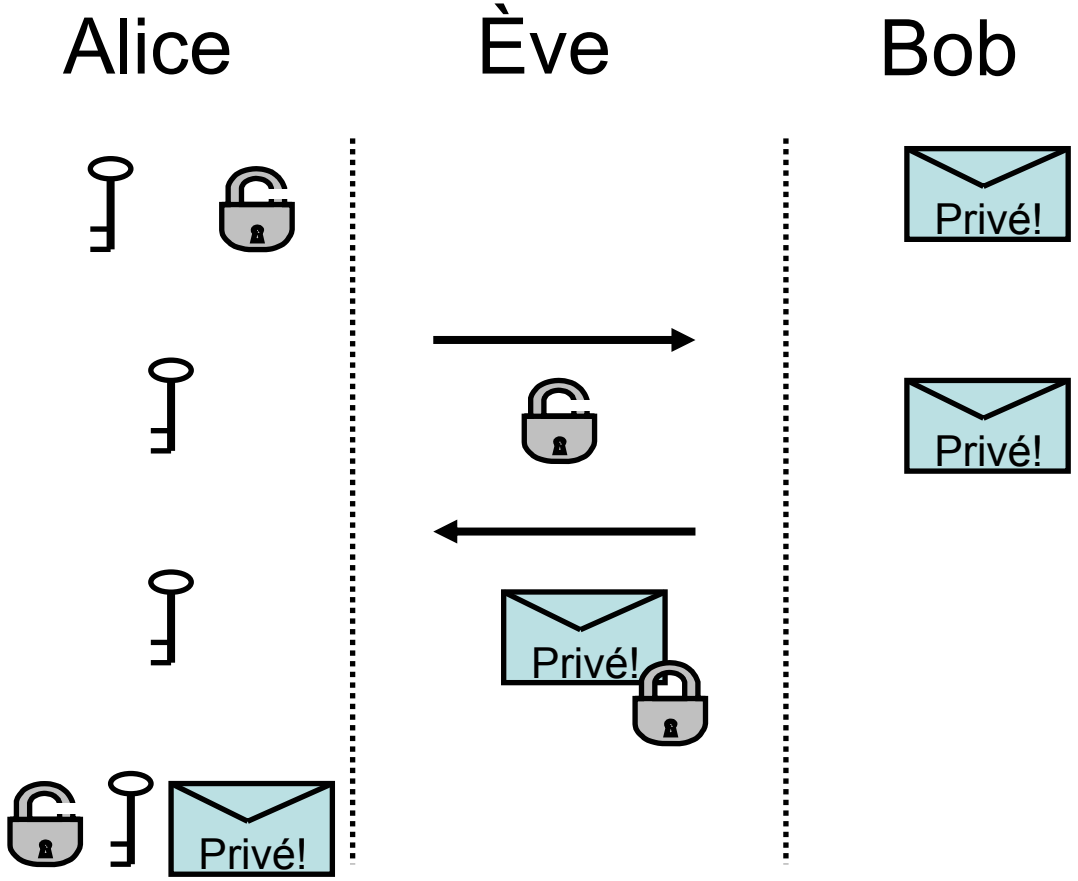
Informatique quantique IFT6155

Factorisation

Cryptographie à clef publique

Comment Alice et Bob peuvent-ils échanger de l'information secrète s'ils ne partagent pas de clef privée?



Arithmétique modulaire

$$a_1 = a_2 \ mod \ n \quad \Leftrightarrow \quad \exists r, 0 \leq r \leq n-1, a_1 = b_1 n + r, a_2 = b_2 n + r$$

$$(a+b) \ mod \ n = ((a \ mod \ n) + (b \ mod \ n) \ mod \ n)$$

$$(ab) \ mod \ n = ((a \ mod \ n)(b \ mod \ n) \ mod \ n)$$

Exponentiation modulaire

Étant donnés e, a et n on peut efficacement

$$O(\log(a)\log(n)\log(\log(n))))$$

calculer $e^a \ mod \ n$.

Soit $k \simeq \log(a)$ et $a = a_k a_{k-1} a_{k-2} \cdots a_1 = a_1 + 2a_2 + \cdots 2^k a_k$ alors

$$e^a \ mod \ n = e^{a_1} e^{(2a_2)} \cdots e^{2^k a_k} \ mod \ n.$$

Calculer $e, e^2, e^4, \cdots, e^{2^k}$ demande de faire k mises au carré. Calculer e^a demande au plus $2k$ multiplications.

Exponentiation modulaire

$$
\begin{aligned}
15^5 \ mod\ 17 &= (15^4 * 15^1)\ mod\ 17 \\
&= (15^2)^2 * 15\ mod\ 17 \\
&= (225)^2 * 15\ mod\ 17 \\
&= (13 * 17 + 4)^2 15\ mod\ 17 \\
&= 4^2 * 15\ mod\ 17 \\
&= 16 * 15\ mod\ 17 \\
&= 240\ mod\ 17 \\
&= 14 * 17 + 2\ mod\ 17 \\
&= 2\ mod\ 17
\end{aligned}
$$

$pgcd$

Le $pgcd(n, m)$ est le plus grand commun diviseur de n et m.

$$pgcd(30, 45) = 15 \quad pgcd(10, 20) = 10 \quad pgcd(13, 11) = 1$$

Algorithme d'Euclide:

pgcd$(n, m) = d$
Si $m > n$ alors $m \leftarrow n, n \leftarrow m$
Tant que $n \neq 0$
: $\quad m \leftarrow n, n \leftarrow m \ mod \ n$
$d \leftarrow m$

L'algorithme **pgcd**(n, m) est polynomial dans $\log(m) + \log(n)$.

$pgcd$

pgcd(6825, 1430)
$m = 6825, n = 1430$
$6825 = 4 * 1430 + 1105$
$m = 1430, n = 1105$
$1430 = 1105 + 325$
$m = 1105, n = 325$
$1105 = 3 * 325 + 130$
$m = 325, n = 130$
$325 = 2 * 130 + 65$
$m = 130, n = 65$
$130 = 2 * 65$
$m = 65, n = 0$
Retourne $d = 65$

$pgcd$

$$pgcd(n,m) = d \;\Rightarrow\; \exists, i, j \in Z; in + jm = d$$

On a que d est le plus petit entier positif tel que $in + jm = d$.

En particulier

$$pgcd(n,m) = 1 \quad \Leftrightarrow \quad \exists, i, j \in Z; in + jm = 1 \quad \Leftrightarrow \quad jm = 1 - in = 1 \; mod \; n$$

et donc j est l'inverse multiplicatif de m modulo n.

Pour obtenir i et j on effectue des substitutions en partant de la fin dans l'algorithme d'Euclide.

Inverse modulo n

Trouvons l'inverse de 31 modulo 101. Premièrement, on trouve le $pgcd$.

pgcd$(101, 31)$
$m = 101, n = 31$
$101 = 3 * 31 + 8$
$m = 31, n = 8$
$31 = 3 * 8 + 7$
$m = 8, n = 7$
$8 = 7 + 1$
$m = 7, n = 1$
$7 = 7 * 1 + 0$
$m = 1$, on retourne $pgcd(101, 31) = 1$.

Renversons la vapeur.

$1 = 1$
$1 = 8 - 7$ puisque $8 = 7 + 1$
$1 = 8 - (31 - 3 * 8) = -31 + 4 * 8$ puisque $31 = 3 * 8 + 7$
$1 = -31 + 4 * (101 - 3 * 31) = 4 * 101 - 13 * 31$ puisque $101 = 3 * 31 + 8$
$1 = 4 * 101 - 13 * 31$

On a bel et bien que $88 = -13 \ mod \ 101$ est l'inverse multiplicatif de 31 modulo 101 puisque $31 * 88 = 2728 = 27 * 101 + 1 = 1 \ mod \ 101$.

$\phi(n)$

Pour un entier n on définit $\phi(n)$ comme le nombre d'entiers inférieurs ou égaux à n qui sont premiers relativement à n.

On a que $\phi(n) \geq \frac{n}{2}$.

En particulier, si $n = pq$ pour p et q premiers, alors $\phi(n) = (p-1)(q-1)$.

Théorème (Euler):
Si $pgcd(n, a) = 1$ alors $a^{\phi(n)} = 1 \ mod \ n$.

Primalité et factorisation

Si n est un entier de L bits, il existe un algorithme polynomial en L qui permet de tester la primalité de n. C'est un résultat récent de Manindra Agrawal, Neeraj Kayal and Nitin Saxena dans $O(L^{12})$ (amélioré depuis à $O(L^{6.5})$ je crois...).

On avait déjà des algorithmes probabilistes polynomiaux très efficaces.
Par exemple le test de Miller-Rabin.

Si n est un nombre composé de L bits alors le meilleur algorithme connu permettant

de factoriser n est l'algorithme *General Number Field Sieve*, qui prend un temps dans

$$\Theta(2^{cL^{1/3}\log(L)^{2/3}})$$

RSA

Inventé par **Rivest, Shamir et Adelman en 1977**, le protocole RSA est une véritable révolution en cryptographie.

Alice choisit aléatoirement deux grands nombres premiers p et q.
On note $n = pq$ et $\phi(n) = (p-1)(q-1)$.

Alice choisit aléatoirement un entier e premier relativement à $\phi(n)$.

Alice calcule d (l'inverse de e modulo $\phi(n)$)
tel que $ed = 1 \ mod \ \phi(n)$.

Alice rend publique la paire (e, n).

L'algorithme public de chiffrement est $E(x) = x^e \ mod \ n$.

L'algorithme privé de déchiffrement est $D(y) = y^d \ mod \ n$.

Pour x copremier avec n, on a

$$D(E(x)) = (x^e)^d = x^{(ed)} = x^{1+k\phi(n)} = x(x^{\phi(n)})^k = x(1)^k = x \ mod \ n$$

Il est clair que si un espion connaît la factorisation de n, il pourra lui aussi déchiffrer les messages.

Concours RSA-129

Briser un exemplaire de RSA où

$n = 114381625757888867669235779976146612010218296721242362562561842$
$935706935245733897830597123563958705058989075147599290026879543541$

Il a fallu 8 mois à 600 ordinateurs pour factoriser ce nombre.

$n = 349052951084765094914784961990389813341776463849338784399082057 7 *$
$327691329932667095499619881908344614131776429679929425397982885 33$

Le message secret était:

THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE

RSA, exemple

Alice choisit $p = 124567$ et $q = 133559$ et vérifie qu'ils sont premiers.

$$n \;=\; pq \;=\; 124567 * 133559 \;=\; 16637043953$$

$$\phi(n) \;=\; (p-1)(q-1) \;=\; 16636785828$$

Alice choisit $d = 3$ et calcule $e = 9982071497$.

Alice rend publics $[n, e] = [16637043953, 9982071497]$ et garde d secret.

Bob désire transmettre le message $m = 12345$.

$$E(m) \;=\; m^{9982071497} \; mod \; 16637043953 \;=\; 3139468514$$

Bob transmet à Alice le message $c = 3139468514$, qu'Alice peut décoder.

$$D(c) = c^d \; mod \; n = 3139468514^3 \; mod \; 16637043953 \;=\; 12345$$

Ordre et factorisation

Ordre:
Étant donné n et x relativement premiers, trouver le plus petit r tel que $x^r = 1 \ mod \ n$.

On peut trouver un facteur non trivial d'un entier n, et donc factoriser, si on sait calculer efficacement l'ordre d'un élément.

Ordre et factorisation

Lemme:
Soit n un nombre composé et x tel que $x \neq 1$, $x \neq n-1$ et $x^2 = 1(mod\ n)$. Alors $pgcd(x-1,n)$ ou $pgcd(x+1,n)$ est un facteur non trivial de n.

Preuve:
Si $x^2 - 1 = 0(mod\ n)$ alors $(x-1)(x+1) = 0(mod\ n)$ et donc $(x-1)(x+1) = kn$ et donc si $(x-1) \neq 0$ et $(x+1) \neq N$ alors $pgcd(x-1,n)$ ou $pgcd(x+1,n)$ divise n.

Lemme:
Si n est composé et impair alors pour $x \in_R \{1,\ldots,n-1\}$ tel que $pgcd(x,n) = 1$, si r est l'ordre de x modulo n, la probabilité que r soit pair et $x^{r/2} \neq -1(mod\ n)$ est supérieure ou égale à $1/2$.

Ordre et factorisation

Factoriser(n)

1. Si n est pair retourner 2.
2. Chercher a et b tels que $n = a^b$, auquel cas retourner a.
   (On peut essayer tous les b possibles puisque $2 \leq b \leq \log(n)$.)
3. Choisir $x \in_R \{2, n-1\}$.
4. Si $pgcd(x, n) = a > 1$ retourner a.
5. r =Ordre(x, n)
6. Si r est impair ou si $x^{r/2} = -1 \ mod \ n$, retourner échec.
   (Par le lemme, ceci arrive moins d'une fois sur deux)
7. Calculer $a = pgcd(x^{r/2} - 1, n)$ et $b = pgcd(x^{r/2} + 1, n)$.
   Retourner l'une des deux valeurs étant un facteur non trivial.

Ordre

Nous savons facilement calculer le produit de deux entiers modulo n.
Il existe donc une transformation unitaire U_x tel que

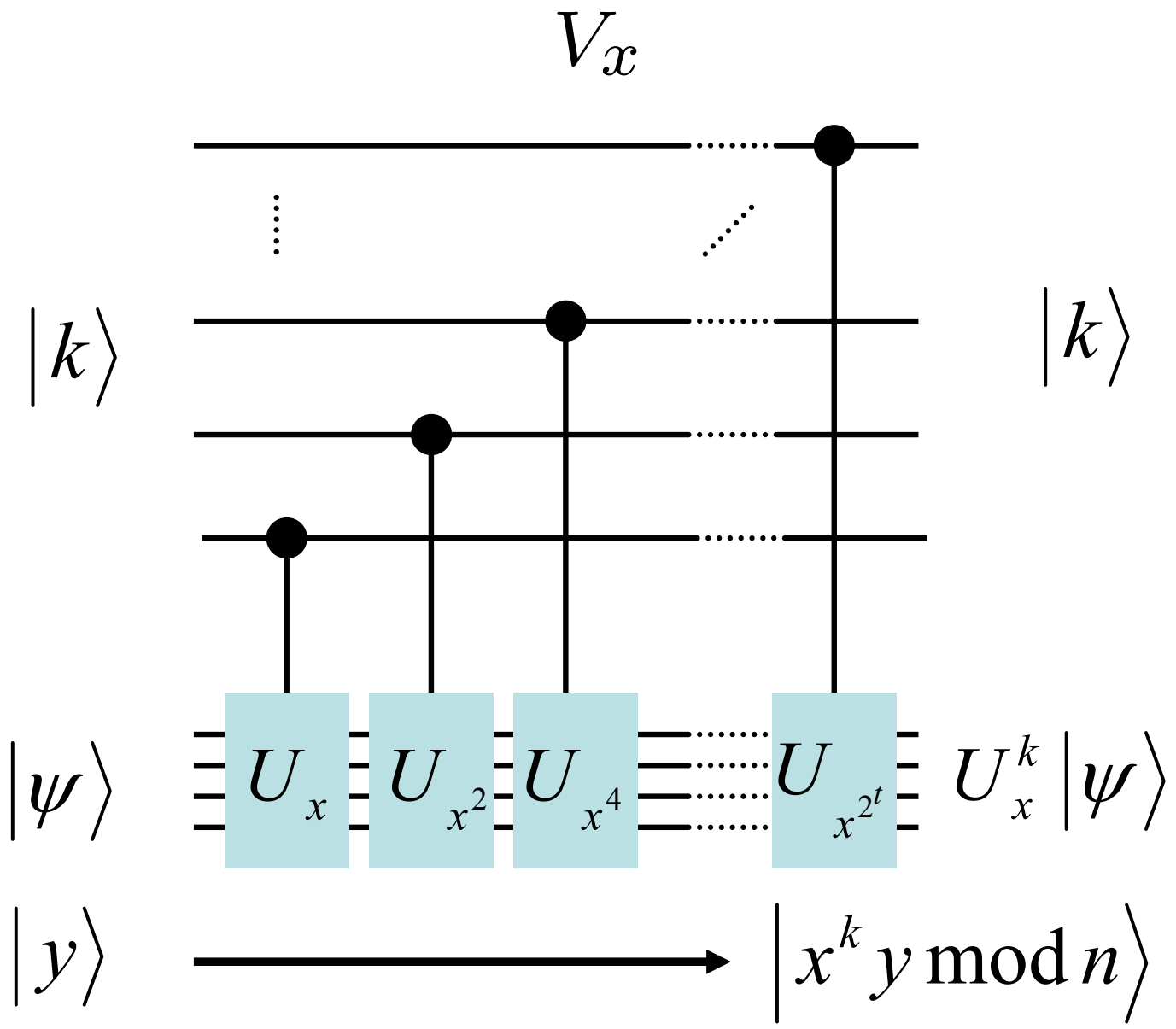
$$U_x \left|y\right\rangle = \left|xy \ mod \ n\right\rangle$$

ainsi que pour tout k

$$U_{x^k} \left|y\right\rangle = U_x^k \left|y\right\rangle = \left|x^k y \ mod \ n\right\rangle$$

en particulier pour tout $k = 2^i$ on peut calculer efficacement $(U_x)^k$, et donc il existe V (polynomial) tel que

$$V_x \left|k\right\rangle \left|y\right\rangle = \left|k\right\rangle \left(U_x^k \left|y\right\rangle\right) = \left|k\right\rangle \left|x^k y \ mod \ n\right\rangle$$


V_x
$|k\rangle$
$|k\rangle$
$|\psi\rangle$
U_x
U_{x^2}
U_{x^4}
$U_{x^{2^t}}$
$U_x^k|\psi\rangle$
$|y\rangle$
$|x^k y \bmod n\rangle$

Vecteurs propres de U_x

Soit r l'ordre de x modulo N et pour $0 \leq s \leq r-1$

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi isk/r} \left|x^k \ mod \ n\right\rangle$$

Nous avons

$$\begin{aligned}
U_x |u_s\rangle &= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi isk/r} \left|x^{k+1} \ mod \ n\right\rangle \\
&= \frac{1}{\sqrt{r}} \sum_{k=1}^{r} e^{-2\pi is(k-1)/r} \left|x^k \ mod \ n\right\rangle \\
&= \frac{1}{\sqrt{r}} \sum_{k=1}^{r} e^{-2\pi isk/r} e^{2\pi is/r} \left|x^k \ mod \ n\right\rangle \\
&= e^{2\pi is/r} \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi isk/r} \left|x^k \ mod \ n\right\rangle \\
&= e^{2\pi is/r} |u_s\rangle
\end{aligned}$$

Observation utile

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi isk/r} \left|x^k \ mod \ n\right\rangle$$

Si $k = 0$ alors

$$\frac{1}{r} \sum_{s=0}^{r-1} e^{-2\pi isk/r} = \frac{1}{r} \sum_{s=0}^{r-1} 1 = 1$$

et si $k \neq 0$ alors

$$\frac{1}{r} \sum_{s=0}^{r-1} e^{-2\pi isk/r} = \frac{1}{r} \sum_{s=0}^{r-1} (e^{-2\pi ik/r})^s = \left(\frac{1}{r}\right) \frac{(e^{-2\pi ik/r})^r - 1}{e^{-2\pi ik/r} - 1} = 0.$$

On obtient donc

$$\begin{aligned} \sum_{s=0}^{r-1} \frac{1}{\sqrt{r}} |u_s\rangle &= \frac{1}{r} \sum_{s=0}^{r-1} \sum_{k=0}^{r-1} e^{-2\pi isk/r} \left|x^k \ mod \ n\right\rangle \\ &= \sum_{k=0}^{r-1} \left(\frac{1}{r} \sum_{s=0}^{r-1} e^{-2\pi isk/r} \right) \left|x^k \ mod \ n\right\rangle \\ &= |1\rangle \end{aligned}$$

Algorithme

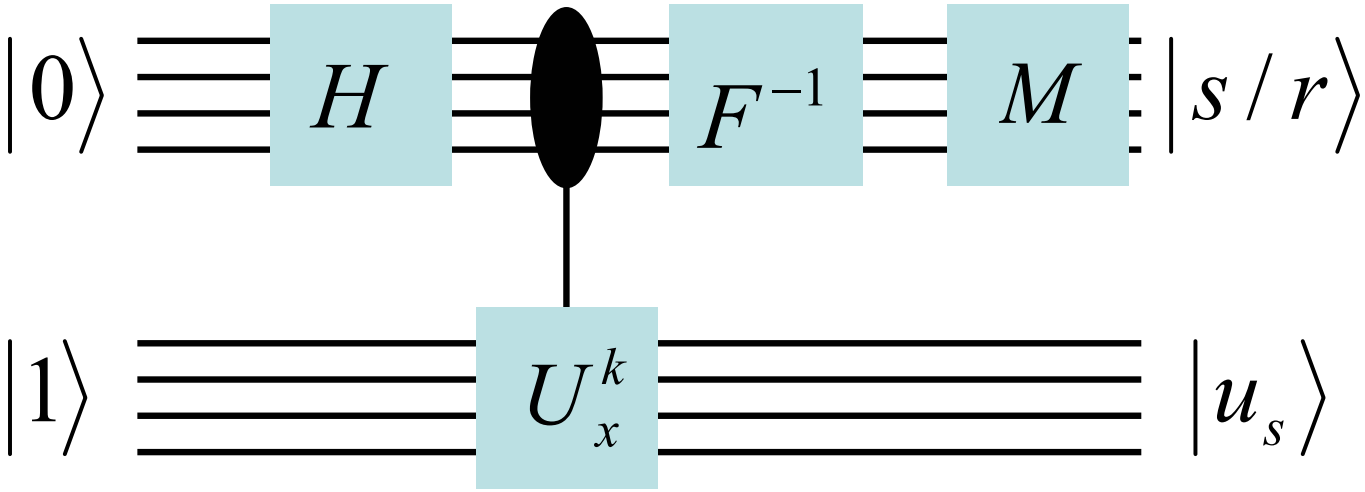
Pour un x donné (d'ordre r) on peut obtenir une approximation de s/r pour s uniformément distribué sur $\{0, \ldots, r-1\}$ en mesurant le premier registre de l'état suivant.

$$|\psi\rangle \;=\; F_t^\dagger \; V_x \; (H \otimes I) \; |0\rangle \, |1\rangle$$

C'est une application directe de l'estimation de phase.

$$\begin{aligned}
|\psi\rangle &= F_t^\dagger \; V_x \; (H \otimes I) \; |0\rangle \, |1\rangle \\
&= F_t^\dagger \; V_x \; (H \otimes I) \; |0\rangle \left(\sum_{s=0}^{r-1} \frac{1}{\sqrt{r}} \, |u_s\rangle \right) \\
&= F_t^\dagger \; V_x \; \left(\sum_{k=0}^{2^t-1} \frac{1}{\sqrt{2^t}} \, |k\rangle \right) \left(\sum_{s=0}^{r-1} \frac{1}{\sqrt{r}} \, |u_s\rangle \right) \\
&= F_t^\dagger \; \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \left(\sum_{k=0}^{2^t-1} \frac{1}{\sqrt{2^t}} e^{-2\pi i k s/r} \, |k\rangle \right) |u_s\rangle \\
&\simeq \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \left| \widetilde{s/r} \right\rangle |u_s\rangle
\end{aligned}$$

Estimation de s/r



Qualité de l'estimation

Si le premier registre contient t qubits et si ϕ est observé alors on sait que $|\frac{s}{r} - \phi| \leq \frac{1}{2^{(t-2)}}$ avec probabilité au moins $\frac{3}{4}$.

Prenons $t = 2\lceil log(n) \rceil + 3$; on aura donc

$$\left|\frac{s}{r} - \phi\right| \leq \frac{1}{2^{(t-2)}} \leq \frac{1}{2n^2} \leq \frac{1}{2r^2}$$

Comme ϕ est proche de s/r, l'algorithme de fraction continue nous donne s/r.

Comme s est aléatoire, il est copremier avec r avec probabilité au moins $1/2$ et donc on obtient r que l'on peut vérifier efficacement.

Fractions continues

Si x est un nombre rationnel, la décomposition en fraction continue de x est

$$[a_0, a_1, \ldots, a_n] \equiv a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots \cfrac{1}{a_n}}}} = x$$

La fraction continue d'un nombre rationnel est toujours finie et si x est un nombre binaire fractionnaire de L bit alors $x \equiv [a_0, a_1, \ldots, a_n]$ avec n dans $O(L)$.

Fractions continues, exemple

$$
\begin{aligned}
\frac{31}{13} &= 2+\frac{5}{13} \\
&= 2+\frac{1}{\frac{13}{5}} \\
&= 2+\frac{1}{2+\frac{3}{5}} \\
&= 2+\frac{1}{2+\frac{1}{\frac{5}{3}}} \\
&= 2+\frac{1}{2+\frac{1}{1+\frac{2}{3}}} \\
&= 2+\frac{1}{2+\frac{1}{1+\frac{2}{3}}} \\
&= 2+\frac{1}{2+\frac{1}{1+\frac{1}{\frac{3}{2}}}} \\
&= 2+\frac{1}{2+\frac{1}{1+\frac{1}{1+\frac{1}{2}}}} \\
&\equiv [2,2,1,1,2]
\end{aligned}
$$

Fractions continues; convergent

Si $x \equiv [a_0, a_1, \ldots, a_n]$ alors un convergent de x est un nombre rationnel y tel que $y \equiv [a_0, a_1, \ldots, a_k]$ pour $1 \leq k \leq n$.

Théorème:
Si

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{2q^2}$$

alors $\frac{p}{q}$ est un convergent de x.

Fractions continues, exemple

Supposons que

$$\frac{s}{r} = 4/15$$

et que nous ayons observé le nombre rationnel binaire

$$x = 0.01000100 = \frac{17}{64}$$

Clairement

$$|x - \frac{s}{r}| = |\frac{17}{64} - \frac{4}{15}| = \frac{1}{960} \leq \frac{1}{450} = \frac{1}{2r^2}$$

On a que

$$x = \frac{17}{64} \equiv [0, 3, 1, 3, 4]$$

et

$$\frac{r}{s} = \frac{4}{15} \equiv [0, 3, 1, 3]$$

qui est bien un convergent de x.

Factorisation de 15

Nous allons appliquer l'algorithme de Shor pour factoriser $n = 15$, qui est le plus petit nombre composé impair qui n'est pas de la forme $a^b = n$.

Premièrement, on choisit $x \in_R \{1, \cdots, 15\}$ tel que $pgcd(x, 15) = 1$ - prenons $x = 2$.

Calculons d'abord l'ordre de x modulo n, c'est-à-dire le plus petit r tel que $2^r = 1 \ mod \ 15$. On utilisera l'algorithme de Shor pour trouver l'ordre en espérant que le r obtenu sera utile.

Ordre de 2 modulo 15

Dans l'algorithme on doit choisir t, comme $n = 15$ on choisit $t = 2\lceil log(n) \rceil + 3$ ce qui nous donne $t = 7$.

L'algorithme initialise le registre quantique avec $|0\rangle |1\rangle$ puis applique H sur les 7 premiers qubits pour obtenir

$$\frac{1}{\sqrt{128}} \sum_{i=0}^{2^7-1} |i\rangle |1\rangle$$

Ensuite on applique la transformation V_x qui passe de $|k\rangle |y\rangle$ à $|k\rangle \left|x^k y\right\rangle$ et on obtient

$$\frac{1}{\sqrt{128}} \sum_{i=0}^{2^7-1} |i\rangle \left|x^i\right\rangle$$

Après la transformée de Fourier

$$\frac{1}{\sqrt{128}} \sum_{i=0}^{2^7-1} |i\rangle \left|x^i\right\rangle$$

À partir de maintenant, rien ne sera fait avec le deuxième registre. Ce que l'on fait avec le registre n'aura pas d'influence sur la distribution des résultats sur le premier registre. On peut donc supposer qu'on le mesure. On obtiendra $2^i \ mod$ 15 pour un i aléatoire. Supposons que l'on observe 4. Il y aura donc un *collapse* et on obtiendra la superposition égale des paires $|i\rangle \left|x^i\right\rangle$ telles que $x^i = 4$.

$$S = \{i | x^i = 3 \ mod \ 15\} = \{2, 6, 10, 14, \cdots, 122, 126\}$$

donc

$$\frac{1}{\sqrt{|S|}} \sum_{i \in S} |i\rangle |4\rangle$$

et en se séparant du $|4\rangle$ on obtient

$$\frac{1}{\sqrt{|S|}} \sum_{i \in S} |i\rangle$$

Après la transformée de Fourier

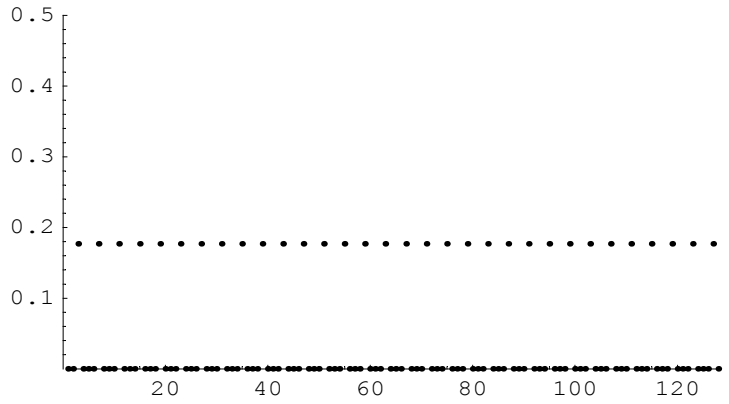
$$\frac{1}{\sqrt{|S|}} \sum_{i \in S} |i\rangle$$

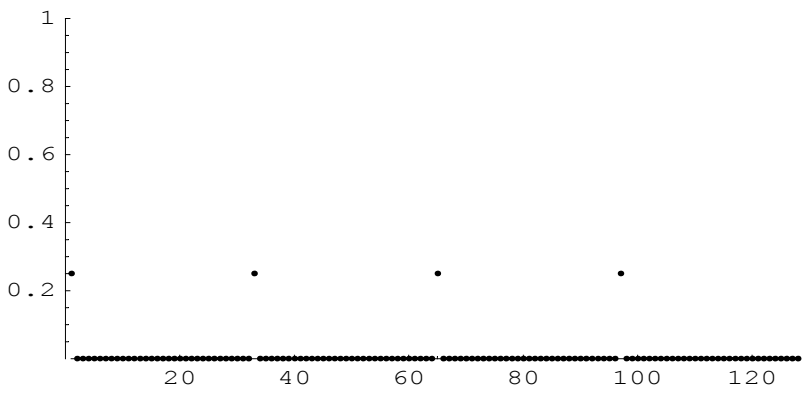
On applique maintenant F_7 et on mesure. On obtient facilement que la probabilité d'observer

$$P[|0\rangle] = P[|32\rangle] = P[|64\rangle] = P[|96\rangle] \simeq \frac{1}{4}$$

et la probabilité d'observer autre chose est très proche de 0.

Visualisation





Supposons que l'on observe 96.

On observe 96

Ce qui signifie que notre évaluation de la phase, s/r est de $96/128 = 3/4$. On peut donc espérer que $r = 4$.

On vérifie notre résultat et on obtient bien que $x^r = 2^4 = 16 = 1 \ mod \ 15$. De plus r est pair et $x^{r/2} = 2^2 = 4 \neq -1 \ mod \ 15$. On peut donc conclure que $r - 1$ ou $r + 1$ possèdent un facteur commun avec 15.

Clairement $pgcd(r - 1, 15) = pgcd(3, 15) = 3$ et $pgcd(r + 1, 15) = pgcd(5, 15) = 5$ qui sont tous les deux des facteurs de 15.

On aurait aussi pu observer 32 qui nous donne $1/4$. L'observation de 0 ne donne aucune information utile et 64 nous donne $2/4 = 1/2$ qui n'est pas utile non plus.