A quantum algorithm for computing the unit group of a number field and connections to post-quantum cryptography

Joint work with Sean Hallgren, Alexei Kitaev and Fang Song.

Exponential speedups by quantum algorithms

- Factoring integers, discrete log (Shor '94)
  - ↳ Breaks RSA
- for real quadratic number fields $\mathbb{Q}(\sqrt{d})$, $d>0$ can compute the unit gp, class gp, and solve the Principal Ideal Problem in quantum poly time (Hallgren '02)
- same for number fields of constant degree (Hallgren, Schmidt-Vollmer '05)
  - ⟶ this talk: number fields of arbitrary degree (E-Hallgren-Kitaev-Song)
- with Hallgren: solved same questions for function fields

Main Theorem (E-H-K-S)

Let K be a number field (i.e. a finite extension of $\mathbb{Q}$)

Let $\mathcal{O}$ be its ring of integers.

There is a poly time quantum alg. (poly in $n = [K:\mathbb{Q}]$ and $\log|D|$) for computing the unit group $\mathcal{O}^*$.

$\mathcal{O}$ = elts. of K that are roots of monic polys with coeffs in $\mathbb{Z}$.

Dirichlet's theorem : $\mathcal{O}^* \simeq \underset{\text{roots of unity}}{\mu(K)} \times \mathbb{Z}^{s+t-1}$

$s = \#$ real embeddings of K
$t = \#$ of complex conjugate pairs of embedding

Post-quantum cryptography

Goal: find and use cryptosystems that quantum computers cannot be break.

Proposals : → (1) systems based on lattice problems
(2) systems based on supersingular isogenies

Problem (Shortest vector problem)
Given $b_1, \ldots, b_m \in \mathbb{R}^m$ generating a lattice, $L = \sum_{i=1}^{m} a_i b_i$, $a_i \in \mathbb{Z}$
Compute the shortest nonzero vector.

To improve efficiency, special assumptions

(a) Assume Problem is hard if L corresponds to an ideal I in a number field.

(b) Assume still hard if I is principal.

(c) same setup as (b), but assume there is a short generator α for I.
Assume it's hard to find α.

"Short gen. principal ideal problem" (SGPIP)

Systems based on hardness of SGPIP.
- fully homomorphic encryption scheme Smart-Vercauteren '10
- multilinear maps (Garg-Gentry-Halevi '13)
- Soliloquy (GCHQ, Campbell-Groves-Shepard)

All of these systems can be broken in quantum poly time, so they are not suitable for post-quantum crypto.

Algorithm to solve SGPIP

Given K and $I \subseteq \mathcal{O}$ $\quad K=$ cyclotomic

Quantum (1) Compute the unit group of K (E-H-K-S)

Quantum (2) Use the unit group to solve the principal (Biasse-Song)
This gives some generator β for I.

Classical (3) classical alg. for BDD in unit lattice (of a cyclotomic field).
$\hookrightarrow$ turns generator β into small generator α

Overview of Quantum Algorithm for unit group

K, unit gp $\mathcal{O}^*$, $\quad \mathrm{Log}\,\mathcal{O}^* \subseteq \mathbb{R}^{s+t-1}$

$$\tau : \mathcal{O}^* \longrightarrow \underline{\mathrm{Log}\,\mathcal{O}^*}$$

$$\tau(z) = \left(\log|\tau_1(z)|, \ldots, 2\log|\tau_{s+t-1}(z)|\right)$$

$\tau_1, \ldots, \tau_s$ real emb.

$\tau_{s+1}, \ldots, \tau_{s+t-1}$ complex.

$$\boxed{K \xrightarrow[\text{reduction}]{\text{quantum}} \begin{array}{c}\text{continuous}\\ \text{Hidden Subgroup}\\ \text{Problem}\\ f: \mathbb{R}^{s+t-1} \longrightarrow S\end{array}} \xrightarrow[\text{HSP algorithm}]{\text{quantum}} \begin{array}{c}\text{basis of}\\ \underline{\underline{\mathrm{Log}\,\mathcal{O}^* \subseteq \mathbb{R}^{s+t-1}}}\end{array}$$

HSP: Let G be a group, S a set.
Given $f: G \to S$ that is constant and distinct on cosets of a subgroup H of G, find H.

<u>Challenge</u>: • $\mathbb{R}^{s+t-1}$ uncountable, unbounded dimension
$\rightsquigarrow$ rounding errors

<u>Our work</u>: new setup and analysis to deal with this

• there is no canonical basis for $\mathrm{Log}\,\mathcal{O}^*$
$\rightsquigarrow$ need S to be a set of superpositions

The HSP is set up as follows:

$$f: \mathbb{R}^{s+t-1} \longrightarrow \left\{ \begin{array}{l} \text{lattices in } \mathbb{R}^s \times \mathbb{C}^t \\ \text{(represented by superpos. of lattice points)} \end{array} \right\}$$

$$u \longmapsto e^{u}\, \underline{\mathcal{O}}$$

If $\underline{\mathcal{O}} = \tau(\mathcal{O})$ is a lattice with basis $z_1, \ldots, z_n$

$$z_1 = \begin{pmatrix} z_{11} \\ \vdots \\ z_{n1} \end{pmatrix} \qquad z_n = \begin{pmatrix} z_{1n} \\ \vdots \\ z_{nn} \end{pmatrix}$$

Then $e^{u}\,\mathcal{O}$ is a lattice with basis

$$\begin{pmatrix} e^{u_1} z_{11} \\ \vdots \\ e^{u_n} z_{n1} \end{pmatrix}, \ldots, \begin{pmatrix} e^{u_1} z_{1n} \\ \vdots \\ e^{u_n} z_{nn} \end{pmatrix}$$

This function f hides the lattice $\mathrm{Log}\,\mathcal{O}^*$.