COLLÈGE DE FRANCE
1530

Algorithmes quantiques

Transformée de Fourier quantique

12-05-2021

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 2 - Les bases algorithmiques

- Concepts du calcul et principales méthodes algorithmiques
- Mise en évidence de propriétés algébriques (déchiffrement)
- Optimisation et applications algorithmiques

05 mai 2021

Cours : Circuits quantiques, premiers algorithmes : portes universelles, algorithmes de Deutsch-Jozsa et Bernstein-Vazirani, supériorité des algorithmes quantiques

Séminaire : Langages graphiques pour programmer et raisonner en informatique quantique
Simon PERDRIX, *CNRS*, *Nancy*

12 mai 2021

Cours : Transformée de Fourier quantique : réalisation, estimation de phase, algorithmes de Simon et de Shor (recherche de période et factorisation) et généralisations récentes

Séminaire : Le problème du sous-groupe caché, Miklos SANTHA, *CNRS*, *Paris et CQT*, *Singapour*

19 mai 2021

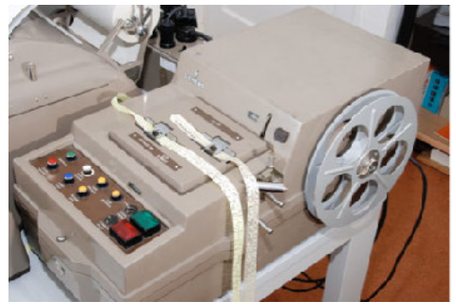
Cours : Optimisation quantique : algorithme de Grover, estimateurs quantiques, chaînes de Markov quantiques, heuristiques quantiques

Séminaire : A Unified Framework for Quantum Walk Search, Stacey JEFFERY, *CWI*, *Amsterdam*

Cryptographie pré-quantique

One-time pad

Message :	0	1	1	0	0	1	0	1	1	1	0
Clé privée :	1	1	0	1	0	0	1	0	1	0	0
XOR bit à bit :	1	0	1	1	0	1	1	1	0	1	0



Washington-Moscow hotline (1963)

- Théorème : Sécurité parfaite si chaque bit de clé est utilisé une seule fois !

Alternatives utilisées en pratique

- Permettent d'utiliser plusieurs fois une même et plus petite clé

  Exemple : Advanced Encryption Standard (AES)

- Sécurité combinatoire : pas de preuve de sécurité mais semble résister aux tentatives de déchiffrement, y compris quantiques

  En pratique, très sûr si la clé n'est pas trop utilisée...

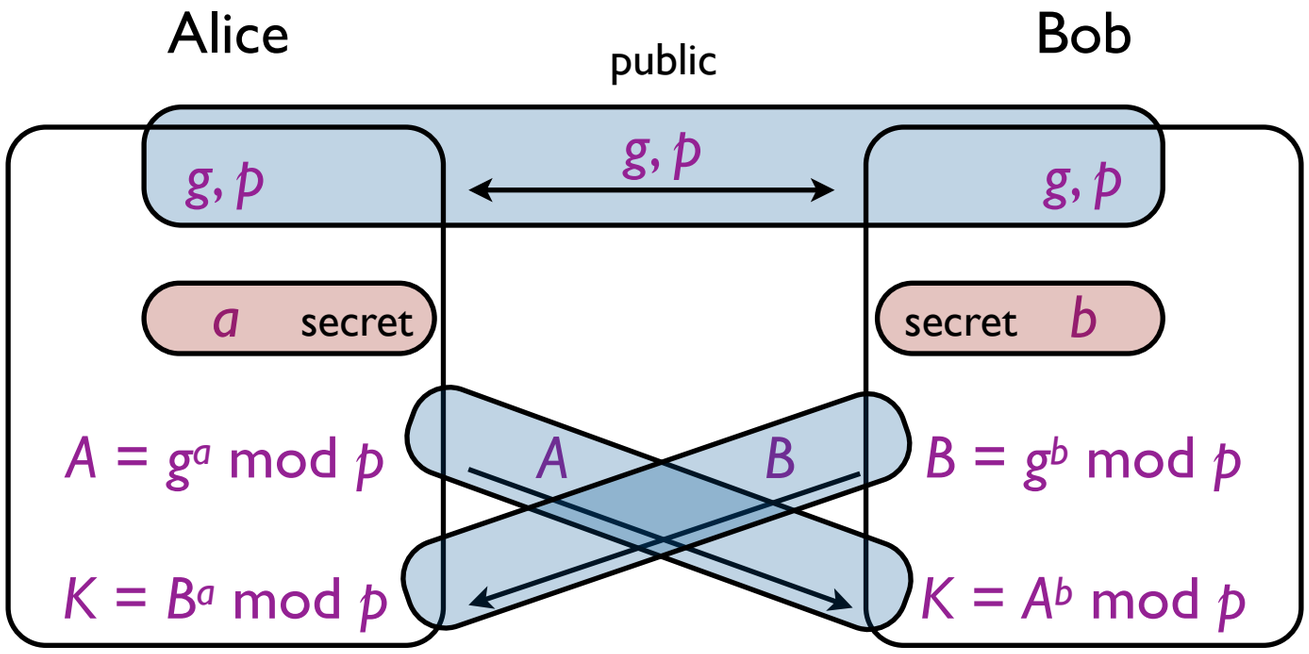
Génération de la clé secrète

- Méthode courante : la clé privée est générée à l'aide d'un protocole à clé publique, dont RSA et Diffie-Hellman
- Méthode quantique : utiliser le protocole quantique (cours 1) [BB84]

Idée : fonction à sens unique

- Calculer $g^a \bmod p$ se fait en $\log a$ multiplications
- Trouver a tq $A = g^a \bmod p$ se fait en a multiplications

Protocole



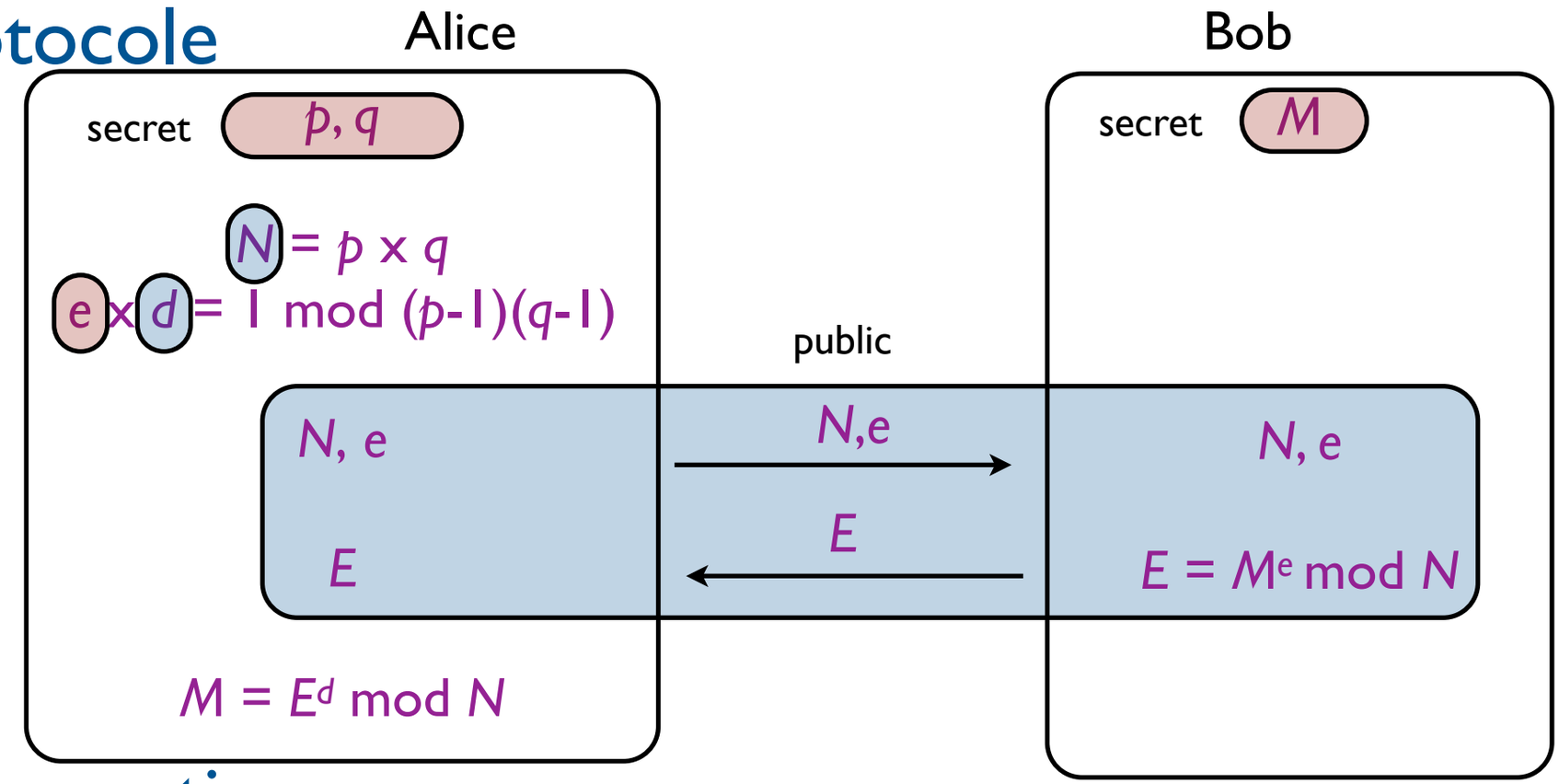
Commentaires

- Alice et Bob ont la même clé : $(g^a)^b \bmod p = (g^b)^a \bmod p = g^{ab} \bmod p$
- Travailler avec des secrets de plusieurs milliers de bits
- Utilisation de courbes elliptiques rend les attaques plus difficiles

Idée : fonction à sens unique

- Calculer $p \times q$ se fait en $\log p$ additions
- Trouver p, q tq $N = p \times q$ se fait en p divisions

Protocole



Observations

- $M^{ed} = M \bmod N$
- Toute le monde peut chiffrer avec la connaissance de N et e
- Pour déchiffrer, il faut connaître/trouver d

  En particulier, il suffit de factoriser N

Records

Nb chiffres	Date	Groupe
193	2/11/2005	Franke (Bonn)
212	2/7/2012	Bai, Thomé, Zimmermann (Camberra, Nancy)
250	28/2/2020	Boudout, Gaudry, Guillevic, Heninger, Thomé, Zimmermannn (Limoges, Nancy, San Diego)

- Exemple à 193 chiffres

  310741824049004372135075003588856793003734602284272754572016194882320644051808150455634682967172328678243791627283803341547107310850191954852900733772482278352574238645401469173660247765234660 9

  =

  163473364580925384844313388386509085984178367003309231218111085238933310010450851212118167511579

  x

  190087128166482211312685157393541397547189678996851549366663853908802710380210449895719126146557 1

- Ressources utilisées en 2020

  This computation was performed with the Number Field Sieve algorithm, using the open-source CADO-NFS software

  The total computation time was roughly 2700 core-years

  Distributed computing resources in France, Germany and US

Cryptographie post-quantique

Sécurité compromise ou affaiblie

- Peter Shor [1994] : algorithme quantique qui résout Logarithme discret, Factorisation. Nombreuses extensions à d'autres pbs algébriques.

  → Attaque directe de nombreux protocoles à clé publique

- Lov Grover [1996] : algorithme quantique qui accélère toute recherche exhaustive. Nombreuses extensions aux heuristiques.

  → Protocoles à clé privée affaiblis : Ils nécessitent une plus grande clé

Nouvelle communauté

- Conférence Post-Quantum Cryptography voit le jour en 2006
- Objectifs complémentaires aux protocoles quantiques

  Sans technologie dédiée

  Sécurité face aux ordinateurs quantiques

Compétition internationale

- Lancée par NIST durant PQCrypto 2016
- Nouveaux standards de la cryptographie à définir

Transparents de l'annonce de NIST durant PQCrypto'16 :

The sky is falling?

- When will a quantum computer be built?
  - 15 years, $1 billion USD, nuclear power plant (PQCrypto 2014, Matteo Mariantoni)
- Impact:
  - Public key crypto:
    - ~~RSA~~
    - ~~Elliptic Curve Cryptography (ECDSA)~~
    - ~~Finite Field Cryptography (DSA)~~
    - ~~Diffie-Hellman key exchange~~
  - Symmetric key crypto:
    - AES — Need larger keys
    - Triple DES — Need larger keys
  - Hash functions:
    - SHA-1, SHA-2 and SHA-3 — Use longer output

Daniel Simon, 1994

- Résout un problème (encore) à oracle
- Objectif : trouver la période d'une fonction (sous certaines hypothèses)
- Solution
  - Classique : nombre exponentiel de questions
  - Quantique : nombre linéaire de questions
- Ingrédient : transformée de Fourier quantique
- Article d'abord refusé, mais…

Peter Shor, 1994

- Montre comment factoriser (sans oracle) *rapidement*
- Ingrédients
  - Construction d'une fonction à partir du nombre à factoriser
    - dont la période révèle les facteurs
  - Transformée de Fourier quantique
- Remarque : Oracle simulé à partir du nombre à factoriser

Portes

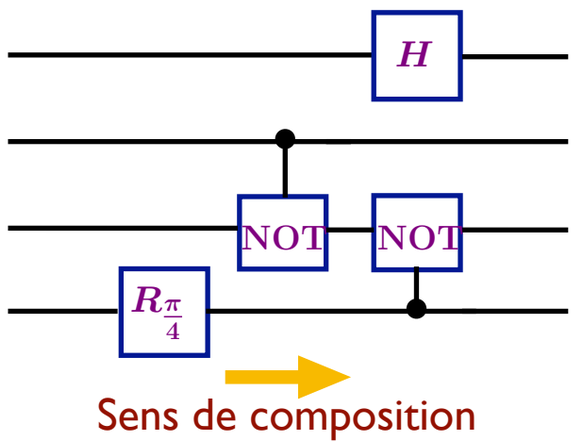
- Une porte quantique est une transformation unitaire sur au plus 3 qubits

Circuit

- Un circuit quantique

  est la composition de portes (étendues par ⊗ Id)

- Complexités : taille (nb de portes) et profondeur

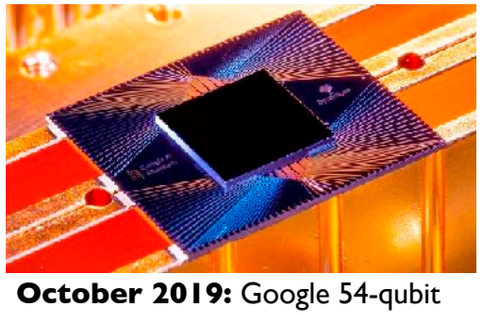


Programmer les circuits quantiques

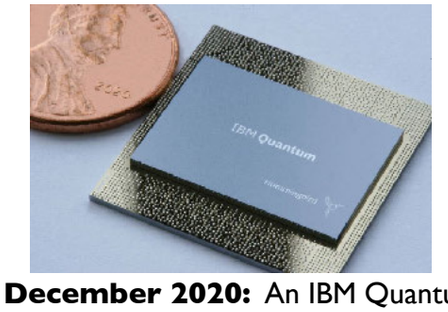
- Description du circuit à la charge d'un algorithme classique

  Multitude de langages, y compris avec implémentation dans le cloud

- Interactions possibles entre algorithme et circuit
- Modèle proche de certaines expériences y compris dans le cloud ou de "suprématie quantique"



October 2019: Google 54-qubit processor, named "Sycamore"



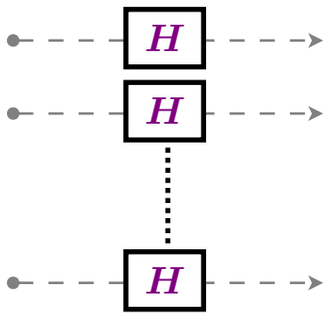
December 2020: An IBM Quantum Hummingbird r2 Processor (65 qubits).

Transformée de Fourier quantique

Définition

$$|b\rangle \text{ ---} \boxed{H} \text{---} \frac{1}{\sqrt{2}}(|0\rangle + (-1)^b|1\rangle)$$

$QFT_n \equiv$



$$QFT_n|x\rangle = \frac{1}{2^{n/2}} \sum_y (-1)^{x \cdot y} |y\rangle$$

avec $x \cdot y = \sum_i x_i y_i \mod 2$

Changement de base

$$QFT\left(\sum_x \alpha_x |x\rangle\right) = \sum_y \hat{\alpha}_y |y\rangle \qquad \text{avec } \hat{\alpha}_y = \frac{1}{2^{n/2}} \sum_x (-1)^{x \cdot y} \alpha_x$$

$\hat{\alpha}_y$: coefficients de Fourier dans le groupe $(0,1,\oplus)^n = (\mathbb{Z}_2)^n$

Complexité

- Calculer $\hat{\alpha}_y$ requiert 2^n opérations, tous les avoir $n \times 2^n$ opérations
- *QFT* requiert n opérations au total

Applications

Classique
- Cryptographie : bonne diffusion, pour générer des nombres aléatoires

Classique
- Signal : adaptée à la compression vidéo (H.264)

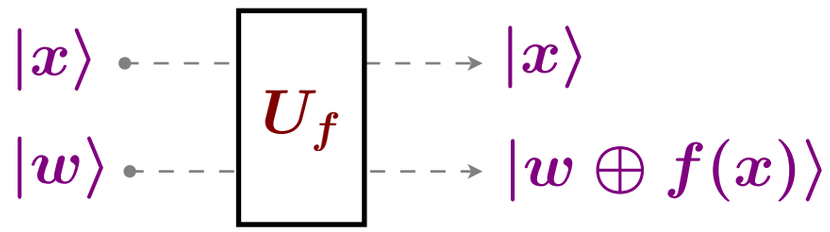
Quantique
- Signal : liens entre transformée de Fourier et périodicité

Problème

- Entrée : $f : \{0,1\}^n \to \{0,1\}^n$ telle que

$$\exists s \in \{0,1\}^n : \forall x \neq y,\ f(x) = f(y) \iff y = x \oplus s$$

- Sortie : s
- Contrainte : f est une boîte noire



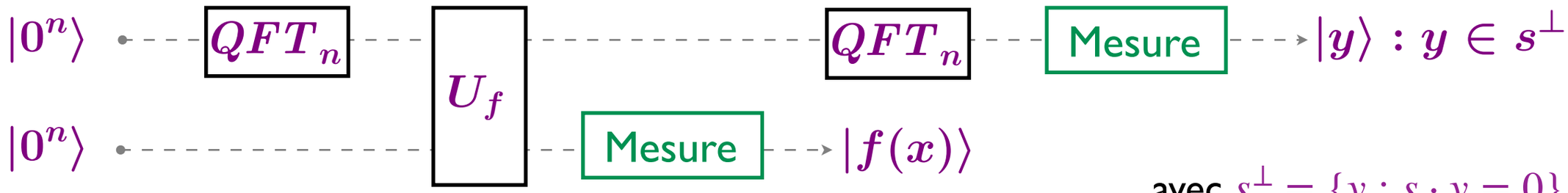
Complexité en requêtes

- Probabiliste : $\Omega(2^{n/2})$
- Quantique : $n + O(1)$

Idée

Utiliser *QFT* pour rechercher la période s.

Solution quantique



avec $s^\perp = \{y : s \cdot y = 0\}$

Initialisation : $|0^n\rangle|0^n\rangle$

Parallélisation : $\frac{1}{2^{n/2}} \sum_x |x\rangle|0^n\rangle$

Appel de f : $\frac{1}{2^{n/2}} \sum_x |x\rangle|f(x)\rangle$

Mesure partielle : $\frac{1}{\sqrt{2}}(|x\rangle + |x \oplus s\rangle)|f(x)\rangle$

Interférences : $\frac{1}{2^{(n+1)/2}} \sum_y ((-1)^{x \cdot y} + (-1)^{(x \oplus s) \cdot y})|y\rangle|f(x)\rangle$

$$\frac{1}{2^{(n+1)/2}} \sum_y (-1)^{x \cdot y}(1 + (-1)^{s \cdot y})|y\rangle|f(x)\rangle$$

$$\frac{1}{2^{(n-1)/2}} \sum_{u : s \cdot y = 0} (-1)^{x \cdot y}|y\rangle|f(x)\rangle$$

Création du système

- Après n+k itérations, échantillons $y^1, y^2, \ldots, y^{n+k} \in s^\perp$
- Système à résoudre :

$$\begin{cases} y^1 \cdot t = 0 \\ y^2 \cdot t = 0 \\ \vdots \\ y^{n+k} \cdot t = 0 \end{cases}$$

- Si $s = 0^n$, les y^i sont de rang n avec probabilité $\geq 1 - \frac{1}{2^k}$
- Si $s \neq 0^n$, les y^i sont de rang n-1 avec proba $\geq 1 - \frac{1}{2^k}$

  Solutions du système : 0^n et s !

Bilan

- Complexités

Simon	Requêtes	Temps
Classique	$\Omega(2^{n/2})$	$\Omega(2^{n/2})$
Quantique	n+$O(1)$	$O(n^3)$

- Réfutation de la thèse de Church-Turing quantitative (avec oracle) !

Vers la factorisation

Calcul de l'ordre

- Entrée : entiers N, a tels que $\text{pgcd}(a,N)=1$
- Sortie : le plus petit entier $r \neq 0$ tel que $a^r = 1 \bmod N$
- Observation : La fonction $f(x)=a^x \bmod N$ est périodique de période r

  elle est de plus facilement calculable en $O(\log N)$ multiplications

Factorisation

- Entrée : entier N
- Sortie : un diviseur non trivial de N

Réduction [Miller 1976]: Factorisation $<_R$ Calcul de l'ordre

- Vérifier que $\text{pgcd}(a,N)=1$
- Calculer l'ordre r de $a \bmod N$
- Recommencer si r impair ou $a^{r/2} = -1 \bmod N$
- Sinon $(a^{r/2} -1)(a^{r/2} +1)=0 \bmod N$
- Renvoyer $\text{pgcd}(a^{r/2} \pm 1, N)$

Analyse : succès avec probabilité $\geq 1/2$, sauf quand N est une puissance d'un nombre premier, mais alors N est facilement divisible !

Définition

$$QFT_{\mathbb{Z}_N}|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega_N^{xy} |y\rangle \qquad \text{avec } \omega_N = e^{2\pi i/N}$$

Changement de base

$$QFT_{\mathbb{Z}_N}\Big(\sum_x \alpha_x |x\rangle \Big) = \sum_y \hat{\alpha}_y |y\rangle \qquad \text{avec } \hat{\alpha}_y = \frac{1}{\sqrt{N}} \sum_x \omega_N^{xy} \alpha_x$$

$\hat{\alpha}_y$: coefficients de Fourier dans le groupe $\mathbb{Z}_N$

Complexité

- Calculer $\hat{\alpha}_y$ requiert N opérations, tous les avoir $N \times \log N$ opérations
- Et en quantique ?

Applications

- Mathématiques, physique
- Analyse de signaux, compression de données
- Accélération algorithmiques (ex : multiplication de grand nombres)
- ….

Forme récursive

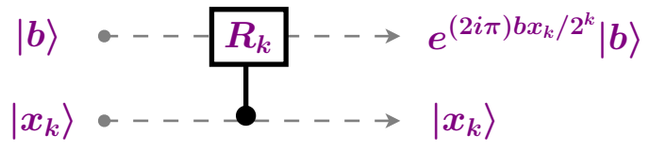
$$QFT_{\mathbb{Z}_{2^n}}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} \omega_{2^n}^{xy} |y\rangle \qquad \text{avec } y = y_1 2^{n-1} + y_2 2^{n-2} + \ldots + y_n$$

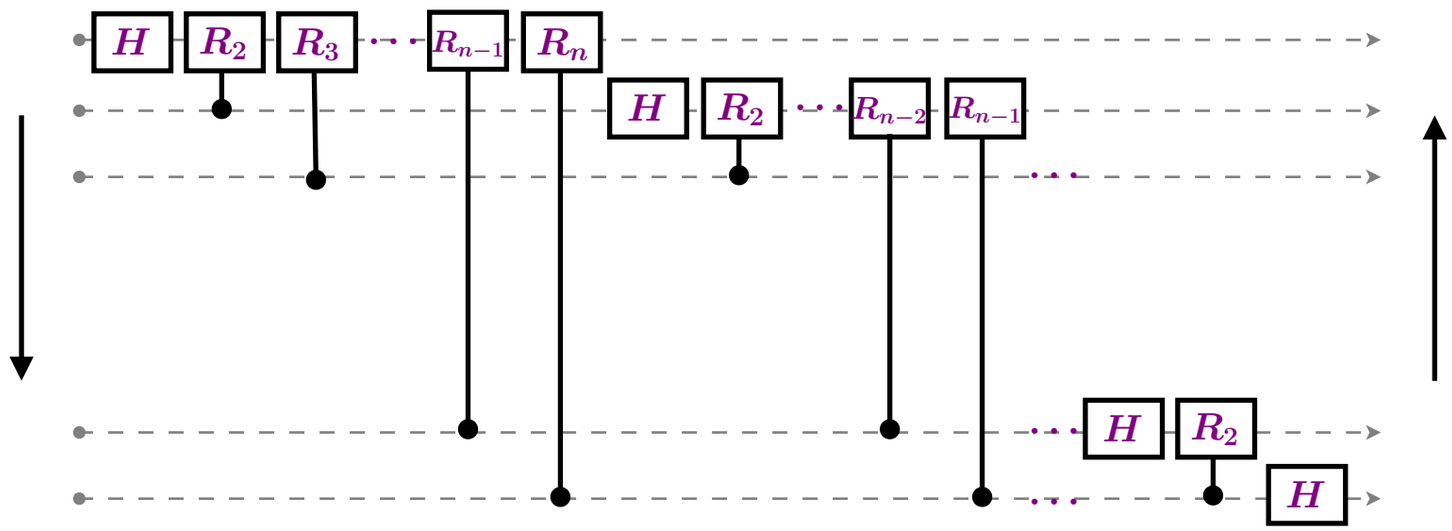
$$= \frac{1}{\sqrt{2^n}} (|0\rangle + \omega_{2^n}^{2^{n-1}x}|1\rangle)(|0\rangle + \omega_{2^n}^{2^{n-2}x}|1\rangle)\ldots(|0\rangle + \omega_{2^n}^{x}|1\rangle)$$

$$= \frac{1}{\sqrt{2^n}} (|0\rangle + \omega_{2}^{x}|1\rangle)(|0\rangle + \omega_{2^2}^{x}|1\rangle)\ldots(|0\rangle + \omega_{2^n}^{x}|1\rangle)$$

$$= \frac{1}{\sqrt{2^n}} (|0\rangle + \omega_{2}^{x_n}|1\rangle)(|0\rangle + \omega_{2^2}^{2x_{n-1}+x_n}|1\rangle)\ldots(|0\rangle + \omega_{2^n}^{x_1 2^{n-1}+x_2 2^{n-2}+\ldots+x_n}|1\rangle)$$

Circuit de taille $O(n^2)$





Cas $N = 2^n$ (ou produit de petits facteurs)

- Simulation exacte

  Taille des circuits : $O(n^2) \rightarrow O(n(\log n)^2 \log\log n)$

  Profondeur des circuits : $O(n) \rightarrow O(n)$

- Simulation avec précision $\varepsilon > 0$

  Taille des circuits : $O(n \log(n/\varepsilon))$

  Profondeur des circuits : $O(\log n + \log\log(1/\varepsilon))$

Cas N quelconque - $n = \log N$

- Simulation exacte

  Taille des circuits : $O(n^2)$

- Simulation avec précision $\varepsilon > 0$

  Taille des circuits : $O(n \log(n/\varepsilon) + \log^2(1/\varepsilon))$

  Profondeur : $O(\log n + \log\log(1/\varepsilon))$

Utilisation : calcul de l'ordre

Rappel du problème

- Entrée : $N, a \in \mathbb{N}$ tels que $\mathbf{pgcd}(a, N) = 1$
- Sortie : le plus petit entier $r \neq 0$ tel que $a^r = 1 \mod N$

Encodage

- Oracle = Fonction puissance : $f_a : \mathbb{Z} \to \mathbb{Z}_N, x \mapsto a^x \mod N$

Propriétés

- f_a est <u>strictement</u> périodique de période r
- Si $f_a(x) = f_a(y)$ alors $(x - y)$ est un multiple de r

Obstacles

- La fonction est définie sur un domaine infini

  → Se restreindre à un sous ensemble {0,1,…,*M*-1} fini

- Problème du bord

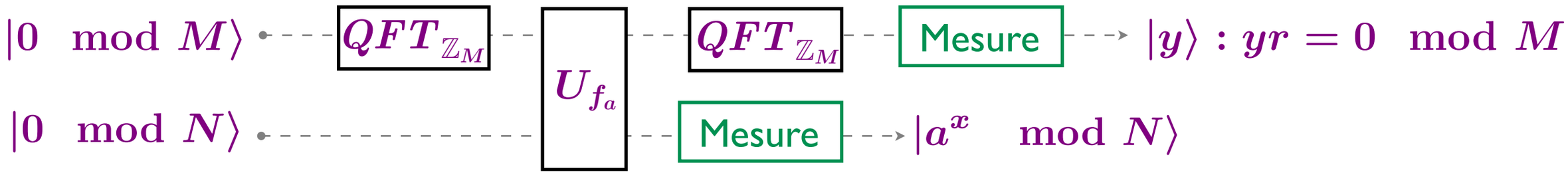
  → Etendre la fonction modulo *M*

- La fonction n'est plus périodique sauf si *M* est un multiple de *r*

  → Prendre *M* grand (~N^2) pour que *M* soit *à peu près* multiple de *r*

  Dans la suite on suppose que *M* est un multiple de *r*

Cas *M* est multiple de *r*



Initialisation : $|0 \mod M\rangle|0 \mod N\rangle$

Parallélisation : $\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle|0\rangle$

Appel de f_a: $\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle|a^x \mod N\rangle \qquad 0 \leq x < r$

Mesure partielle : $\sqrt{\frac{r}{M}} \sum_{j=0}^{M/r-1} |x + jr\rangle|a^x \mod N\rangle$

Interférences : $\frac{\sqrt{r}}{M} \sum_{y=0}^{M-1} \omega_M^{xy} \Big(\sum_{j=0}^{M/r-1} (\omega_M^{ry})^j \Big) |y\rangle|a^x \mod N\rangle$

$$\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \omega_r^{xk} |kM/r\rangle|a^x \mod N\rangle$$

$y \cdot s = 0 \leftrightarrow yr = 0 \mod M : y = kM/r,\ k = 0, \ldots, r-1$

Bilan

- Echantillons : $y=kM/r$ avec $k=0,1,\ldots,r-1$ inconnu et aléatoire

Reconstruction de *r* avec *y* et *M*

1. Réduire la fraction y/M ($=k/r$) en t/z permet d'obtenir z qui divise r

   Analyse : Si k/r est irréductible (avec prob$\geq 1/\log\log N$), alors $z=r$

   Sinon z divise r

2. Si $a^z = 1 \mod n$, alors déclarer "l'ordre de a est z"

   Preuve : Puisque $1 \leq z \leq r$, si $a^z = 1 \mod n$ alors $z = r$

3. Sinon récupérer un nouvel échantillon y' puis z' comme en 1

   Nécessairement ppcm(z,z') divise r

   Retourner en 2 avec $z \leftarrow$ ppcm(z,z')

Théorème

$$\Pr_{k,k'=0,\ldots,r-1}[\mathrm{ppcm}(z,z') = r] \geq 0.4$$

Conclusion

- Si M est multiple de r, alors avec $O(\log(1/\varepsilon))$ exécutions de l'algorithme de Shor fournit un facteur non trivial de N avec probabilité $\geq 1-\varepsilon$.

Cas général : M n'est pas multiple de r

Choix de M

- Contrainte : $N^2 < M < 2N^2$
- Pour simplifier la transformée de Fourier : $M = 2^m$

Même algorithme...

- Après mesure

  Précédemment

  $$\Pr_y[yr = 0 \mod M] = 1$$

  Maintenant

  $$\Pr_y[|yr|_{\mod M} \leq r/2] \geq \frac{1}{3}$$

Analyse

- Si $|yr|_{\mod M} \leq r/2$, alors il existe une unique fraction $\frac{k}{r}$ telle que

  $$-\frac{1}{2M} \leq \frac{y}{M} - \frac{k}{r} \leq \frac{1}{2M}$$

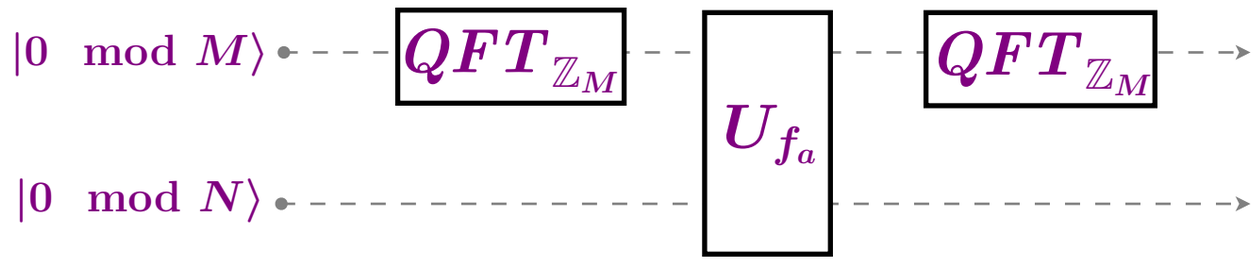
- L'algorithme des fractions continues trouve $\frac{k}{r}$ en temps $O(\log(N)^3)$
- Conclusion identique au cas précédent :

  Calculer le ppcm de toutes les paires de $O(\log(1/\varepsilon))$ échantillons

  Le plus petit des candidats z tq $a^z = 1 \mod n$ est bien r

  avec probabilité $\geq \varepsilon$

Taille du circuit



- $M = 2^m \sim N^2$
- $n = \log N$
- Nb qubits : $3n$
- Taille circuit : $O(n \log n)$
- Profondeur circuit : $O(\log n)$
- Partie exponentiation : $f_a(x) = a^x \bmod N$

  Taille circuit : $O(n^5 \log n) \rightarrow O(n^3)$

  Profondeur circuit : $O(\log n) \rightarrow O((\log n)^2)$
- Réfutation de la thèse de Church-Turing quantitative (sans oracle) !

  (sauf si un algorithme classique et rapide pour Factorisation venait à être découvert)

D'autres possibilités

- Nb qubits : $2n+2$
- Taille circuit : $O(n^3)$
- Profondeur circuit : $O(n^3 \log n)$

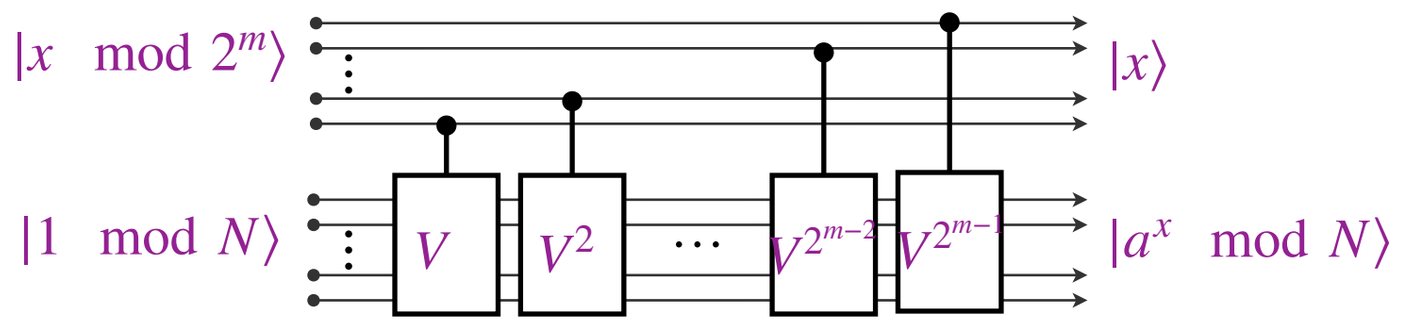
Estimation de phase

Exponentiation rapide

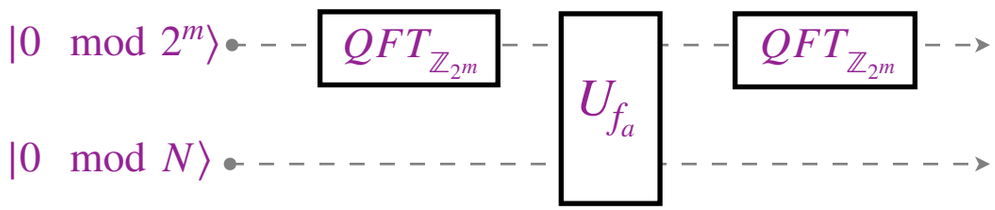
- Précalcul

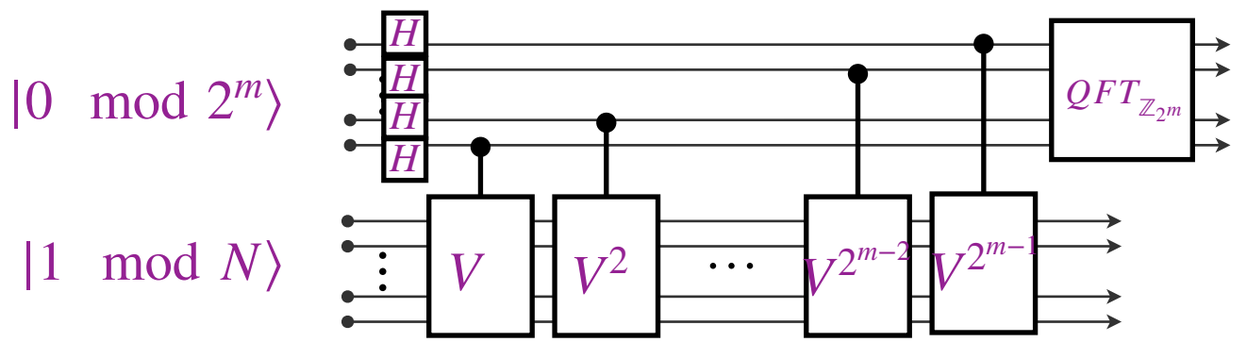
  Puissances a^k, k=1,2,2^2, …, 2^{m-1}, pour réaliser : $|z\rangle$ — V^k → $|z\, a^k \mod N\rangle$

- Circuit profondeur



Circuit complet revu





Problème

- Entrée

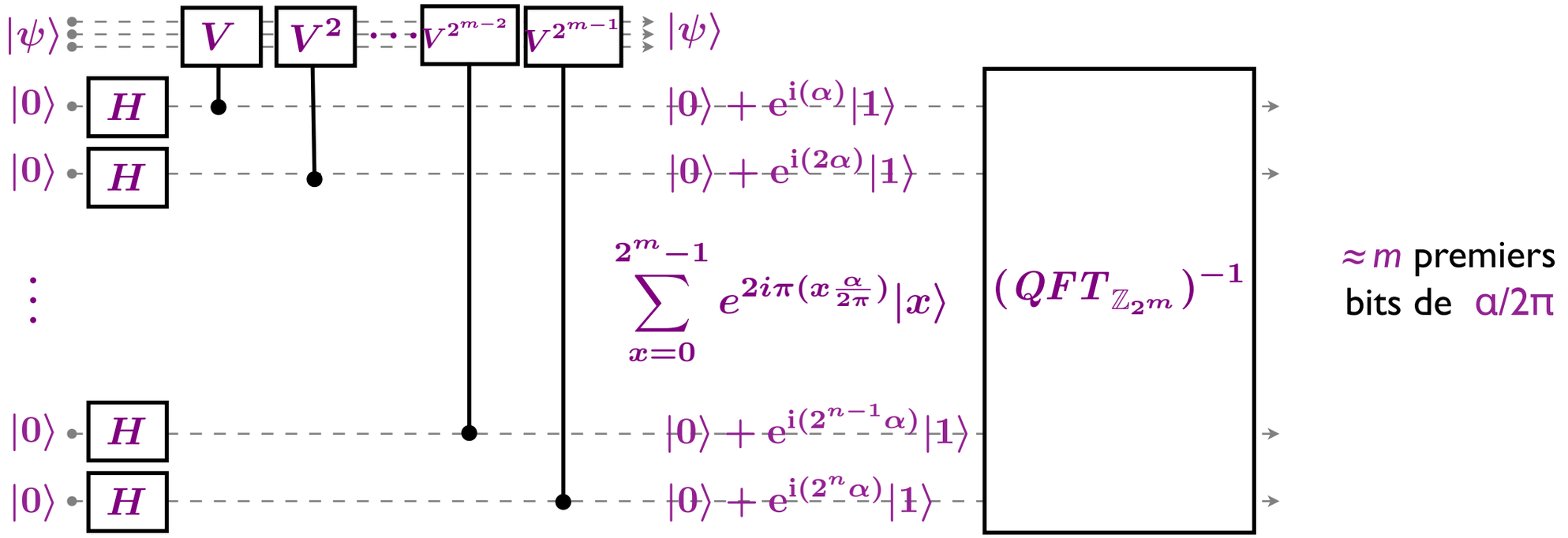
  Transformation unitaire V avec ses "portes" c-V^k pour $k=1,2,\ldots,2^{m-1}$

  Une superposition $|\psi\rangle$ telle que $V|\psi\rangle = e^{i\alpha}|\psi\rangle$

- Sortie

  La valeur de $\alpha/(2\pi)$ à m bits de précision près

Circuit [Kitaev'95] [Cleve, Ekert, Macchiavello, Mosca'98]



Autres développements

Problème

- Entrée :

  Entier p premier et $g \in \{1,2,\ldots,p-1\}$

  Un entier $A \in \{1,2,\ldots,p-1\}$

- Sortie

  Entier $a \in \{0,1,2,\ldots,p-2\}$ tel que $A = g^a \mod p$ (s'il existe)

Peter Shor, 1994

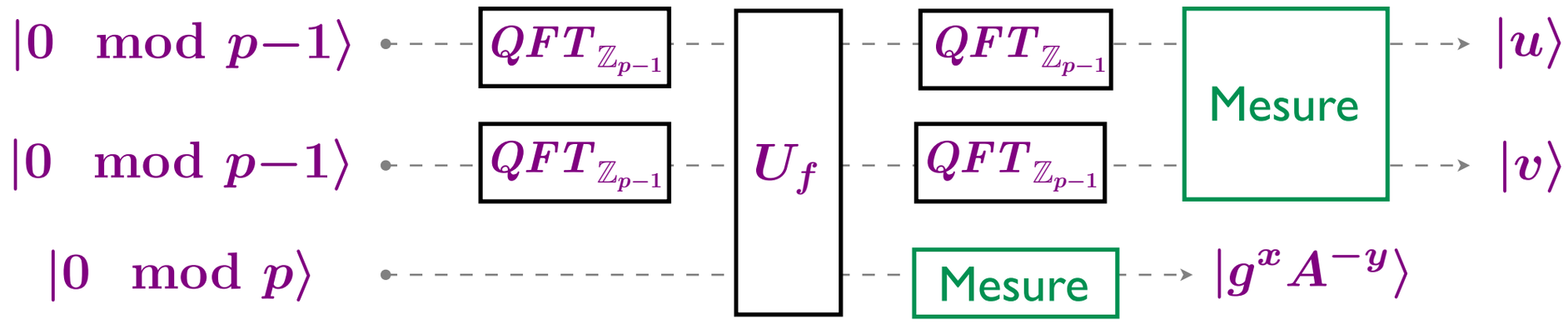
- Montre comment calculer Logarithme discret (sans oracle) *rapidement*

Applications et généralisation

- Attaque de l'Algorithme de Diffie-Hellman

  y compris sur des courbes elliptiques

Partie quantique



- Lorsque $A = g^a \mod p$,

  la fonction $f(x,y) = g^x A^{-y} = g^{x-ay}$ est strictement $(a,1)$ périodique

- La sortie (u,v) du circuit satisfait

  $$ua + v = 0 \mod (p-1)$$

Partie classique

- Si l'échantillon (u,v) vérifie

  si u inversible $\mod (p-1)$ alors $a = -v/u \mod (p-1)$

- Sinon on recommence quelque fois (au plus log p), ou on applique la technique précédente

Recherche de périodes sur des groupes complexes

(Problème dit du sous-groupe caché)

- Groupe symétrique : isomorphisme de graphes
- Nombres réels : équations de Pell-Fermat $(x^2 - ny^2 = m)$
- Isogénies…

Décompositions algébriques

- Décomposition de groupes “boîtes noires”
- Vérification de structures algébriques
- …

Transformées de Fourier

- Circuits quantiques pour de nombreux groupes

Estimation de phase

- D’autres applications à venir dans le cours et les séminaires

  Marches quantiques

  Résolution de systèmes linéaires

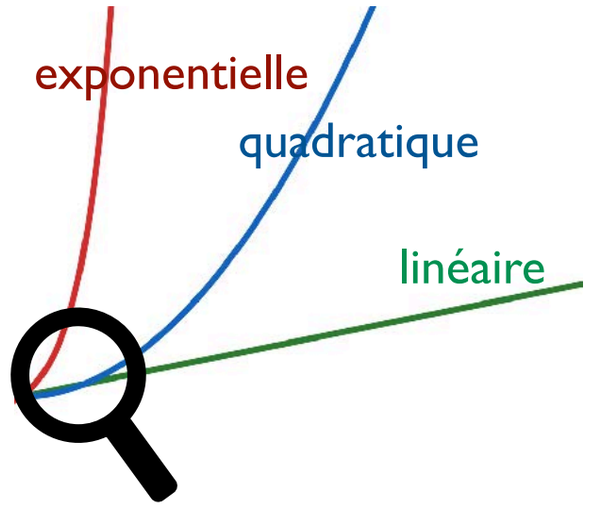
  Apprentissage quantique

Réalisable prochainement ?

A quand la supériorité quantique “utile” ?

Avantage asymptotique

- Plus les données sont grandes, plus l’avantage l’est aussi



Quelle taille nécessaire ?

- Algorithme de Shor

  Milliers de bits quantiques logiques (parfaits)

  ≈ millions de bits quantiques physiques (imparfaits)

  ≈ 1 méga-octet quantique !

Quelles prévisions ?

- Prévision à court terme

  Plusieurs centaines de bits quantiques physiques

- Mais des prévisions plus optimistes existent…

  Google & IBM : 1 000 qubits en 2023, 1 million vers 2030

Algorithmes

- Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer

  Peter W. Shor

- Fast parallel circuits for the quantum Fourier transform

  Richard Cleve, John Watrous

- Dihedral Hidden Subgroup Problem: A Survey

  Hirotada Kobayashi, François Le Gall

Programmation

- Qiskit

  https://qiskit.org/textbook/ch-algorithms/shor.html

Séminaire du cours !

- Le problème du sous-groupe caché

  avec Miklos Santha, CNRS, Paris / CQT, Singapour