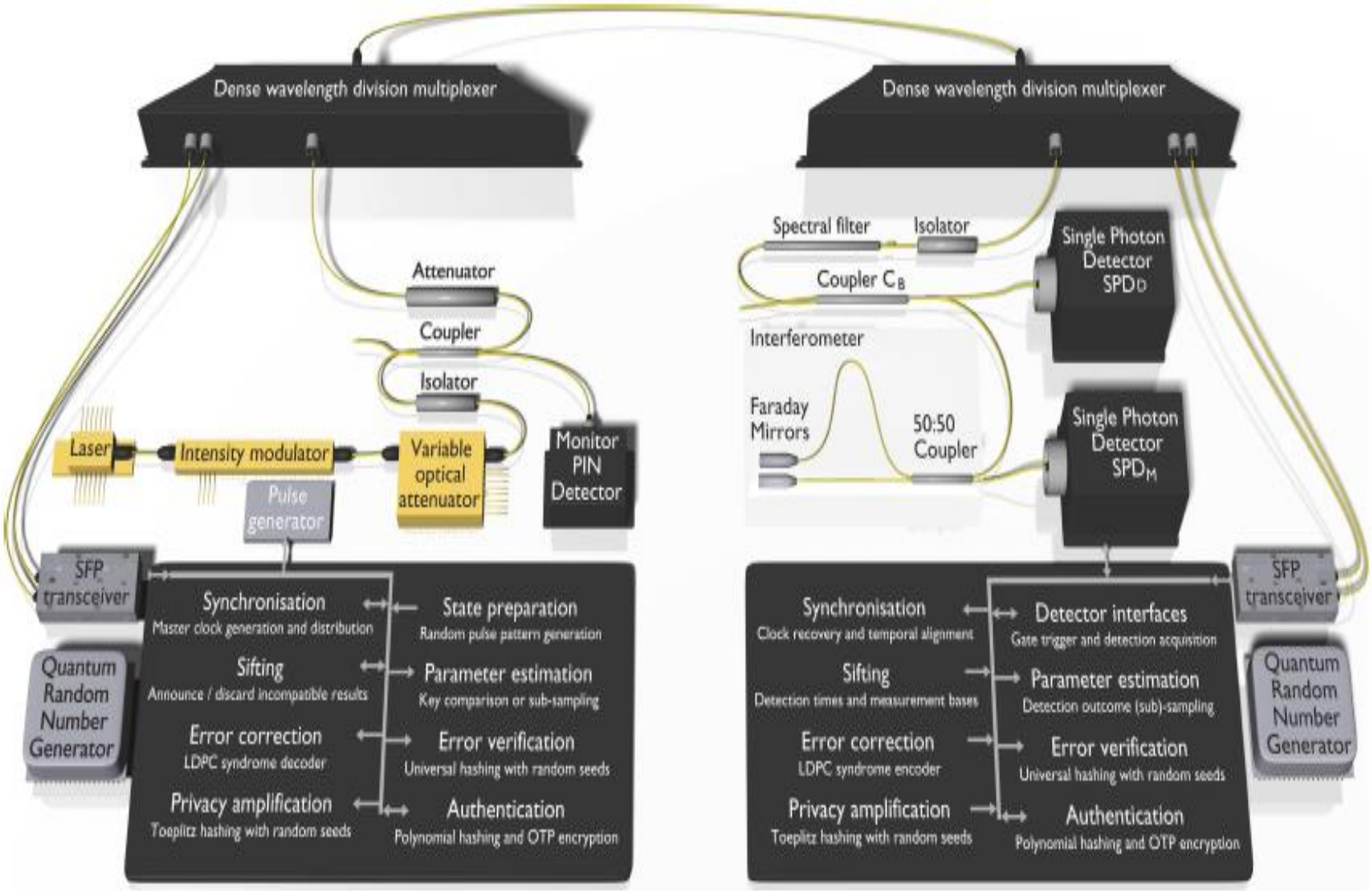






GAP quantique

Machine DQC @ 625 MHz



GAP quantique

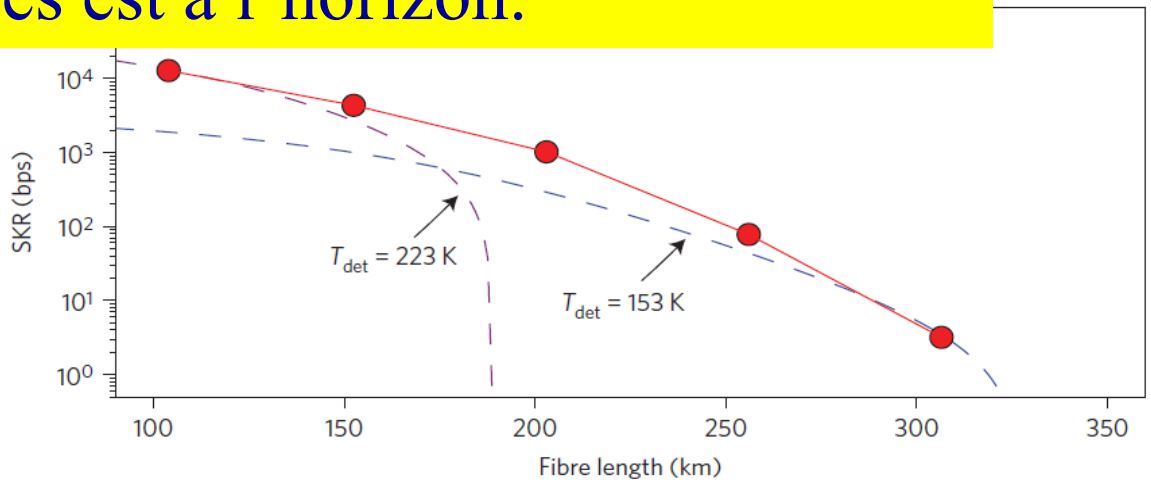
Machine DQC intégrée

- Conçue sur le modèle de l'information industrielle et des télécommunications (*Advanced Telecommunication Computing Architecture ATCA*).
- Fournit une puissance mécanique normalisée et des interfaces de services.
- Fournit des services réseau, un système de refroidissement, des alimentations électriques.
- Architecture évolutive, connue des clients potentiels.

GAP quantique

DQC sur 307 km avec distillation de clés secrètes en temps réel et analyse des clés finies

- Intégration dans des lames ATCA
- Une machine DQC produisant 1 Go/s de bits secrets prouvés est à l'horizon.



B. Korzh, C. W. Lim et al., Nature Photonics 9, 163-168 (2015)

GAP quantique

Exemple d'un lien commercial en opération depuis 2011

Lausanne

Nyon

67 km

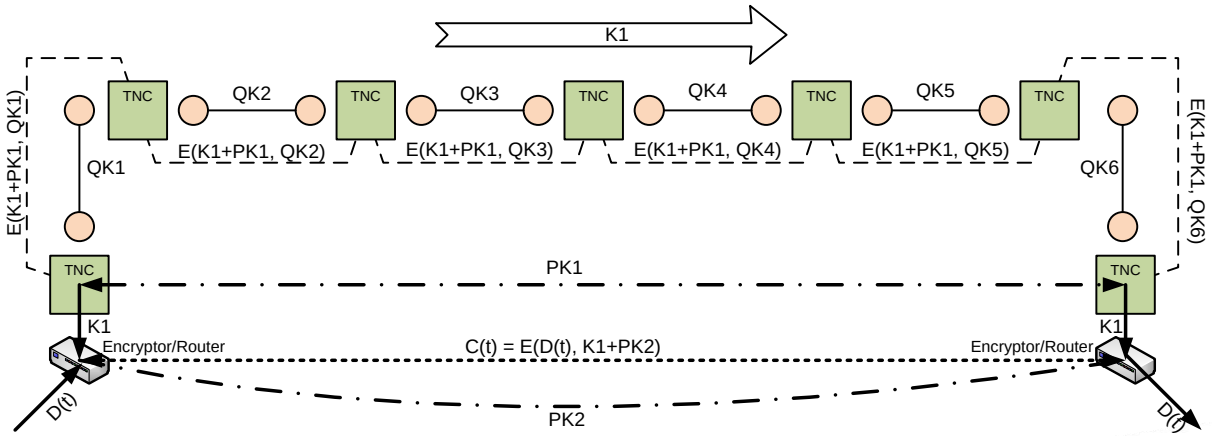
Genève

IDQ
FROM VISION TO TECHNOLOGY

Chaîne quantique multiplexe installée pour un usage commercial

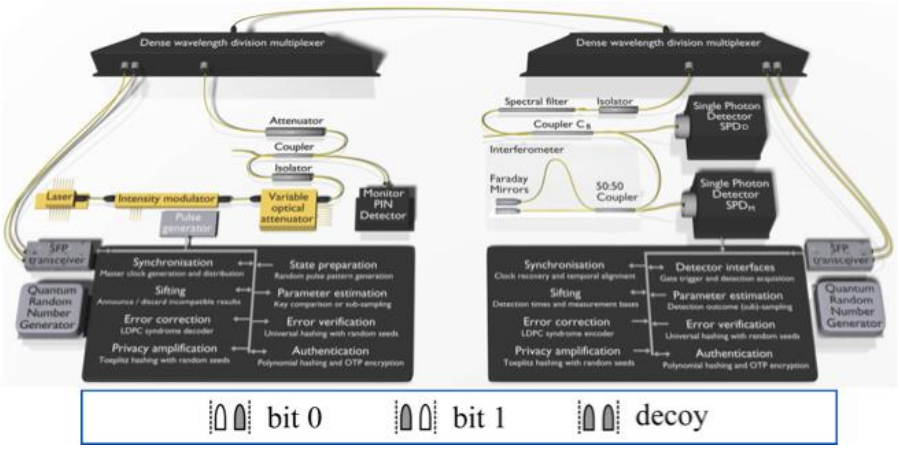
GAP quantique

Nœud de confiance DQC



Les clés se déplacent en toute sécurité dans le réseau selon le mode de la fonction affine par morceaux

Protocole à sens unique cohérent (COW)



Architecture compatible avec les télécommunications (ATCA)

Plus de 8 lames quantiques par châssis

Certification FIPS 140-2 (projetée)

Evaluation CC (projetée)

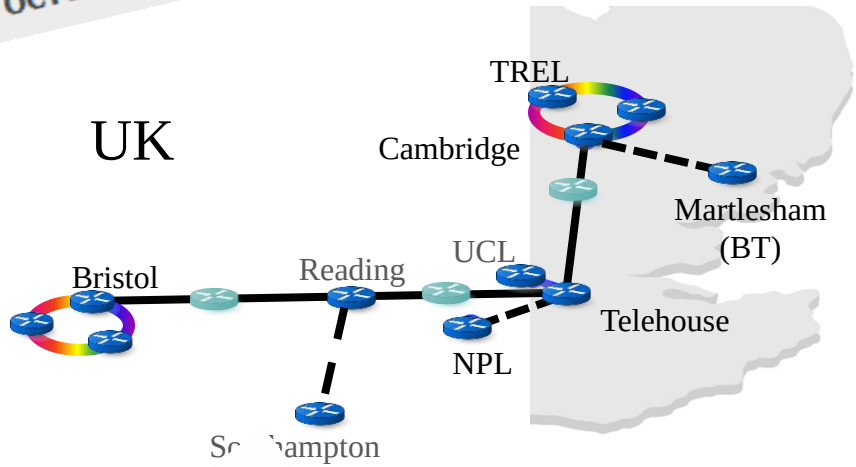
GAP quantique

21

3rd ETSI/IQC Workshop on Quantum-Safe Cryptography

ADD THIS TO MY CALENDAR

5-7 OCTOBER 2015



Battelle
The Business of Innovation

Que permet d'atteindre la distribution quantique des clés cryptographiques (DQC)?

1. Les attaques doivent être lancées sur le champ
   ⇒ immunisation contre les progrès futurs
2. Seulement dans l'hypothèse d'une propre implantation
   ⇒ développement des clés
3. Si une fonction à sens unique de sécurité à court terme
   ⇒ distribution de clés cryptographiques sécurisées à long terme

I. Si la DQC a un masque jetable (limité au débit binaire de la DQC)
   ⇒ permet pour information une sécurité théoriquement à long terme

II. La DQC permet de changer très souvent la valeur initiale de la clé AES
   ⇒ nombre limité de données disponibles pour une analyse cryptographique et motivation limitée pour un adversaire.

GAP quantique

AES = Advanced Encryption Standard (standard de chiffrement avancé)

Que doit-on faire?

- Aujourd'hui, la collaboration entre les physiciens et les cryptographes est inexistante.

➔ Créer une communauté de physiciens et de cryptographes qui travaillent ensemble sur une cryptographie quantique sécurisée.

➔ Trouver des applications appropriées pour les algorithmes quantiques, par ex. téléphones mobiles, applications grand public, la majorité du commerce en ligne, etc.

➔ Trouver des applications appropriées pour la cryptographie quantique (GQNA & DQC), par ex. une **dorsale quantique suisse** pour les infrastructures critiques et les sauvegardes de grands ensembles de données.

Que doit-on faire?

- Aujourd'hui, la collaboration entre les physiciens et les cryptographes est inexistante.

➔ Créer une communauté de physiciens et de cryptographes qui travaillent ensemble sur une cryptographie quantique sécurisée.

➔ Trouver des ap
quantiques, pa
public, la majo

➔ Trouver des ap
quantique (GQ
suisse pour les
de grands ense

GAP quantique