Le problème du sous-groupe caché

Miklos Santha

CNRS, IRIF, Université Paris Diderot, France

et

Centre for Quantum Technologies, NUS, Singapore

Problème du Sous-groupe Caché (PSC)

Problème du Sous-groupe Caché (PSC)

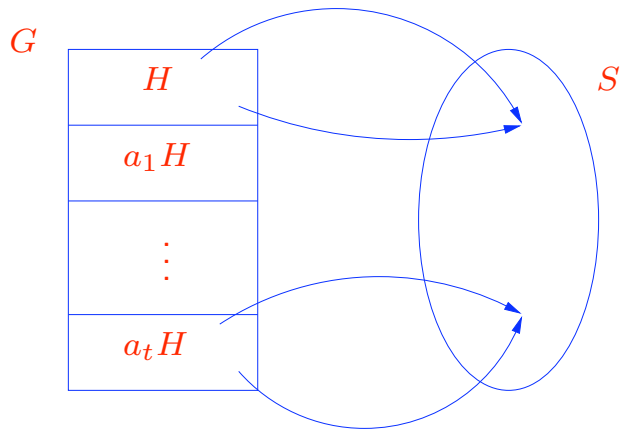
$\mathrm{PSC}(G; \mathcal{H})$ où G groupe, $\mathcal{H}$ famille de sous-groupes de G

Entrée (éventuellement par oracle): une fonction $f : G \to S$

Promesse: f cache un sous-groupe $H \in \mathcal{H}$:

$$f(x) = E(xH),$$

où E est injective sur les cosets gauches de H.



Sortie: Générateurs pour H.

Complexité: Nombre de requêtes à l'oracle et temps

Solutions quantiques efficaces pour le PSC

Le succès du PSC:

Théorème[Shor'94]: Le PSC est solvable dans les groupes abéliens finis en temps polynomial quantique en $\log(|G|)$.

Corollaire Factorisation (PSC en $\mathbb{Z}_q$) et le logarithme discret (PSC en $\mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$) sont calculables en temps polynomial quantique.

Extension à $\mathbb{R}$ et $\mathbb{R}^m$

Extension à certains groupes non-abéliens

Extension aux ensembles algébriques cachés de degré supérieur

Plan de l'exposé

1. Problème du sous-groupe caché (PSC)
2. PSC en groupes abéliens (finis et infinis)
3. Cryptographie post-quantique
4. PSC en groupes non abéliens
5. Le groupe diédral
6. Groupes diédraux généralisés

Groupes abéliens finis

Caractères d'un groupe abélien fini

Soit G un groupe abélien fini.

Definition: Un caractère $\chi : G \to \mathbb{C}^*$ est un homorphisme de groupes.

Remarque: $\chi(x)$ est une racine $|G|^{\text{e}}$ de l'unité.

$\widehat{G} = \{\text{caractères } G\}$.

Théorème: G et $\widehat{G}$ sont isomorphes. $\widehat{G} = \{\chi_y : y \in G\}$.

Exemples: $G = \mathbb{Z}_q$: $\chi_y(x) = \omega_q^{x \cdot y}$.

$G = G_1 \times G_2$: $\chi_y(x) = \chi_{y_1}(x_1)\chi_{y_2}(x_2)$.

Définition: Soit $H \leq G$. Son sous-groupe orthogonal est

$$H^\perp = \{y \in G : \forall h \in H, \chi_y(h) = 1\}.$$

Théorème: Soit $H \leq G$. Il existe un algorithme déterministe qui calcule H à partir de $H^\perp$ en temps $O(\log^3 |G|)$.

Transformée de Fourier quantique

Soit G un groupe abélien fini.
On considère $\mathbb{C}^G$, l'espace de Hilbert engendré par G.

Bases:

- Dirac: $\{|x\rangle : x \in G\}$.
- Caractères: $\{|\chi_y\rangle : y \in G\}$,
  où $|\chi_y\rangle = \sum_x \chi_y(x)|x\rangle$.

Définition: $\mathrm{TFQ}_G : |y\rangle \mapsto \frac{1}{\sqrt{G}}|\chi_y\rangle$.

Propriété principale: Soit $H \leq G$, $x \in G$. Alors

$$\mathrm{TFQ}_G|x + H\rangle = |H^\perp(x)\rangle, \quad \text{où}$$

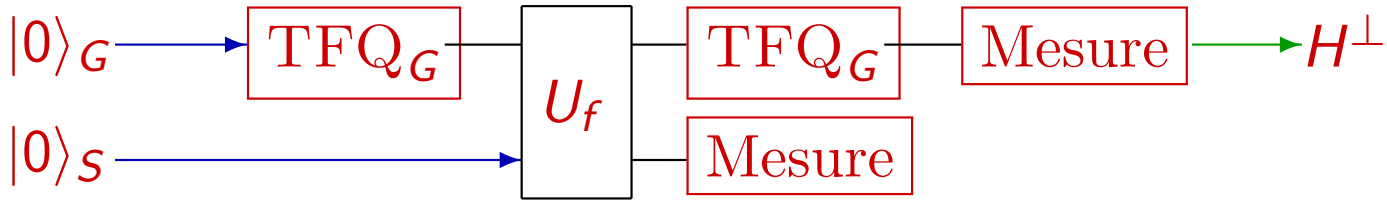
$|x + H\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |x + h\rangle$ et
$|H^\perp(x)\rangle = \frac{1}{\sqrt{|H^\perp|}} \sum_{y \in H^\perp} \chi_y(x)|y\rangle$.

Théorème: TFQ_G approché est calculable en temps polynomial quantique.

Solution standard pour PSC en un groupe abélien fini G

Echantillonage quantique de Fourier répété de f qui cache H:

Circuit : **Fourier sampling^f (G)**



Analyse

- TFQ_G sur 1$^{\mathrm{er}}$ registre: $1/\sqrt{|G|}\ \sum_{x\in G}\ |x\rangle\ |0\rangle$
- Requête à f : $1/\sqrt{|G|}\ \sum_{x\in G}\ |x\rangle\ |f(x)\rangle$
- Mesure du 2$^{\mathrm{ème}}$ registre: $|a+H\rangle\ |f(a)\rangle$
- TFQ_G sur 1$^{\mathrm{er}}$ registre: $|H^\perp(a)\rangle$
- Mesure du 1$^{\mathrm{er}}$ registre: y uniforme en $H^\perp$.

On peut aussi considérer comme entrée à PSC des états cosets aléatoires

$$|a+H\rangle = \sum_{h\in H}|a+h\rangle$$

Simon et Ordre (Shor) revisités

Simon:

$G = \{0,1\}^n$, $H = \{0^n, s\}$ pour un $0^n \neq s \in \{0,1\}^n$

$f(x) = f(y)$ ssi $x = y$ où $x \oplus y = s$

Caractères

$$\chi_y : \begin{array}{ccc} \{0,1\}^n & \to & \mathbb{C} \\ x & \mapsto & (-1)^{x \cdot y} \end{array} \quad \text{for } y \in \{0,1\}^n$$

où $x \cdot y = \sum_{i=1}^{n} x_i y_i \mod 2$ $H^\perp = \{y : s \cdot y = 0\}$

Ordre: $N, a \in \mathbb{Z}_N^*$, on cherche l'ordre de a modulo N

$G = \mathbb{Z}$, $H = \{0, r, 2r, \ldots\}$, on remplace $\mathbb{Z}$ par $\mathbb{Z}_q$ pour $q \approx N^2$

La fonction qui cache H (supposons que $r|q$):

$$f : \begin{array}{ccc} \mathbb{Z}_q & \to & \mathbb{Z}_N \\ x & \mapsto & a^x \bmod N \end{array}$$

Caractères:

$$\chi_c : \begin{array}{ccc} \mathbb{Z}_q & \to & \mathbb{C} \\ x & \to & \omega_q^{cx} \end{array} \quad \text{pour } k \in \mathbb{Z}_q$$

$\chi_c(r) = 1$ ssi q/r divides c, $H^\perp = \{c : q/r \text{ divise } c\}$

Cryptographie post-quantique

Systèmes cryptographiques en danger

Théorème[Shor'94]: Le PSC est solvable dans les groupes abéliens finis en temps polynomial (en $\log(|G|)$) quantique.

Corollaire: Factorisation, logarithme discret, logarithme discret en courbes elliptiques sont solvable en temps polynomial quantique.

Un ordinateur quantique casserait les systèmes suivants:

- RSA
- Echange de clés Diffie-Hellman (DH)
- Chiffrement El Gamal
- Digital Signature Algorithm (DSA)
- ECDH, ECDSA, EC integrated Encryption Scheme
- Cryptographie à base de couplage
- etc.

L'histoire du système de chiffrement SOLILOQUY

SOLILOQUY: A cautionary tale[Campbell, Groves, Shepherd '14]
Une publication de Communications-Electronics Security Group dans le Government Communications Headquarters

Développé 2007, abandonné 2014 suites aux attaques quantiques

"We would like to state clearly that, following our work on the quantum algorithm, we have stopped the development of SOLILOQUY as a potential quantum-resistant primitive and we do not recommend its use for real-world deployement.

As of late 2014, when novel types of quantum-resistant cryptography are being developed for real world deployment, we caution that much care and patience will be required to ensure that each design receives a thorough security assessment.

It would seem that quantum algorithms for resolving Abelian Hidden Subgroup Problems have broader applicability to cryptography than 'traditionally' documented".

Recommandation de NSA pour une crypto post-quantique

National Security Agency (NSA) "guidance" en Août 2015:

"Our ultimate goal is to provide cost effective security against a potential quantum computer.

We are working with partners across the USG, vendors, and standards bodies to ensure there is a clear plan for getting a new Suite of algorithms that are developed in an open and transparent manner that will form the foundation of our next Suite of cryptographic algorithms.

Until this new suite is developed and products are available implementing the quantum resistant suite, we will rely on current algorithms. For those partners and vendors that have not yet made the transition to Suite B algorithms, we recommend not making a significant expenditure to do so at this point but instead to prepare for the upcoming quantum resistant algorithm transition".

Projet post-quantique de NIST

http://csrc.nist.gov/groups/ST/post-quantum-crypto/

15 Décembre 2016: "The National Institute of Standards and Technology (NIST) is now accepting submissions for quantum-resistant public-key cryptographic algorithms. The deadline for submission is November 30, 2017.

In recent years, there has been a substantial amount of research on quantum computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use.

The question of when a large-scale quantum computer will be built is a complicated one. While in the past it was less clear that large quantum computers are a physical possibility, many scientists now believe it to be merely a significant engineering challenge.

It has taken almost two decades to deploy our modern public key cryptography infrastructure. We must begin now to prepare our information security systems to resist quantum computing".

Méthodes pour une cryptographie post-quantique

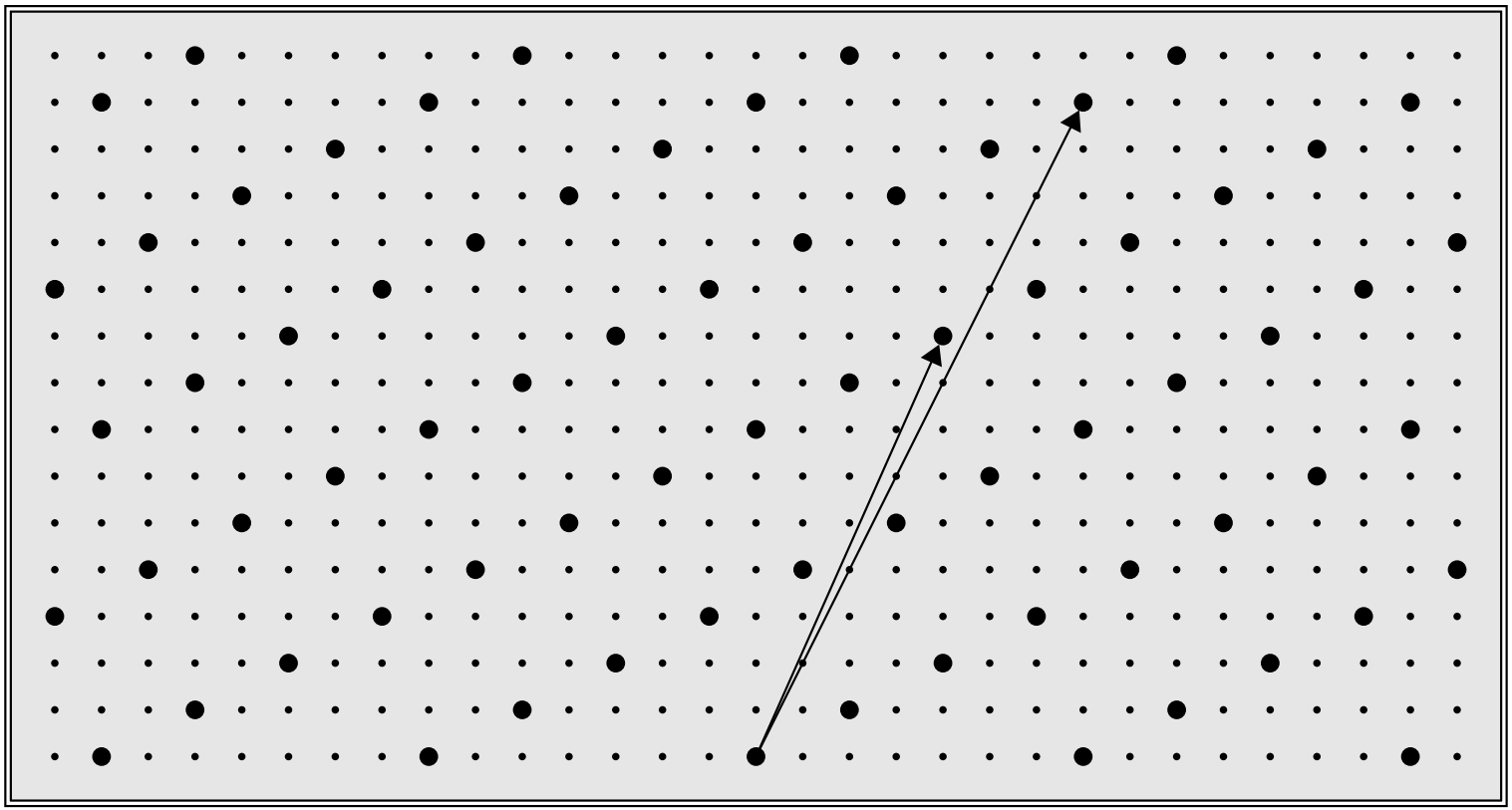
- Codes correcteurs d'erreur (McElice 1978)
- Hachage (Merkle 1979)
- Réseaux (Ajtai 1996)
- Polynômes multivariés (Patarin 1996)
- Isogénie de courbes elliptiques supersingulières (Rostovtsev et Stolbunov 2006)
- Cryptographie symétrique (AES)

Réseaux

Définition: Un réseau $\mathcal{L}$ est un sous-groupe discret de $\mathbb{R}^m$

Déf. équivalente: un ensemble de combinaisons linéaires entières

$$\alpha_1 \vec{b_1} + \cdots + \alpha_k \vec{b_k} \quad \text{with } k \leq m$$

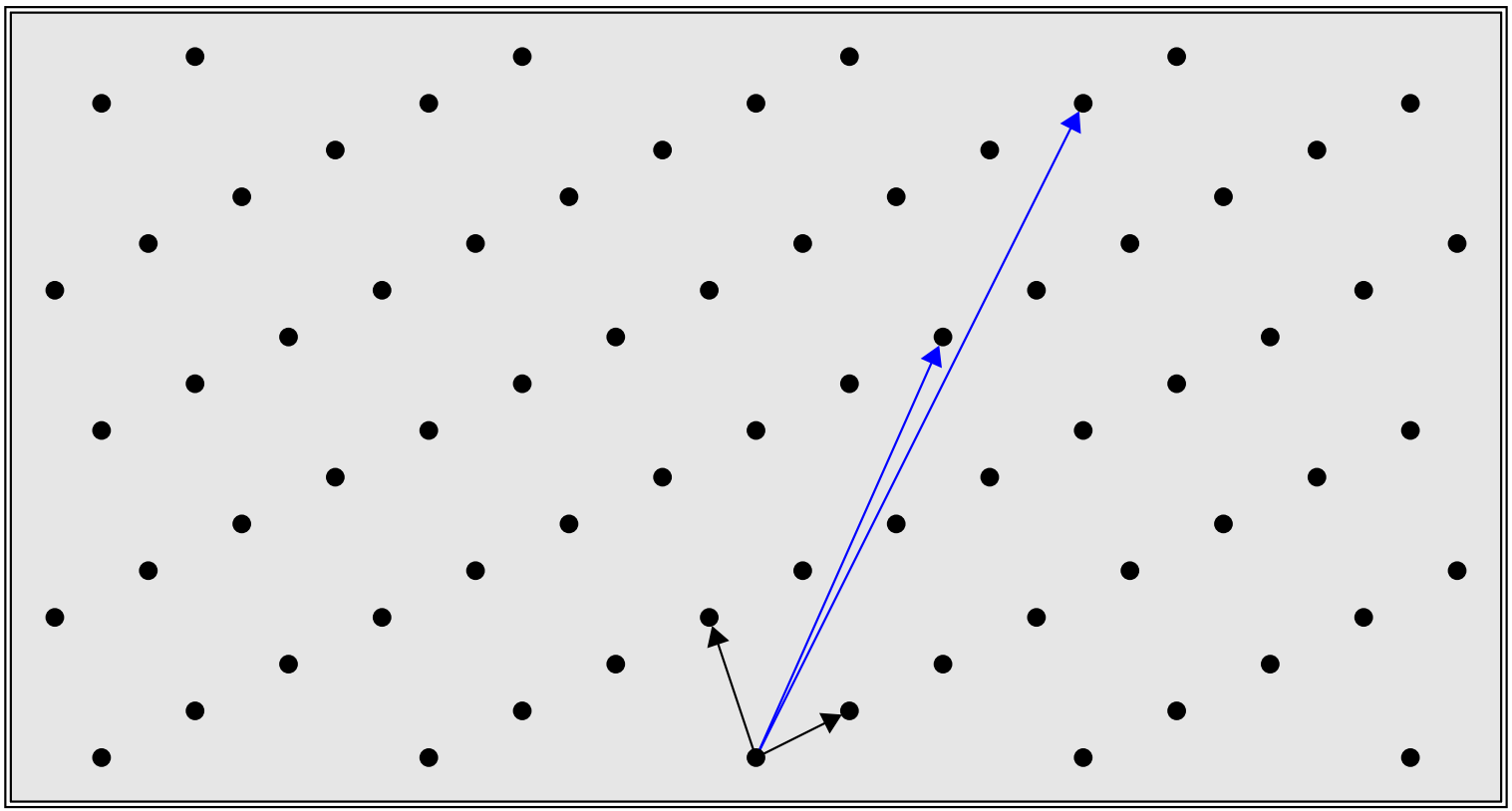


Vecteurs courts

Vecteur(s) Court(s)

Entrée: La base d'un réseau $\mathcal{L}$

Sortie: Le(s) vecteur(s) le(s) plus court(s) de $\mathcal{L}$



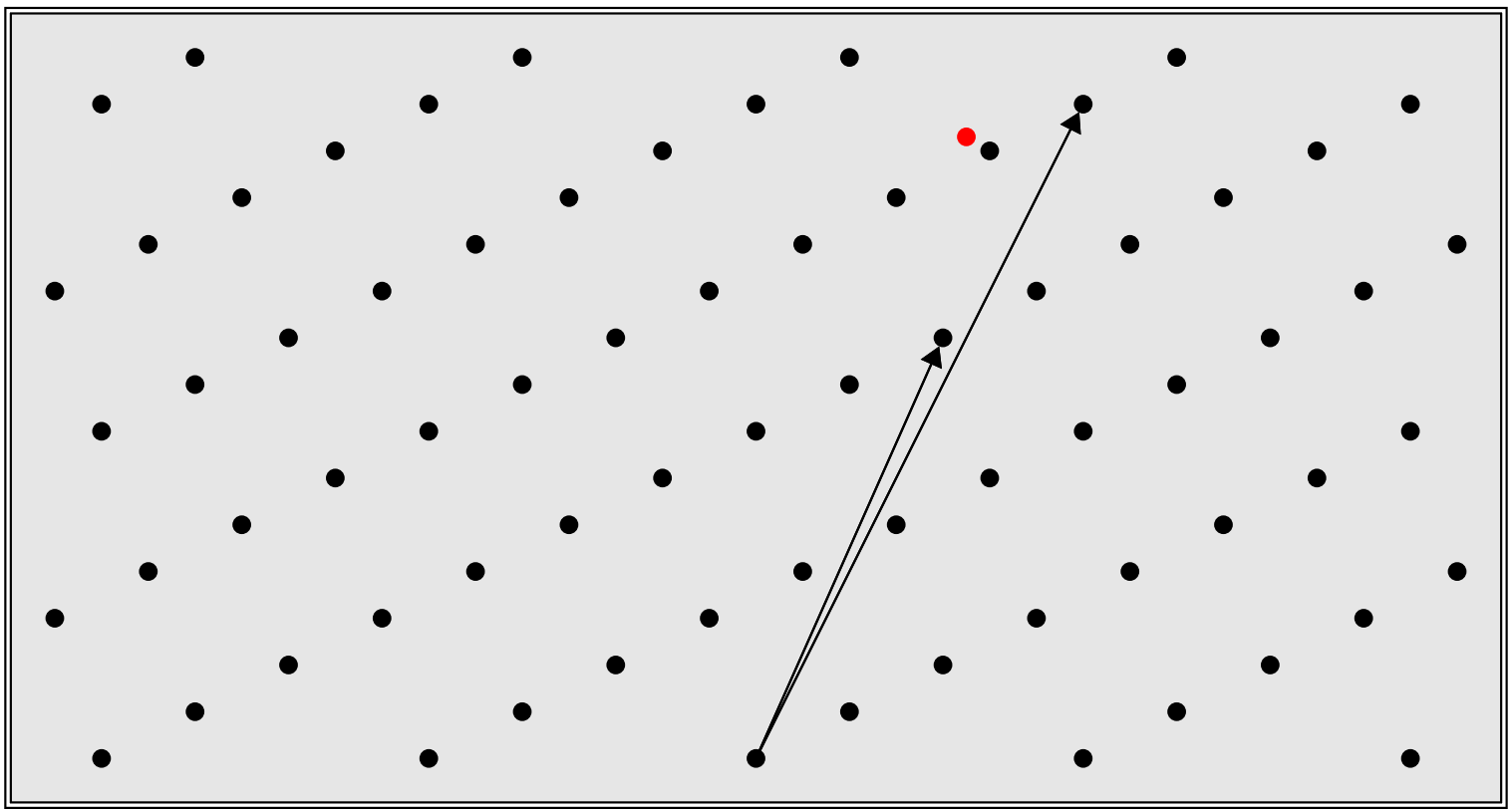
Vecteur plus proche

Vecteur plus proche

Entrée: La base d'un réseau $\mathcal{L}$ et $b \in \mathbb{R}^m$

Promesse: $\mathrm{dist}(\mathcal{L}, x)$ garantit l'unicité du vecteur le plus proche

Sortie: a, où a est le vecteur le plus proche de $\mathcal{L}$



Complexité en moyenne et en pire cas

- Cryptographie nécessite l'intractabilité en moyenne: problèmes dont les instance aléatoires sont difficiles
- La théorie de la NP-complétude est basée sur la notion de la difficulté en pire cas
- De nombreux problèmes NP-complets sont faciles en moyenne
- Théorème[Ajtai'96]: Réduction dans les réseaux des problèmes en pire cas aux problèmes en moyenne
- Corollaire: Constructions cryptographiques incassables sauf si toutes les instances de certains problèmes de réseau sont faciles

Groupes Abéliens infinis

Généralisation du PSC pour $\mathbb{R}^m$

- PSC dans une approximation discrétisée et borné de $\mathbb{R}^m$
  Algorithme quantique polynomial pour calculer
  - équation de Pell [Hallgren'02]
  - dans les corps de nombres de degré constant
    groupe des unités, idéal principal, groupe des classes d'idéaux
    [Hallgren'05, Schmidt, Vollmer'05]
- PSC continu sur $\mathbb{R}^m$
  Algorithme quantique polynomial pour calculer dans les corps de nombres de degré arbitraire
  - groupe des unités [Eisenträger, Hallgren, Kitaev, Song'14]
  - idéal principal, groupe des classes d'idéaux [Biasse, Song'16]

Attaques quantiques efficaces contre certains systèmes cryptographiques dans des réseaux d'idéaux [Cramer, Ducas, Peikert, Regev'16]

Equation de Pell

Définition: L'équation de Pell est l'équation diophantienne

$$x^2 - dy^2 = 1$$

où $p^2 \nmid d$, pour tout premier p. On suppose $x, y > 0$.

La solution (x_0, y_0) est fondamentale si $x_0 + \sqrt{d}y_0 \in \mathbb{Q}[\sqrt{d}]$ est le plus petit parmi les solutions. On dénote $\xi(d) = x_0 + y_0\sqrt{d}$.

Exemple: $\xi(2) = 3 + 2\sqrt{2}$.

Fait: Pour chaque solution (x, y), il existe $n \in \mathbb{N}$ tel que

$$x + y\sqrt{d} = \xi(d)^n.$$

On ne peut même pas écrire $\xi(d)$ en temps polynomial:

$$\xi(d) = \mathrm{e}^{O(\sqrt{d}\log d)}$$

Définition : Le régulateur est $R(d) = \ln(\xi(d))$.

Le meilleur algorithme classique calcule $\lceil R \rceil$ en temps $2^{O(\sqrt{\log d})}$.

Algorithme de Hallgren:

1. Trouve une fonction sur $\mathbb{R}$ dont la période est R
2. Donne une solution quantique en temps polynomial pour trouver une période (irrationnelle) sur $\mathbb{R}$.

Groupes non Abéliens

La complexité de requête de PSC

Théorème[Ettinger, Høyer, Knill'04]: La complexité de requête de PSC est polynomial en $\log(|G|)$.

Le nombre de sous-groupes en G est $r = 2^{O(\log^2(|G|))}$

L'etat initial est $|\Psi\rangle = |0\rangle \bigotimes \left(\frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle \, |f(x)\rangle \right)^{\otimes s}$

On numérote les sous-groupes $|K_1| \geq \ldots \geq |K_r|$

L'algorithme est $\mathrm{Test} = \mathrm{Test}_r \cdots \mathrm{Test}_1$ où Test_i

- signale si les registres de $|\Psi\rangle$ sont en superpositions des états coset $\frac{1}{\sqrt{|K_i|}} \sum_{k \in K_i} |ak\rangle$ de K_i
- applique l'identité sur leur complément orthogonal

Fait: Si f cache H alors Test le signale avec probabilité $\geq 1 - \frac{4r}{2^{s/2}}$

L'algorithme standard?

Généraliser l'algorithme standard pour les groupes abéliens?

Problèmes:

- Définir et implémenter efficacement la transformée de Fourier
- Est-ce que l'information fournie par l'échantillonage de Fourier est suffisante pour déterminer le sous-groupe caché?
- Trouver un post-traitement efficace

Transformée de Fourier

Déf: Représentation linéaire de G sur $\mathbb{C}^n$ est un homomorphisme

$$\sigma : G \to \mathrm{GL}(\mathbb{C}^n)$$

La dimension de σ est $d_\sigma = n$.

La somme directe de $\sigma : G \to V$ et $\sigma' : G \to V'$ est

$$\sigma \oplus \sigma' : G \to V \oplus V'$$

de dimension $d_\sigma + d_{\sigma'}$.

σ est irréductible si elle n'a pas de sous-espace stable non-trivial.

Théorème: Soit $\widehat{G}$ l'ensemble des représentations irréductibles:

$$\sum_{\sigma \in \widehat{G}} d_\sigma^2 = |G|.$$

Déf: Transformée de Fourier $\mathrm{TFQ}_G : \mathbb{C}^G \to \bigoplus_{\sigma \in \widehat{G}} (\mathbb{C}^{d_\sigma} \otimes \mathbb{C}^{d_\sigma})$ où

$$\mathrm{TFQ}_G |g\rangle = \sum_{\sigma \in \widehat{G}} \frac{d_\sigma}{\sqrt{|G|}} \sum_{j,k=1}^{d_\sigma} \frac{1}{\sqrt{d_\sigma}} \sigma(g)_{j,k} |\sigma, j, k\rangle$$

Exemple: Efficace dans le groupe symétrique, diédral,...

Echantillonnage de Fourier et post-traitement

TFQ_G sur un état coset

$$\mathrm{TFQ}_G|aH\rangle = \sum_{\sigma\in\widehat{G}} \sqrt{\frac{d_\sigma}{|G|}} \sqrt{\frac{1}{|H|}} \sum_{j,k=1}^{d_\sigma} \left(\sum_{h\in H} \sigma(ah) \right)_{j,k} |\sigma, j, k\rangle$$

1. Echantillonnage de Fourier faible: on mesure la représentation

$$\Pr[\sigma] = \| \sum_{h\in H} \sigma(h) \|_{\mathrm{F}}^2$$

Théorème[Hallgren, Russel, Ta-Sma'00]: Cela suffisant pour déterminer les sous-groupes normaux

2. Echantillonnage de Fourier fort: on mesure aussi les indices de $\sum_{h\in H} \sigma(ah)$. Il existe un choix pour la base

Théorème[Ettinger, Høyer00]: Dans le groupe diédral l'information est suffisante, mais pas de post-traitement connu

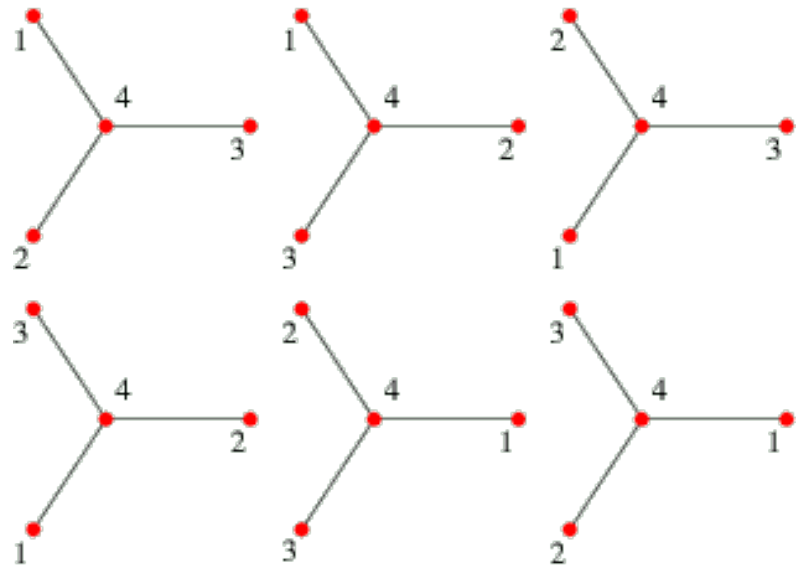
Théorème[HRT'00]: Dans le groupe symétrique l'information n'est pas suffisante

PSC et l'isomorphisme de graphes

Définition: Soit $G = ([n], E)$ et $\pi \in S_n$. Alors $\pi(G) = ([n], \pi(E))$, où $\{i, j\} \in E \iff \{\pi(i), \pi(j)\} \in \pi(E)$

Le groupe d'automorphismes de G est

$$\mathrm{Aut}(G) = \{\pi \in S_n : \pi(G) = G\}$$



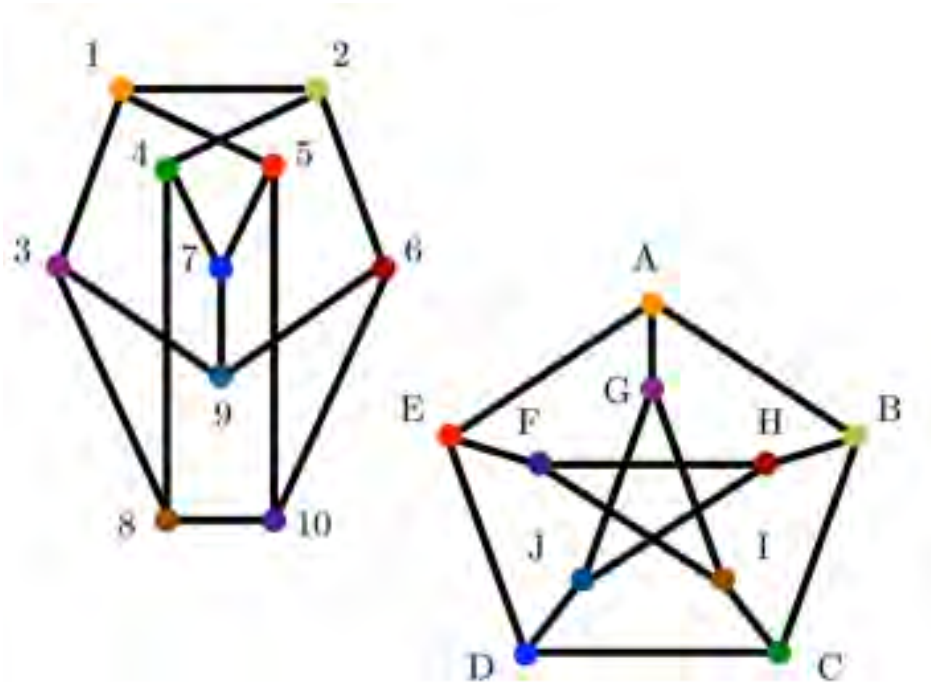
Fait: La fonction $f : S_n \to \{$ graphes sur n sommets $\}$ définie par

$$f(\pi) = \pi(G)$$

cache le sous-groupe $\mathrm{Aut}(G)$ de S_n

PSC et l'isomorphisme de graphes

Définition: $G_1 = (V_1, E_1)$ et $G_2 = (V_2, E_2)$ sont isomorphes s'il existe $\pi \in S_n$ telle que $\{i, j\} \in E_1 \iff \{\pi(i), \pi(j)\} \in E_2$



Soient $G_1 = (V_1, E_1)$ et $G_2 = (V_2, E_2)$ connexes avec $|V_1| = |V_2| = n$ et $V_1 \cap V_2 = \emptyset$. Soit $G = (V_1 \cup V_2, E_1 \cup E_2)$.

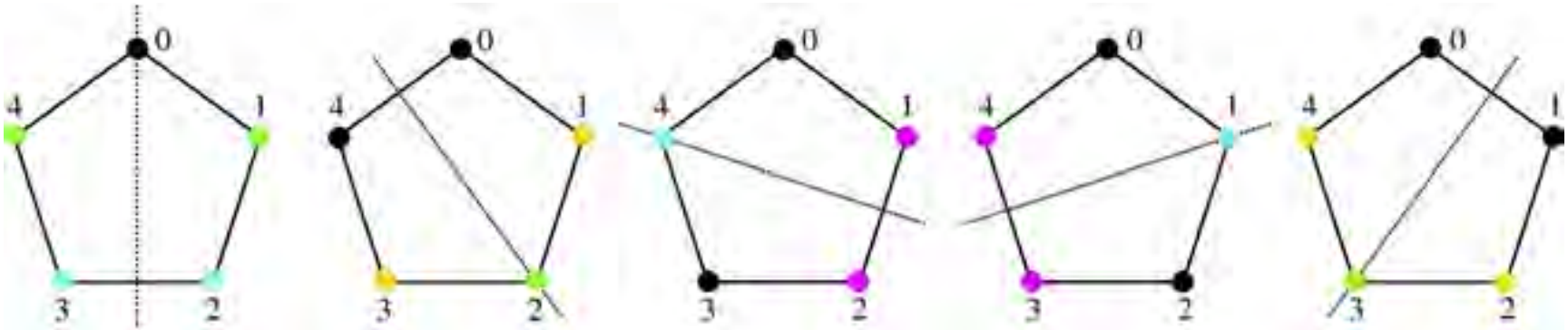
Théorème : G_1 et G_2 sont isomorphes ssi $\mathrm{Aut}(G)$ contient une permutation qui échange V_1 et V_2.

Le groupe diédral

Attaques quantiques potentielles

PSC dans les groupes non-abéliens

Example: Groupe diédral D_N: le groupe des isométries qui conservent un polygone régulier à N côtés



D_N : N rotations $(t, 0)$ et N réflexions $(t, 1)$ pour $0 \leq t \leq N-1$.

$$(t_1, b_1) \cdot (t_2, b_2) = (t_1 + (-1)^{b_1} t_2, b_1 \oplus b_2)$$

Famille de sous-groupes $\mathcal{H} = \{H_s : 0 \leq s \leq N-1\}$, où

$$H_s = \{(0,0), (s,1)\}$$

Cosets droites de H_s sont $\{(t,0), (t+s,1)\}$ pour $0 \leq t \leq N-1$

Entrée à $\mathrm{PSC}(D_N, \mathcal{H})$ est un état coset pour t aléatoire:

$$\frac{1}{\sqrt{2}}(|t,0\rangle + |t+s,1\rangle)$$

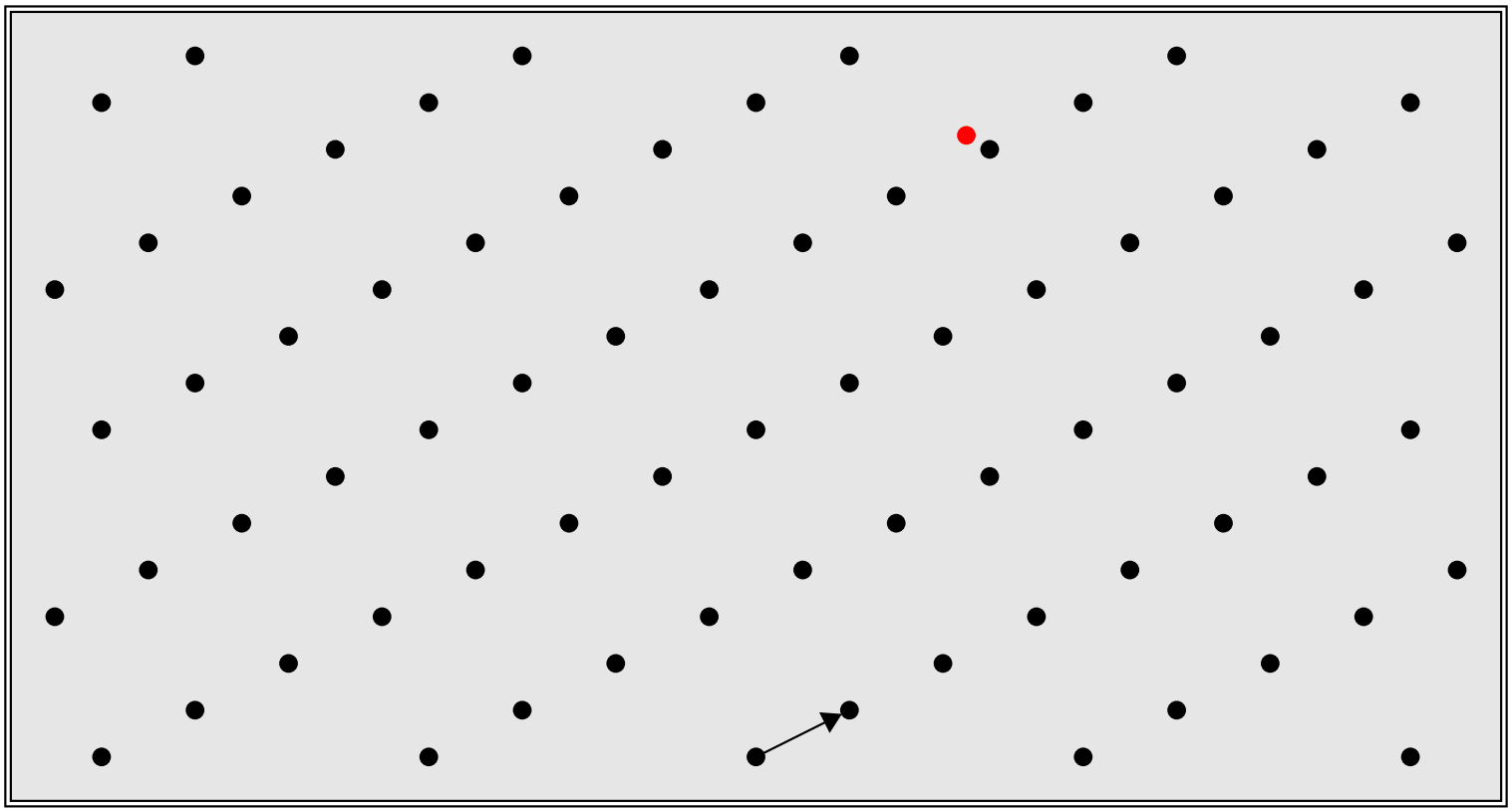
Problèmes de réseaux et le groupe diédral

Example: Réduction de VECTEUR PLUS PROCHE modulo N au PSC dans le groupe diédral D_N.

Supposons que $\mathcal{L}$ est de dimension 1, engendré par a

Entrée: $(a, b = sa + e) \in \mathbb{Z}_N^m \times \mathbb{Z}_N^m$ où $\|e\|$ est suffisamment courte pour que s soit unique

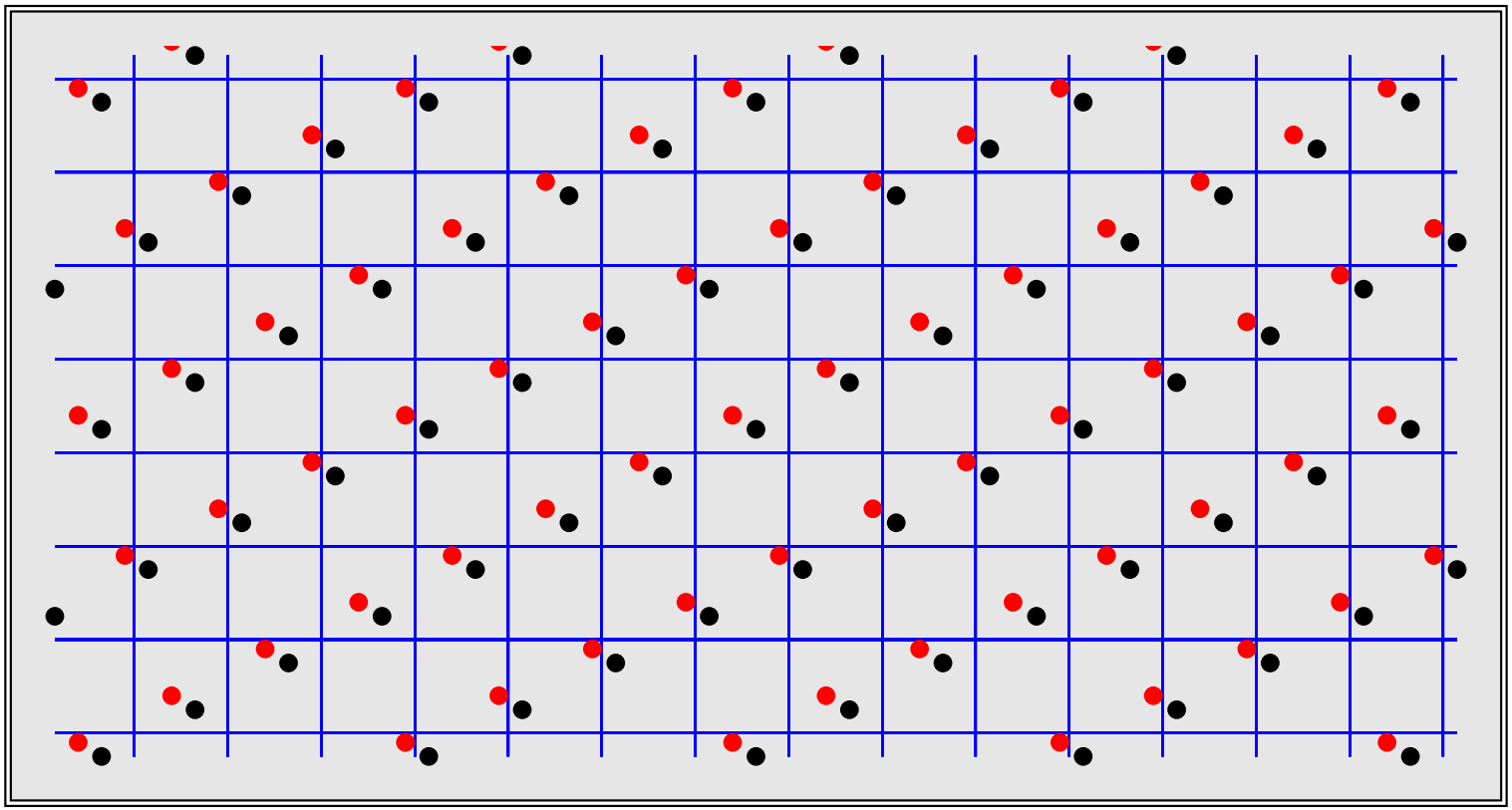
Sortie: $s \in \mathbb{Z}_N$



Réduction de réseau à PSC dans le groupe diédral

On partitionne $\mathbb{Z}_N^m$ en cubes de côté ℓ où $\ell\sqrt{m} < \|a\|$ et $\|e\| \ll \ell$

On définit $\phi : \mathbb{Z}_N^m \to \{\text{cubes}\}$, où $\phi(x) =$ le cube qui contient x



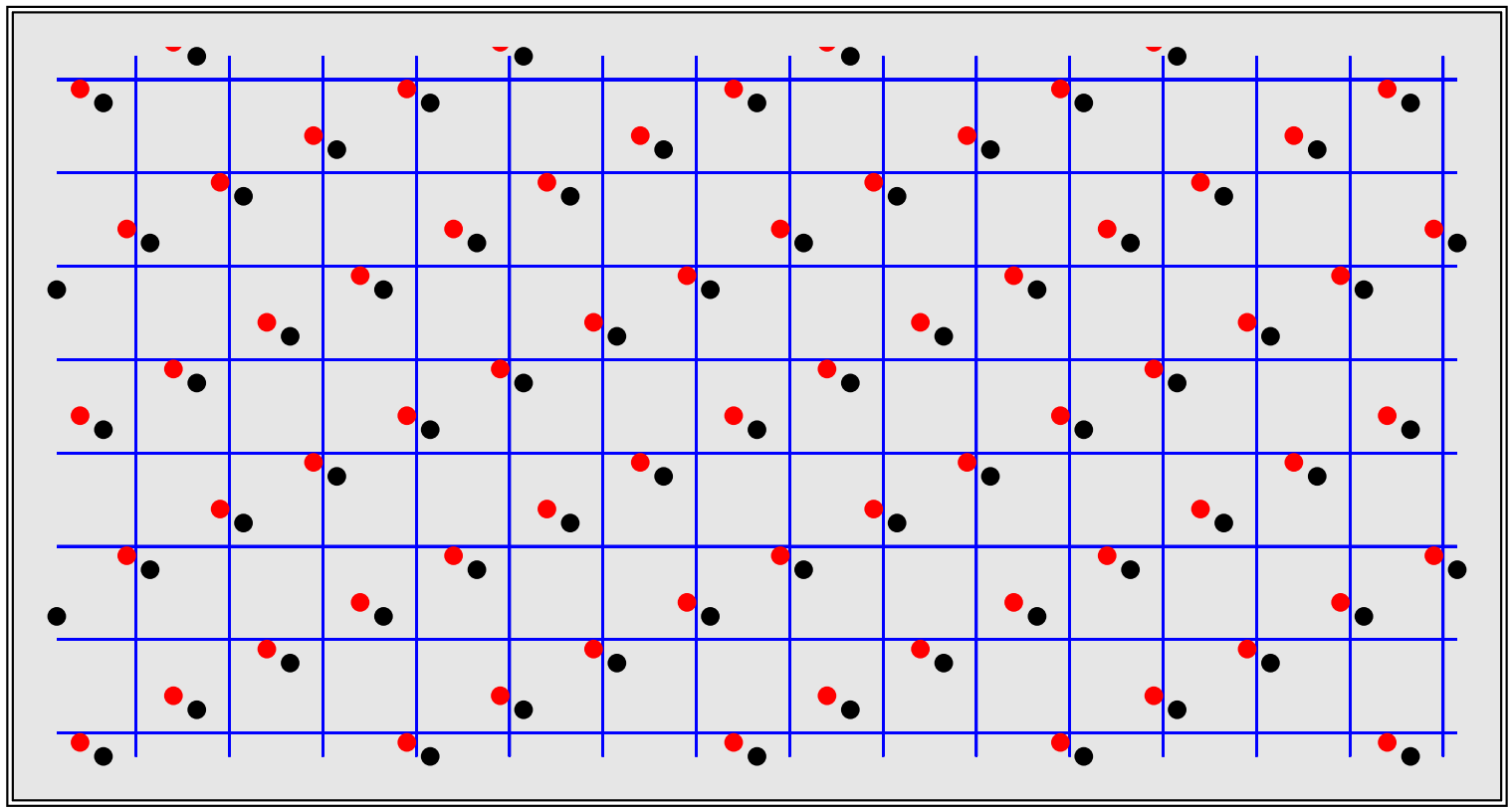
Réduction de réseau à PSC dans le groupe diédral

On crée l'état

$$\sum_{t\in\mathbb{Z}_N}|t\rangle|\phi(ta)\rangle|0\rangle+\sum_{t\in\mathbb{Z}_N}|t\rangle|\phi(b+ta)\rangle|1\rangle=$$
$$\sum_{t\in\mathbb{Z}_N}|t\rangle|\phi(ta)\rangle|0\rangle+\sum_{t\in\mathbb{Z}_N}|t-s\rangle|\phi(e+ta)\rangle|1\rangle$$

On mesure le 2ème registre, l'état s'effondre à un singleton ou à

$$|t\rangle|0\rangle+|t-s\rangle|1\rangle$$



Algorithme de Kuperberg'2003 pour le groupe diédral

Theorème: $\mathrm{PSC}(D_{2^n}, \mathcal{H})$ est solvable en temps quantique $2^{O(\sqrt{n})}$.

Preuve: Secret $s = s_{n-1} \dots s_1 s_0$. On montre comment trouver s_0.

L'entrée venant de la réduction:

$$|t, 0\rangle + |t + s, 1\rangle \qquad \text{où } t \in \mathbb{Z}_{2^n} \text{ est aléatoire}$$

Après TFQ sur le deuxième registre on "obtient l'étiquette x":

$$|0\rangle + \omega_{2^n}^{sx}|1\rangle \qquad \text{pour } x \in \mathbb{Z}_{2^n} \text{ aléatoire}$$

Si $x = 2^{n-1}$, Hadamard donne s_0. Comment obtenir $x = 2^{n-1}$?

Combiner les étiquettes x et y en produit tensoriel:

$$|00\rangle + \omega^{sx}|10\rangle + \omega^{sy}|01\rangle + \omega^{s(x+y)}|11\rangle$$

Mesure de la parité des qubits donne avec probabilité $\frac{1}{2} - \frac{1}{2}$:

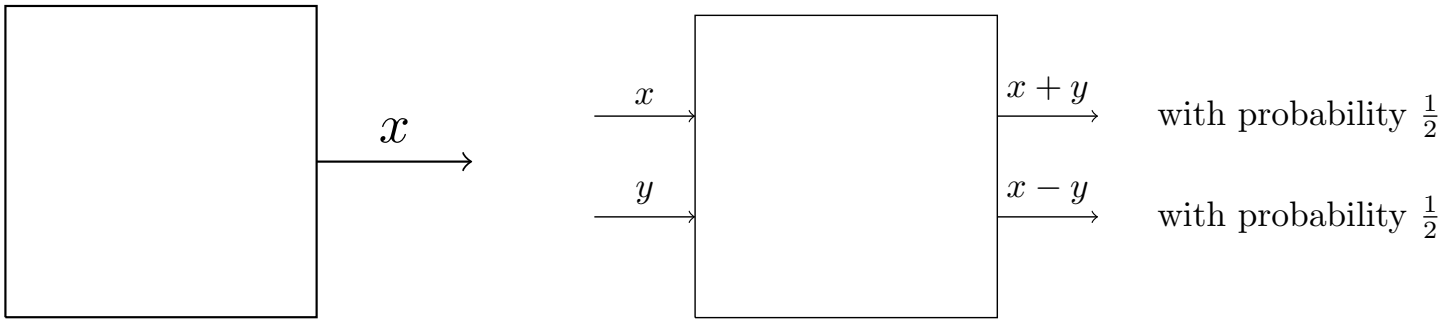
$$|00\rangle + \omega^{s(x+y)}|11\rangle \quad \rightsquigarrow \quad |0\rangle + \omega^{s(x+y)}|1\rangle$$

et

$$|01\rangle + \omega^{s(x-y)}|10\rangle \quad \rightsquigarrow \quad |0\rangle + \omega^{s(x-y)}|1\rangle$$

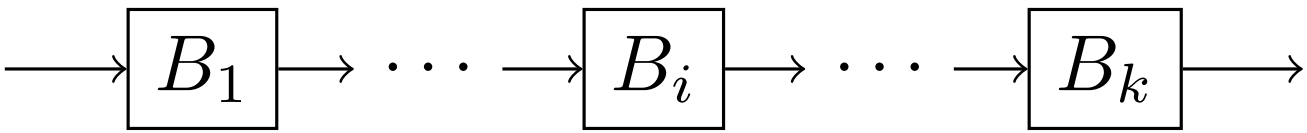
Problème des deux boîtes magiques

Soit $n = k^2 + 1$. On voudrait obtenir l'étiquette $2^{n-1} \mod 2^n$:

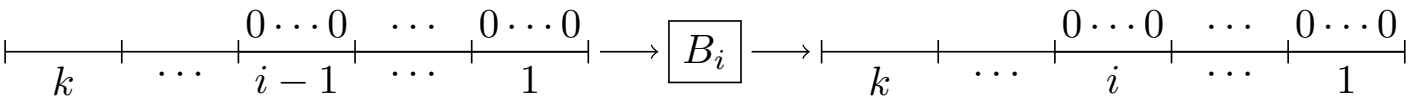


On prend $8^k \cdot 2^k = 2^{O(\sqrt{n})}$ étiquettes aléatoires de la boîte type 1

On enchaîne k boîtes type 2:



A l'aide de la boîte numéro i: met à 0 les bits du bloc i



Nombre d'éléments après B_i est $\geq 8^{k-i}2^k$

Groupes diédraux généralisés

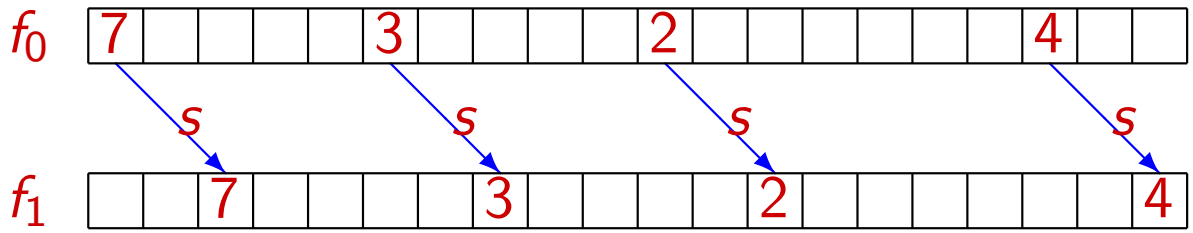
Problème de la Translation Cachée PTC

Entrée: deux fonctions injectives $f_0, f_1 : G \to S$

Promesse: Il y a une translation $s \in G$ entre f_0 et f_1:

$$\forall x \in G, \quad f_0(x) = f_1(xs).$$

Sortie: s.



Théorème [Ettinger, Høyer'00]: Si G est un groupe Abélien alors

$$\mathrm{PTC} \text{ sur } G \qquad \text{et} \qquad \mathrm{PSC} \text{ sur } G \rtimes \mathbb{Z}_2$$

sont essentiellement les mêmes problèmes.

Algorithme quantique efficace pour $\mathbb{Z}_p^n \rtimes \mathbb{Z}_2$

Les groupes diédraux généralisés: Pour un groupe Abélien G

$$\mathrm{Dih}(G) = G \rtimes \mathbb{Z}_2 \qquad \text{où}$$

$$(x_1, b_1) \cdot (x_2, b_2) = (x_1 + (-1)^{b_1} x_2, b_1 \oplus b_2).$$

On considère $G = \mathbb{Z}_p^n$

Théorème [Friedl, Ivanyos, Magniez, Santha, Sen'03]:

$\mathrm{PSC}(\mathbb{Z}_p^n \rtimes \mathbb{Z}_2, \mathcal{H})$ est solvable en temps quantique $(n+p)^{O(p)}$, où

$$\mathcal{H} = \{H_s : s \in \mathbb{Z}_p^n\} \quad \text{et.} \quad H_s = \{(0,0), (s,1)\}.$$

Cet algorithme est polynomial quand p est constant.

Algorithme: 1ère partie (quantique)

On applique TFQ sur le produit direct $\mathbb{Z}_p^n \times \mathbb{Z}_2$. Etat:

$$\frac{1}{2p^n} \sum_{x \in \mathbb{Z}_p^n} \sum_{b=0}^{1} \sum_{y \in \mathbb{Z}_p^n} \sum_{c=0}^{1} \omega_p^{x \cdot y} (-1)^{bc} |y\rangle |c\rangle |f(x,b)\rangle$$

On utilise la propriété du groupe caché: $f(x,0) = f(x+s,1)$

$$\frac{1}{2p^n} \sum_{x \in \mathbb{Z}_p^n} \sum_{y \in \mathbb{Z}_p^n} \sum_{c=0}^{1} (\omega_p^{x \cdot y} + \omega_p^{(x+s) \cdot y} (-1)^c) |y\rangle |c\rangle |f(x,0)\rangle$$

Pour tout x, y l'amplitude de $|y\rangle|1\rangle|f(x,0)\rangle$ est:

$$\frac{1}{2p^n} \omega_p^{x \cdot y} (1 - \omega_p^{y \cdot s})$$

Après mesure:

$$\Pr[\text{sortie} = (y,1)] = \frac{1}{4p^{2n}} \left|1 - \omega_p^{y \cdot s}\right|^2.$$

Propriétés de la distribution sortie:

- $\Pr[c = 1] = 1/2$
- dépend seulement de $y \cdot s$
- pour chaque $(y,1)$ observé: $y \cdot s \neq 0 \mod p$.

Algorithme: 2ème partie (postprocessing classique)

On échantillone $(y, 1)$ tel que $y \cdot s \neq 0 \mod p$ (*i.e.* $y \notin s^{\perp}$)

Inéquations linéaires $\mapsto$ Equations polynomiales

$$y \cdot s \neq 0 \mod p \iff (y \cdot s)^{p-1} = 1 \mod p$$

Fact: Résoudre des équations polynomiales est NP-complet.

Idée: On linéarise le système dans la puissance symétrique de $\mathbb{Z}_p^n$

Définition: $\mathbb{Z}_p^{(p-1)}[x_1, \ldots, x_n]$ est l'espace vectoriel des polynômes homogènes en n-variables de degré $(p-1)$ sur $\mathbb{Z}_p$.

- Une base: Les monômes de degré $(p-1)$
- Dimension: $\binom{n+p-2}{p-1}$

On transfère de $\mathbb{Z}_p^n$ à $\mathbb{Z}_p^{(p-1)}[x_1, \ldots, x_n]$:

Définition: Pour $y = (y_1, \ldots, y_n) \in \mathbb{Z}_p^n$ soit

$$y^{(p-1)} = (\textstyle\sum_j y_j x_j)^{p-1}. \text{ Alors}$$

$$y \cdot s \neq 0 \mod p \implies y^{(p-1)} \cdot s^* = (y \cdot s)^{p-1} = 1 \mod p,$$

où en $s^* \in \mathbb{Z}_p^{(p-1)}$ la coordonnée de $x_1^{e_1} \cdots x_n^{e_n}$ est $s_1^{e_1} \cdots s_n^{e_n}$.

Algorithme: 2ème partie (postprocessing classique)

A la fin de l'algorithme:

- On espère que le système linéaire en $\mathbb{Z}_p^{(p-1)}[x_1, \ldots, x_n]$ possède une unique solution
- On trouve la solution $S = s^*$
- On essaie les $(p-1)$ candidats v tels que $v^* = s^*$

Exemple. $p = 3$, $n = 3$, $s = (1, 2, 0)$.

Echant. en $\mathbb{Z}_3^3$	Inéquation en $\mathbb{Z}_3^3$	Equation en $\mathbb{Z}_3^{(2)}[x_1, x_2, x_3]$
$y_1 = (0, 1, 0)$	$x_2 \cdot s \neq 0$	$x_2^2 \cdot S = 1$
$y_2 = (0, 2, 1)$	$(2x_2 + x_3) \cdot s \neq 0$	$(x_2^2 + x_3^2 + x_2 x_3) \cdot S = 1$
$y_3 = (0, 2, 2)$	$(2x_2 + 2x_3) \cdot s \neq 0$	$(x_2^2 + x_3^2 + 2x_2 x_3) \cdot S = 1$
$\vdots$	$\vdots$	$\vdots$

où $x_1 = (1, 0, 0)$, $x_2 = (0, 1, 0)$, $x_3 = (0, 0, 1)$,
$x_1^2 = (1, 0, 0, 0, 0, 0)$, $\ldots$

Système de rang plein $\implies$ solution unique $S = x_1^2 + x_2^2 + 2x_1 x_2$.
Essaie les translations possibles $(1, 2, 0)$ et $(2, 1, 0) \rightsquigarrow s = (1, 2, 0)$.

Lemme de ligne

Lemma de ligne: Soit $L_{z,y} = \{(z + ay)^{(p-1)} : 0 \leq a \leq p-1\}$ pour $y, z \in \mathbb{Z}_p^n$. Alors:

$$y^{(p-1)} \in \mathrm{Span}(L_{z,y}).$$

Preuve: Let $M_{z,y} = \{\binom{p-1}{k} z^{(k)} y^{(p-1-k)} : 0 \leq k \leq p-1\}$.

Fait: $\mathrm{Span}(L_{z,y}) = \mathrm{Span}(M_{z,y})$.

	$z^{(p-1)}$	$\dots$	$(z+ay)^{(p-1)}$	$\dots$	$(z+(p-1)y)^{(p-1)}$
$\binom{p-1}{0} z^{(p-1)}$	1	$\dots$	1	$\dots$	1
$\binom{p-1}{1} z^{(p-2)} y^{(1)}$	0	$\dots$	a	$\dots$	$(p-1)$
$\binom{p-1}{2} z^{(p-3)} y^{(2)}$	0	$\dots$	a^2	$\dots$	$(p-1)^2$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
$\binom{p-1}{p-1} y^{(p-1)}$	0	$\dots$	a^{p-1}	$\dots$	$(p-1)^{p-1}$

Corollaire: $\mathbb{Z}_p^{(p-1)}[x_1, \dots, x_n]$ est engendré par $\{y^{(p-1)} : y \in \mathbb{Z}_p^n\}$.

Rang plein

Lemme: Soit $W \leq \mathbb{Z}_p^{(p-1)}[x_1, \ldots, x_n]$, $R = \{y \in \mathbb{Z}_p^n : y^{(p-1)} \in W\}$
On définit $V_k = \{y \in \mathbb{Z}_p^n : y \cdot s = k\}$, et $R_k = R \cap V_k$.

Si $W \neq \mathbb{Z}_p^{(p-1)}[x_1, \ldots, x_n]$ alors $\frac{|R_k|}{|V_k|} \leq \frac{p-1}{p}$ pour $k = 1, \ldots, p-1$.

Preuve: Corollaire $\implies R \neq \mathbb{Z}_p^n$.

Cas 1: $R_0 = V_0$. Alors $R_k \neq V_k$ for $k = 1, \ldots, p-1$. Soit $y \in V_1 - R_1$. Lemme de ligne $\implies$ dans chaque coset of $<y>$ un élément est en dehors de R.

	$<y>$	$\ldots$	$z + <y>$	$\ldots$
V_0	0	$\ldots$	z	$\ldots$
V_1	y	$\ldots$	$z + y$	$\ldots$
$\vdots$	$\vdots$	$\ldots$	$\vdots$	$\ldots$
V_{p-1}	$(p-1)y$	$\ldots$	$z + (p-1)y$	$\ldots$

$\implies \frac{|R|}{|Z_p^n|} \leq \frac{p-1}{p} \implies \frac{|R_k|}{|V_k|} \leq \frac{p-1}{p}$.

Cas 2: $R_0 \neq V_0$. If $y \in V_0 \setminus R_0$ alors V_k l'union de cosets de $<y>$.
Lemme de ligne $\implies \frac{|R_k|}{|V_k|} \leq \frac{p-1}{p}$.

Plan de l'exposé était

1. Problème du sous-groupe caché (PSC)
2. PSC en groupes Abéliens (finis et infinis)
3. Cryptographie post-quantique
4. PSC en groupes non Abéliens
5. Le groupe diédral
6. Groupes diédraux généralisés

Merci!