Information, calcul, communication et cryptographie quantiques et leurs applications

Une introduction rapide et partielle

Dimitri Petritis

Institut de recherche mathématique
Université de Rennes 1 et CNRS (UMR 6625)

Lannion, 4 mai 2007

« Information quantique » le domaine scientifique décrivant les

- méthodes théoriques,
- algorithmes,
- protocoles expérimentaux,
- dispositifs physiques

utilisés pour

- coder,
- traiter,
- transporter,
- extraire,
- crypter

l'information basés sur des phénomènes quantiques ou inspirés du formalisme quantique

Le contexte scientifique

Domaine interdisciplinaire à la frontière de

- mathématiques (algèbre non-commutative, probabilités, logique, théorie des opérateurs),
- physique (mécanique quantique, mécanique statistique, théorie quantique des champs, optique quantique),
- informatique (calculabilité, complexité algorithme, automates, machines de Turing)
- ingénierie (électronique quantique, photonique, nanotechnologie).

Réalisations

Réalisations à des stades différents :

- Information : recherche mathématique (entropie quantique),
- Calcul : preuve de principe, recherche en laboratoire, (industrielle ?), algorithmes de factorisation, s
- Communication : codes correcteurs d'erreur quantiques, codage dense, téléportation et applications en authentification, transmission en fibre optique et en air libre,
- Cryptographie : stade pré-industriel (cf. SmartQuantum),
- Applications inspirées par formalisme quantique : linguistique (traduction automatique en tenant compte du contexte), distillation sémantique en génomique.

UNIVERSITÉ DE RENNES 1

Notions de base

- Alphabet : $\mathbb{A}$ ensemble fini, ex. $\mathbb{A} = \{a, \ldots, z\}$, binaire, symbolique, ...
- Language : partie de $\mathbb{A}^* = \cup_{n \in \mathbb{N}} \mathbb{A}^n$.
- Message : $m \in \mathbb{A}^*$.
- Chiffrement : $C : \mathbb{A}^* \to \mathbb{A}^*$.
- Déchiffrement : $D : \mathbb{A}^* \to \mathbb{A}^*$ t.q. $D \circ C(m) = m$.
- Exigence : transformation D facile à calculer mais très difficile à deviner.

UNIVERSITÉ DE RENNES 1

Une idée ancienne

Code de Vernam 1917

- $m = m_1 m_2 \cdots m_{|m|}$, avec $m_i \in \mathbb{A}$.
- $k = k_1 k_2 \cdots k_{|m|}$, avec $k_i \in \mathbb{A}$ aléatoirement choisies.
- $c = c_1 c_2 \cdots c_{|m|}$, avec $c_i = m_i + k_i \mod |\mathbb{A}|$.
- Les k_i sont des variables aléatoires indépendantes équidistribuées à valeurs sur $\mathbb{A}$.
  - Si on connaît k alors $m_i = c_i - k_i \mod |\mathbb{A}|$.
  - Sinon tous les $|\mathbb{A}|^{|m|}$ « messages » équiprobables !

`wewonthebattlebutwelostthewar`

`blattantvictoryagainstevilaxis`

Sécurité du code de Vernam

. . . où il faut trouver une aiguille dans une botte de foin

Théorème (Shannon (1949) :)

1. *Si k utilisée une seule fois (one-time-pad),*
2. *Si k_i vraiment aléatoires uniformément distribuées,*
3. *Si $|m|$ suffisamment long,*

Alors, le code de Vernam est « inviolable » dans le sens :

- *Tous les messages de longueur $|m|$ sont des « candidats » possibles pour m,*
- $\mathbb{E}\mathcal{T} \geq |\mathbb{A}|^{|m|}$.

Problèmes avec le code de Vernam

- Distribution de la clé.
- Production aléatoire.
- Stockage sécurisé de la clé.

Méthodes introduites par Rivest-Shamir-Adleman (1978) pour résoudre problème de distribution : basées sur la difficulté conjecturée de factoriser classiquement un grand entier.

Factorisation de grands entiers ...
... avec seulement deux facteurs premiers

p et q grands premiers, $N = pq$, $n = \log N$

- Débuts protocole RSA (1978), $\tau = \mathcal{O}(\exp(n))$.
- Lenstra-Lenstra (1997), $\tau = \mathcal{O}(\exp(n^{1/3}(\log n)^{2/3}))$.
- Shor (1994), si ordinateur quantique existait $\tau = \mathcal{O}(n^3)$.

Estimation grossière : 1 opération par nanoseconde, $n = 1000$

$\mathcal{O}(\exp(n))$	$\mathcal{O}(\exp(n^{1/3}(\log n)^{2/3}))$	$\mathcal{O}(n^3)$
10^{417} yr [1]	0.2 yr	1 s

[1] Pour mémoire : âge de l'univers 1.5×10^{10} yr

Postulat 1

L'espace de phases

Postulat (de l'espace des phases)

1. *L'espace des phases d'un système quantique est un espace de Hilbert complexe et séparable* $\mathbb{H}$.
2. *Vecteurs unitaires de* $\mathbb{H}$ *correspondent aux états quantiques purs.*
3. *Si un système est composé de deux sous-systèmes* $\mathbb{H}_1$ *et* $\mathbb{H}_2$ *l'espace des phases est* $\mathbb{H}_1 \otimes \mathbb{H}_2$.

Postulat 2

L'évolution temporelle

Postulat (de l'évolution temporelle)

Toute évolution temporelle d'un système quantique isolé est décrit par un opérateur unitaire qui agit sur $\mathbb{H}$.

Postulat 3

Les observables

Postulat (des observables)

1. *À toute observable physique, O_X, est associé un opérateur auto-adjoint X agissant sur l'espace des phases $\mathbb{H}$ du système.*
2. *Les questions « oui-non » associées aux projecteurs.*
3. *Toute mesure physique d'une observable représentée par opérateur auto-adjoint X dans état décrit pat vecteur unitaire ψ correspond à la mesure spectrale induite sur $\mathbb{R}$ par le produit scalaire $\langle \psi \,|\, X\psi \rangle$.*

Interprétation du postulat 1

- Cas non-trivial le plus simple $\mathbb{H} = \mathbb{C}^2$.
- $\forall f \in \mathbb{H}$:
$$f = f_1 \epsilon_1 + f_2 \epsilon_2$$
avec $f_1, f_2 \in \mathbb{C}$ et $\epsilon_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $\epsilon_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.
- Si $\|f\| \neq 0$, notons $\phi = \frac{f}{\|f\|} = \phi_1 \epsilon_1 + \phi_2 \epsilon_2$ l'état pur correspondant. Un tel état correspond à un qubit.
- $|\phi_1|^2 + |\phi_2|^2 = 1$, donc $|\phi_1|^2$ and $|\phi_2|^2$ définissent une probabilité sur l'ensemble des coordonnées $\{1, 2\}$.
- Les nombres complexes $\phi_1 = \langle \epsilon_1 \mid \phi \rangle$ et $\phi_2 = \langle \epsilon_2 \mid \phi \rangle$ sont des amplitudes complexes de probabilité.

Interprétation du postulat 2

- Un opérateur unitaire U sur $\mathbb{H}$ est matrice 2×2 vérifiant $UU^* = U^*U = I$.
- Si ϕ état pur, alors $\psi = U\phi$ vérifie $\|\psi\|^2 = \langle U\phi \mid U\phi \rangle = \langle \phi \mid U^*U\phi \rangle = \|\phi\|^2$. Par conséquent, l'évolution quantique préserve les états purs.
- U^* est aussi unitaire. Donc $\phi = U^*\psi$. L'évolution temporelle de tout système quantique isolé est réversible.

Interprétation du postulat 3

- Tout opérateur linéaire X admet décomposition spectrale $X = \int_{\mathrm{spec}(X)} \lambda P(d\lambda)$. Si X est auto-adjoint, alors $\mathrm{spec}(X) \subseteq \mathbb{R}$.
- Illustration : Pour $X = \begin{pmatrix} 1 & 2i \\ -2i & 2 \end{pmatrix}$, on a :

Valeurs propres λ	Vecteurs propres $u(\lambda)$	Projecteurs $P(\{\lambda\})$
-3	$\frac{1}{\sqrt{5}} \begin{pmatrix} -i \\ 2 \end{pmatrix}$	$\frac{1}{5} \begin{pmatrix} 1 & -2i \\ 2i & 4 \end{pmatrix}$
2	$\frac{1}{\sqrt{5}} \begin{pmatrix} 2i \\ 1 \end{pmatrix}$	$\frac{1}{5} \begin{pmatrix} 4 & 2i \\ -2i & 1 \end{pmatrix}$

- Donc

$$\begin{aligned} X &= \sum_{\lambda \in \{-3,2\}} \lambda P(\{\lambda\}) \\ &= (-3)\frac{1}{5} \begin{pmatrix} 1 & -2i \\ 2i & 4 \end{pmatrix} + 2\frac{1}{5} \begin{pmatrix} 4 & 2i \\ -2i & 1 \end{pmatrix}. \end{aligned}$$

UNIVERSITÉ DE RENNES 1

Interprétation du postulat 3 (bis)

- Opérateurs $P(\{-3\})$ et $P(\{2\})$ correspondent à des observables binaires.
- Soit $\psi \in \mathbb{H}$ état pur ; comme $u(-3)$ et $u(2)$ orthonormaux $\psi = \alpha_{-3} u(-3) + \alpha_2 u(2)$, avec $\|\psi\|^2 = |\alpha_{-3}|^2 + |\alpha_2|^2 = 1$.
- $$\begin{aligned} \langle\, \psi \,|\, X\psi \,\rangle &= \sum_{\lambda,\lambda',\lambda''} \alpha^*_\lambda \alpha_{\lambda''} \lambda' \langle\, u(\lambda) \,|\, P(\lambda') u(\lambda'') \,\rangle \\ &= \sum_{\lambda \in \mathrm{spec}(X)} \lambda |\alpha_\lambda|^2. \end{aligned}$$

Interprétation du postulat 3 (ter)

- $(|\alpha_\lambda|^2)_{\lambda \in \mathrm{spec}(X)}$ interprété comme probabilité sur l'ensemble de valeurs spectrales.
- $\langle \psi \,|\, X\psi \rangle$ est l'espérance de valeurs spectrales par rapport à la décomposition de ψ sur la base de vecteurs propres.
- Pour variable aléatoire classique X prenant des valeurs dans $\{x_1, \ldots, x_n\}$ avec probabilités $p_1, \ldots, p_n$,

$$\begin{aligned}\mathbb{E}X &= \sum_{i=1}^{n} x_i p_i = \sum_{i=1}^{n} \sqrt{p_i} x_i \sqrt{p_i} \\ &= \sum_{i=1}^{n} \sqrt{p_i} \exp(-i\theta_i) x_i \sqrt{p_i} \exp(i\theta_i),\end{aligned}$$

avec $\theta_i \in \mathbb{R}, i = 1, \ldots, n$ arbitraire.

Interprétation du postulat 3 (quater)

- Classiquement $\mathbb{E}X = \langle \psi \,|\, X\psi \rangle$ avec $\psi = \begin{pmatrix} \sqrt{p_1}\exp(i\theta_1) \\ \vdots \\ \sqrt{p_n}\exp(i\theta_n) \end{pmatrix}$, vérifiant $\|\psi\| = 1$ et avec $X = \begin{pmatrix} x_1 & & 0 \\ & \ddots & \\ 0 & & x_n \end{pmatrix}$.
- Physique classique équivalente
  - aux probabilités classiques
  - à la physique quantique avec opérateurs auto-adjoints diagonaux.
- Physique quantique est généralisation non-commutative de physique classique et des probabilités classiques.

Mesure physique
Où observer perturbe

- $$f_\lambda = P(\{\lambda\})\psi = \begin{cases} \langle\, u(\lambda) \,|\, \psi \,\rangle u(\lambda) & \text{si } \lambda \in \mathrm{spec}(X) \\ 0 & \text{sinon.} \end{cases}$$
- État pur correspondant : $\phi_\lambda = \frac{P(\{\lambda\})\psi}{\|P(\{\lambda\})\psi\|}$ (bien défini si $\lambda \in \mathrm{spec}(X)$) a interprétation très spéciale :
- « l'observable physique O_X prend-elle la valeur -3 ? ». Comme en cas classique, réponse probabiliste : $\mathbb{P}(\{O_X = -3\}) = |\alpha_{-3}|^2 = \langle\, f_{-3} \,|\, f_{-3} \,\rangle = \|P(\{-3\})\psi\|^2$.
- Une fois question posée, l'état ψ projeté sur l'espace propre $P(\{-3\})\mathbb{H}$ et représenté par l'état ϕ_{-3}.
- Poser une question sur système entraîne un changement irréversible de son état !

Notation de Dirac

Notation usuelle	Notation de Dirac
Base orthonormée $(e_1, \ldots, e_n)$	n symboles, ex. $\{1, \ldots, n\}$ $\|1\rangle, \ldots \|n\rangle$
$\psi = \sum_i \psi_i e_i$ $\langle \phi \| \psi \rangle = \sum \overline{\phi}_i \psi_i$	$\|\psi\rangle = \sum_i \psi_i \|i\rangle$ $\langle \phi \| \psi \rangle = \sum \overline{\phi}_i \psi_i$
$\mathbb{H}^* = \{f : \mathbb{H} \to \mathbb{C}, \text{linéaire}\}$ $\dagger : \mathbb{H} \to \mathbb{H}^*$ $\dagger : \phi \mapsto f_\phi(\cdot) = \langle \phi \| \cdot \rangle$ $\langle \phi \| \psi \rangle = f_\phi(\psi)$	$\mathbb{H}^* = \{f : \mathbb{H} \to \mathbb{C}, \text{linéaire}\}$ $\dagger : \mathbb{H} \to \mathbb{H}^*$ $\dagger : \|\phi\rangle \mapsto \langle \phi \|$ $\langle \phi \| \psi \rangle = \langle \phi \| \| \psi \rangle$
$X = X^*$ $\langle \phi \| X\psi \rangle = \langle X^* \phi \| \psi \rangle = \langle X\phi \| \psi \rangle$	$X = X^*$ $\langle \phi \| X \| \psi \rangle$
$Xu(\lambda_i) = \lambda_i u(\lambda_i)$ $P(\{\lambda_i\})$ Projecteur $X = \sum_i \lambda_i P(\{\lambda_i\})$	$X\|\lambda_i\rangle = \lambda_i \|\lambda_i\rangle$ $\|\lambda_i\rangle\langle \lambda_i \|$ $X = \sum_i \lambda_i \|\lambda_i\rangle\langle \lambda_i \|$

UNIVERSITÉ DE RENNES 1

Non-clonage des états quantiques

Il n'existe pas de … « photocopieur » quantique

Théorème

Soient $|\phi\rangle$ *et* $|\psi\rangle$ *deux vecteurs unitaires de* $\mathbb{H}$ *tels que* $\langle\phi|\psi\rangle \neq 0$ *et* $|\phi\rangle \neq \exp(i\theta)|\psi\rangle$*. Alors, il n'existe pas d'appareil quantique permettant la duplication de* ϕ *et* ψ*.*

- Joue rôle crucial dans tous protocoles (BB84, B92, EPR) de distribution quantique de clé.
- Seul protocole de Bennett et Brassard (1984) présenté car
  - Prototypes pré-industriels disponibles pour environ 5000 EUR,
  - pédagogiquement, les mêmes idées dans tous les protocoles.

Les ressources d'Aisha et Boubakar

Des qubits, des photons et des fibres optiques

- Communication à travers canaux publics quantique et classique
- Deux bases orthonormales de $\mathbb{H} = \mathbb{C}^2$

$$
\begin{aligned}
B_+ &= \{\epsilon_0^+ = |\,0\,\rangle, \epsilon_1^+ = |\,1\,\rangle\} \\
B_\times &= \{\epsilon_0^\times = \frac{|\,0\,\rangle - |\,1\,\rangle}{\sqrt{2}}, \epsilon_1^\times = \frac{|\,0\,\rangle + |\,1\,\rangle}{\sqrt{2}}\}.
\end{aligned}
$$

- Premier élément de chaque base bit 0 ; second élément bit 1
- Un dispositif préparant polarisation des états photoniques

$$
T(x,y) = \begin{cases} \epsilon_0^+ & \text{if } (x,y) = (0,0) \\ \epsilon_1^+ & \text{if } (x,y) = (0,1) \\ \epsilon_0^\times & \text{if } (x,y) = (1,0) \\ \epsilon_1^\times & \text{if } (x,y) = (1,1). \end{cases}
$$

Algorithme

GénérationCléAisha

Requiert: GÉNÉRATEURALÉATOIREUNIF($\{0,1\}$), T, n

Retourne: Deux chaînes de n bits aléatoires $\mathbf{a}, \mathbf{b} \in \{0,1\}^n$ et une suite de n qubits $(|\,\psi_i\,\rangle)_{i=1,\ldots,n}$

Générer aléatoirement $a_1, \ldots, a_n$

$\mathbf{a} \leftarrow (a_1, \ldots, a_n) \in \{0,1\}^n$

Générer aléatoirement $b_1, \ldots, b_n$

$\mathbf{b} \leftarrow (b_1, \ldots, b_n) \in \{0,1\}^n$

$i \leftarrow 1$

répéter

  $|\,\psi_i\,\rangle \leftarrow T(b_i, a_i)$

  Transmettre $|\,\psi_i\,\rangle$ à Boubakar à travers le canal public quantique

  $i \leftarrow i+1$

jusqu'à $i > n$

Algorithme

GénérationCléBoubakar

Requiert: GÉNÉRATEURALÉATOIREUNIF($\{0,1\}$), n, suite $|\psi_i\rangle$ for $i = 1, \ldots, n$, $P^\sharp$ for $\sharp \in \{+, \times\}$
Retourne: Deux chaînes de n bits $\mathbf{a}', \mathbf{b}' \in \{0,1\}^n$

Générer aléatoirement $b'_1, \ldots, b'_n$
$\mathbf{b}' \leftarrow (b'_1, \ldots, b'_n) \in \{0,1\}^n$
$i \leftarrow 1$
répéter
  si $b'_i = 0$ **alors**
    P^+ prend-il la valeur 1 ?
  sinon
    $P^\times$ prend-il la valeur 1 ?
  fin si
  si oui **alors**
    $a'_i \leftarrow 1$
  sinon
    $a'_i \leftarrow 0$
  fin si
  $i \leftarrow i + 1$
jusqu'à $i > n$
$\mathbf{a}' \leftarrow (a'_1, \ldots, a'_n) \in \{0,1\}^n$
Transmettre chaîne $\mathbf{b}' \in \{0,1\}^n$ à Aisha via canal public classique

Algorithme

Conciliation

Requiert: Chaînes $\mathbf{b}, \mathbf{b}' \in \{0, 1\}$

Retourne: Suite $(k_1, \ldots, k_L)$ avec $L \leq n$ contenant les positions de coïncidence

$\mathbf{c} \leftarrow \mathbf{b} \oplus \mathbf{b}'$
$i \leftarrow 1$
$k \leftarrow 1$
répéter
  $k \leftarrow \min\{j : k \leq j \leq n \text{ tel que } c_j = 0\}$
  si $k \leq n$ **alors**
    $k_i \leftarrow k$
    $i \leftarrow i + 1$
  fin si
jusqu'à $k > n$
$L \leftarrow i - 1$
Transmettre $(k_1, \ldots, k_L)$ à Boubakar via le canal public classique

Théorème

Si pas d'écoute sur canal quantique alors

$$\mathbb{P}((a'_{k_1}, \ldots, a'_{k_L}) = (a_{k_1}, \ldots, a_{k_L}) | \mathbf{a}, \mathbf{b}) = 1.$$

Démonstration :

- Calculer $\langle \psi_i \,|\, P^+ \psi_i \rangle$ et $\langle \psi_i \,|\, P^\times \psi_i \rangle$ pour choix différents de $\psi_i \in B^+ \cup B^\times$.
- Observer que pour les i t.q. $b'_i = b_i$, on a $\mathbb{P}(a'_i = a_i) = 1$.
- Si uniquement sous-chaînes de $\mathbf{a}$ et de $\mathbf{a}'$ où $\mathbf{b}$ et $\mathbf{b}'$ coïncident, certitude de partager des sous-chaînes rigoureusement identiques malgré le fait que $\mathbf{a}$ et $\mathbf{a}'$ n'ont jamais été échangés.

Lemme

S'il n'y a pas d'écoute sur le canal quantique, alors pour N suffisamment grand L est d'ordre $2N$.

Démonstration : Utilisation élémentaire de la loi forte de grands nombres.

Écoute indésirable

- Si Ève écoute illicitement, elle ne peut pas copier états quantiques arbitraires (théorème de non clonage).
- elle peut mesurer selon la même procédure que Boubakar ; elle re-émet une suite de qubits $|\,\tilde{\psi}_i\,\rangle$ à Boubakar.
- De nouveau L est d'ordre $2N$ mais puisque choix d'Ève indépendants d'Aisha et Boubakar, chaîne $\mathbf{a}'$ calculée par Boubakar coïncidera avec chaîne $\mathbf{a}$ d'Aisha sur seulement $L/2 \simeq N$ positions.
- Pour établir communication sure, Aisha et Boubakar doivent effectuer un test d'écoute illicite et de réconciliation.

UNIVERSITÉ DE RENNES 1

Établissement de la clé

- Boubakar choisit aléatoirement moitié des bits de la sous-chaîne $(a'_{k_1}, \ldots, a'_{k_L})$, i.e. $(a'_{r_1}, \ldots, a'_{r_{L/2}})$ avec $r_i \in \{k_1, \ldots, k_L\}$ et $r_i \neq r_j$ pour $i \neq j$.
- Il envoie à Aisha positions ainsi choisies $(r_1, \ldots, r_{L/2})$ ainsi que valeurs des bits correspondant $(a'_{r_1}, \ldots, a'_{r_{L/2}})$.
- Si $(a'_{r_1}, \ldots, a'_{r_{L/2}}) = (a_{r_1}, \ldots, a_{r_{L/2}})$ (réconciliation)
  - alors Aisha annonce ce fait à Boubakar et ils utilisent alors sous-chaîne complémentaire (de longueur $L/2 \simeq N$) qui n'a jamais été échangée comme clé de chiffrement de l'algorithme de Vernam.
  - Sinon, ils recommencent le protocole BB84.

Distillation sémantique quantique

Position du problème : appartenance floue de documents dans un ensemble indexé par des attributs.

- Espace abstrait de concepts = espace de Hilbert, $\mathcal{H}$, libre sur l'ensemble des attributs.
- Tout document codé par un vecteur de $\mathcal{H}$.
- Graphe pondéré : ensemble de vertex = documents ; poids des arêtes = fonction de la distance hilbertienne.
- Laplacien pondéré sur le graphe.
- Sous-espace propre du Laplacien associé aux premières valeurs propres.
- Re-étiquettage des ensembles de documents et d'attributs permettant la partition de l'ensemble des attributs.
- Projection sur le sous-espace hilbertien libre sur l'un des sous-ensemble d'attributs = distillation sémantique.
- Détermination de l'appartenance floue des documents dans des ensembles indexés par les sous-ensembles d'attributs.