COLLÈGE DE FRANCE
1530

Algorithmes quantiques

Conclusion et ouverture

09-06-2021

Frédéric Magniez

Professeur invité sur la chaire Informatique et sciences numériques
En partenariat avec Inria
Année académique 2020-2021

frederic.magniez@college-de-france.fr

Partie 3 - Algorithmique avancée

- Apprentissage automatique
- Limites du calcul quantique
- Usage décentralisé de type Internet

26 mai 2021

Cours : Simulation hamiltonienne, résolution ultra-rapide de systèmes linéaires, et applications

Séminaire : Quantum Machine Learning, Iordanis KERENIDIS, *CNRS, Paris*

02 juin 2021

Cours : Limites du calcul quantique : liens entre complexité classique et quantique

Séminaire : Suprématie quantique : où en sommes-nous aujourd'hui ?
André CHAILLOUX, *Inria, Paris*

09 juin 2021

Cours : Conclusion et ouverture vers le calcul distribué quantique

Séminaire : Quantum Computing as a Service:
Secure and Verifiable Multi-Tenant Quantum Data Centre
Elham KASHEFI, *CNRS, Paris et University of Edinburgh*

Conclusion du cours

Algorithmes quantiques

Liste des thèmes abordés

Technologie existante

Superposition, non clonage
Distribution quantique de clés secrètes
Développement en pratique

Enchevêtrement, inégalité de Bell, téléportation
Cryptographie avancée
Certification de nombres aléatoires

Large Scale Quantum Computers

Circuits, premiers algorithmes “inutiles” avec avantages exponentiels
Représentations pour programmer et raisonner

Outils pour les algorithmes quantiques
Algorithmes à gain exponentiel
Problème du sous-groupe caché

Amplification quantique
Algorithmes à gain polynomiaux
Cadre algorithmique pour les marches quantiques

Noisy Intermediate-Scale Quantum Computers

Algorithmes pour la simulation physique
Résolution de systèmes linéaires ultra-rapide
Algorithmes d’apprentissage quantique

Simulation classique d’algorithmes quantiques
Limitation des algorithmes quantiques
Suprématie quantique

Distributed-Scale Quantum Computers

ET APRÈS ?
Calcul distribué quantique
Calcul quantique en tant que service

Des thèmes qui n'auront pas été abordés

NISQ

Heuristiques algorithmiques

- Quantum annealing
- Quantum approximate optimization algorithm
- Quantum variational circuits

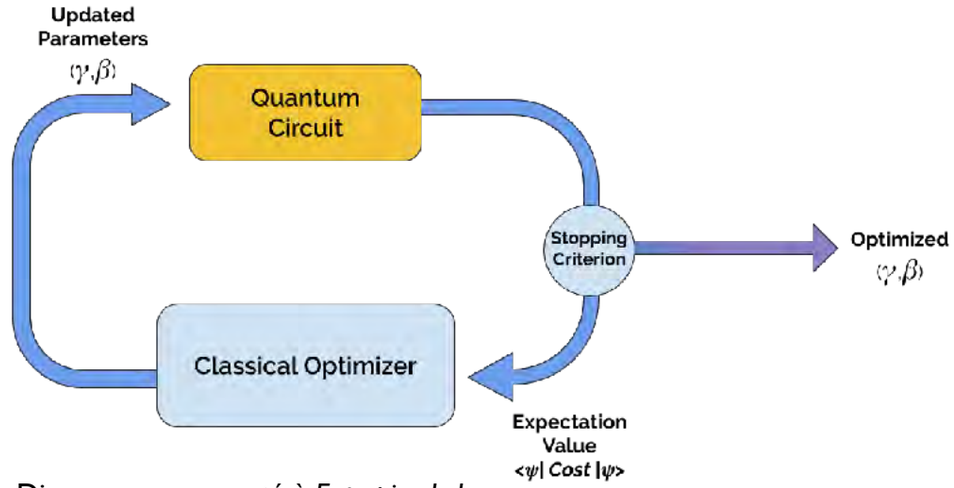
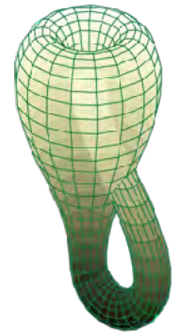


Diagramme emprunté à *Entropica Labs*

LSQ

Concepts connexes

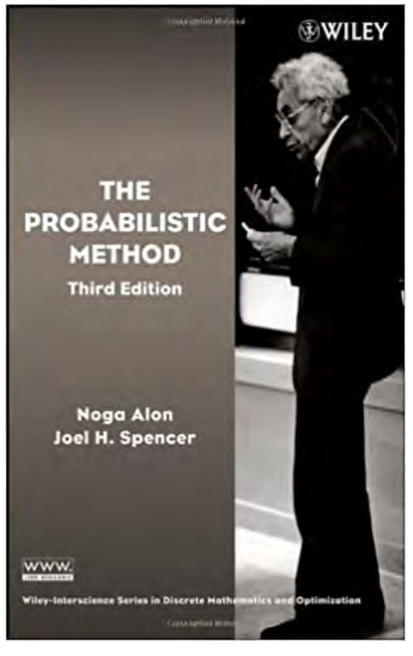
- Théorie de l'information quantique
- Preuve quantique, argent quantique
- Codes correcteurs quantiques
- Programmation, compilation, vérification



NQA

Méthode quantique

- Algorithmes, Complexité
- Codes correcteurs classiques
- Combinatoire, algèbre
- Physique



Quantum Algorithm Zoo

https://quantumalgorithmzoo.org

Stephen Jordan
Microsoft Quantum

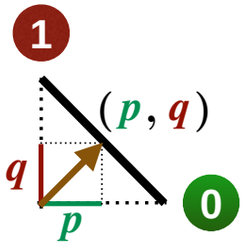
- 62 entrées
- 430 références
- 4 catégories
  - Algebraic & Number Theoretic
  - Oracular
  - Approximation and Simulation
  - Optimization, Numerics, & Machine Learning

Origine des accélérations

- Nombre exponentiel de configurations possibles : Non
  - Mais avec enchevêtrement et nombres négatifs : Oui
- Nombres complexes : Non
- Calcul "euclidien" (Géométrie / Matrices unitaires) : Oui

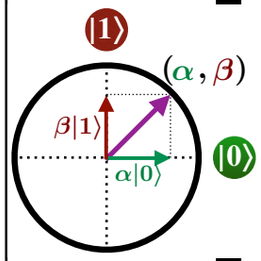
Les outils du calcul quantique

Calcul probabiliste

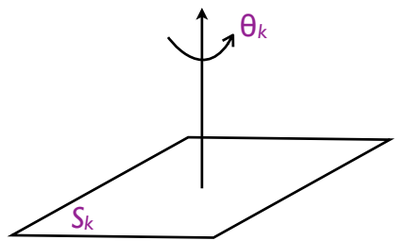


- Etat de n bits aléatoires
  - Vecteur de proba. de taille 2^n
  - Norme L_1 (Manhattan)
- Coordonnées non négatives
  - Interférences constructives
- Transformations linéaires
  - Matrice stochastique

Calcul quantique



- Etats de n bits quantiques
  - Vecteur d'amplitudes de taille 2^n
  - Norme L_2 (euclidienne)
- Coordonnées quelconques
  - Interférences cons/des-tructives
- Transformations linéaires
  - Matrice unitaire



Outils

- Mathématiques
  - Algèbre linéaire, tensorielle, spectrale
  - Géométrie euclidienne
  - Groupes, représentation
  - Analyse de Fourier, polynômes
  - Algèbre non-commutative, d'opérateurs
- Importés et adaptés du classique

Aujourd'hui
Calcul distribué

Données décentralisées

- Calcul dans le cloud
- Communication entre serveurs

Puissance répartie

- Petits calculateurs réunis entre eux sur un grand réseau de calcul

Réseau inconnu

- Tâche en commun : synchronisation, localisation…

Défis

- Concilier à grande échelle/distance les avantages du calcul quantique

  Confidentialité :Vis à vis de l'extérieur ou du réseau

  Accélération calculatoire

Internet quantique

- *The QIA project aims at building a Quantum Internet that enables quantum communication applications between any two points on Earth*

  https://quantum-internet.team

QUANTUM INTERNET ALLIANCE

Complexité de la communication

Modèle [Yao 1979]

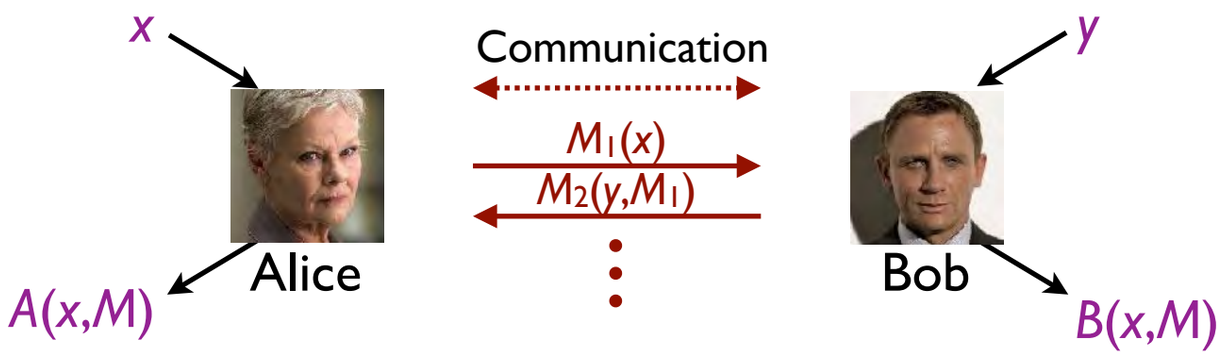
Contexte

- Données distribuées : (x,y)
- Protocole définit l'échange

  de messages : $M=M_1M_2,\ldots$
- Calcul collaboratif

  En général évaluation d'une même fonction F : $A(x,M) = B(y,M) = F(x,y)$
- Complexité : nombre maximum de bits échangés (lorsque x,y varient)

  Autre quantité intéressante : nombre maximum d'allers-retours



Applications

- Formidable outil pour prouver des bornes inférieures sur des modèles dont l'accès à l'entrée est contraint

  Complexité en requêtes, algorithmes de streaming, calcul distribué, conception de circuits imprimés, …
- Point d'entrée vers des notions plus complexes

  théorie de l'information, confidentialité, confidentialité, …

Complexités

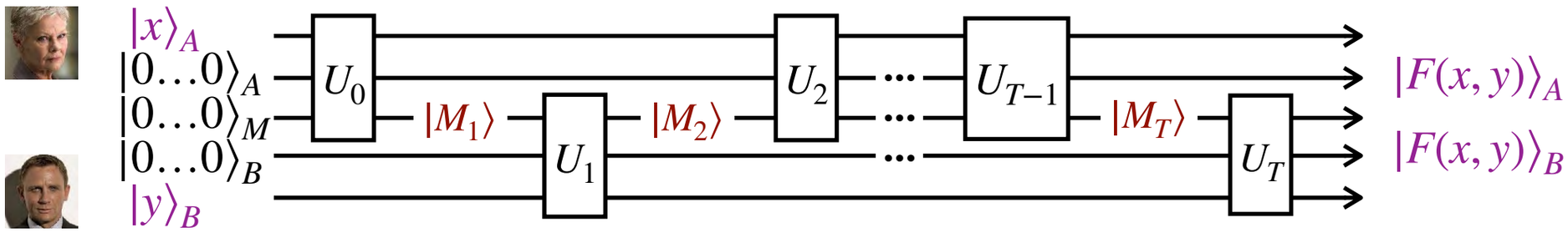
- D(F) : meilleur complexité pour calculer F par un protocole déterministe
- R(F) / Q(F) : idem pour un protocole probabiliste / quantique

  Remarque : variantes avec aléa/enchevêtrement initial

  Dans ce cours : aucun (sauf mention contraire)

Modèle quantique

- Entrées distribuées : $x, y \in \{0,1\}^N$
- Fonction $F : \{0,1\}^N \times \{0,1\}^N \to \{0,1\}$

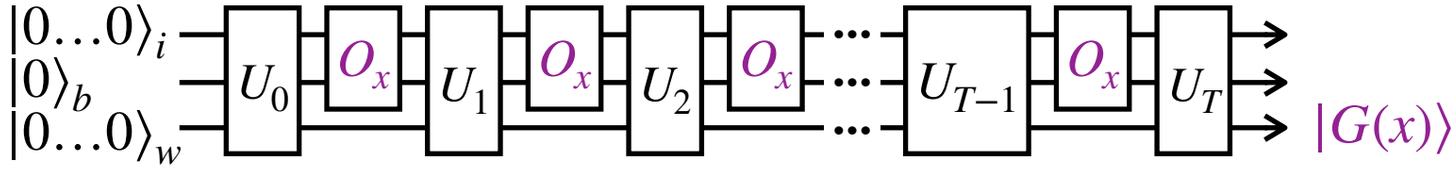


exemple avec T impair

Des protocoles inspirés d'algorithmes

Des algorithmes (à oracle) aux protocoles

- Entrée : $x \in \{0,1\}^N$ - Requêtes : $O_x : |i, b\rangle \mapsto |i, b \oplus x_i\rangle$
- Fonction $G : \{0,1\}^N \to \{0,1\}$



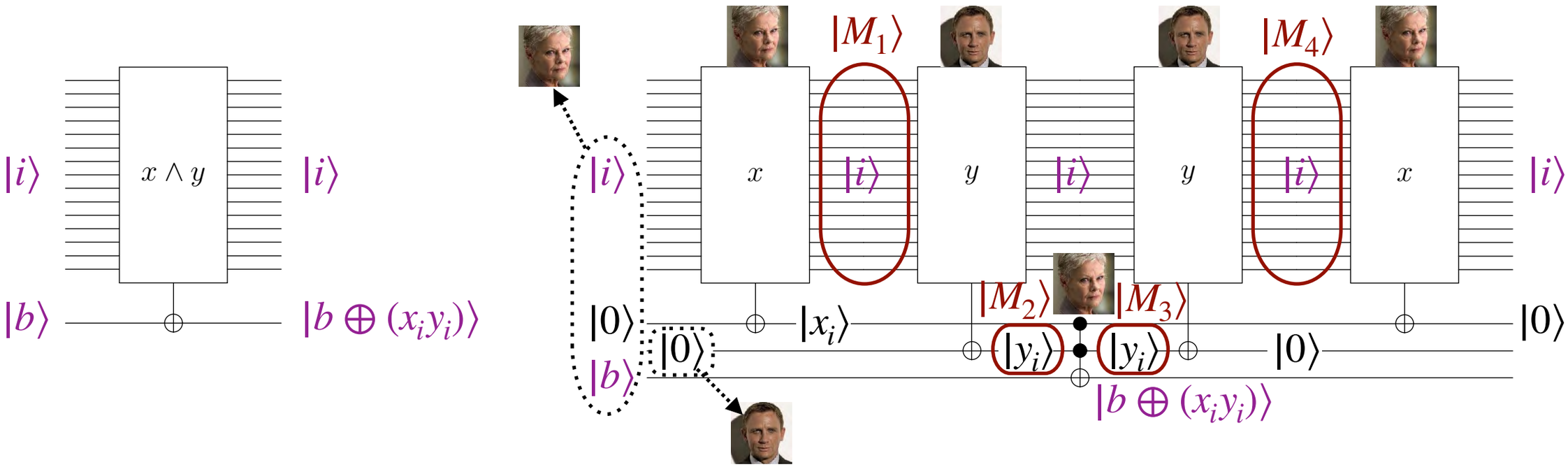
- Distribution des entrées (lifting)

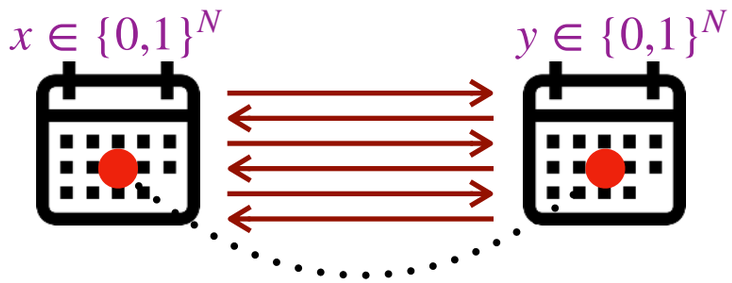
Exemple : $F(x, y) = G(x_0y_0, x_1y_1, \ldots, x_{N-1}y_{N-1})$

Théorème : Communication(F) ≤ (2 + 2log N)×Requêtes(G)

Preuve

- Alice simule l'algorithme seule, et l'appel à l'oracle avec l'aide de Bob





Set Disjointness

- Entrées distribués : $x, y \in \{0,1\}^N$
- Sortie DISJ(*x*,*y*) = 1 s'il existe *i* tel que $x_i = y_i = 1$, 0 sinon
- D(DISJ)=$\Theta(N)$=R(DISJ)

Motivations (The Story of Set Disjointness [Hemaspaandra 2010])

- Capture la difficulté du modèle. Utilisé dans de nombreuses preuves de difficultés (streaming, distribué, …)
- Techniques développées et extensions importantes

Protocole

- DISJ(*x*,*y*) = OR(x_0y_0,x_1y_1,…,$x_{N-1}y_{N-1}$)
- Donc Q(DISJ)=$O(\log N \times \sqrt{N})$ [Buhrman, Cleve, Wigderson 1998]

Améliorations

- Q(DISJ)= $\Theta(\sqrt{N})$ [Razborov 2003][Aaronson, Ambainis 2003]
- Q(DISJ)= $\tilde{\Theta}(T + N/T)$ *T* : nb d'allers-retours

  [Braverman, Garg, Ko, Mao, Touchette 2015]

Deutsch-Jozsa distribué

- Entrées distribués : $x, y \in \{0,1\}^N$
- Sortie DJ(*x*,*y*) = 1 si $x = y$, 0 sinon

  Promesse : $x = y$ ou x, y diffèrent en $N/2$ positions (N pair)
- D(DJ)=$\Theta(N)$

Protocole quantique

- DJ(*x*,*y*) = 1 si la fonction $i \mapsto x_i \oplus y_i$ est constante, et 0 si elle est équilibrée
- Donc Q(DJ)=$O(\log N)$

  le protocole est sans erreur [Buhrman, Cleve, Wigderson 1998]

Protocole probabiliste

- R(DJ)=$O(\log N)$ (probabilité d'erreur tolérée ≤ 1/3)

Produit scalaire distribué

- Entrées distribués : $x, y \in \{0,1\}^N$
- IP(*x*,*y*) = $\sum_i x_i y_i \mod 2$, R(IP)=$\Theta(N)$=Q(IP) [Kremer 1995]

Deutsch-Jozsa distribué

- Ressources initiales : Aléa ou enchevêtrement partagé
- Entrées distribués : $x, y \in \{0,1\}^N$
- Sortie $a, b \in \{0,1\}^{\log N}$: $a = b$ si $x = y$, et $a \neq b$ sinon

  Promesse : $x = y$ ou x, y diffèrent en $N/2$ positions (N pair)
- $R^{\text{aléa partagé}}(DJ)=\Theta(N)$ si aucune erreur tolérée
- $Q^{\text{enchevêtrement partagée}}(DJ)=0$ et aucune erreur

Protocole quantique

- Alice et Bob partagent $\log N$ paires EPR $(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)/\sqrt{2}$

  soit donc l'état : $\sum_{i=0}^{N-1} |i\rangle_A|i\rangle_B$
- Avec leurs entrées, ils créent l'état : $\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (-1)^{x_i+y_i}|i\rangle_A|i\rangle_B$
- Ils appliquent Hadamard sur leurs qubits
- Ils mesurent leur registre et renvoient le résultat correspondant

Cas *x*=*y*

- Alice et Bob partagent l'état : $\sum_{i=0}^{N-1} |i\rangle_A |i\rangle_B$

- Avec leurs entrées, ils calculent l'état : $\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (-1)^{x_i+y_i} |i\rangle_A |i\rangle_B$

  Comme $x = y$, l'état est donc inchangé : $\sum_{i=0}^{N-1} |i\rangle_A |i\rangle_B$

- Ils appliquent Hadamard sur leurs qubits. Rien ne se produit rien :

  Nous avions vu que : $(H \otimes I)(|00\rangle + |11\rangle)/\sqrt{2} = (I \otimes H)(|00\rangle + |11\rangle)/\sqrt{2}$

  et donc $(H \otimes H)(|00\rangle + |11\rangle)/\sqrt{2} = (|00\rangle + |11\rangle)/\sqrt{2}$

- Ils mesurent leur registre et renvoient le bit correspondant de leur entrée :

  L'état partagé est $\sum_{i=0}^{N-1} |i\rangle_A |i\rangle_B$

  Ils mesurent et renvoient donc la même valeur *i* aléatoire

Cas $x \neq y$ (et diffèrent en $N/2$ positions)

- Alice et Bob partagent l'état : $\sum_{i=0}^{N-1} |i\rangle_A |i\rangle_B$

- Avec leurs entrées, ils calculent l'état : $\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (-1)^{x_i+y_i} |i\rangle_A |i\rangle_B$

- Ils appliquent Hadamard sur leurs qubits, soit la transformation
  $H^{\otimes \log N} : |i\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{a=0}^{N-1} (-1)^{a \cdot i} |a\rangle$.
  et obtiennent $\frac{1}{N\sqrt{N}} \sum_{i,a,b=0}^{N-1} (-1)^{x_i+y_i+i\cdot(a \oplus b)} |a\rangle_A |b\rangle_B$

- Ils mesurent leur registre et renvoient le bit correspondant de leur entrée :
  Pour tout a, l'amplitude de $|a\rangle|a\rangle$ est : $\frac{1}{N\sqrt{N}} \sum_{i}^{N-1} (-1)^{x_i+y_i} = 0$

  car x et y diffèrent en $N/2$ positions (N pair)

  Ils mesurent et renvoient donc chacun une <u>valeur distincte</u>

Quantum fingerprint

Egalité

- Entrées distribués : $x, y \in \{0,1\}^N$
- Sortie EQ(*x*,*y*) = 1 si $x = y$, 0 sinon
- D(EQ)=$\Theta(N)$ et R(EQ)=$\Theta(\log N)$

Protocole

- Idée 1 : Alice envoie un (i, x_i) au hasard, Bob renvoie 1 si $x_i = y_i$
- Analyse : Complexité : $2 + \log N$ bits échangés

  Si $x = y$, aucune erreur

  Si $x \neq y$, le protocole renvoie 0 avec probabilité $\Pr_i[x_i \neq y_i] \geq 1/N$

  Cette probabilité est trop basse

- Idée 2

  Utiliser un code (déterministe) $E : \{0,1\}^N \to \{0,1\}^M$ tel que

  $$x \neq y \implies \Pr_j[E(x)_j \neq E(y)_j] \geq 2/3$$

  De tels codes existent avec $M = O(N)$ [Justesen 1972]

  Quitte à remplacer *x*,*y* par *E*(*x*), *E*(*y*), on peut donc supposer que soit $x = y$, soit $\Pr_i[x_i \neq y_i] \geq 2/3$ et utiliser l'idée 1 !

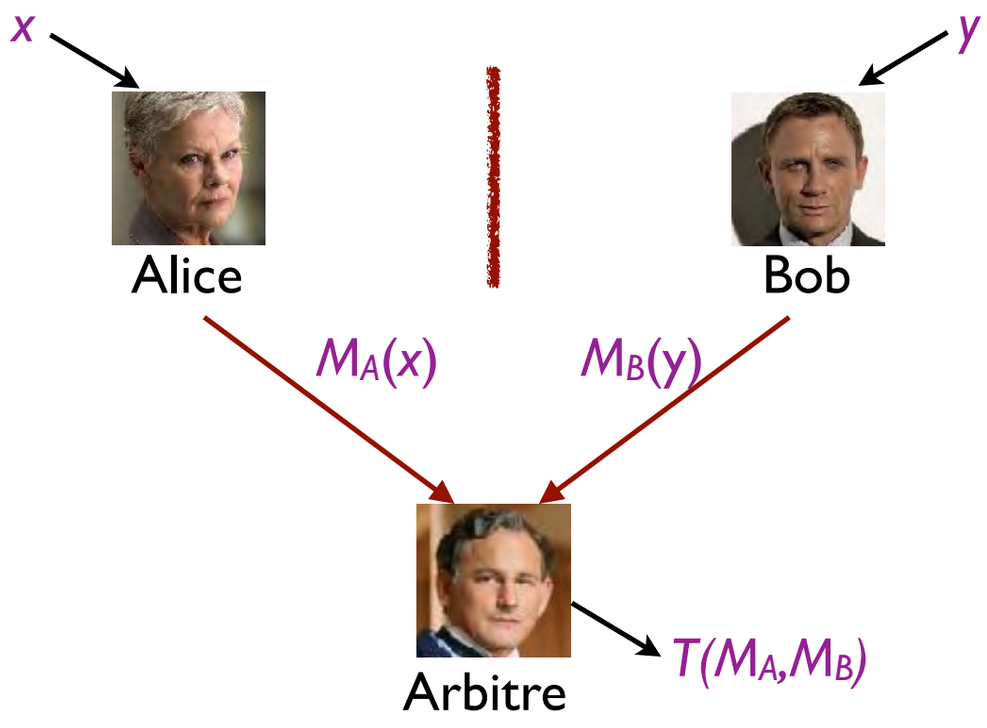
Communication avec arbitre

- Simultaneous message passing [Yao 1979]
- Données distribuées : (x,y)
- Protocole : unique message M_A d'Alice et M_B de Bob à un Arbitre

  L'Arbitre produit une réponse T en fonction de M_A et M_B

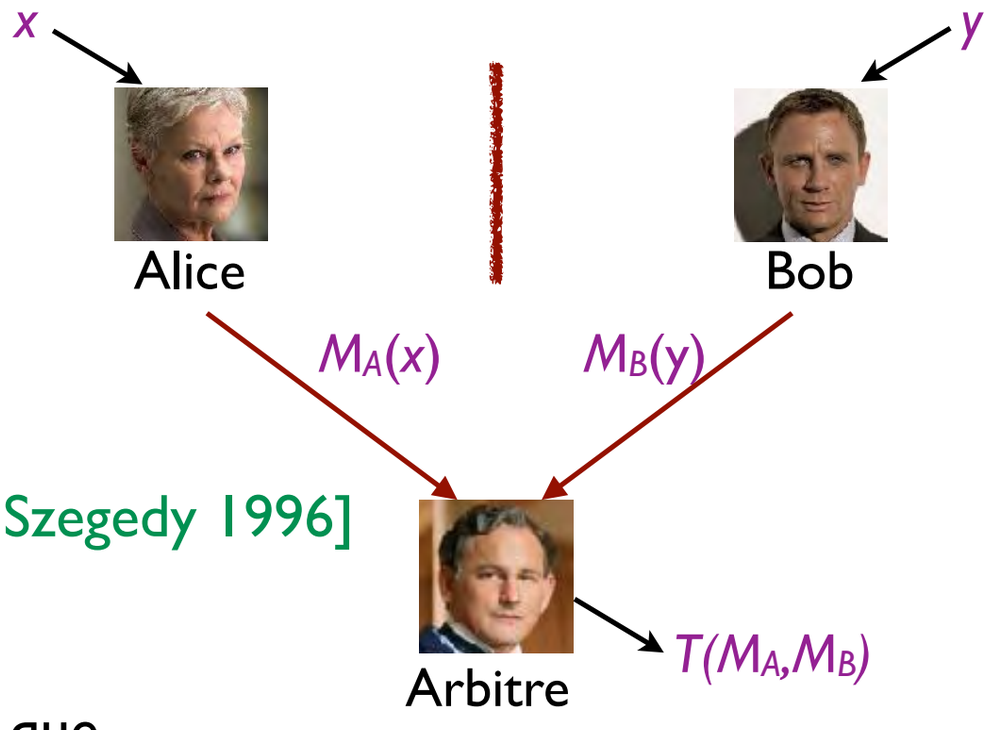
  Aucune autre interaction !
- Objectif collaboratif : $T(M_A,M_B) = F(x,y)$
- Complexité : Nombre maximum de bits envoyés (lorsque x,y varient)

Déterministe : $D^{||}(F)$ Probabiliste : $R^{||}(F)$ Quantique : $Q^{||}(F)$



Egalité avec arbitre

- Entrées distribués : $x, y \in \{0,1\}^N$
- Sortie EQ(*x*,*y*) = 1 si $x = y$, 0 sinon
- D||(EQ)=$\Theta(N)$
- R||(EQ)=$\Theta(\sqrt{N})$ [Ambainis 1996][Newman, Szegedy 1996]

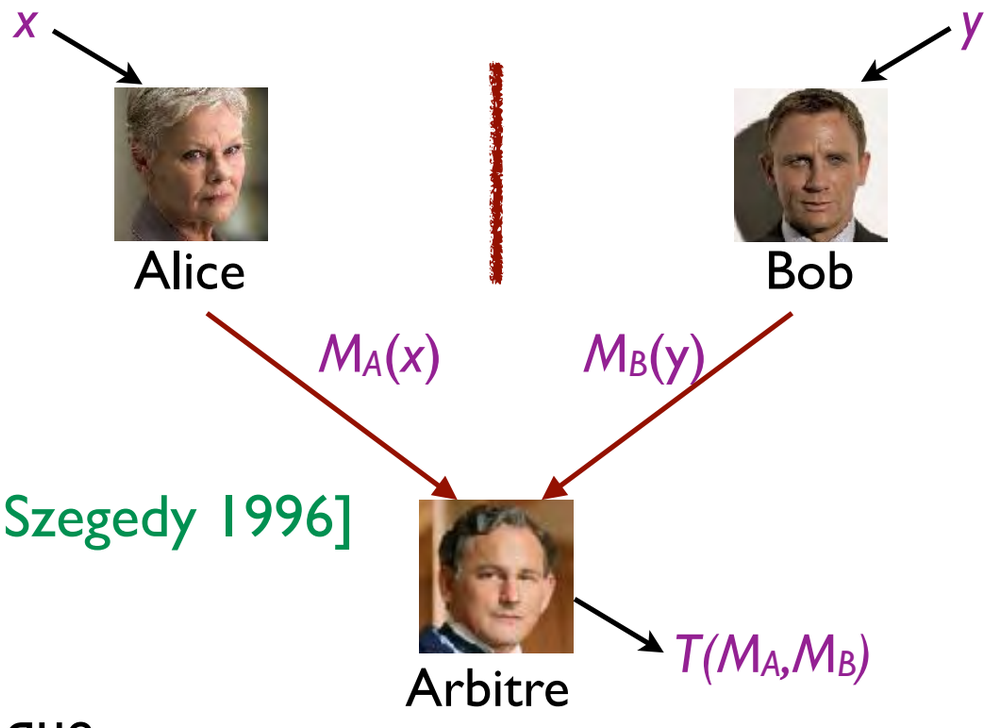


Cas probabiliste

- Rappel : Sans perte de généralité, supposons que
  $x = y$ ou $\Pr_i[x_i \neq y_i] \geq 2/3$
- Idée : Considérer *x* et *y* comme des matrices $\sqrt{N} \times \sqrt{N}$
- Protocole
  - Alice/Bob envoie une ligne/colonne au hasard de *x*/*y*
  - Charlie vérifie que l'entrée commune coïncide
- Analyse
  - Si $x = y$ alors Charlie accepte toujours
  - Sinon la position vérifiée par Charlie est aléatoire, et donc Charlie rejette avec probabilité 2/3

Egalité avec arbitre

- Entrées distribués : $x, y \in \{0,1\}^N$
- Sortie EQ||(x,y) = 1 si $x = y$, 0 sinon
- D||(EQ)=$\Theta(N)$
- R||(EQ)=$\Theta(\sqrt{N})$ [Ambainis 1996][Newman, Szegedy 1996]



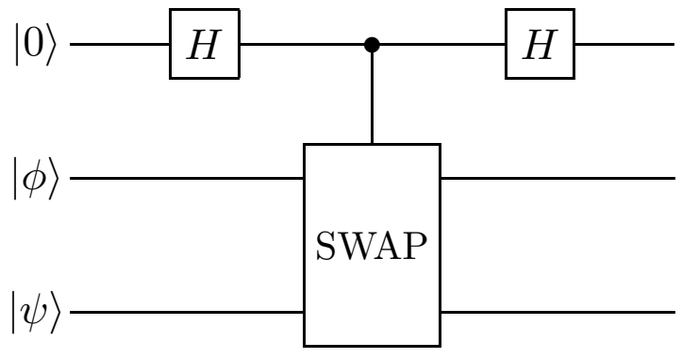
Cas quantique

- Rappel : sans perte de généralité, supposons que
  $x = y$ ou $\Pr_i[x_i \neq y_i] \geq 2/3$
- Encodage quantique sur $1 + \log N$ qubits des entrées de *N* bits
  $|A(x)\rangle = \frac{1}{\sqrt{N}} \sum_i |i, x_i\rangle$ et $B(y) = \frac{1}{\sqrt{N}} \sum_i |i, y_i\rangle$
- Si $x = y$ alors $|A(x)\rangle = |B(y)\rangle$
- Si $\Pr_i[x_i \neq y_i] \geq 2/3$ alors $0 \leq \langle A(x) | B(y) \rangle = \Pr_i[x_i = y_i] \leq 1/3$
- Question : Comment distinguer ces 2 cas ?
  Réponse : SWAP-Test
- Donc Q||(EQ)=$O(\log N)$ [Buhrman, Cleve, Watrous, Wolf 2001]

Problème

- Entrée : 2 états quantiques sur n qubits : $|\phi\rangle$ et $|\psi\rangle$
- Sortie : Estimer $\langle\phi|\psi\rangle$

Circuit



Analyse

- Avant control-SWAP : $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|\phi\rangle|\psi\rangle$
- Après control-SWAP : $\frac{1}{\sqrt{2}}|0\rangle|\phi\rangle|\psi\rangle \; + \; \frac{1}{\sqrt{2}}|1\rangle|\psi\rangle|\phi\rangle$
- En fin de circuit : $\frac{1}{2}|0\rangle\cdots \; + \; \frac{1}{2}|1\rangle(|\phi\rangle|\psi\rangle - |\psi\rangle|\phi\rangle)$
- Probabilité d'observer 1 : $\frac{1-|\langle\phi|\psi\rangle|^2}{2}$

Pour l'emprunte quantique : probabilité 0 ou au moins 4/9

Communication et inégalité de Bells

- The communication complexity of non-signaling distributions [Degorre, Kaplan, Laplante, Roland 2009]
- Classical and quantum partition bound and detector inefficiency [Laplante, Lerays, Roland 2012]
- Quantum communication complexity advantage implies violation of a Bell inequality [Buhrman et al 2016]

Plus de séparations, et applications

- Exponential Separations for One-Way Quantum Communication Complexity, with Applications to Cryptography [Gavinsky et al 2007]
- Lower bounds on information complexity via zero-communication protocols and applications [Kerenidis, Laplante, Lerays, Roland, Xiao 2012]
- Linear vs. Semidefinite Extended Formulations: Exponential Separation and Strong Lower Bounds [Fiorini et al 2012]

Calcul parallèle

Calcul classique

- Compromis architecture / temps : accélérer le calcul en effectuant des tâches indépendantes en parallèle
- Lorsque la loi de Moore s'arrêtera, l'architecture multi-processeurs sera l'une des possibilités pour continuer d'accélérer les calculs
- Données et utilisateurs distribués : résoudre des problèmes distribués en utilisant les ressources elles-mêmes distribuées

Circuits et parallélisme

- Circuits logiques de profondeur polylogarithmique et de taille polynomiale
- Algorithmes parallèles utilisant un nombre polynomial de processeurs avec mémoire partagée (PRAM) et un temps parallèle polylogarithmique
- Nombreux problèmes

  Algèbre linéaire, dont transformée de Fourier,

  Programmation dynamique, …

Topologie

- Grille 2D-calcul
- Réseaux arbitraires de ressources partagées

Super calculateur de Genci au CNRS

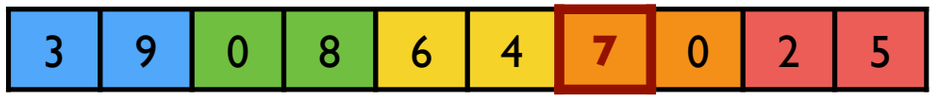
Complexité en requête parallèle

- p requêtes parallèles et simultanées par unité de temps
- Observation : Nb de blocs de p requêtes parallèles ≥ (nb de requêtes)/p

Accélération classique avec p processeurs

- Recherche d'une pré-image de $H : [N] \to [N]$ aléatoire

  Diviser les données en p parties de taille N/p



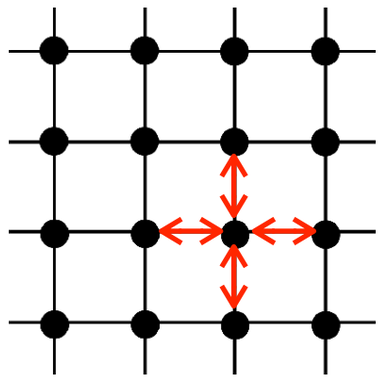
  Chaque processeur faire une recherche dans sa partie

  → Temps parallèle : N/p (blocks de p requêtes en parallèle)

- Recherche d'une collision dans $H : [N] \to [N]$ aléatoire

  Paradoxe des anniversaires → Temps parallèle : $\sqrt{N}/p$

Architecture à grand nombre de processeurs

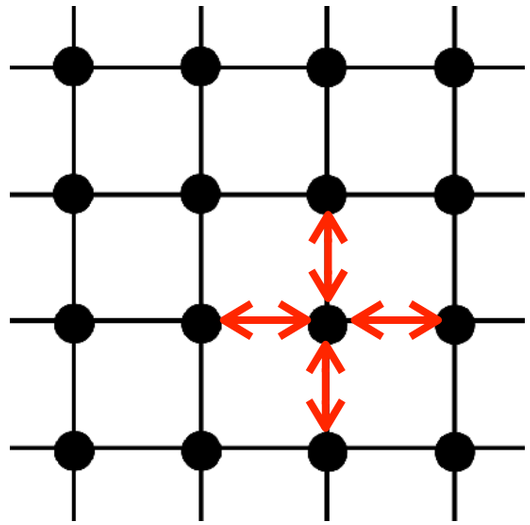


- Accès à une grande mémoire S en $\sqrt{S}$ (principe holographique)
- Grille 2D de taille $\sqrt{p} \times \sqrt{p}$ de processeurs, chacun de petite mémoire

  Communication / Tri : $\sqrt{p}$ cycles de communication [Schnorr, Shamir 1986]

Comment comparer ? [Bernstein 2009]

- C-2D : Nb de requêtes parallèles sur une grille 2D
  de p processeurs classiques de mémoire logarithmique
- Q : Nb de requêtes sur un seul processeur quantique
  de s qubits



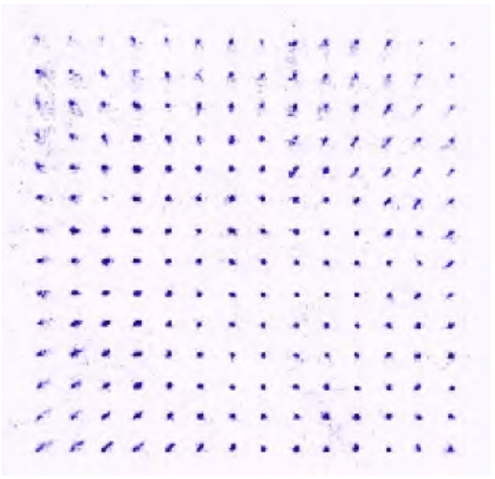
Grille imaginaire de calculateurs quantiques

Pré-image

- Q : $\sqrt{N}$ avec $s = \log N$ qubits
- C-2D : $N/p + \sqrt{p}$
  → $N^{1/3}$ avec $p = N^{2/3}$ processeurs
  → $\sqrt{N}$ avec $p = \sqrt{N}$ processeurs

Collision

- Q : $N^{1/3}$ avec $s = N^{1/3}$ qubits (QRAM)
- C-2D : $\sqrt{N}/p + \sqrt{p}$ [Oorschot, Wiener 1996]
  → $N^{1/6}$ avec $p = N^{1/3}$ processeurs
  → $N^{1/3}$ avec $p = N^{1/6}$ processeurs



Grille 14×14 de qubits faits d'atomes de Rydberg
(IOGS, Laboratoire Charles Fabry)

Motivations supplémentaires

- Effectuer plus d'opérations durant le temps de stabilité quantique (temps avant décohérence)
- Stratégique pour l'ère du NISQ (Noisy Intermediate-Scale Quantum)

Circuits quantiques de petite profondeur

- Fast parallel circuits for the quantum Fourier transform [Cleve, Watrous 00]
- Parallelizing Quantum Circuits [Broadbent, Kashefi 2009]
- Efficient Distributed Quantum Computing [Beals et al, 2012]
- A quantum approximate optimization algorithm [Farhi, Goldstone, Gutmann 2014]
- Parallel Quantum Algorithm for Hamiltonian Simulation [Zhang, Wang, Ying 2021]

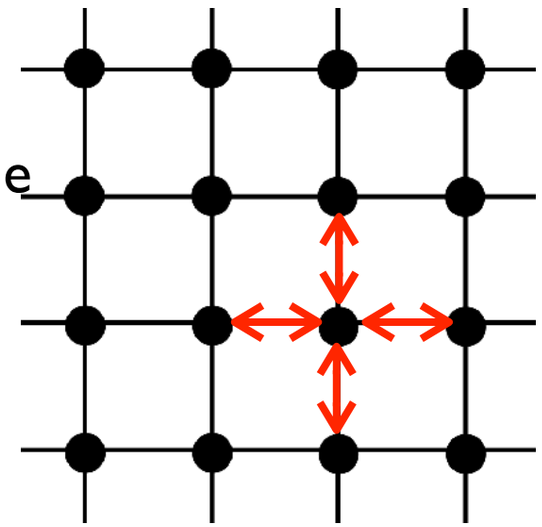
Requêtes parallèles

- Préimage : $\sqrt{N/p}$ [Zalka'99]
- Collision : $N^{1/3}/p^{2/3}$ [Chung, Fehr, Huang, Liao 2021]

Architecture 2D ?

Comment comparer ? [Jeffery 2011]

- Q-2D : Nb de requêtes parallèles sur une grille 2D de p processeurs quantiques de mémoire logarithmique



Grille imaginaire de calculateurs quantiques

Pré-image

- C-2D : $N/p + \sqrt{p}$

  → $\sqrt[3]{N}$ avec $p = N^{2/3}$ processeurs

- Q-2D : $\sqrt{N/p} + \sqrt{p}$

  → $\sqrt[4]{N}$ avec $p = \sqrt{N}$ processeurs quantiques

Collision

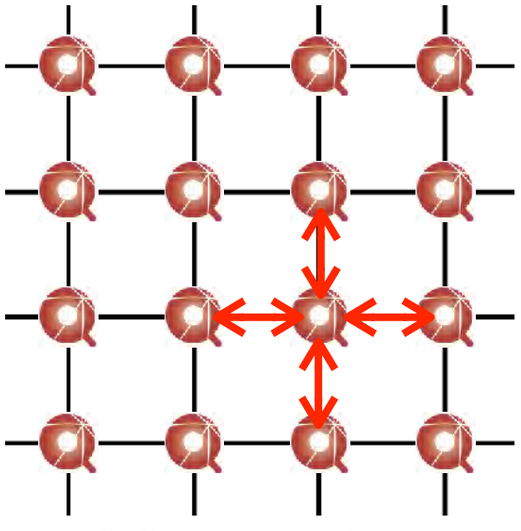
- C-2D : $\sqrt{N}/p + \sqrt{p}$

  → $N^{1/6}$ avec $p = N^{1/3}$ processeurs

- **Q-2D : Question ouverte !**

  Meilleur possible : $N^{1/3}/p^{2/3} + \sqrt{p}$

  → $N^{1/7}$ avec $p = N^{2/7}$ processeurs quantiques



Grille imaginaire de calculateurs quantiques

Références en lien avec le cours

Complexité de la communication

- Non-locality and Communication Complexity [Buhrman, Cleve, Serge Massar, Wolf 2010]
- Communication Complexity and Applications [Rao, Yehudayoff 2020]

Calcul parallèle

- Collision finding with many classical or quantum processors [Jeffery 2011]
- Efficient Distributed Quantum Computing [Beals et al, 2012]

Séminaire du cours !

- Quantum Computing as a Service: Secure and Verifiable Multi-Tenant Quantum Data Centre

  avec Elham KASHEFI, CNRS, Paris et University of Edinburgh

Merci au Collège de France

- Formidable soutien pour l'informatique quantique
- Occasion unique pour des publics variés

Merci au Public

- En salle
- A distance
- Questions

  Continuez à en poser à

  frederic.magniez@college-de-france.fr

Mais ce n'est pas encore fini…

Colloque - **June 17th - 18th, 2021**

Recent Advances on Quantum Computing

Organisateurs : Frédéric Magniez (Collège de France),
Alex Bredariol Grilo (LIP6)

Chaire Informatique et sciences numériques

Program

10 h > 18 h - salle 2

Open to the public, within space limits, subject to availability.
Ouvert au public, en demi-jauge, dans la limite des places disponibles.

June 17th

10.00 Nicolas Sangouard, *IPhT - CEA/CNRS*
Quantum Safe Crypto-System with Device-Independent Security Guarantees

11.00 Paul Renault, *LKB - SU/CNRS/ENS*
Optimisation Using Machine Learning of the Pump Spectrale Shape to Generate Multimode Squeezing

11.40 Federico Centrone, *LIP6 - SU/CNRS*
Charging Batteries with Quantum Squeezing

12.20 *Break*

14.00 Ivan Šupić, *LIP6 - SU/CNRS*
Quantum Networks Self-Test all Entangled States

15.00 Jonas Landman, *IRIF - UP/CNRS*
Recent Quantum Algorithms for Machine Learning and Neural Networks

15.40 *Break*

16.20 Robert Booth, *LIP6 - SU/CNRS*
Outcome Determinism in Measurement-Based Quantum Computing with Qudits

17.00 Pierre-Emmanuel Emeriau, *LIP6 - SU/CNRS*
Witnessing Wigner Negativity

17.40 Discussion

June 18th

10.00 Simon Apers, *ULB/CWI*
Quantum Complexity of Minimum Cut

11.00 Daniel Szilagyi, *IRIF - UP/CNRS*
A Gradient Descent Perspective on Quantum Linear System Solvers

11.40 Léo Colisson, *LIP6 - SU/CNRS*
Non-Destructive Zero-Knowledge Proofs on Quantum States, and Multi-Party Generation of Authorized Hidden GHZ States

12.20 *Break*

14.00 David Barral, *LKB - SU/CNRS/ENS*
Nonlinear Waveguide Arrays and Triple Photons: Gaussian and Non-gaussian Resources for Continuous-Variable Quantum Information

15.00 Nathan Shettell, *LIP6 - SU/CNRS*
A Cryptographic Approach to Quantum Metrology

15.40 *Break*

16.20 Félicien Appas, *MPQ - UP/CNRS*
Flexible Entanglement-Distribution Network with an AlGaAs chip for Secure Communications

17.20 Eleni Diamanti, *LIP6 - SU/CNRS*
Updates on Paris Hub

17.40 Discussion

Chaire crée avec le soutien de Inria

COLLÈGE DE FRANCE 1530
Thomas Römer
Administrateur du Collège de France
11, place Marcelin-Berthelot, 75005 Paris
www.college-de-france.fr

Année académique 2020/2021