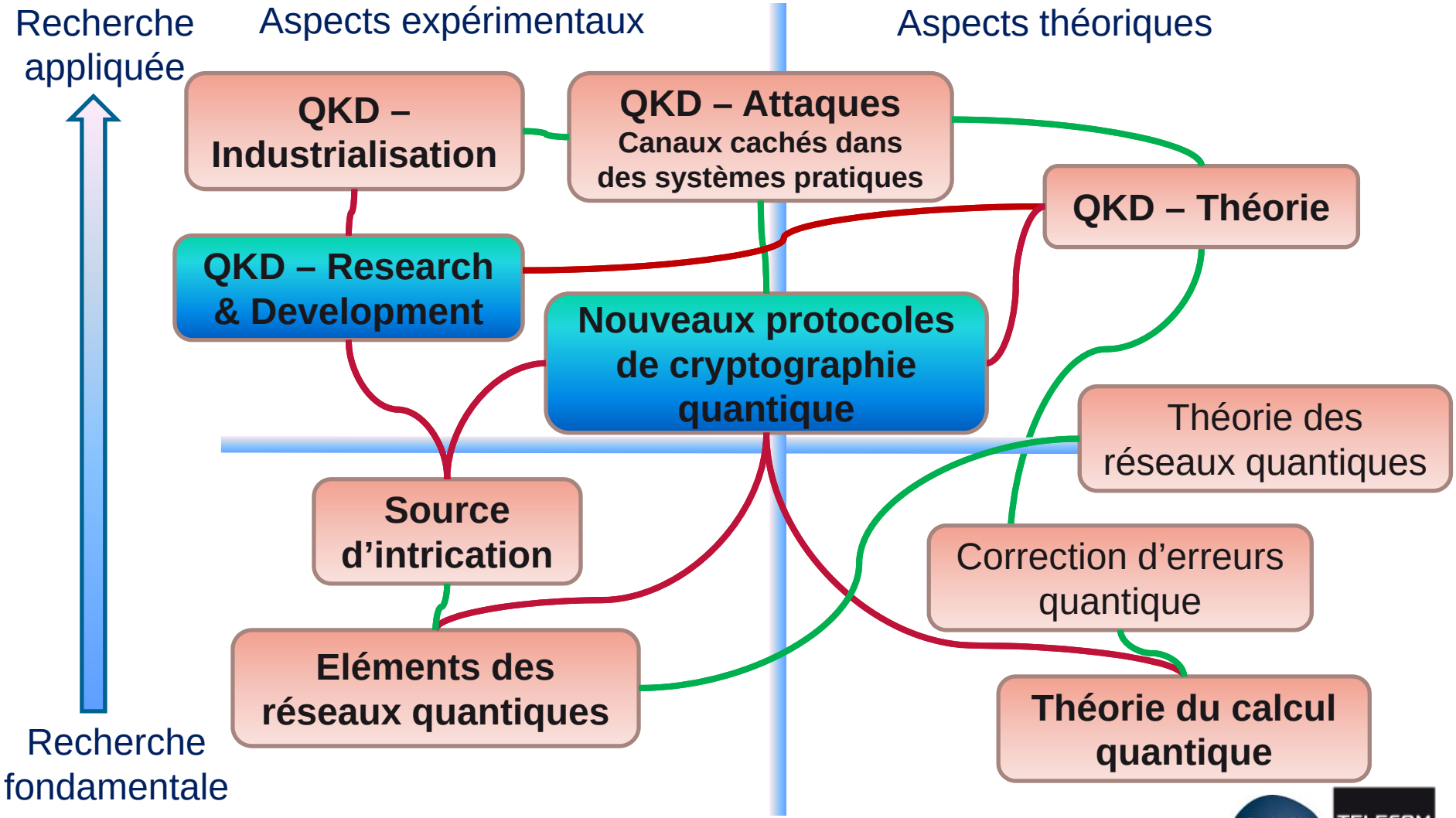
Primitives de cryptographie quantique en environnement réaliste

Eleni Diamanti
LTCI – CNRS, Télécom ParisTech
Equipe Information Quantique (INFRES)

9 Juin 2010

Vue d'ensemble de notre recherche



Communications sécurisées

Alice et Bob veulent effectuer une opération jointe à travers un canal

- Alice fait confiance à Bob mais pas au canal → client – banque sur Internet
  primitive: distribution d'une clé secrète
- Alice ne fait confiance ni à Bob ni au canal → client – site Internet inconnu
  identification, récupération d'information privée, vote ou signature électronique,…
  primitives: tirage à pile ou face, « bit commitment », « oblivious transfer »

→ Protocoles sophistiqués basés sur des primitives cryptographiques

…dans le monde classique

Les systèmes cryptographiques actuels garantissent une sécurité algorithmique

→ incapacité *non-prouvée* d'un espion ou d'une partie tricheuse d'effectuer certaines opérations mathématiques

- Est-ce qu'on peut utiliser la mécanique quantique pour obtenir une sécurité inconditionnelle → garantie pour *toute capacité de calcul* de l'espion ou d'une partie tricheuse?
- Même si cela n'est pas possible, est-ce qu'on peut obtenir des performances supérieures à celles obtenues dans le monde classique avec un niveau de sécurité élevé?
- Est-ce qu'on peut développer des systèmes de cryptographie quantique pratiques, compatibles avec les communications classiques, fonctionnant dans un environnement avec des pertes, du bruit, des composants imparfaits?

Distribution de clé secrète

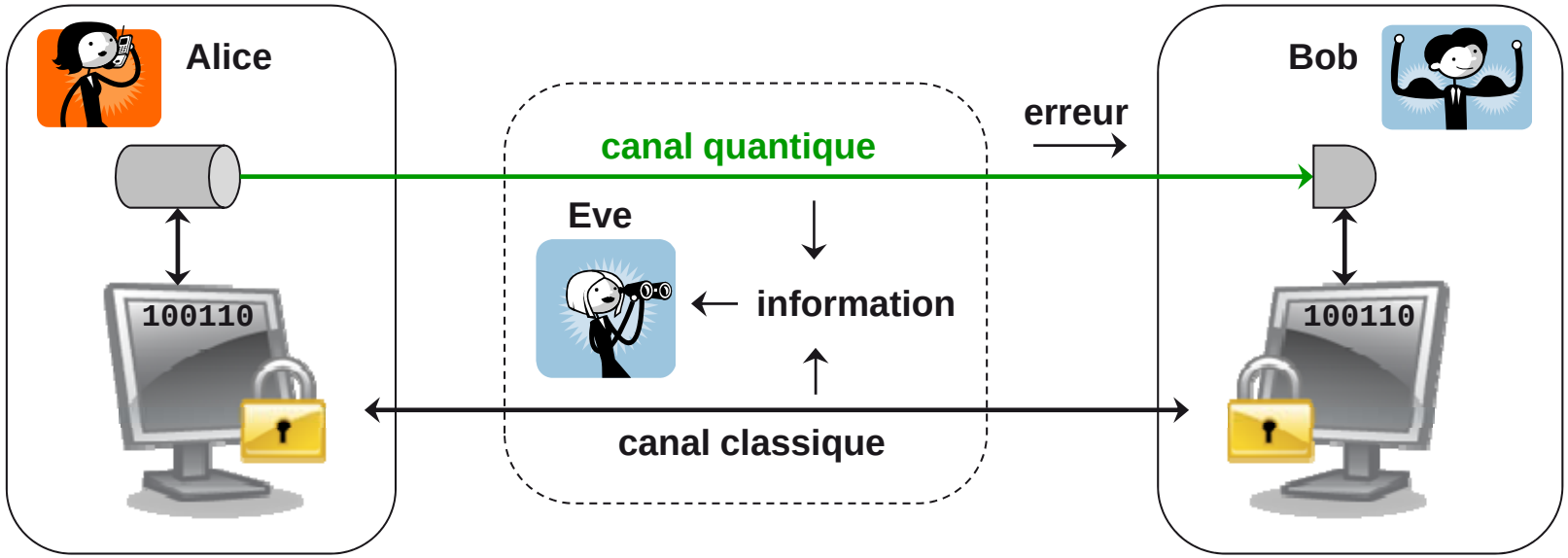
Alice veut envoyer à Bob un message secret à travers un canal observé par Ève

→ le protocole « one-time pad » garantit une sécurité inconditionnelle si la clé est aussi longue que le message et utilisée une seule fois

→ implémentation pratique difficile, cryptographie à clé publique

Distribution quantique de clé

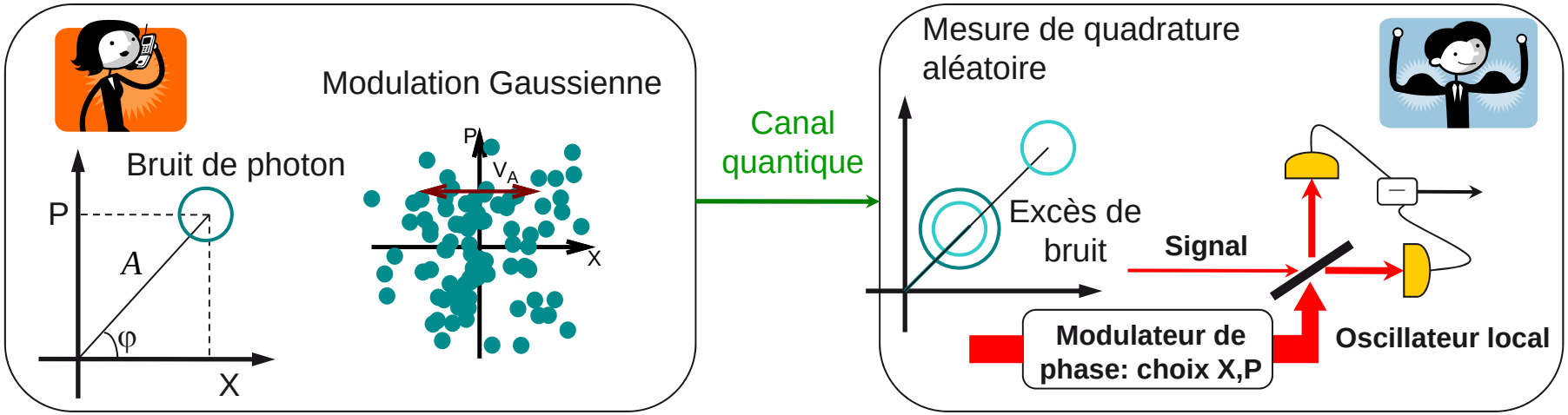
Alice envoie des éléments quantiques à Bob



Les mesures d'Eve introduisent des perturbations observables
→ génération de clé secrète

Distribution quantique de clé à variables continues

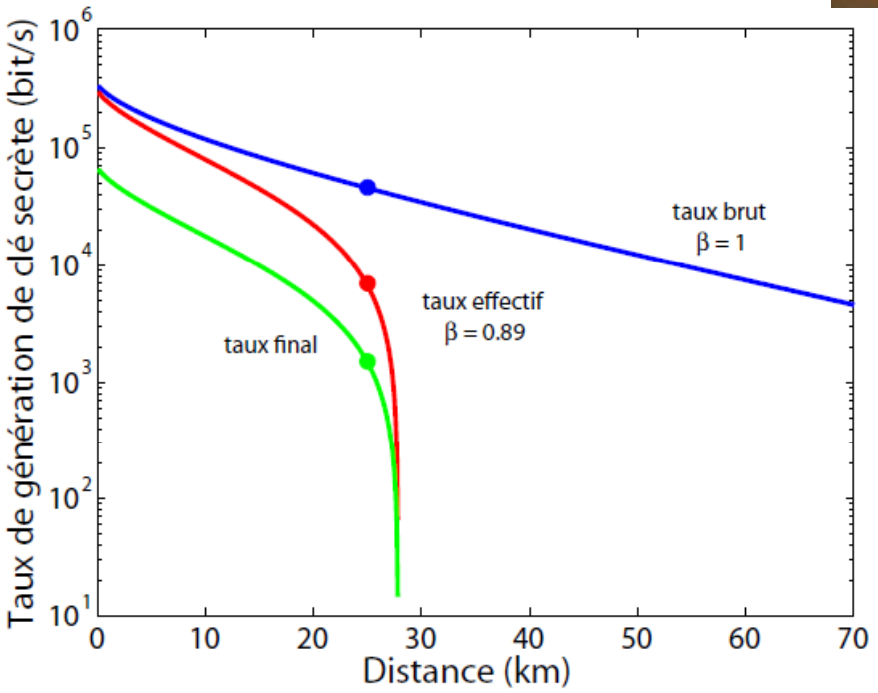
- Alice code l'information de la clé dans des variables continues quantiques → modulation aléatoire de l'amplitude et de la phase d'états cohérents
- Bob effectue des mesures aléatoires de la quadrature de chaque état en utilisant un système de détection homodyne



- Les pertes et le bruit diminuent le rapport signal-à-bruit → la présence d'Eve est révélée par des mesures de variances de bruit

Taux de génération de clé vs. distance

Fonctionnement stable et automatique
Prototype robuste et compact
Composants télécom standards
Génération de clés en temps réel



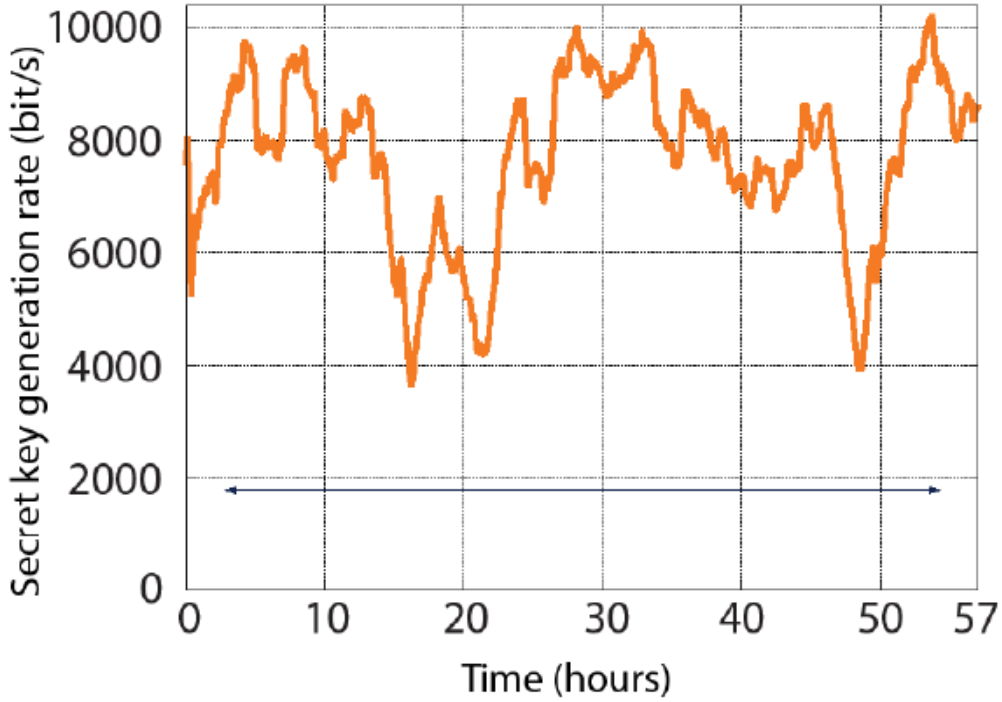
Performance limitée par la vitesse et l'efficacité du processus de réconciliation
→ discrétisation + correction d'erreurs

J. Lodewyck et al, PRA 2007

S. Fossier, ED, T. Debuisschert, R. Tualle-Brouri, P. Grangier, J. Phys. B 2009

Performance du prototype dans le réseau

Intégration des technologies QKD diverses dans le premier réseau quantique sécurisé Européen sur le réseau en fibre optique de Siemens à Vienne en octobre 2008



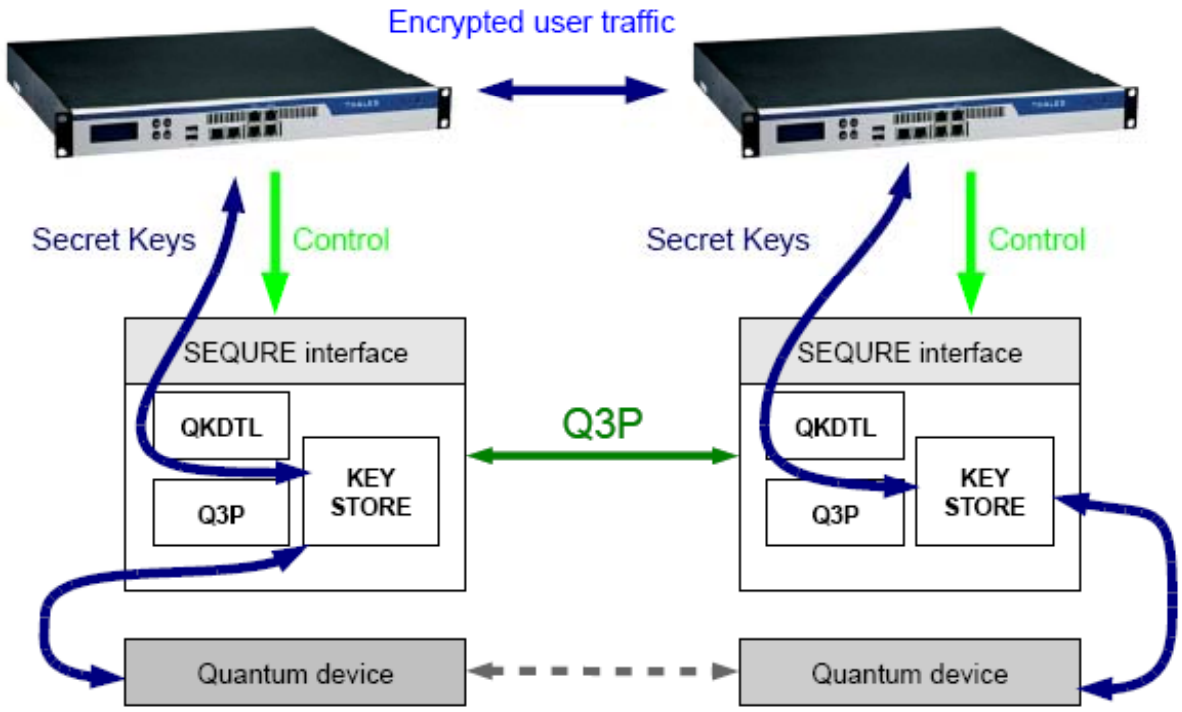
8 kbit/s @ 10 km (3 dB)
pendant ~3 jours

S. Fossier, ED, T. Debuisschert, R. Tualle-Brouri, A. Villing, P. Grangier
New J. Phys. 2009

M. Peev et al, New J. Phys. 2009

Démonstration projet ANR SEQURE

Système de chiffrement symétrique avec renouvellement des clés quantique

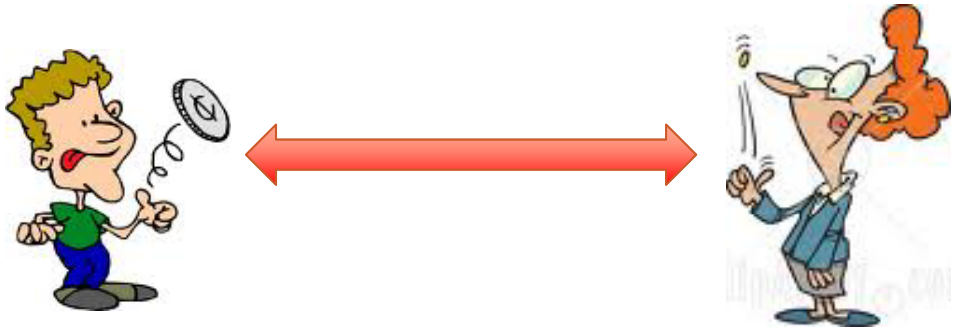


- Compatibilité avec des chiffreurs commerciaux de Thales
- Cible de sécurité réaliste
- Distance métropolitaine typique → 20 km (5,5 dB)
- Démonstration en Ile-de France été 2010

collaboration avec Insitut d'Optique, Thales

Tirage à pile ou face

- Protocoles avec une Alice et un Bob qui ne font pas confiance l'un à l'autre → jusqu'à présent presque ignorés dans le cadre quantique
- Sécurité inconditionnelle impossible…



Alice et Bob doivent tirer une pièce à pile ou face

→ une partie tricheuse ne devrait pas pouvoir biaiser la pièce

$$\text{prob}(\text{Alice ou Bob triche}) \leq \frac{1}{2} + \varepsilon$$

→ sécurité algorithmique: $\varepsilon \approx 0$

→ sécurité inconditionnelle: $\varepsilon = \frac{1}{2}$

Tirage à pile ou face quantique

- Le tirage à pile ou face quantique parfait est impossible: $\varepsilon > 0$

  mais des protocoles meilleurs que les classiques existent: $\varepsilon = \frac{1}{\sqrt{2}} - \frac{1}{2} \approx 0,21$

- Ces protocoles ne fonctionnent pas en présence d'erreurs et de pertes, nécessitent des mémoires quantiques, des sources de photons uniques…

- Développer des protocoles robustes et pratiques et les implémenter avec des « boîtes » optiques
- Structure multipartite afin d'augmenter la distance de communication et de s'approcher à des situations réalistes avec plusieurs parties communicants

  → modèles de sécurité et implémentation des protocoles de « vote électronique » et d'« election de leader »

collaboration avec LRI, Edinburgh

Perspectives

• QKD à variables continues

→ amélioration des performances (taux, distance, stabilité) avec des nouveaux protocoles, meilleurs composants (détection homodyne), procédure de réconciliation plus efficace

→ sécurité face aux canaux cachés

→ étude des réseaux QKD

R. Alléaume, A. Leverrier, thèse CIFRE P. Jouguet
ANR SEQURE, FREQUENCY QCERT
SESAME Sécurité Quantique
Institut d'Optique, Thales, ENS Cachan, U. Génève, SeQureNet, idQuantique, U. Calgary, U. Waterloo, U. Montréal, Keio U.

• Primitives cryptographiques quantiques (tirage à pile ou face,…)

→ développement des protocoles robustes face aux pertes, bruits, composants imparfaits

→ implémentation optique des primitives dans le cadre bipartite ou multi-partite

→ étude du rôle d'intrication dans l'implémentation sur des réseaux quantiques

D. Markham, I. Zaquine, post-doc S. Felloni, thèse à venir
ANR CRYQ, FREQUENCY INSTITUT TELECOM QPRIM
LRI, Edinburgh, JST-CNRS (Japan)