Cryptographie quantique

Une introduction élémentaire

Dimitri Petritis

UFR de mathématiques
Université de Rennes 1 et CNRS (UMR 6625)

Rennes, le 4 octobre 2018

Plan du cours
Fondements

1. Brève histoire des sciences.
   - Informatique : de la machine de Babbage à Xeon E3-1230.
   - Physique : ≤ 1900, > 1900.
   - Les enseignements de l'histoire.
   - Bref aperçu des quelques phénomènes quantiques contre-intuitifs.
2. Postulats de la mécanique classique.
   - Modèle statistique.
   - Réductibilité de l'aléa classique ; insuffisance de la description classique.
3. Postulats de la mécanique quantique.
   - Illustration par modèle simple.
   - Le rôle de l'espace de Hilbert.
4. Quelques notions hilbertiennes.
   - Classes d'opérateurs ; théorème spectral.
   - Produit tensoriel ; trace partielle ; intrication ; marginales quantiques.
   - Irréductibilité de l'aléa quantique.
   - Opérateurs complètement positifs ; PVP et mesures franches ; POVP et mesures floues.

Plan du cours
Applications

5. Principes de cryptographie quantique.
   - Étude détaillé du protocole BB84.
   - Analyse des effets d'intrusion ; gain d'information / perturbation.
   - Autres protocoles.
6. Communication quantique.
   - Téléportation ; codage dense.
   - Codes correcteurs d'erreur quantiques.
7. Calcul quantique.
   - Portes quantiques et calcul réversible.
   - Algorithme quantique de Shor pour la factorisation en premiers.
   - Algorithmes quantiques pour des courbes elliptiques.

UNIVERSITÉ DE RENNES 1

La position du problème

- Des pans entiers de l'activité scientifique (et plus généralement humaine) reposent sur
  - l'extraction,
  - le traitement,
  - la transmission et
  - **la protection**

  de l'information.
- On raisonne sur des **catégories abstraites** : portes logiques, opérations logiques, fonctions booléennes, etc. Car nous pouvons **et pour quelque temps encore** le faire !
- Mais toutes les opérations logiques sur **substrat physique**.
- Information véhiculée par **vecteur** physique. Nous devons de nouveau nous intéresser au substrat physique.

UNIVERSITÉ DE RENNES 1

La pré-histoire

Avant la . . . révolution ($\leq$ 1946)

Charles Babbage (Londres 1791– Londres 1871) inventa la machine à calculer et imprimer les valeurs des polynômes ; fonctionna avec des cartes perforées sur le modèle des métiers à tisser de Joseph Marie Jacquard.

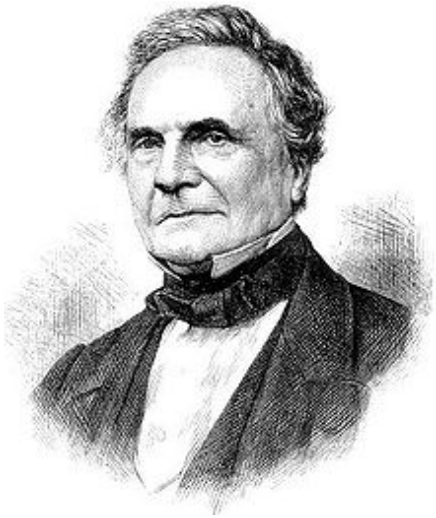


Figure: Charles Babbage et . . . sa source d'inspiration : le métier à tisser de Jacquard.

La pré-histoire
La machine analytique de Babbage

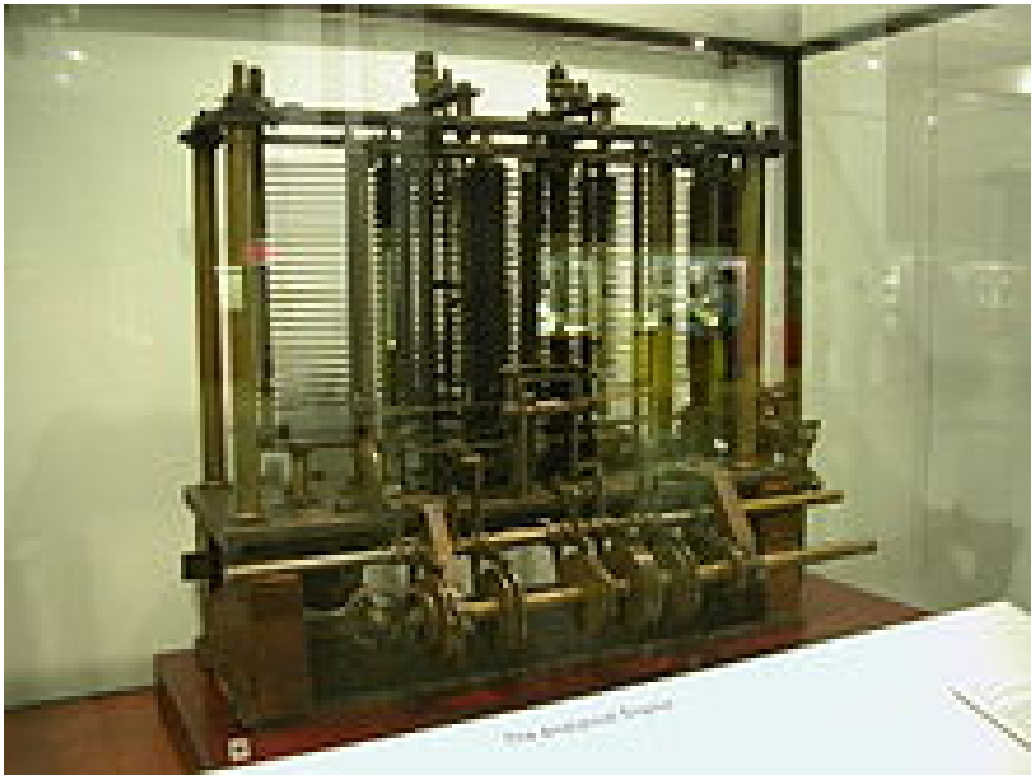


Figure: La machine analytique construite par Babbage et les cartes perforées nécessaires pour sa programmation.

La pré-histoire

La programmation de la machine de Babbage

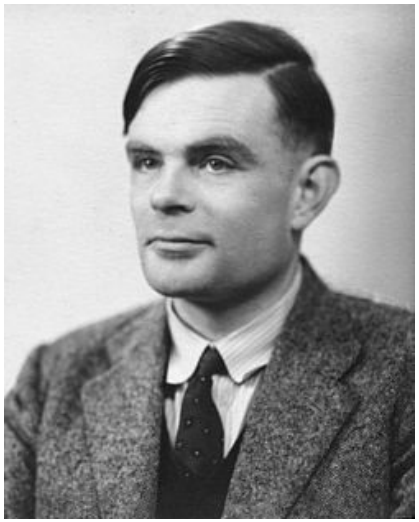
Augusta Ada King, comtesse de Lovelace, née Ada Byron (Londres 1815 – Londres 1852) rédige méthode de calcul des nombres de Bernoulli (B_n)

$$S_m(n) = \sum_{k=1}^{n} k^m = \frac{1}{m+1} \sum_{k=0}^{m} C_{m+1}^{k} B_k n^{m+1-k}.$$

Premier algorithme conçu pour être exécuté sur machine (de Babbage).

La pré-histoire
Les travaux de Turing

Alan Mathison Turing (Londres 1912 – Cheshire 1954), mathématicien, logicien, cryptanalyste et informaticien (avant l'heure !) qui cassa le code de cryptage Enigma utilisé par les sous-marins allemands pendant la guerre à l'aide de la machine « bombe ».



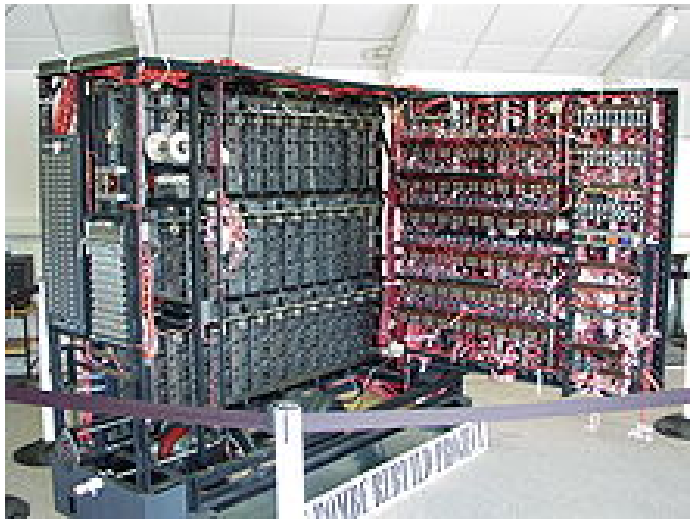


Figure: Alan Turing et une d'environ 200 répliques de la « bombe ».

La proto-histoire ($\simeq$ 1946)

Les travaux de von Neumann

Margittai Neumann János Lajos Budapest 1903 – **John von Neumann** Princeton 1954, mathématicien et physicien avec des contributions essentielles en mécanique quantique, analyse fonctionnelle, théorie des ensembles, informatique, sciences économiques ainsi que dans beaucoup d'autres domaines des mathématiques et de la physique. Il a participé aux programmes militaires américains.

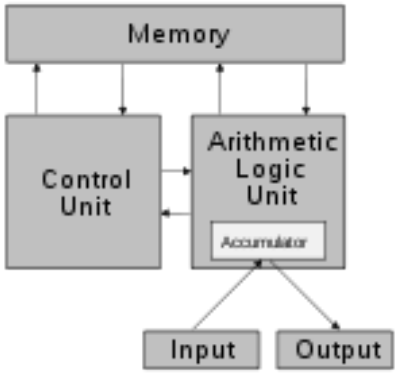


Figure: John von Neumann et un schéma de l'architecture qui porte son nom.

La proto-histoire ($\simeq$ 1946)

- Il fut un temps où l'on devait se soucier du substrat physique !
- 1946 : Electronic numerical integrator and computer (ENIAC) premier ordinateur universel construit par l'ingénieur John Adam Presper Eckert Jr. (Philadelphia, PA, 1919 – Bryn Mawr, PA, 1995) et le physicien John William Mauchly (Cincinatti, OH, 1907 – Ambler, PA, 1980).
  - 19000 tubes cathodiques
  - masse 30 tonnes
  - 72m^2 d'emprise au sol
  - puissance électrique 140kW
  - fréquence d'horloge 100kHz (330 multiplications par seconde).

UNIVERSITÉ DE RENNES 1

1946 : ENIAC

Un aperçu de la salle machine

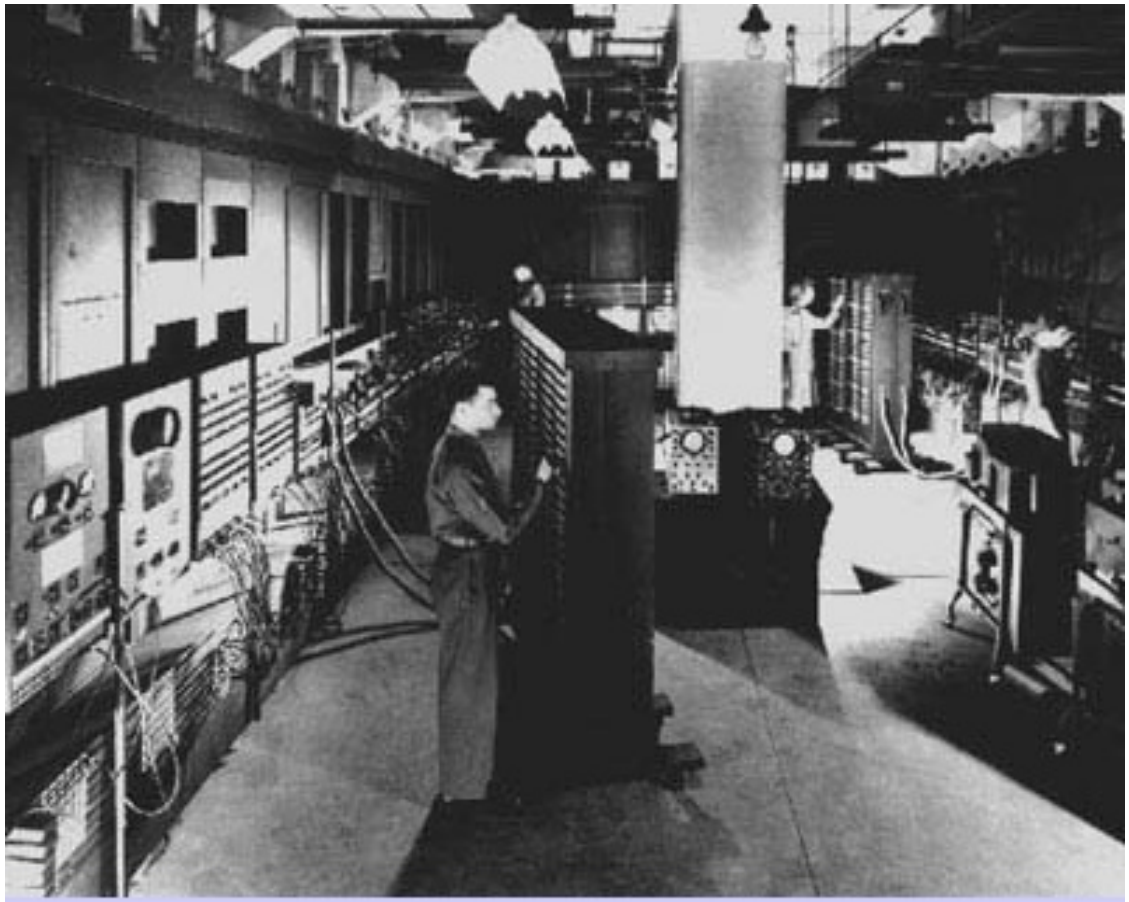


Figure: La salle machine de l'ENIAC.

1946 : ENIAC

Son pouponnage

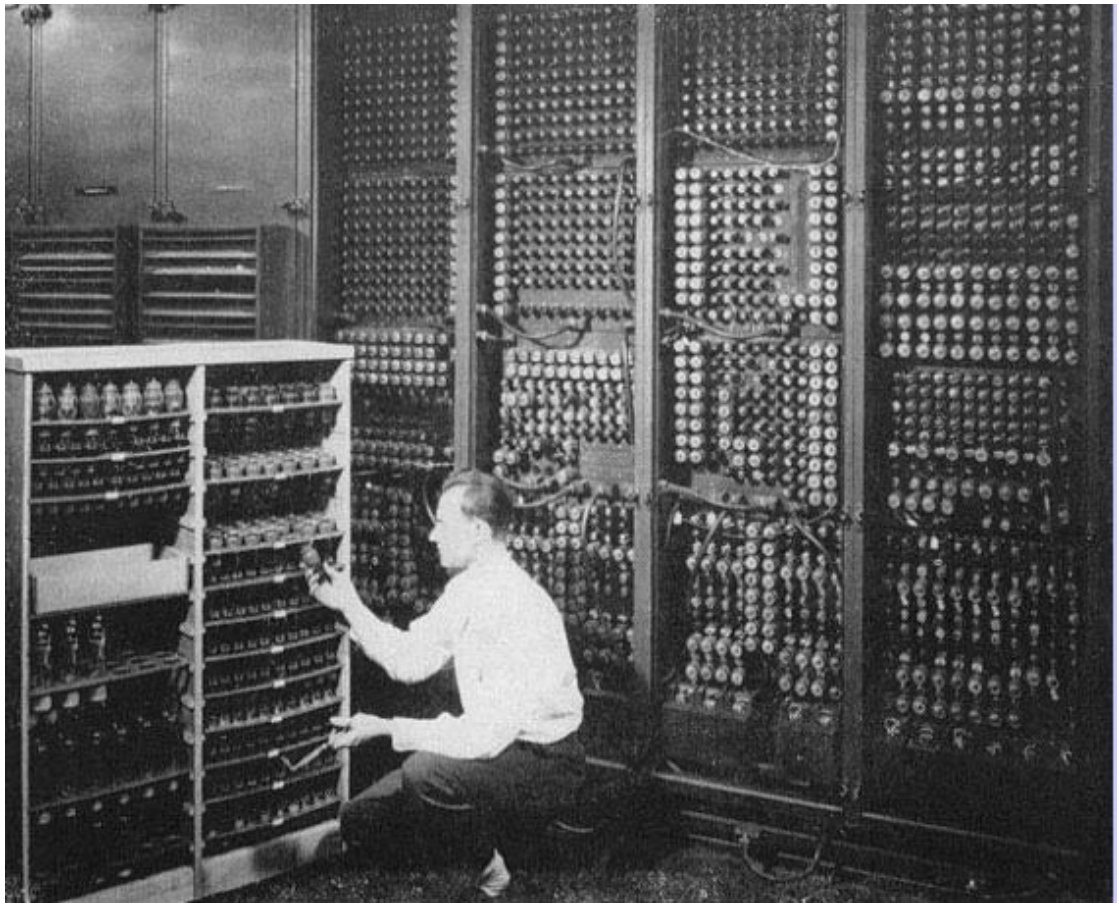


Figure: Un technicien en train de changer un des 19000 tubes de l'ENIAC.

1946 : ENIAC
Sa programmation

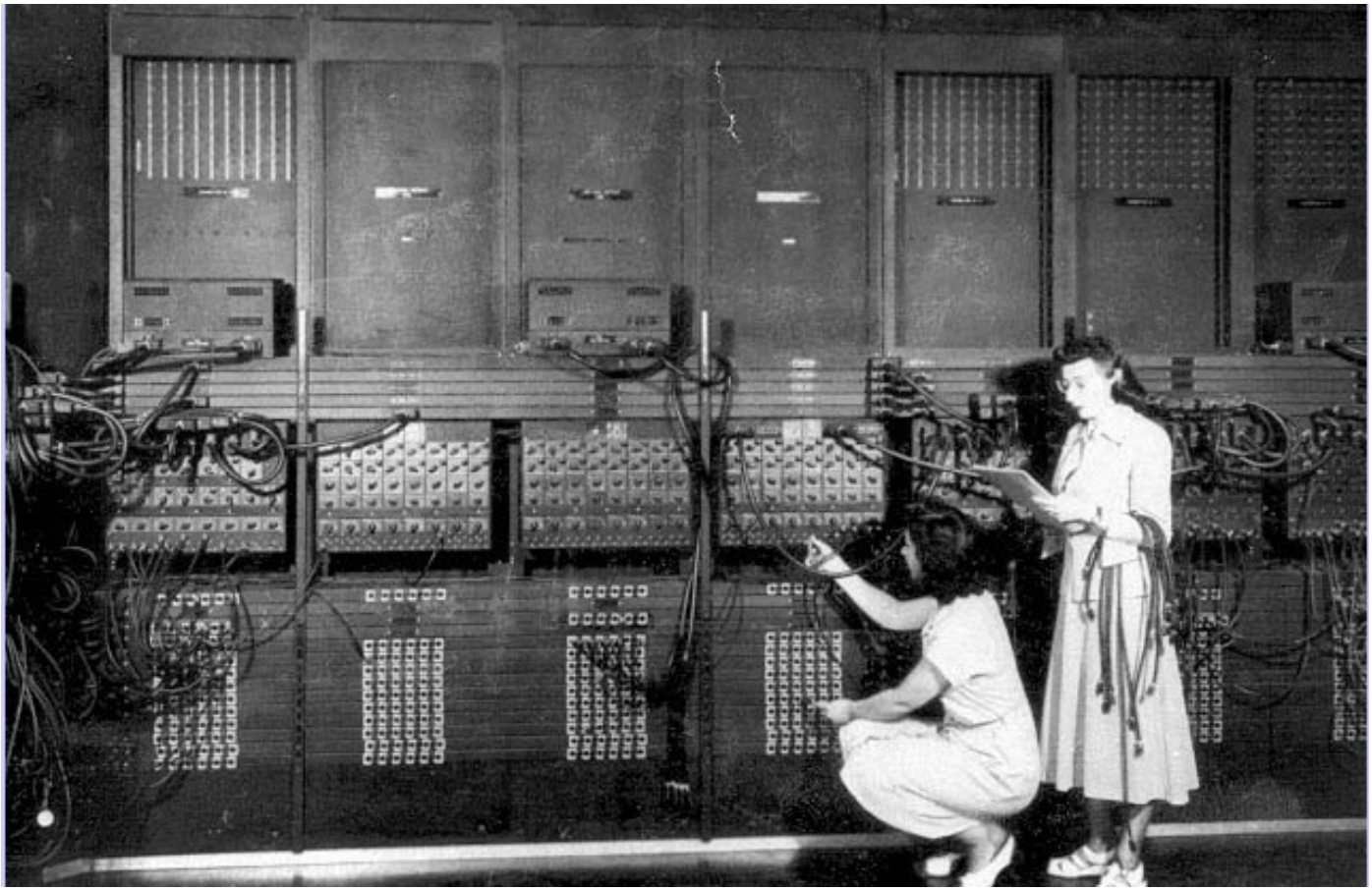


Figure: Deux opératrices en train de . . . programmer l'ENIAC.

1946 : ENIAC

Sa programmation est maintenant finie . . .

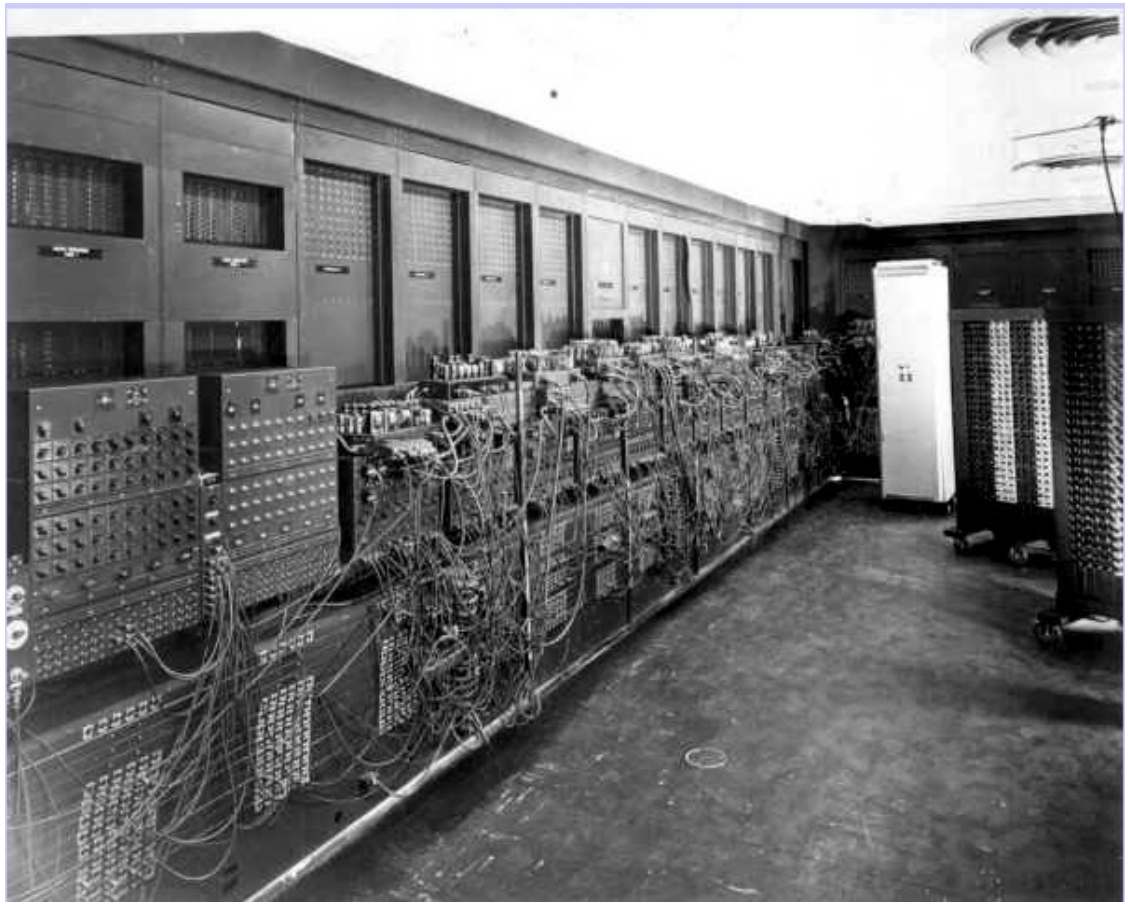


Figure: Ça y est, la programmation est maintenant finie !

L'histoire
1947

Décembre 1947 : Invention du transistor par les physiciens **William Bradford Shockley** (Londres 1910 – Palo Alto, CA 1989), **Walter Houser Brattain** (Amoy, Chine, 1902 – Seattle, WA, 1987) et **John Bardeen** (Madison, WI, 1908 – Boston, MA, 1991) dans les laboratoires de Bell Telephon.

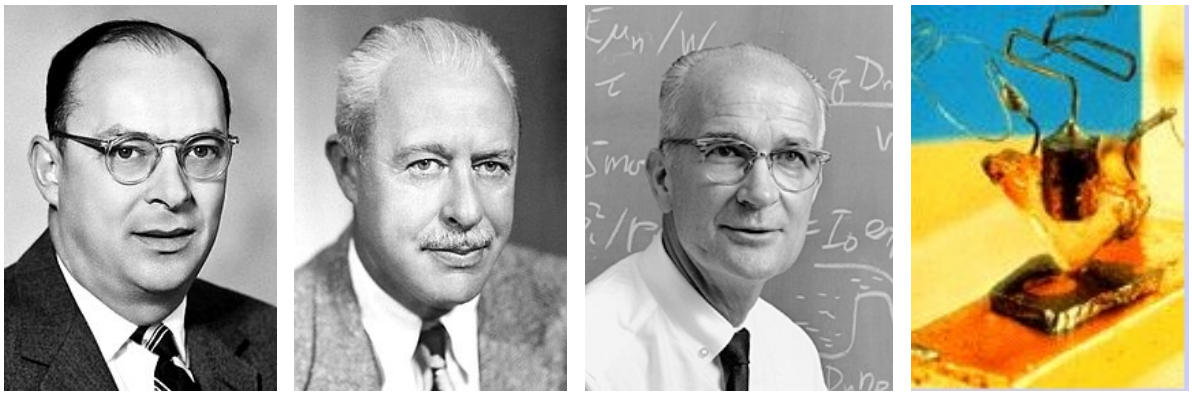


Figure: Bardeen, Brattain et Shockley et un accident de laboratoire qui ne tardera à être utilisé en informatique : le transistor !

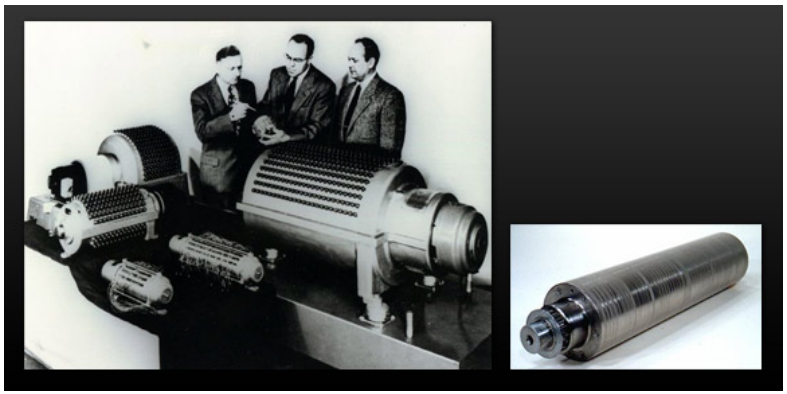
L'histoire
1947–1950

- Janvier 1948 : Wallace Eckert de chez IBM et son équipe terminent le SSEC (Selective Sequence Electronic Calculator).
- Juin 1948 : NewMan, Williams et leur équipe de l'université de Manchester terminent une machine prototype appelée Manchester Mark I.
- Août 1949 : P. Eckert et J. Mauchly, ayant formé leur propre compagnie, mettent au point le premier ordinateur bi-processeur : le BINAC pour l'US Navy. Les deux processeurs effectuaient les mêmes opérations en parallèle pour augmenter la fiabilité des calculs.
- 1950 : Le calculateur de Konrad Zuse, le Z4 fabriqué pendant la guerre, est finalement remonté à l'école polytechnique de Zurich puis modifié pour pouvoir réaliser des sauts et branchements conditionnels.

UNIVERSITÉ DE RENNES 1

L'histoire
1950–1951

- 1950 : Assembleur, inventé par Maurice V. Wilkes de l'université de Cambridge, remplace le binaire.
- Janvier 1951 : Création du premier ordinateur soviétique MESM sous la direction de Sergei Alexeevich Lebedev à l'académie des Sciences d'Ukraine.
- 1951 : Mise au point du tambour de masse magnétique ERA 1101.



Première mémoire de masse de 1 Mbit.

- 1951 : P. Eckert et J. Mauchly lancent l'UNIVAC I (UNIversal Automatic Computer). Premier ordinateur commercial. 8333 additions ou 555 multiplications par seconde. 56 exemplaires vendus. Prix catalogue :
  - Ordinateur : 750 000 USD (1951) = 7 163 269 USD (2018),
  - Imprimante rapide : 185 000 USD (1951) = 1 766 932 USD (2018).

UNIVERSITÉ DE RENNES 1

L'histoire
1952–1955

- 1952 : IBM produit l'IBM 701 pour la défense américaine (19 exemplaires produits). Mémoire à tubes cathodiques de 2048 ou 4096 mots de 36 bits et 16000 additions ou 2200 multiplications par seconde. La première machine sera installée à Los Alamos pour le projet de bombe thermo-nucléaire US.
- 1952 : Le premier ordinateur français, le CUBA (Calculateur Universel Binaire de l'Armement), est construit par la société SEA.
- Juillet 1953 : IBM premier ordinateur commercial en série : l'IBM 650, conçu pour être compatible avec les machines de comptabilité mécanique à cartes perforées de la marque.
- 1955 : Premier réseau informatique à but commercial : SABRE (Semi Automated Business Related Environment) réalisé par IBM, relie 1200 téléscripteurs à travers les États-Unis pour la réservation des vols de la compagnie American Airlines.
- 1955 : IBM 704 développé par Gene Amdahl. Première machine commerciale disposant d'un coprocesseur mathématique. Puissance : 5 kflops (milliers d'opérations en virgule flottante par seconde). Machine très . . . fiable ne tombant en panne qu'une fois par . . . semaine.

UNIVERSITÉ DE RENNES 1

La première révolution = la deuxième génération

1956-1970 : l'ère du transistor

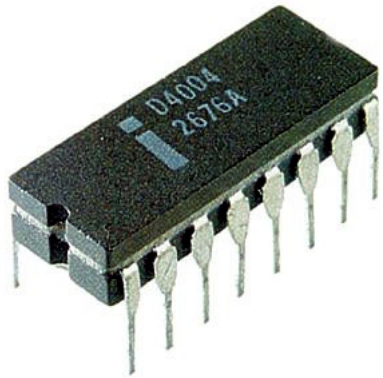
- 1956 : Premier ordinateur à transistors par la Bell : le TRADIC qui amorce la seconde génération d'ordinateurs.
- 1958 : Lancement du premier ordinateur commercial entièrement transistorisé, le CDC 1604, développé par Seymour Cray.
- 1959 : Démonstration du premier circuit intégré crée par Texas Instruments.
- 1961 : Le projet MAC (Multi Access Computer) du MIT dirigé par John Mc Carthy. But : permettre à plusieurs personnes de travailler sur un même ordinateur.
- 1970 : Première puce mémoire créée par Intel et contenant l'équivalent de 1024 tores de ferrite très encombrants sur un carré de 0.5mm de côté (capacité : 1kBit soit 128 octets).

UNIVERSITÉ DE RENNES 1

La deuxième révolution = a troisième génération

1971-aujourd'hui : l'ère du microprocesseur

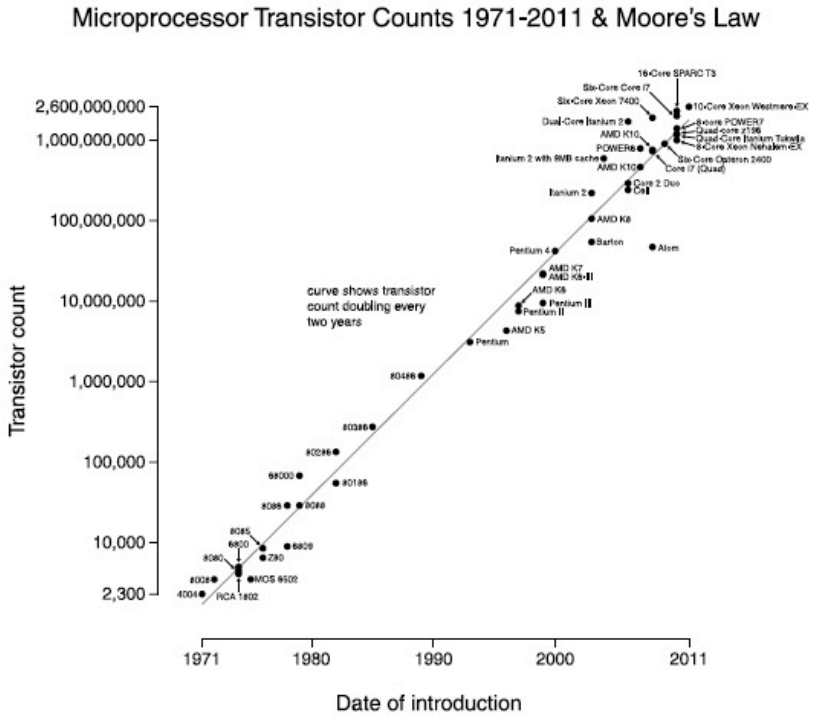
- Novembre 1971 : Intel met en vente le premier microprocesseur Intel 4004 conçu par Marcian Hoff.
  - Processeur 4 bits tournant à 108 KHz,
  - Permet d'adresser 640 octets de mémoire,
  - 60000 instructions par seconde,
  - 2300 transistors en technologie 10 microns,
  - Prix catalogue : 200 USD (1971) = 1 239 USD (2018).

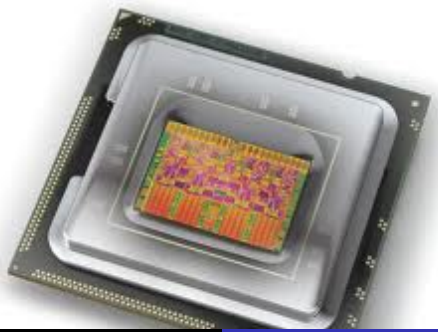


UNIVERSITÉ DE RENNES 1

Les « 46 glorieuses » . . .

. . . ou le temps béni à un taux de croissance annuelle de 41%





Processor	Transistor count	Year	Designer	Process	Area
Intel 4004	2 300	1971	Intel	10 000 nm	12 mm²
Intel 8008	3 500	1972	Intel	10 000 nm	14 mm²
Motorola 6800	4 100	1974	Motorola	6 000 nm	16 mm²
Intel 8080	4 500	1974	Intel	6 000 nm	20 mm²
RCA 1802	5 000	1974	RCA	5 000 nm	27 mm²
MOS Technology 6502	3 510	1975	MOS Technology	8 000 nm	21 mm²
Intel 8085	6 500	1976	Intel	3 000 nm	20 mm²
Zilog Z80	8 500	1976	Zilog	4 000 nm	18 mm²
Motorola 6809	9 000	1978	Motorola	5 000 nm	21 mm²
Intel 8086	29 000	1978	Intel	3 000 nm	33 mm²
Intel 8088	29 000	1979	Intel	3 000 nm	33 mm²
Motorola 68000	68 000	1979	Motorola	3 500 nm	44 mm²
WDC 65C02	11 500	1981	WDC	3 000 nm	6 mm²
Intel 80186	55 000	1982	Intel	3 000 nm	60 mm²
Intel 80286	134 000	1982	Intel	1 500 nm	49 mm²
WDC 65C816	22 000	1983	WDC		9 mm²
Motorola 68020	190 000	1984	Motorola	2 000 nm	85 mm²
Intel 80386	275 000	1985	Intel	1 500 nm	104 mm²
MultiTitan	180 000	1988	DEC WRL	1 500 nm	61 mm²
Intel 80486	1 180 235	1989	Intel	1 000 nm	173 mm²
R4000	1 350 000	1991	MIPS	1 000 nm	213 mm²
Pentium	3 100 000	1993	Intel	800 nm	294 mm²
SA-110	2 500 000	1995	Acorn/DEC/Apple	350 nm	50 mm²
Pentium Pro	5 500 000	1995	Intel	500 nm	307 mm²
AMD K5	4 300 000	1996	AMD	500 nm	251 mm²
Pentium II Klamath	7 500 000	1997	Intel	350 nm	195 mm²
AMD K6	8 800 000	1997	AMD	350 nm	162 mm²
Pentium II Deschutes	7 500 000	1998	Intel	250 nm	113 mm²
Pentium III Katmai	9 500 000	1999	Intel	250 nm	128 mm²
Pentium II Mobile Dixon	27 400 000	1999	Intel	180 nm	180 mm²
Pentium III Coppermine	21 000 000	2000	Intel	180 nm	80 mm²
Pentium 4 Willamette	42 000 000	2000	Intel	180 nm	217 mm²
Pentium III Tualatin	45 000 000	2001	Intel	130 nm	81 mm²
Pentium 4 Northwood	55 000 000	2002	Intel	130 nm	145 mm²
Itanium 2 Madison 6M	410 000 000	2003	Intel	130 nm	374 mm²
Pentium 4 Prescott	112 000 000	2004	Intel	90 nm	110 mm²
Itanium 2 with 9 MB cache	592 000 000	2004	Intel	130 nm	432 mm²

Pentium 4 Prescott-2M	169 000 000	2005	Intel	90 nm	143 mm²
Pentium D Smithfield	228 000 000	2005	Intel	90 nm	206 mm²
Pentium 4 Cedar Mill	184 000 000	2006	Intel	65 nm	90 mm²
Pentium D Presler	362 000 000	2006	Intel	65 nm	162 mm²
Core 2 Duo Wolfdale	411 000 000	2007	Intel	45 nm	107 mm²
AMD K10 quad-core 2M L3	463 000 000	2007	AMD	65 nm	283 mm²
POWER6	789 000 000	2007	IBM	65 nm	341 mm²
Core 2 Duo Wolfdale 3M	230 000 000	2008	Intel	45 nm	83 mm²
Core i7 (Quad)	731 000 000	2008	Intel	45 nm	263 mm²
AMD K10 quad-core 6M L3	758 000 000	2008	AMD	45 nm	258 mm²
Six-core Opteron 2400	904 000 000	2009	AMD	45 nm	346 mm²
16-core SPARC T3	1 000 000 000	2010	Sun/Oracle	40 nm	377 mm²
Six-core Core i7 (Gulftown)	1 170 000 000	2010	Intel	32 nm	240 mm²
8-core POWER7 32M L3	1 200 000 000	2010	IBM	45 nm	567 mm²
Quad-core z196[20]	1 400 000 000	2010	IBM	45 nm	512 mm²
Quad-core Itanium Tukwila	2 000 000 000	2010	Intel	65 nm	699 mm²
8-core Xeon Nehalem-EX	2 300 000 000	2010	Intel	45 nm	684 mm²
Quad-core + GPU Core i7	1 160 000 000	2011	Intel	32 nm	216 mm²
10-core Xeon Westmere-EX	2 600 000 000	2011	Intel	32 nm	512 mm²
8-core AMD Bulldozer	1 200 000 000	2012	AMD	32 nm	315 mm²
Quad-core + GPU AMD Trinity	1 303 000 000	2012	AMD	32 nm	246 mm²
Six-core zEC12	2 750 000 000	2012	IBM	32 nm	597 mm²
8-core Itanium Poulson	3 100 000 000	2012	Intel	32 nm	544 mm²
61-core Xeon Phi	5 000 000 000	2012	Intel	22 nm	720 mm²
Apple A7 (dual-core ARM64)	1 000 000 000	2013	Apple	28 nm	102 mm²
Six-core Core i7 Ivy Bridge E	1 860 000 000	2013	Intel	22 nm	256 mm²
12-core POWER8	4 200 000 000	2013	IBM	22 nm	650 mm²
Xbox One main SoC	5 000 000 000	2013	Microsoft/AMD	28 nm	363 mm²
Quad-core Core i7 Haswell	1 400 000 000	2014	Intel	22 nm	177 mm²
8-core Core i7 Haswell-E	2 600 000 000	2014	Intel	22 nm	355 mm²
Apple A8X (tri-core ARM64)	3 000 000 000	2014	Apple	20 nm	128 mm²
15-core Xeon Ivy Bridge-EX	4 310 000 000	2014	Intel	22 nm	541 mm²
18-core Xeon Haswell-E5	5 560 000 000	2014	Intel	22 nm	661 mm²
Quad-+ore i7 Skylake K	1 750 000 000	2015	Intel	14 nm	122 mm²
Duo-Core i7 Broadwell-U	1 900 000 000	2015	Intel	14 nm	133 mm²
IBM z13	3 990 000 000	2015	IBM	22 nm	678 mm²
IBM z13 Storage Controller	7 100 000 000	2015	IBM	22 nm	678 mm²
22-core Xeon Broadwell-E5	7 200 000 000	2016	Intel	14 nm	456 mm²

Trois prédictions d'un « géant »

1959, 1981, 1986

Feynman [1], dans trois travaux pionniers et visionnaires, parus en 1959, 1981 et 1986, lance plusieurs idées révolutionnaires.

1959 : There's **plenty** of room at the bottom. Une « ode » en faveur de la miniaturisation. Peut-on écrire les 25000 pages de l'Encyclopedia Brittanica sur la tête d'une épingle ? Germe de la conception du microprocesseur, des moteurs moléculaires [2], etc. Prévoit apparition du « mur » quantique.

1981 : Simulating physics with computers. Tout calcul quantique exécuté sur ordinateur classique est à complexité exponentielle.

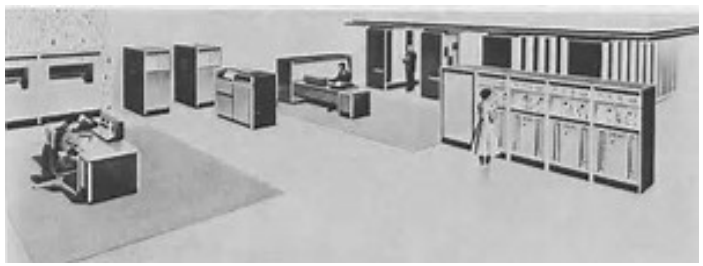
1986 : Quantum mechanical computers. Évolutivité [3] polynomiale vs. complexité exponentielle.

1. Richard Phillips Feynman 1918–1988, prix Nobel de Physique (1965).
2. Découverts par Jean-Pierre Sauvage, né en 1944, prix Nobel de Chimie (2016).
3. Scalability.

Qu'en est-il des prévisions de Feynman ?

Celle de 1959

1959 : IBM 7000
premier IBM transistorisé



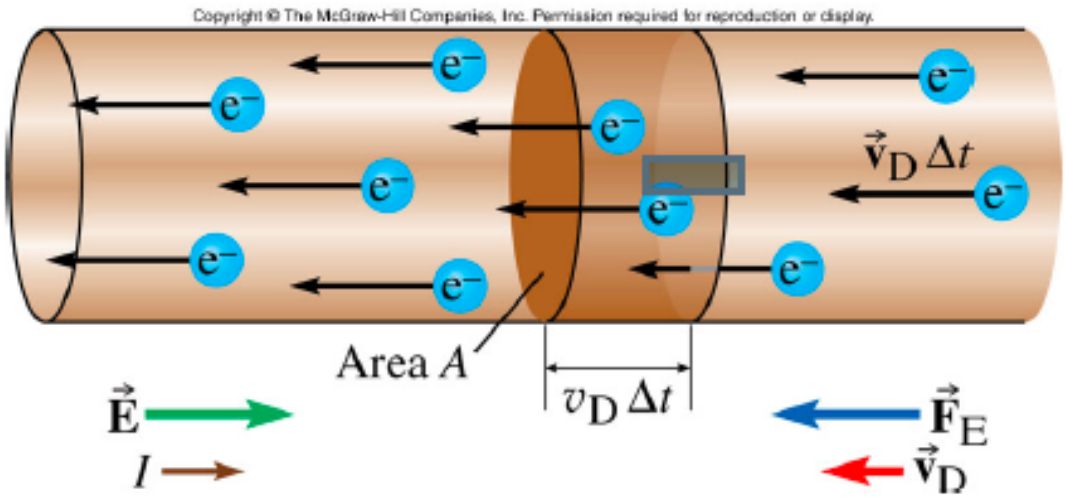
2016 : MacBookAir avec
Intel Core i5

Regardez sur la table !

- Mêmes catégories logiques.
- Même vecteur de transmission : courant électrique.

Qu'est-ce le courant électrique ?

Un flux d'électrons



$$I = \frac{\Delta q}{\Delta t} = \frac{nev_d S \Delta t}{\Delta t} = nev_d S,$$

où $n =$ densité d'électrons libres.

Câble de cuivre : $n \simeq 10^{29}$ électrons$/m^3$.

Si $I = 2$ A et $S = 1$ mm^2, alors $v_d = 0.11 mm/s$.

Que se passerait-il si le vecteur était l'électron individuel ?

Peut-on utiliser des vecteurs plus rapides ?

De la physique
ou de la vérité expérimentale

La physique est une science expérimentale

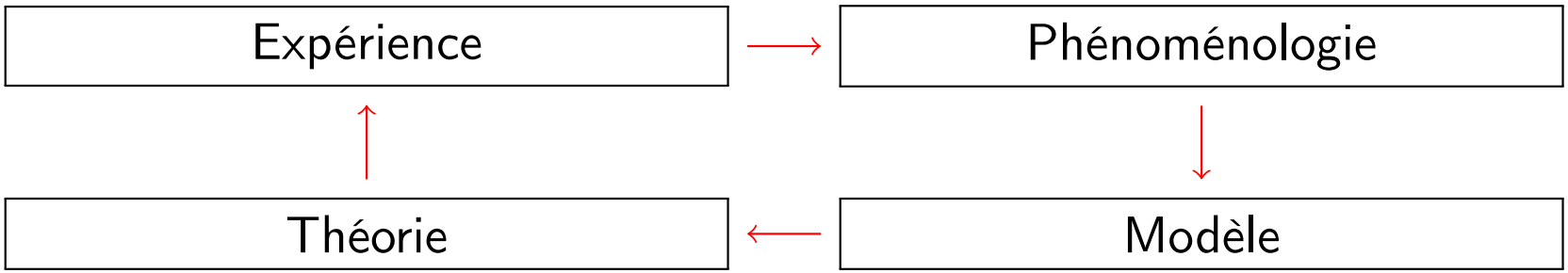


Illustration
du cycle incessant de la physique

Exemple : Un piston contenant un gaz parfait, **quasiment isolé** du reste du monde.

- Préparation précise du système : **état**.
- L'expérience : Interaction avec appareils de mesure
  - manomètre (mesure l'observable p),
  - thermomètre (mesure l'observable T),
  - règle (mesure l'observable V),

  introduisant une **perturbation négligeable** sur l'état.
- La phénoménologie : $pV/T = \text{const}$ (loi de Boyle-Mariotte).
- Le modèle (après beaucoup d'autres expériences) : la thermodynamique des gaz parfaits.
- La théorie (explication microscopique) : théorie cinétique des gaz. (Théorie plus complète : physique statistique.)

[Tableau : Boyle-Mariotte vs. théorie cinétique des gaz. cf. Boltzmann 1848]

Premiers enseignements
de la nature expérimentale de la Physique

- Théories physiques ont **temps de vie fini** ; acceptées tant que non contredites par expérience.
- Vérité physique basée sur **expérience** :
  - préparation du système dans un **état** $\rho \in \mathbf{S}$ précis,
  - interaction du système avec **appareil de mesure**,
  - enregistrement des résultats de mesure d'une **observable** $X \in \mathbf{O}$, prenant des valeurs dans $(\mathbb{X}, \mathcal{X})$.
- Conséquences de la nature expérimentale de la Physique
  - **erreurs** statistiques mais **réproductibilité** statistique,
  - **perturbation** induite par appareil de mesure peut devenir **négligeable**,
  - **Expérience :** modèle statistique $(\mathbf{S}, \mathbf{O})$

$$\mathbf{S} \times \mathbf{O} \ni (\rho, X) \mapsto \nu_X^\rho \in \mathcal{M}_1(\mathbb{X}, \mathcal{X}).$$

- Physique doit être **universelle**. Dans quête d'universalité, la Physique a un allié : les Mathématiques.

UNIVERSITÉ DE RENNES 1

Physique, Mathématiques, Physique Mathématique

Histoire d'une osmose

- Physique utilise Mathématiques pour formuler concepts et faire prédictions quantitatives.
- Mathématiques développent nouveaux outils inspirés par problèmes physiques.
- Physique mathématiqie est
  - Physique : affirmations doivent être corroborées expérimentalement,
  - Mathématiques : affirmations doivent être obtenues comme théorèmes découlant d'un petit nombre d'axiomes (postulats).

UNIVERSITÉ DE RENNES 1

Fausses certitudes . . .

. . . et une bonne dose d'arrogance

- Fin du 19e siècle : « Physique terminée en tant que science fondamentale » ; quelques . . . problèmes mineurs à résoudre.
- Il ne reste plus rien à découvrir en Physique ; les jeunes conseillés ne pas perdre temps avec Physique mais s'orienter vers . . . finance ou technologie.
- Mais attendons une minute !
-

MC	locale complète	$\mathbf{x}' = g \cdot \mathbf{x}\,;\ t' = t$ $\mathbf{x}' = \mathbf{x} + \mathbf{a}\,;\ t' = t + s$	$g \in O(3)$ groupe de Galilée
EM	locale complète	$(t', \mathbf{x}') = g \cdot (t, \mathbf{x})$ $(t', \mathbf{x}') = (t, \mathbf{x}) + (s, \mathbf{a})$	$g \in O(1,3)$ groupe de Poincaré

- Pourquoi 2 groupes d'invariance différents ?

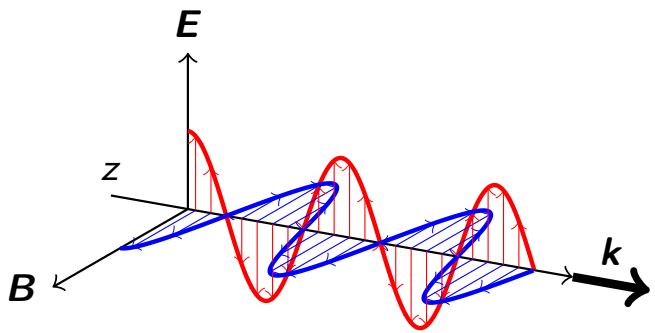
Début du 20e siècle
Tout s'écroule 1

- Le . . . petit problème : équations de Maxwell.

$$\nabla \cdot \boldsymbol{E} = \frac{\rho}{\varepsilon_0} \quad ; \quad \nabla \times \boldsymbol{E} = -\frac{\partial \boldsymbol{B}}{\partial t}$$
$$\nabla \cdot \boldsymbol{B} = 0 \quad ; \quad \nabla \times \boldsymbol{B} = \mu_0(\boldsymbol{J} + \varepsilon_0 \frac{\partial \boldsymbol{E}}{\partial t})$$

- Dans le vide : $\rho = 0$; $\mathbf{J} = 0$; $c^{-2} = \varepsilon_0 \mu_0$.

$$\mathbf{E} = \mathrm{Re}(\mathbf{a} \exp(2\pi i(z - ct)/\lambda)); \mathbf{B} = \mathbf{a} \times \mathbf{E}; \mathbf{a} = \begin{pmatrix} \cos\alpha \\ \sin\alpha \\ 0 \end{pmatrix}.$$



Début du 20e siècle
Tout s'écroule 2

- Expérience de Michelson-Moreley (1887, 1902–1905) : L'éther n'existe pas !
- Becquerel (1896) découvre radioactivité : la matière n'est pas stable !
- Boltzmann, Thomson, Einstein, Perrin (1897–1908) établissent existence de atomes : la matière n'est pas continue !

UNIVERSITÉ DE RENNES 1

Début du 20e siècle
Tout s'écroule 3

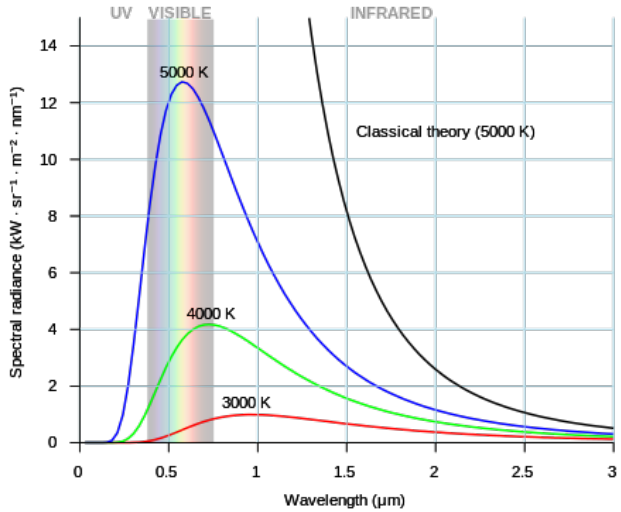


Figure: Théorie classique (Rayleigh) de rayonnement du corps noir en désaccord avec obervation expérimentale (source de la figure : wikipedia).

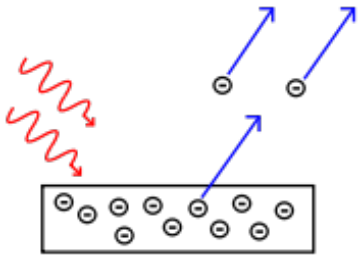


Figure. Théorie classique n'explique pas phénomène photoélectrique, découvert par Hertz (1837) (source de la figure : wikipedia).

Début du 20e siècle
La révolution

- Planck (1900) propose explication phénoménologique audacieuse du rayonnement du corps noir : les niveaux d'énergie sont discrets.
- Einstein (1905) introduit relativité restreinte : unification de mécanique classique et électromagnétisme . Deux principes simples :
  - Vitesse de la lumière c constante universelle, la même dans tous référentiels.
  - Lois de Physique invariantes dans tous référentiels inertiels.

  Conséquences : pas besoin d'éther mais espace et temps non absolus !
- Bohr, Heisenberg, Pauli, Dirac, Schrödinger, von Neumann (1913–1932) considèrent l'idée de Planck sérieusement et introduisent nouvelle Mécanique où l'énergie n'est pas continue mais « quantifiée ».

UNIVERSITÉ DE RENNES 1

Une théorie physique générale
doit décrire tout phénomène dans l'univers

- Unités de mesure introduites lors de la Révolution pour que les grandeurs de tous les jours aient de valeurs numériques raisonnables, typiquement $10^{-3} - 10^{3}$.
- Longueur l : $10^{-15} m$ (rayon du proton) – $10^{26} m$ (rayon de l'univers).
- Masse m : $10^{-30} kg$ (masse de l'électron) – $10^{50} kg$ (masse de l'univers).
- Temps t : $10^{-23} s$ (temps de traversée du noyau atomique) – $10^{17} s$ (âge de l'univers).

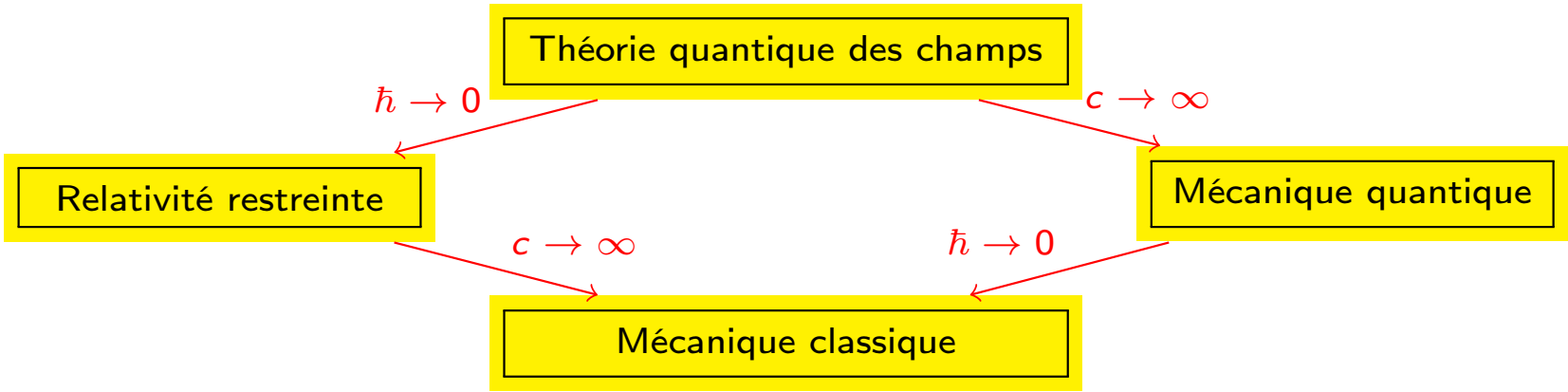
Théorie quantique des champs

Deux constantes physiques :

- constante de Planck $\hbar = 10^{-34} Js$,
- vitesse de la lumière dans le vide $c = 3 \times 10^8 m/s$.

Moustique : m =2.5mg, v =1cm/s, $A = 2.5 \times 10^{-7}$J·s= $2.5 \times 10^{27} \hbar$.

Avion de chasse : v = Mach 2 = 680m/s= 2450km/h= $2.2 \times 10^{-6} c$.



L'inévitable « mur » quantique

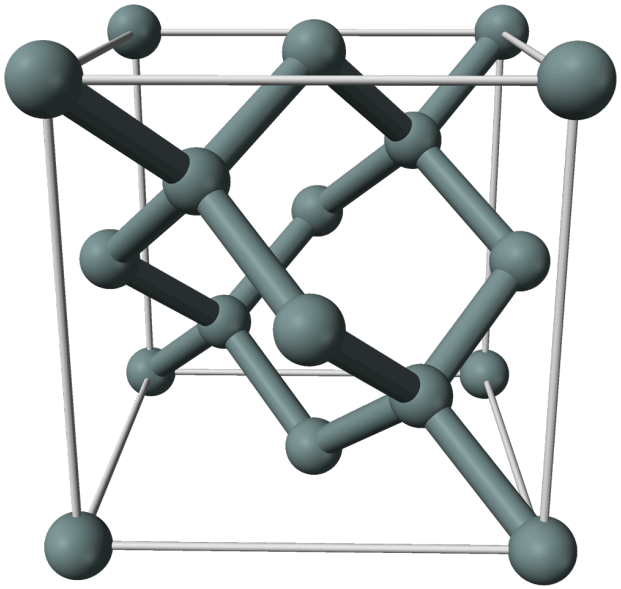
[Ordre de grandeur de l'action $= \hbar$] $\Longrightarrow$ [phénomène quantique].

Partie mobile montre mécanique : $m = 10^{-4}\text{kg}$, $l = 10^{-4}\text{m}$, $t = 1\text{s}$.
$A = 10^{-12}\text{kg} \cdot \text{m}^2 \cdot \text{s}^{-1} = 10^{-12}\text{J} \cdot \text{s} = 10^{22}\hbar \Rightarrow$ classique.

Atome d'hydrogène : Énergie d'ionisation $= E = 2 \times 10^{-18}\text{J}$. Pulsation maximale du spectre : $\omega = 2 \times 10^{16}\text{s}^{-1}$.
$A = E/\omega = 10^{-34}\text{J} \cdot \text{s} = 1\hbar \Rightarrow$ quantique.

« Mur » quantique : Il doit se situer quelque part entre les deux . . .

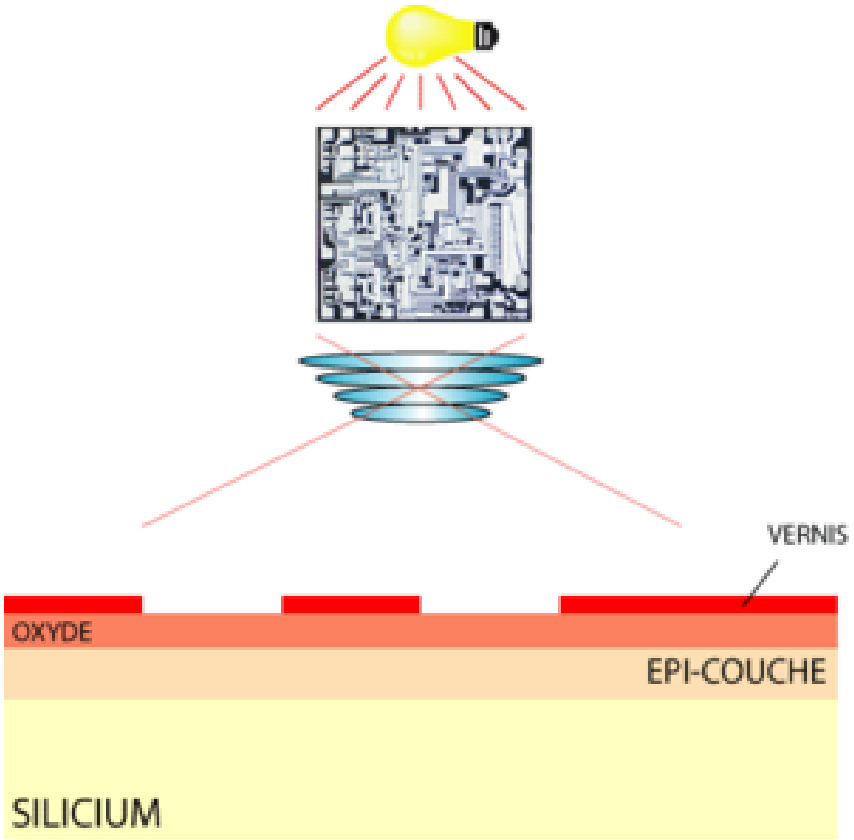
Le cristal de silicium

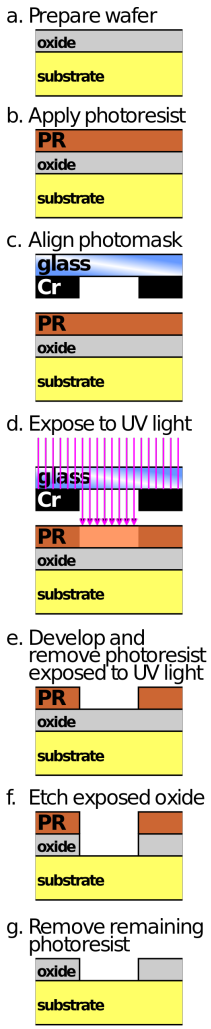


- Matériau extrait d'une matière première abondante sur terre : le sable.
- Cristallisant en structure « diamant ».
- Répétition périodique d'un cube de côté $a = 0.5431$ nm.
- Distance interatomique $\frac{\sqrt{3}}{4}a = 0.2352$ nm.

Comment fabrique-t-on un microprocesseur ?

Procédé photolithographique





Données techniques comparées

- Diamètre de cheveu humain 100 μm$= 10^5$ nm.
- Épaisseur de trait photolithographique

  1971 : 10 μm$=$ 10000 nm,
  2010 : 0.032 μm$=$ 32 nm,
  2013 : 0.022 μm$=$ 22 nm,
  2016 : 0.014 μm$=$ 14 nm.
  Épaisseur de trait $=$ 60 distances interatomiques.
- Vers une pénurie d'un nouveau type : matière première abondante mais pas assez d'atomes par unité de volume élémentaire.
- Production du microprocesseur Skylake (Intel) à 14 nm — initialement prévue à 11 nm — retardée d'un an et épaissie de 3 nm à cause de phénomènes quantiques mal maîtrisés.

UNIVERSITÉ DE RENNES 1

Peut-on ignorer phénomènes quantiques ?

NON !

Qu'en est-il de la 2e prévision (celle de 1981) de Feynman ?

Simulation de phénomène quantique de « taille » N sur ordinateur classique (machine de Turing classique) est de classe de complexité $\exp(N)$.

Qu'en est-il de la 3e prévision (celle de 1986) de Feynman ?

1994

Adleman : Molecular computation of solutions to combinatorial problems.

Résout problème « voyageur du commerce » (NP-complet) par ordinateur en ADN. Travail passé presque inaperçu, pourtant réalisation physique.

Shor : Algorithms for quantum computation : discrete logarithms and factoring.

Démontre la résolution d'un problème de factorisation en temps polynomial. Travail très médiatisé, pourtant conception purement théorique : ordinateur universel quantique.

UNIVERSITÉ DE RENNES 1

Peut-on exploiter Mécanique quantique ?

Oui déjà

Yes, we can !

1/3 de l'économie mondiale repose sur des applications découlant de phénomènes quantiques. Exemples :

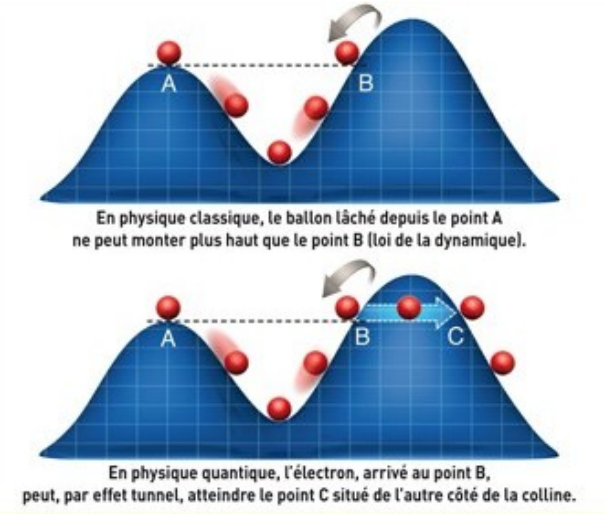
- Semiconducteurs : toute la technologie informatique.
- Laser : CD, DVD, communications par fibre optique, chirurgie, metallurgie, ...
- Supraconductivité : champs magnétiques intenses, effet Meissner et lévitation magnetique, ...
- Effet tunnel : microscope à effet de champs, applications en nanotechnologie, fullerenes, ...
- Superfluidité : aimants supraconducteurs, piègeage de photons, cryogénie, ...
- Cryptographie et communications quantiques : distribution de la clé de manière inviolable, téléportation d'états quantiques, codage superdense, génération de vrais nombres aléatoires ...

UNIVERSITÉ DE RENNES 1

Curiosités quantiques et leurs applications technologiques

Effet tunnel et microscopie

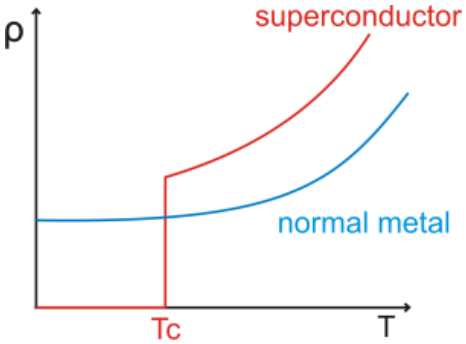
Un phénomène purement quantique.

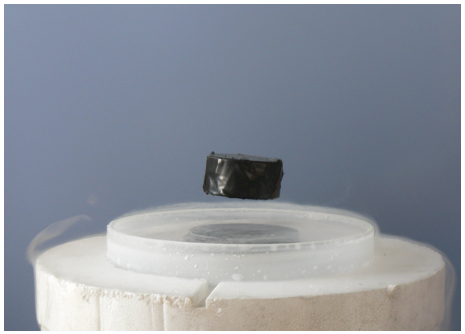


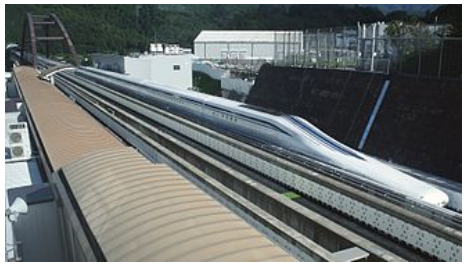
[Tableau : effettunnel.mov]

Curiosités quantiques et leurs applications technologiques

Effet Meissner et trains à lévitation magnétique

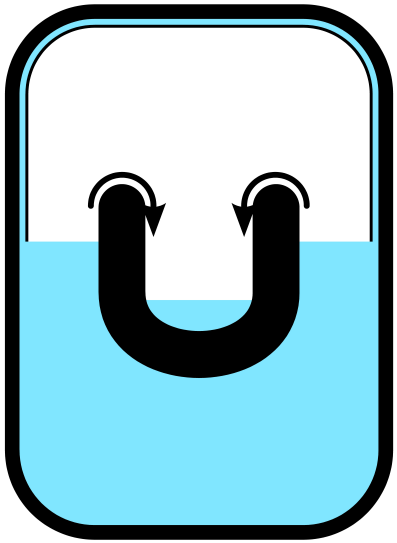


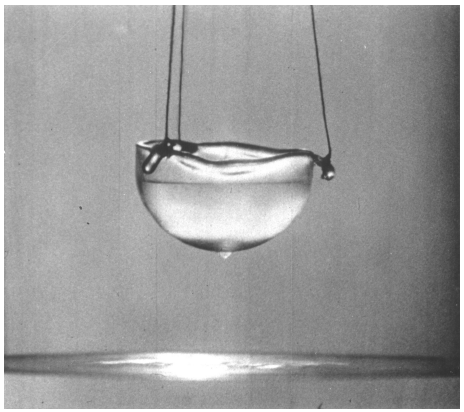




Curiosités quantiques et leurs applications

Superfluidité de ^{4}He et cryogénie





D'autres curiosités quantiques

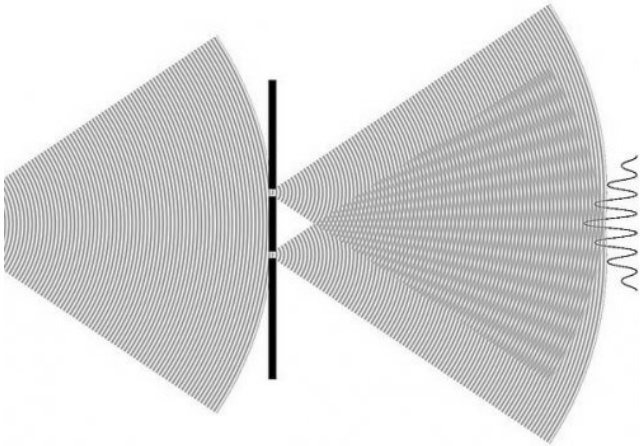
et leurs applications en information quantique

- Interférence quantique des états indiscernables. Protocoles BB84 et B92 de QKD, signature, authentication, calcul quantique, etc.
- Réduction de l'état par la mesure physique. Détection des intrusions.
- Intrication. Autres protocoles de QKD, calcul quantique, signature, authentication, etc.
- Multiplicativité des dimensions. Calcul massivement parallèle.
- Effet tunnel. Ordinateurs quantiques dédiés (D-wave), algorithmes d'optimisation.
- Décohérence. Le phénomène qui empêche le calcul quantique à grande échelle.

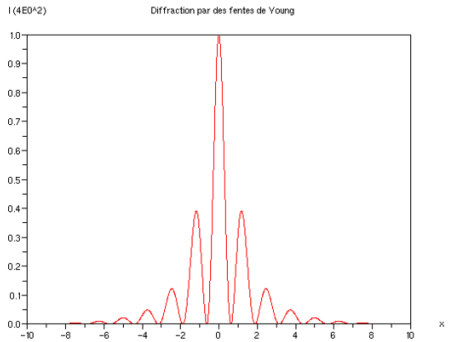
UNIVERSITÉ DE RENNES 1

La superposition des ondes

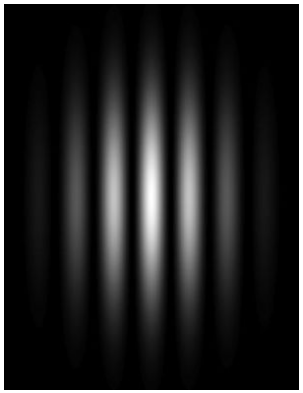
Cristianus Huygens (1629–1695), Augustin Fresnel (1788–1827)



Dispositif expérimental
Young (1801)



Intensité caclulée



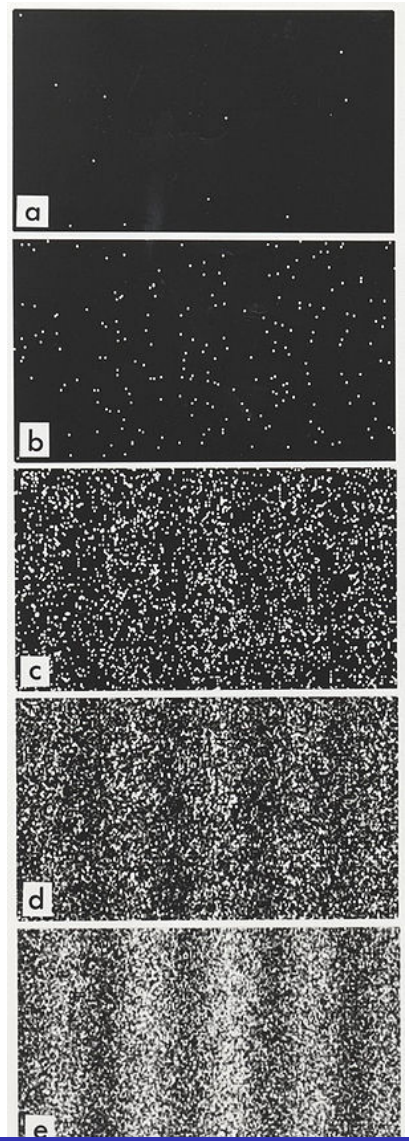
Intensité observée

L'expérience de Young

Superposition avec des électrons : expérience de Tonomura

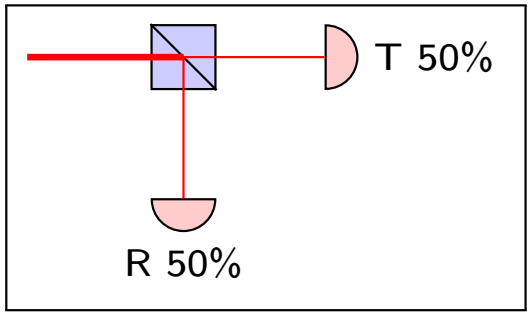
Exposé de Feynman

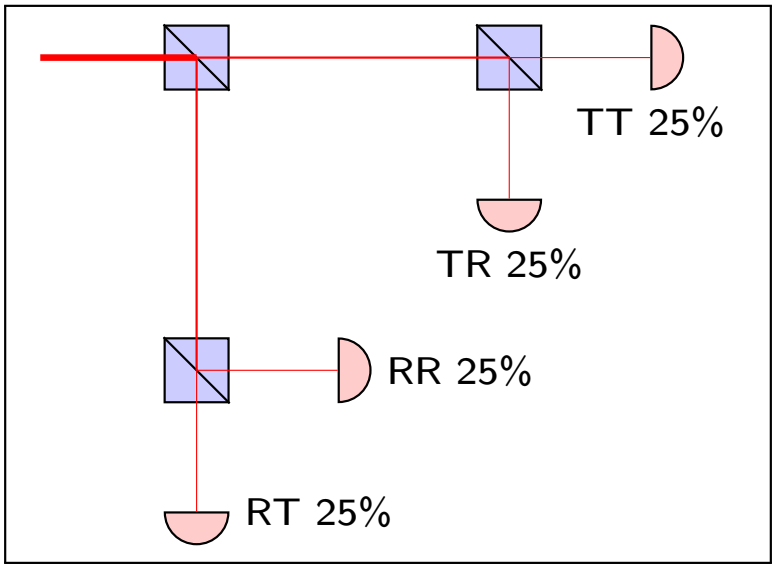
Expérience de Tonomura

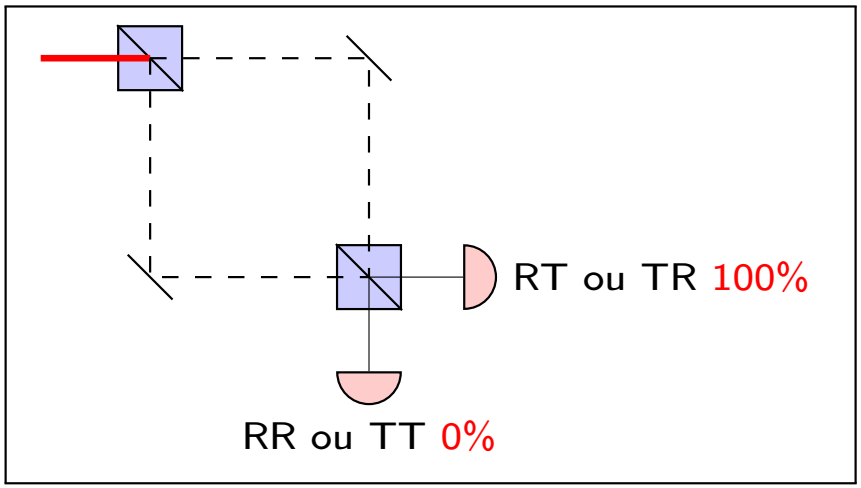


Indiscernabilité $\Rightarrow$ superposition

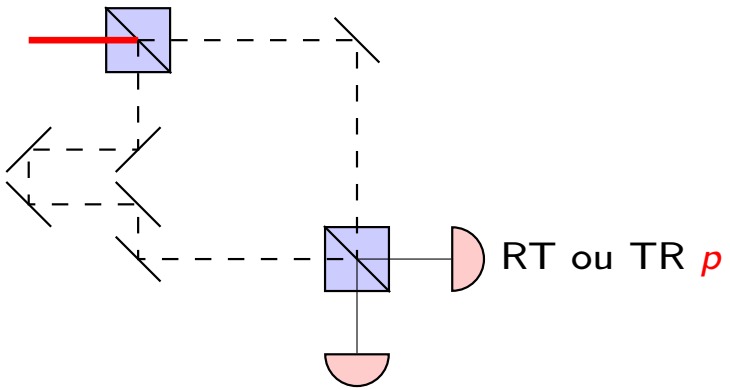
Une autre interprétation de l'expérience de deux fentes (avec des photons)



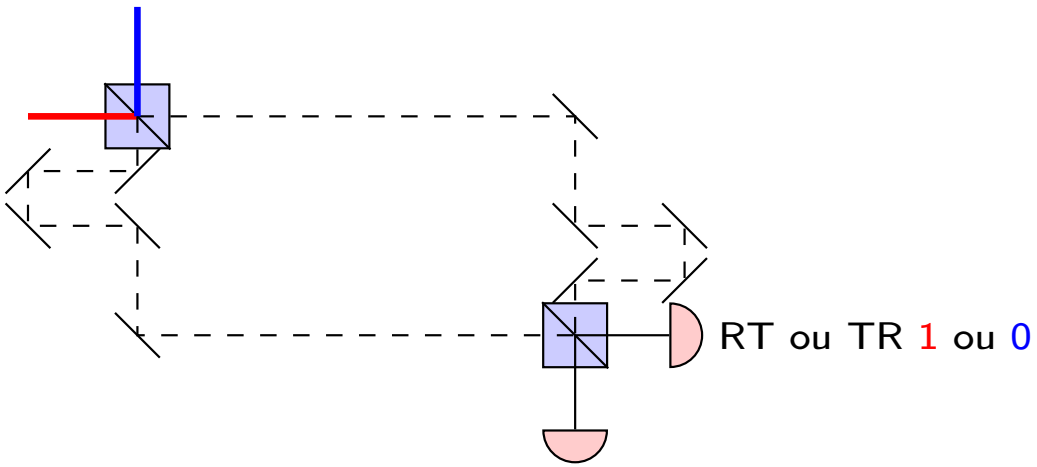




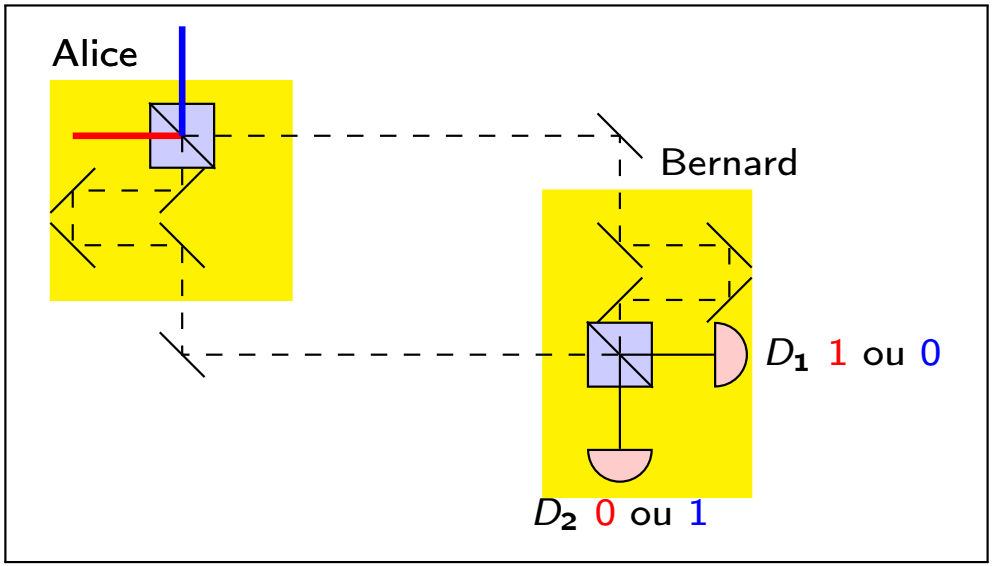
Superposition
(suite)



La valeur $p \in [0, 1]$ dépend de l'élongation du parcours



Application
Protocole Bennett-Brassard (1984)



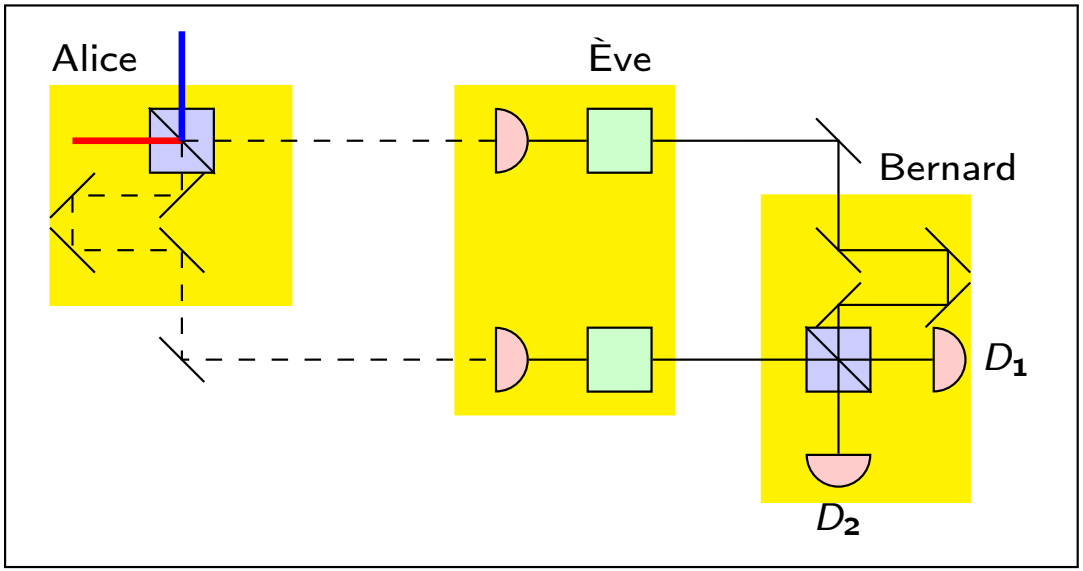
Choisir élongation telle que si unilatère $p = 1/2$.

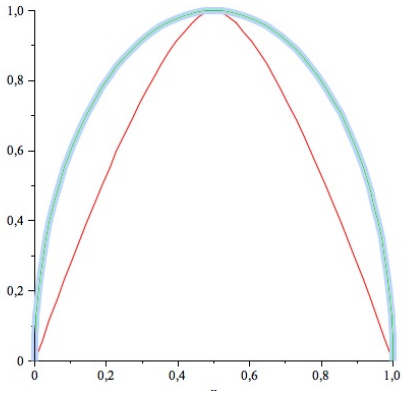
Alice		Bernard	
E	Él	Él	S
0	0	0	D_1
0	0	1	D_1 ou D_2
0	1	0	D_1 ou D_2
0	1	1	D_1
1	0	0	D_2
1	0	1	D_1 ou D_2
1	1	0	D_1 ou D_2
1	1	1	D_2

UNIVERSITÉ DE RENNES 1

Intrusion

Information mutuelle vs. taux d'erreur induite





$I(A : E)$ en fonction du taux d'erreur sur les bits de Bernard

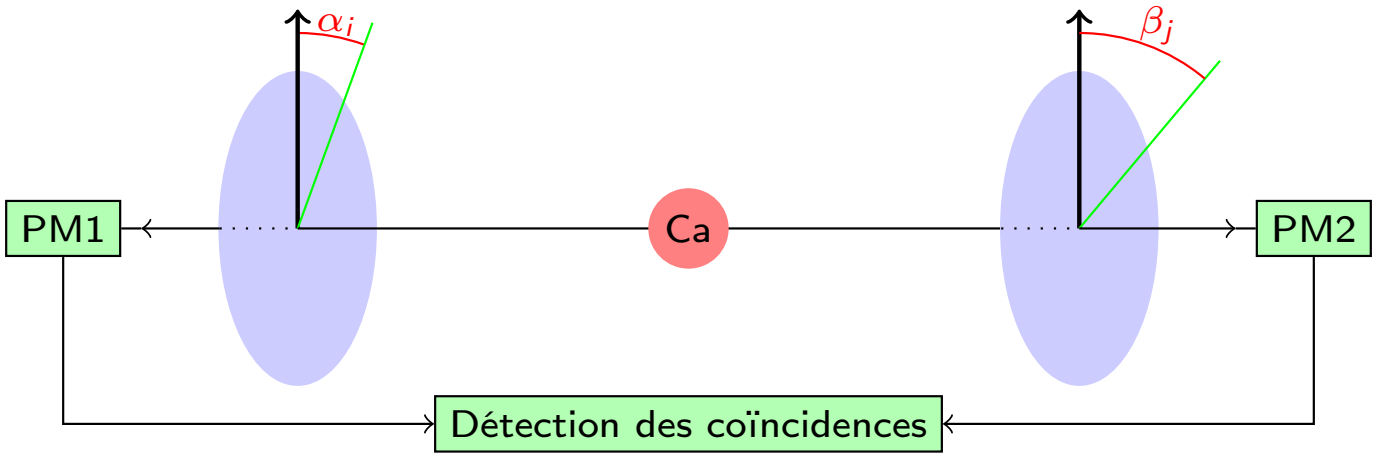
L'intrication

L'expérience d'Orsay et l'irréductibilité de l'aléa quantique

Théorème (Inégalité de Bell)

$X_1, X_2, Y_1, Y_2 \in \{0,1\}$ *v.a. classiques sur* $(\Omega, \mathcal{F}, \mathbb{P})$.

$$\mathbb{P}(X_1 = Y_1) \leq \mathbb{P}(X_1 = Y_2) + \mathbb{P}(X_2 = Y_2) + \mathbb{P}(X_2 = Y_1).$$



- Expérience et formalisme quantique : $\mathbb{P}(X_\alpha = Y_\beta) = \frac{1}{2}\sin^2(\alpha - \beta)$.
- Si $\alpha_1 = 0$, $\alpha_2 = \pi/3$, $\beta_1 = \pi/2$, $\beta_2 = \pi/6$, alors $1 \leq 1/4 + 1/4 + 1/4$.

UNIVERSITÉ DE RENNES 1

L'intrication à quoi ça sert ?

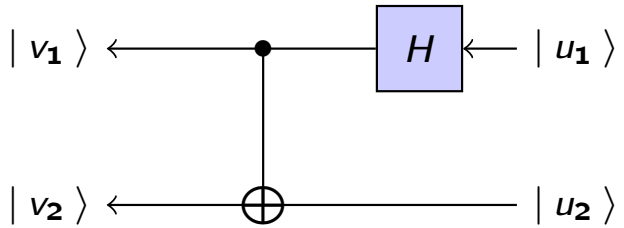
À faire du calcul quantique !

Définition

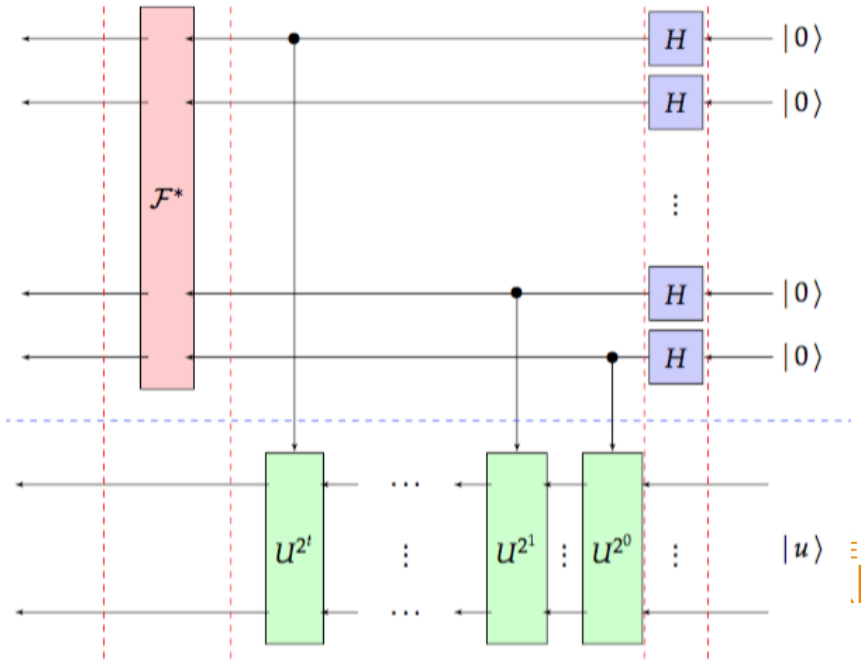
$|\Psi\rangle \in \mathbb{H}_1 \otimes \mathbb{H}_2$ intriqué si $|\Psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle$ avec $|\psi_i\rangle \in \mathbb{H}_i$, $i = 1, 2$.

Remarque

Intrication = phénomène purement quantique.



$$|00\rangle \mapsto \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$



La décohérence

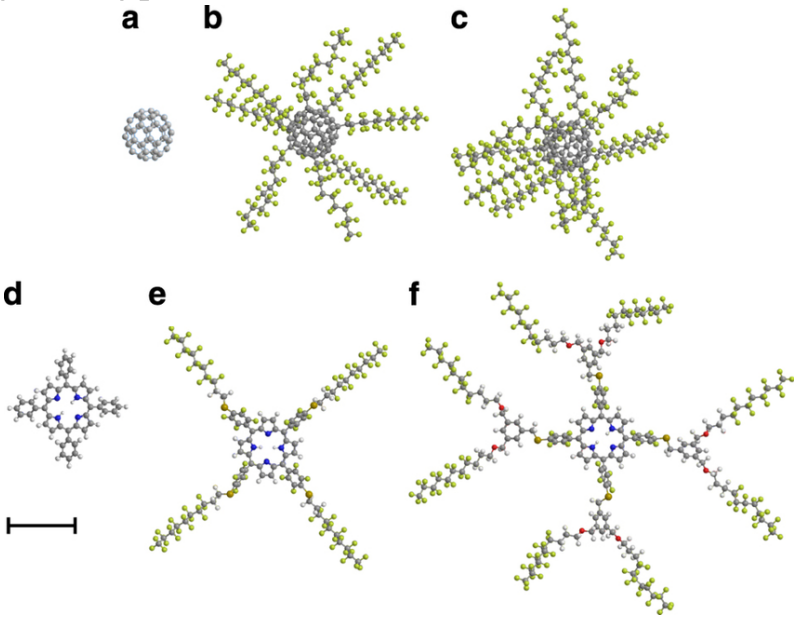
- Lorsque système croît ou se réchauffe, comportement quantique disparaît.
- Existence d'interférences l'expérience de double fentes = signature du caractère quantique.
- Neutrons, électrons, photons présentent interférences.
- Chats [de Schrödinger], voitures etc. n'en présentent pas.

La décohérence

Seules particules subatomiques sont-elles quantiques ?

- Fullerène C_{60} avec 60 atomes [Nairz, Arndt, Zeilinger (2003)]

- Grosses molécules organiques avec jusqu'à 430 atomes [Gerlich et al (2011)]



- Matériaux supraconducteurs (10^{23} atomes) mais très froids $1mK$ –

Ce que l'on sait faire en informatique quantique

Dans un stade pré-industriel

- Générateurs de nombres vraiment aléatoires. Vous pouvez même en acheter un!
- Distribution d'une clé de cryptage à travers
  - fibre optique de 307 km [Korzh et al (2015)]
  - à l'air libre sur 144 km [Lo, Curty, Tamaki (2014)].
- Signature.
- Authentification.
- Communication (codage dense, téléportation, . . .).

UNIVERSITÉ DE RENNES 1

Ce que l'on sait faire en informatique quantique

Dans le stade du prototype

- Écrire (sur papier) quelques algorithmes (Grover, Shor) et des codes correcteurs d'erreurs.
- Construire prototypes d'ordinateurs « universels » pour résoudre des instances simples de l'algorithme de Shor [Vandersypen et al (2001) $15 = 3 \times 5$ avec 7 qubits par résonance magnétique nucléaire], (IBM 5 qubits, mis à disposition du public, factorisation).
- Corriger quelques erreurs.
- Construire ordinateur D-Wave 2000 qubits, prix catalogue 10 MUSD (dédié à l'optimisation par recuit par effet tunnel quantique). Les premières annonces de la compagnie ont été très controversées.

UNIVERSITÉ DE RENNES 1

Et si on disposait d'un calculateur quantique universel ?

Factorisation de grands entiers avec 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	$\mathcal{O}(\exp(n))$	$\mathcal{O}(\exp(n^{1/3}(\log n)^{2/3}))$	$\mathcal{O}(n^3)$
100	1.26×10^{21}s $= 4.01 \times 10^{13}$a	3.13s $= 9.93 \times 10^{-8}$a	1×10^{-3}s $= 3.17 \times 10^{-11}$a
500	3.27×10^{141}s $= 1.31 \times 10^{134}$a	6.74×10^{10}s $= 2139$a	0.125s $= 3.96 \times 10^{-9}$a
1000	1.07×10^{292}s $= 3.39 \times 10^{284}$a	6.42×10^{17}s $= 2.03 \times 10^{10}$a	1s $= 3.17 \times 10^{-8}$a

UNIVERSITÉ DE RENNES 1

Un peu plus de détails
Implémentations universelles

Shor : Pour factoriser entier N de k bits (avec algorithme de Shor complet) en temps $\mathcal{O}(k^3)$, il faut [Beckman et al (1996)]

- $5k + 1$ qubits,
- $72k^3$ portes logiques quantiques.

$k = 4$: 21 qubits, 4608 portes,
$k = 100$: 501 qubits, 7.2×10^7 portes,
$k = 4096$: 20481 qubits, 4.95×10^{12} portes.

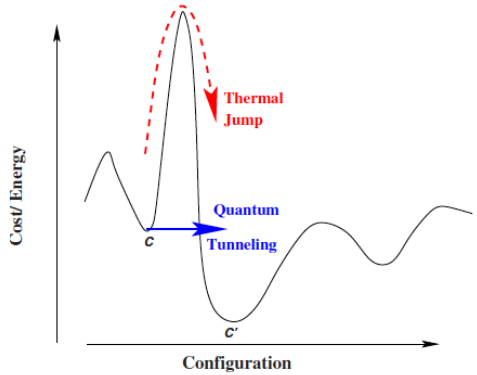
- $15 = 3 \times 5$ ($k = 4$). Factorisé avec 7 qubits.
- $21 = 3 \times 7$ ($k = 5$). Factorisé avec 10 qubits [Martin-López et al. (2012)].

Optimisation :

- $143 = 11 \times 13$ (avec 4 qubits) et $56153 = 233 \times 241$ (avec 4 qubits) [Xu et al (2012)].
- Possibilité de factorisation $291311 = 523 \times 557$ avec 6 qubits [Dattani, Bryans (2014)]. Non encore implémenté.

UNIVERSITÉ DE RENNES 1

Un peu plus de détails
Implémentations sur D-Wave



Principes des recuits simulé et quantique.

Nombres de Ramsey[4] : $R(8,2) = 8$ avec 84 qubits (28 calcul et 56 correction d'erreurs) en 270 ms. [Bian et al. (2013)].

Configurations optimales de protéines : benchmarks avec 81 qubits [Perdomo-Ortíz et al. (2012)].

4. $R(s,t)$ = plus petit entier n t.q. tout coloriage rouge-bleu des arêtes de K_n contient un K_s rouge et un K_t bleu.

Ce que l'on espère pouvoir faire . . .

. . . un jour

Quand pensez-vous qu'un ordinateur quantique universel réellement utilisable (pour factoriser des nombres à 100 bits par exemple) verra le jour ?

> « La prévision est difficile surtout . . . lorsqu'elle concerne l'avenir. »
>
> Pierre Dac

Cochez une case.

Dans 5 ans . . . . . ☐
Dans 10 ans . . . . . ☐
Pas durant ma vie . . . . . ☐
Durant le 21e siècle . . . . . ☐
Jamais . . . . . ☐

UNIVERSITÉ DE RENNES 1