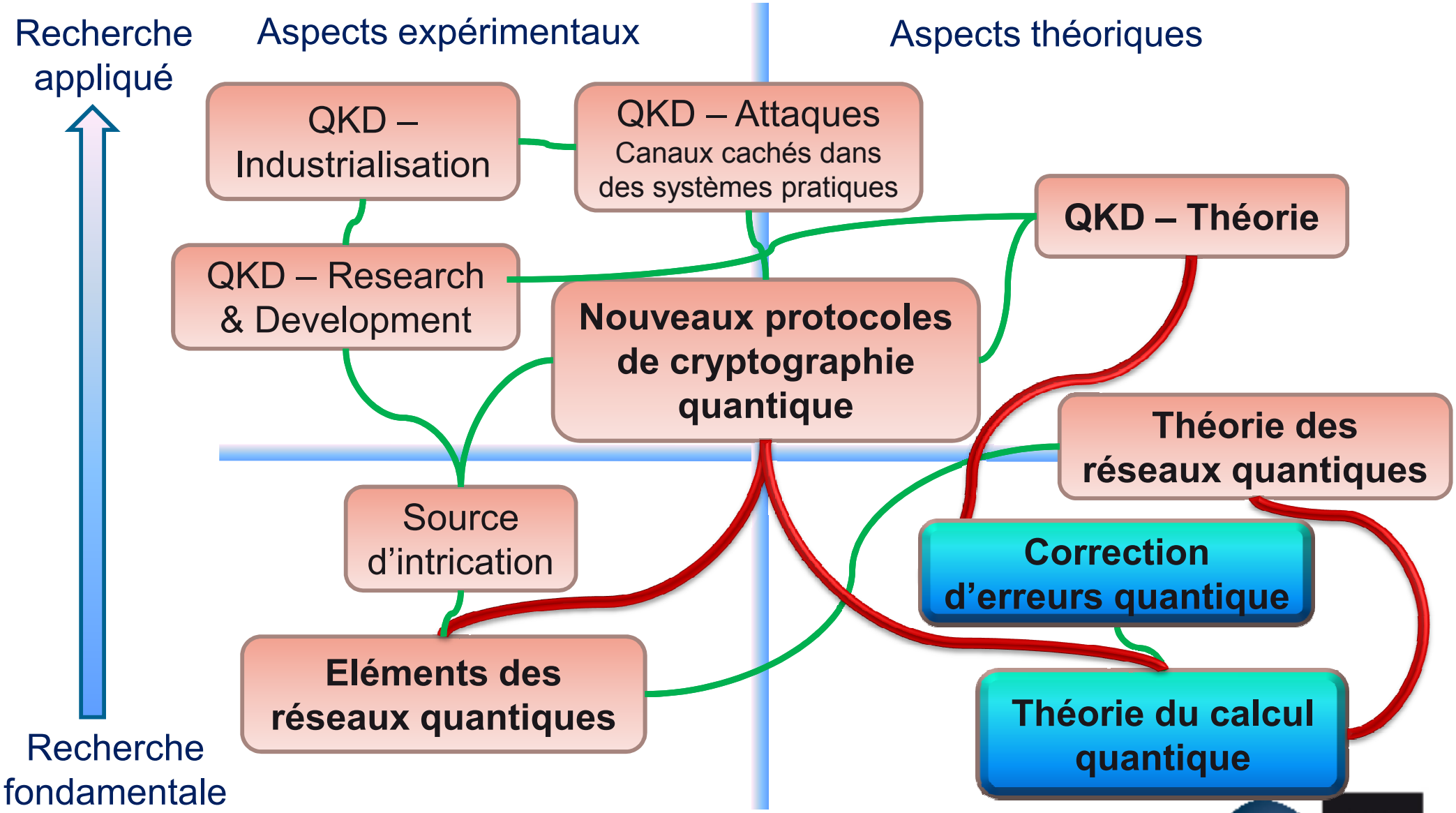
Calcul Quantique multi-party sécurisé

Damian Markham
LTCI – CNRS, Télécom ParisTech
Equipe Information Quantique (INFRES)

9 Juin 2010

Vue d'ensemble de notre recherche



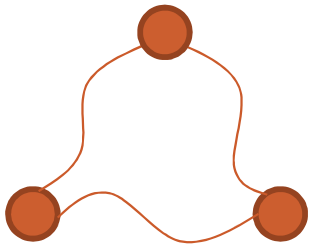
Quantum Computation and Information Processing

Qubit

Vector in 2D Hilbert space

Entanglement

- Spreads information
- Non-local effects



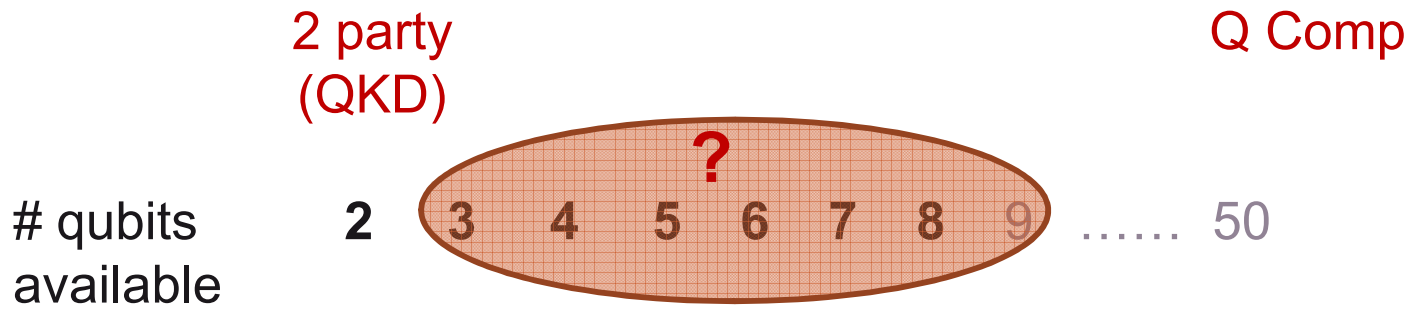
Multipartite Entanglement

- Different *types* ⟹ different *spreading*

- Absolute 2-party security (QKD)
- Exponential speed up (Shor Algorithm)

Challenges for Quantum Computation and Information Processing

- **New applications and protocols**



- **Integration of tasks**

Computation + Communication + Error correction

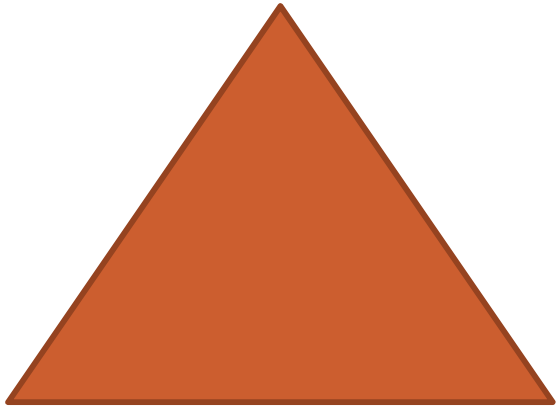
- **Understanding of fundamental role and use of entanglement**

Boundary between classical and quantum?
How far can be pushed?

Approach

Physics of quantum network setting

Multipartite entanglement
Manipulation of information



Computer Science Tools

Formal methods of quantum computing,
Semantics of quantum info. processing

Systems

Implementations in optics and solid state.

Collaborations

LRI, UP7, Grenoble, Bordeaux, INRIA (ANR COCQ)

Oxford, Imperial, Leeds, Edinburgh

Erlangen

Tokyo, ERATO, NII (JST CNRS QComp. The. & Feas., JFLI JFLI)

Calgary (ANR NSERC CRSNG FREQENCY)

Graph states for Secret Sharing

- **Sharing a secret:**

  Dealer distributes a secret to Players such that

  - only authorised sets of players can access it

  - unauthorised players cannot

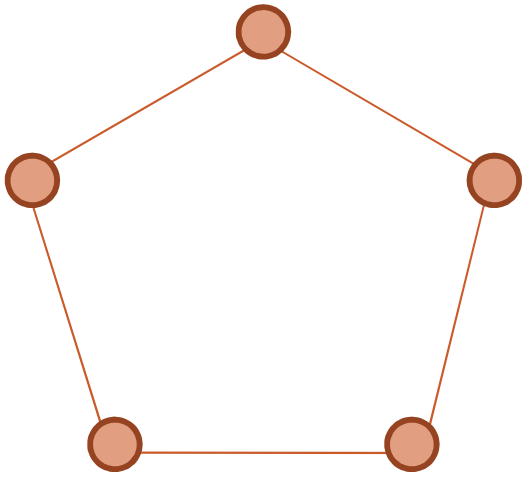
- **Important primitive, many uses and implications (secure multiparty computation, error correction…)**

- **Solved classically by Shamir ’79**

  - Assumes secure channels!

  - Quantum secret?

Graph states for Secret Sharing



Class of multipartite entangled states

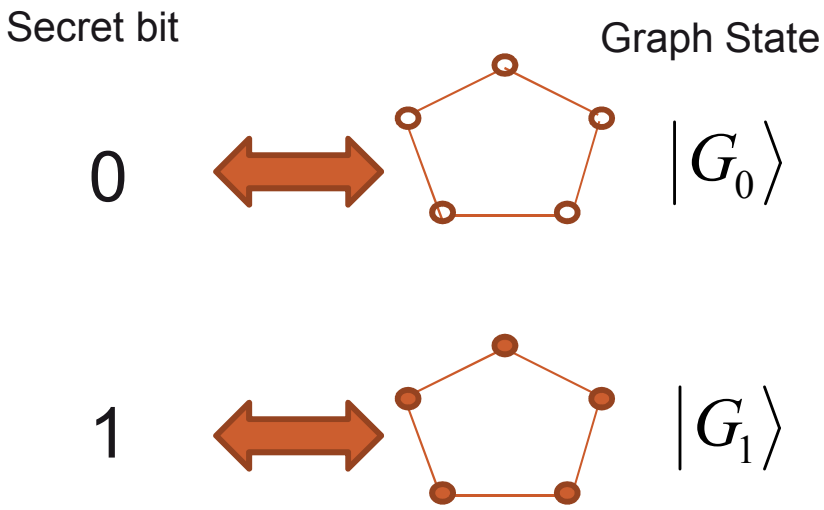
Graph ⟺ quantum state

- Vertex = qubit
- Edge = entanglement

- **Used for quantum computation, error correction**
- **Many implementations (e.g. linear optics, spin systems)**
- **Entanglement and information distribution**

Graph states for Secret Sharing

- **Encode**



Secret qubit

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \alpha|G_0\rangle + \beta|G_1\rangle$$

- **Access of information – local manipulation of information and discrimination**

DM, A. Miyake, S. Virmani, JMP'07 DM, A. Roy and Barry Sanders, PRA'08 A. Keet, B. Fortescue, DM, B. Sanders, PRA 2010.

Graph states for Secret Sharing

- **Graphical Formalism**

(in collaboration with Grenoble, Bordeaux)

Develop formal language based on measurement calculus

Complete graphical representation of quantum secret sharing

Flow conditions* – which class of graphs can do perfect computation

Extension – secret = input, compute identity, restrict who can read output

Players with access:
$X \cup V \,/\, odd\,(X)$

Players no access:
$T(X \cup V \,/\, odd\,(X))$

E.G. some access structures need higher dimension

- **Implementation by linear optics (feasible with current technology)**

(in collaboration with Erlangen, Tokyo, Calgary)

Graph states for Secret Sharing

The next steps...

- Extension to higher dimension
  - Graphical characterisation
  - Efficiency
  - Security proofs
- Integration
- Implementation by linear optics (feasible with current technology)

Perspectives

- **Development and Implementation of graph state networks**
  - Integration and extension to quantum networks (computation, communication and fault tolerance)
  - Implementation in optics

  (PhD Marin, Diamanti, Zaquine)
- **Fundamentals of quantum network setting**
  - Solidify relationship between network tasks and entanglement types
  - Develop general framework for network tasks *common formal language*

  (Alléaume, Diamanti)
- **Exploration of entanglement in physical systems**
  - Entanglement in optics, spin and condensed matter for QIP
  - Exotic entanglement in nature and QIP

  (PhD Wang, Diamanti)