Trade-off between classical and quantum circuit size of the attack against CSIDH

Jean-François Biasse[1], Xavier Bonnetain[2], **Benjamin Pring**[1], André Schrottenloher[2] and William Youmans[1]

18th August 2019

[1]University of South Florida [2]INRIA Paris

Contributions

Kuperberg's algorithm can be fine-tuned to an attack on CSIDH costing

- A quantum circuit-size of $2^{O(n^{\alpha})}$
- A classical circuit-size of $2^{O\left(n^{1-\alpha}\right)}$
- Polynomial classical and quantum memory

where $0 < \alpha < \frac{1}{2}$ and n is proportional to the security parameter.

	Quantum gates	Quantum memory	Classical gates	Classical memory
Kuperberg [Kup03]	$2^{O(\sqrt{n})}$	$2^{O(\sqrt{n})}$	$poly(n)$	$poly(n)$
Regev [Reg04]	$2^{O(\sqrt{n \log n})}$	$poly(n)$	$2^{O(\sqrt{n \log n})}$	$poly(n)$
Kuperberg [Kup13]	$2^{O(\sqrt{n})}$	$poly(n)$	$2^{O(\sqrt{n})}$	$2^{O(\sqrt{n})}$
Ours	$2^{O(n^{\alpha})}$	$poly(n)$	$2^{O(n^{1-\alpha})}$	$poly(n)$

Motivation

Kuperberg's algorithm solves the DHSP $\implies$ break CSIDH

"Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a (K)-bit key (e.g. AES(K))" — NIST PQC Call for Proposals [oST16]

AES-128	2^{170}/MAXDEPTH quantum gates or 2^{143} classical gates
AES-192	2^{333}/MAXDEPTH quantum gates or 2^{207} classical gates
AES-256	2^{298}/MAXDEPTH quantum gates or 2^{272} classical gates

Motivation

Model:

AES-128	2^{170}/MAXDEPTH quantum gates	or	2^{143} classical gates
AES-192	2^{333}/MAXDEPTH quantum gates	or	2^{207} classical gates
AES-256	2^{298}/MAXDEPTH quantum gates	or	2^{272} classical gates

What if allowed $2^{87.5}$ quantum gates (AES-128) and 2^{143} classical gates?

Research question: how can we trade quantum/classical gates?

Motivation

Model:

AES-128	2^{170}/MAXDEPTH quantum gates **and** 2^{143} classical gates
AES-192	2^{333}/MAXDEPTH quantum gates **and** 2^{207} classical gates
AES-256	2^{298}/MAXDEPTH quantum gates **and** 2^{272} classical gates

What if allowed $2^{87.5}$ quantum gates (AES-128) and 2^{143} classical gates?

Research question: how can we trade quantum/classical gates?

Motivation: CSIDH

Super high-level view of CSIDH:

- $E_0 = E(\mathbb{F}_p) : y^2 = x^3 + x$ where $p = 4 \cdot l_1 \dots l_n - 1$ is prime and l_i are small odd primes.
- $\mathcal{O} \cong \mathsf{End}(E_0)$
- We can define the group $G = \mathsf{Cl}(\mathcal{O})$

$$G = \{[\mathfrak{a}] \text{ such that } \mathfrak{a} \text{ is an ideal of } \mathcal{O}\}$$

  where $[\mathfrak{a}] = [\mathfrak{b}] \Leftrightarrow \exists \alpha \neq 0 \in \mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O},\ \mathfrak{a} = (\alpha)\mathfrak{b}$
- Induces group action

$$[\mathfrak{a}] * \overline{E_0} \mapsto \overline{E_0 / \langle [\mathfrak{a}] \rangle}$$

- Fact:

$$[\mathfrak{a}] * \left([\mathfrak{b}] * \overline{E_0}\right) = \overline{E_0 / \langle \mathfrak{a}, \mathfrak{b} \rangle} = \overline{E_0 / \langle \mathfrak{b}, \mathfrak{a} \rangle} = [\mathfrak{b}] * \left([\mathfrak{a}] * \overline{E_0}\right)$$

Motivation: CSIDH

CSIDH public parameters: $E_0, \mathbb{F}_p, p = l_1, \ldots, l_n$

Alice

$\mathfrak{a} \ni [\mathfrak{a}] \xleftarrow{\$} \mathsf{Cl}(\mathcal{O})$

Bob

$\mathfrak{b} \ni [\mathfrak{b}] \xleftarrow{\$} \mathsf{Cl}(\mathcal{O})$

Motivation: CSIDH

CSIDH public parameters: $E_0, \mathbb{F}_p, p = l_1, \ldots, l_n$

Alice

$\mathfrak{a} \ni [\mathfrak{a}] \xleftarrow{\$} \mathsf{Cl}(\mathcal{O})$

Bob

$\mathfrak{b} \ni [\mathfrak{b}] \xleftarrow{\$} \mathsf{Cl}(\mathcal{O})$

$$\xrightarrow{\quad [\mathfrak{a}] * \overline{E_0} \quad}$$

$$\xleftarrow{\quad [\mathfrak{b}] * \overline{E_0} \quad}$$

Motivation: CSIDH

CSIDH public parameters: $E_0, \mathbb{F}_p, p = l_1, \ldots, l_n$

Alice		**Bob**
$\mathfrak{a} \ni [\mathfrak{a}] \xleftarrow{\$} \mathsf{Cl}(\mathcal{O})$		$\mathfrak{b} \ni [\mathfrak{b}] \xleftarrow{\$} \mathsf{Cl}(\mathcal{O})$
	$\xrightarrow{\quad [\mathfrak{a}] * \overline{E_0} \quad}$	
	$\xleftarrow{\quad [\mathfrak{b}] * \overline{E_0} \quad}$	
Computes $[\mathfrak{a}] * \left([\mathfrak{b}] * \overline{E_0}\right)$	$=$	Computes $[\mathfrak{b}] * \left([\mathfrak{a}] * \overline{E_0}\right)$

$$[\mathfrak{a}] * \left([\mathfrak{b}] * \overline{E_0}\right) = \overline{E_0/\langle \mathfrak{a}, \mathfrak{b} \rangle} = \overline{E_0/\langle \mathfrak{b}, \mathfrak{a} \rangle} = [\mathfrak{b}] * \left([\mathfrak{a}] * \overline{E_0}\right)$$

Motivation: CSIDH

Problem: Given $\overline{E_0}$ and $\overline{E_1} = [\mathfrak{s}] * \overline{E_0}$ and $\mathcal{O} \cong \mathsf{End}(E_i)$, find $[\mathfrak{s}]$.

Hidden shift formulation: define $f_0, f_1 : \mathsf{Cl}(\mathcal{O}) \to \mathbb{F}_p$

$$f_0([\mathfrak{r}]) \mapsto [\mathfrak{r}] * \overline{E_0}$$
$$f_1([\mathfrak{r}]) \mapsto [\mathfrak{r}] * \overline{E_1}$$

then equivalently want to find $[\mathfrak{a}]$ such that for all $[\mathfrak{r}] \in \mathsf{Cl}(\mathcal{O})$

$$f_1([\mathfrak{r}]) = f_0([\mathfrak{r}][\mathfrak{a}])$$

Motivation: CSIDH

Problem: Given $\overline{E_0}$ and $\overline{E_1} = [\mathfrak{s}] * \overline{E_0}$ and $\mathcal{O} \cong \mathrm{End}(E_i)$, find $[\mathfrak{s}]$.

Hidden shift formulation: define $f_0, f_1 : \mathrm{Cl}(\mathcal{O}) \to \mathbb{F}_p$

$$f_0([\mathfrak{r}]) \mapsto [\mathfrak{r}] * \overline{E_0}$$
$$f_1([\mathfrak{r}]) \mapsto [\mathfrak{r}] * \overline{E_1}$$

then equivalently want to find $[\mathfrak{a}]$ such that for all $[\mathfrak{r}] \in \mathrm{Cl}(\mathcal{O})$

$$[\mathfrak{r}][\mathfrak{s}] * \overline{E_0} = [\mathfrak{r}] * \overline{E_1} = f_1([\mathfrak{r}]) = f_0([\mathfrak{r}][\mathfrak{a}]) = [\mathfrak{r}\mathfrak{a}] * \overline{E_0} = [\mathfrak{r}][\mathfrak{a}] * \overline{E_0}$$
$$\Downarrow$$
$$[\mathfrak{a}] = [\mathfrak{s}]$$

Motivation: CSIDH

Problem: Given $\overline{E_0}$ and $\overline{E_1} = [\mathfrak{s}] * \overline{E_0}$ and $\mathcal{O} \cong \mathsf{End}(E_i)$, find $[\mathfrak{s}]$.

Dihedral Hidden Subgroup formulation: Solution by Jao et al. [CJS14]:

$$\mathsf{Cl}(\mathcal{O}) \cong A = \underbrace{\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_k} \cong \mathbb{Z}_N}_{\text{Assume that class group is cyclic}}$$

Define $f : \mathbb{Z}_2 \rtimes A \to \mathbb{F}_p$ by

$$f(x, \vec{y}) \mapsto \begin{cases} [\mathfrak{a}_{\vec{y}}] * \overline{E_1} & \text{if } x = 0 \\ [\mathfrak{a}_{\vec{y}}] * \overline{E_0} & \text{if } x = 1 \end{cases}$$

$$f(0, \vec{y}) = \qquad\qquad = f(1, \vec{y} + \vec{s})$$

where $[\mathfrak{s}] = [\mathfrak{a}_{\vec{s}}]$.

Motivation: CSIDH

Problem: Given $\overline{E_0}$ and $\overline{E_1} = [\mathfrak{s}] * \overline{E_0}$ and $\mathcal{O} \cong \mathrm{End}(E_i)$, find $[\mathfrak{s}]$.

Dihedral Hidden Subgroup formulation: Solution by Jao et al. [CJS14]:

$$\mathrm{Cl}(\mathcal{O}) \cong A = \underbrace{\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_k} \cong \mathbb{Z}_N}_{\text{Assume that class group is cyclic}}$$

Define $f : \mathbb{Z}_2 \rtimes A \to \mathbb{F}_p$ by

$$f(x, \vec{y}) \mapsto \begin{cases} [\mathfrak{a}_{\vec{y}}] * \overline{E_1} & \text{if } x = 0 \\ [\mathfrak{a}_{\vec{y}}] * \overline{E_0} & \text{if } x = 1 \end{cases}$$

$$f(0, \vec{y}) = [\mathfrak{a}_{\vec{y}}] * \overline{E}_1 = [\mathfrak{a}_{\vec{y}}] * \left([\mathfrak{s}] * \overline{E}_0\right) = [\mathfrak{a}_{\vec{y}}][\mathfrak{s}] * \overline{E}_0 = f(1, \vec{y} + \vec{s})$$

where $[\mathfrak{s}] = [\mathfrak{a}_{\vec{s}}]$.

Motivation: CSIDH

From hereon in we assume $A \cong \mathbb{Z}_N$ and $N = 2^n$ for simplicity.

$f : \mathbb{Z}_2 \rtimes \mathbb{Z}_N$ is constant and unique on all **cosets** of the form

$$(0, x) \cdot H = \{(0, x), (1, x + s)\} \subset \mathbb{Z}_2 \rtimes \mathbb{Z}_N \cong D_N$$

for $x \in \mathbb{Z}_N$ where

$$H = \{(0, 0), (1, s)\} \leq \mathbb{Z}_2 \rtimes \mathbb{Z}_N \cong D_N$$

Motivation: CSIDH

From hereon in we assume $A \cong \mathbb{Z}_N$ and $N = 2^n$ for simplicity.

$f : \mathbb{Z}_2 \rtimes \mathbb{Z}_N$ is constant and unique on all **cosets** of the form

$$(0, x) \cdot H = \{(0, x), (1, x + s)\} \subset \mathbb{Z}_2 \rtimes \mathbb{Z}_N \cong D_N$$

for $x \in \mathbb{Z}_N$ where

$$H = \{(0, 0), (1, s)\} \leq \mathbb{Z}_2 \rtimes \mathbb{Z}_N \cong D_N$$

Definition (Hidden Subgroup Problem)

Let G be a group and $f : G \longrightarrow X$ for some finite set X such that

$$f(aH) = f(bH)$$

for some unknown $H \leq G$ if and only if $aH = bH$.

Given G and f, the *Hidden Subgroup Problem* (HSP) is to find H.

Kuperberg to the rescue

Definition (Hidden Subgroup Problem)

Let G be a group and $f : G \longrightarrow X$ for some finite set X such that

$$f(aH) = f(bH)$$

for some unknown $H \leq G$ if and only if $aH = bH$.

Given G and f, the *Hidden Subgroup Problem* (HSP) is to find H.

Theorem (Kuperberg's algorithm [Kup03])

There exists a quantum algorithm that solves the HSP for D_N requiring $2^{O(\sqrt{\log N})}$ time and space.

Theorem (Kuperberg's algorithm [Reg04])

There exists a quantum algorithm that solves the HSP for D_N requiring $2^{O(\sqrt{\log N \log \log_N})}$ time and $poly(n)$ space.

The Kuperberg framework

Let $H \leq D_N$ and $f : D_N \longrightarrow R$ for R some finite set such that

$$f(0, x) = f(1, s + x)$$

for all $x \in \mathbb{Z}_N$ where we wish to find $s \in \mathbb{Z}_N$.

By Ettinger-Høyer[1] this reduces to finding the subgroup

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

Aim is to recover the *least significant bit* of s_0 of s.

[1]Ettinger, Mark and Høyer, Peter,
On quantum algorithms for noncommutative hidden subgroups,
Advances in Applied Mathematics volume 25 **3** (2000), 239–251

The Kuperberg framework

Let $H \leq D_N$ and $f : D_N \longrightarrow R$ for R some finite set such that

$$f(0, x) = f(1, s + x)$$

for all $x \in \mathbb{Z}_N$ where we wish to find $s \in \mathbb{Z}_N$.

Least significant bit is $s_0 = 0$:

$$f' \; : D_{N/2} \longrightarrow R \qquad \text{where} \qquad f' \, (a, b) \mapsto f(a, 2b)$$

is constant on

$$(0, x) \cdot H' \; = \{(0, x), (s/2 + x)\}$$

for $x \in \mathbb{Z}_{N/2}$ and secret $s \in \mathbb{Z}_N$.

The Kuperberg framework

Let $H \leq D_N$ and $f : D_N \longrightarrow R$ for R some finite set such that

$$f(0,x) = f(1, s + x)$$

for all $x \in \mathbb{Z}_N$ where we wish to find $s \in \mathbb{Z}_N$.

Least significant bit is $s_0 = 1$:

$$f'' : D_{N/2} \longrightarrow R \qquad \text{where} \qquad f''(a,b) \mapsto f(a, 2b+1)$$

is constant on

$$(0,x) \cdot H'' = \{(0,x), ((s-1)/2 + x)\}$$

for $x \in \mathbb{Z}_{N/2}$ and secret $s \in \mathbb{Z}_N$.

The Kuperberg framework

We possess a quantum oracle $\mathcal{O}_f$ that implements (where $b \in \{0,1\}$ and $x \in \{0,1\}^n$)

$$\mathcal{O}_f \left|b\right\rangle \left|x\right\rangle \left|0^r\right\rangle \mapsto \left|b\right\rangle \left|x\right\rangle \left|f(b,x)\right\rangle$$

we can use this to produce quantum states of the form

$$\left|\psi_k^{s,N}\right\rangle := \frac{1}{\sqrt{2}} \left(\left|0\right\rangle + e^{2\pi i k s/N} \left|1\right\rangle \right)$$

where $k \xleftarrow{\$} \{0, 1, \ldots, N-1\}$ is known.

The aim is to create a state of the form

$$\left|\psi_{2^{n-1}}^{s,N}\right\rangle$$

which allows us to recover the least significant bit of s.

The Kuperberg framework

Recovery of least significant bit of s:

$$\begin{aligned}|\psi^{s,N}_{2^{n-1}}\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2i\pi 2^{n-1}s/N}|1\rangle\right)\\ &= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi s}|1\rangle\right)\\ &= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi s_0}|1\rangle\right)\end{aligned}$$

as

$$e^{i\pi s} = e^{i\pi(s_0+s_1 2^1+\cdots+s_{n-1}2^{n-1})} = e^{i\pi s_0}\cdot\prod_{i=1}^{n-1}\left(e^{i\pi s_i}\right)^{2^i} = e^{i\pi s_0}\cdot\prod_{i=1}^{n-1}1 = e^{i\pi s_0}$$

$$\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \overset{H}{\mapsto} |0\rangle \qquad \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \overset{H}{\mapsto} |1\rangle$$

The Kuperberg framework

$|0\rangle\,|0^n\rangle\,|0^r\rangle$

The Kuperberg framework

$$|0\rangle |0^n\rangle |0^r\rangle$$

$$\overset{H^{\otimes n+1}}{\mapsto} \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \frac{1}{\sqrt{2}} \Big(|0\rangle + |1\rangle \Big) |x\rangle |0^r\rangle$$

The Kuperberg framework

$$|0\rangle\,|0^n\rangle\,|0^r\rangle$$

$$\overset{H^{\otimes n+1}}{\mapsto} \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \frac{1}{\sqrt{2}} \Big(|0\rangle\,|x\rangle\,|0^r\rangle + |1\rangle\,|x + s \bmod N\rangle\,|0^r\rangle \Big)$$

The Kuperberg framework

$$
\begin{aligned}
&|0\rangle\,|0^n\rangle\,|0^r\rangle \\
&\overset{H^{\otimes n+1}}{\mapsto} \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\frac{1}{\sqrt{2}}\Big(\,|0\rangle\,|x\rangle\,|0^r\rangle + |1\rangle\,|x+s \bmod N\rangle\,|0^r\rangle\,\Big) \\
&\overset{\mathcal{O}_f}{\mapsto} \quad \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\frac{1}{\sqrt{2}}\Big(\,|0\rangle\,|x\rangle\,|f(0,x)\rangle + |1\rangle\,|x+s \bmod N\rangle\,|f(1,x+s)\rangle\Big)
\end{aligned}
$$

The Kuperberg framework

$$
\begin{aligned}
&|0\rangle\,|0^n\rangle\,|0^r\rangle \\
&\overset{H^{\otimes n+1}}{\mapsto} \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \frac{1}{\sqrt{2}}\Big(\,|0\rangle\,|x\rangle\,|0^r\rangle + |1\rangle\,|x+s \bmod N\rangle\,|0^r\rangle\,\Big) \\
&\overset{\mathcal{O}_f}{\mapsto} \quad \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \frac{1}{\sqrt{2}}\Big(\,|0\rangle\,|x\rangle\,|y_x\rangle + |1\rangle\,|x+s \bmod N\rangle\,|y_x\rangle\,\Big)
\end{aligned}
$$

The Kuperberg framework

$$
\begin{aligned}
&|0\rangle\,|0^n\rangle\,|0^r\rangle \\
&\overset{H^{\otimes n+1}}{\mapsto} \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\frac{1}{\sqrt{2}}\Big(\,|0\rangle\,|x\rangle\,|0^r\rangle + |1\rangle\,|x+s \bmod N\rangle\,|0^r\rangle\,\Big) \\
&\overset{\mathcal{O}_f}{\mapsto} \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\frac{1}{\sqrt{2}}\Big(\,|0\rangle\,|x\rangle\,|y_x\rangle + |1\rangle\,|x+s \bmod N\rangle\,|y_x\rangle\,\Big) \\
&\overset{\substack{\text{Measure}\\|y_x\rangle}}{\mapsto} \frac{1}{\sqrt{2}}\Big(\,|0\rangle\,|x\rangle + |1\rangle\,|x+s \bmod N\rangle\,\Big)\,|y_x\rangle \qquad \text{for } y_x \xleftarrow{\$} \mathbb{Z}_n
\end{aligned}
$$

The Kuperberg framework

$$|0\rangle\,|0^n\rangle\,|0^r\rangle$$

$$\overset{H^{\otimes n+1}}{\mapsto} \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\frac{1}{\sqrt{2}}\Big(|0\rangle\,|x\rangle\,|0^r\rangle + |1\rangle\,|x+s \bmod N\rangle\,|0^r\rangle\Big)$$

$$\overset{\mathcal{O}_f}{\mapsto} \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\frac{1}{\sqrt{2}}\Big(|0\rangle\,|x\rangle\,|y_x\rangle + |1\rangle\,|x+s \bmod N\rangle\,|y_x\rangle\Big)$$

Measure

$$\overset{|y_x\rangle}{\mapsto} \frac{1}{\sqrt{2}}\Big(|0\rangle\,|x\rangle + |1\rangle\,|x+s \bmod N\rangle\Big)$$

for $x \overset{\$}{\leftarrow} \mathbb{Z}_n$

The Kuperberg framework

$$|0\rangle\,|0^n\rangle\,|0^r\rangle$$

$$\overset{H^{\otimes n+1}}{\mapsto}\ \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\frac{1}{\sqrt{2}}\Big(\,|0\rangle\,|x\rangle\,|0^r\rangle + |1\rangle\,|x+s \bmod N\rangle\,|0^r\rangle\,\Big)$$

$$\overset{\mathcal{O}_f}{\mapsto}\ \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\frac{1}{\sqrt{2}}\Big(\,|0\rangle\,|x\rangle\,|y_x\rangle + |1\rangle\,|x+s \bmod N\rangle\,|y_x\rangle\,\Big)$$

$$\overset{\text{Measure }|y_x\rangle}{\mapsto}\ \frac{1}{\sqrt{2}}\Big(\,|0\rangle\,|x\rangle + |1\rangle\,|x+s \bmod N\rangle\,\Big) \qquad \text{for } x \overset{\$}{\leftarrow} \mathbb{Z}_n$$

$$\overset{\text{QFT}}{\mapsto}\ \frac{1}{\sqrt{2}}\Big(\sum_{k=0}^{N-1} e^{2\pi i x k/N}\,|0\rangle\,|k\rangle + \sum_{k=0}^{N-1} e^{2\pi i (x+s)k/N}\,|1\rangle\,|k\rangle\Big)$$

The Kuperberg framework

$$|0\rangle\,|0^n\rangle\,|0^r\rangle$$

$$\overset{H^{\otimes n+1}}{\mapsto} \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \frac{1}{\sqrt{2}} \Big(|0\rangle\,|x\rangle\,|0^r\rangle + |1\rangle\,|x + s \bmod N\rangle\,|0^r\rangle \Big)$$

$$\overset{\mathcal{O}_f}{\mapsto} \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \frac{1}{\sqrt{2}} \Big(|0\rangle\,|x\rangle\,|y_x\rangle + |1\rangle\,|x + s \bmod N\rangle\,|y_x\rangle \Big)$$

$$\overset{\substack{\text{Measure}\\|y_x\rangle}}{\mapsto} \frac{1}{\sqrt{2}} \Big(|0\rangle\,|x\rangle + |1\rangle\,|x + s \bmod N\rangle \Big) \qquad \text{for } x \overset{\$}{\leftarrow} \mathbb{Z}_n$$

$$\overset{\text{QFT}}{\mapsto} \frac{1}{\sqrt{2}} \Big(\sum_{k=0}^{N-1} e^{2\pi i x k/N}\,|0\rangle\,|k\rangle + \sum_{k=0}^{N-1} e^{2\pi i (x+s) k/N}\,|1\rangle\,|k\rangle \Big)$$

$$\overset{\substack{\text{Measure}\\|k\rangle}}{\mapsto} \frac{1}{\sqrt{2}} \Big(e^{2\pi i x k/N}\,|0\rangle\,|k\rangle + e^{2\pi i x k/N} e^{2\pi i s k/N}\,|1\rangle\,|k\rangle \Big) \qquad \text{for } k \overset{\$}{\leftarrow} \mathbb{Z}_n$$

The Kuperberg framework

$$|0\rangle\,|0^n\rangle\,|0^r\rangle$$

$$\overset{H^{\otimes n+1}}{\mapsto}\ \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\frac{1}{\sqrt{2}}\Big(\,|0\rangle\,|x\rangle\,|0^r\rangle+|1\rangle\,|x+s \bmod N\rangle\,|0^r\rangle\,\Big)$$

$$\overset{\mathcal{O}_f}{\mapsto}\ \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\frac{1}{\sqrt{2}}\Big(\,|0\rangle\,|x\rangle\,|y_x\rangle+|1\rangle\,|x+s \bmod N\rangle\,|y_x\rangle\,\Big)$$

$$\overset{\text{Measure}}{\overset{|y_x\rangle}{\mapsto}}\ \frac{1}{\sqrt{2}}\Big(\,|0\rangle\,|x\rangle+|1\rangle\,|x+s \bmod N\rangle\,\Big) \qquad \text{for } x \overset{\$}{\leftarrow} \mathbb{Z}_n$$

$$\overset{\text{QFT}}{\mapsto}\ \frac{1}{\sqrt{2}}\Big(\sum_{k=0}^{N-1}e^{2\pi ixk/N}\,|0\rangle\,|k\rangle+\sum_{k=0}^{N-1}e^{2\pi i(x+s)k/N}\,|1\rangle\,|k\rangle\Big)$$

$$\overset{\text{Measure}}{\overset{|k\rangle}{\mapsto}}\ \frac{1}{\sqrt{2}}\Big(\,|0\rangle+e^{2\pi iks/N}\,|1\rangle\Big) \quad = \quad |\psi_k^{s,N}\rangle \qquad \text{for } \textit{known } k \overset{\$}{\leftarrow} \mathbb{Z}_n$$

The Kuperberg framework

Kuperberg strategy: Combine states to cancel least-significant bits

- Given $|\psi_{k_1}^{s,N}\rangle$ and $|\psi_{k_2}^{s,N}\rangle$ where we know k_1 and k_2

$$|\psi_{k_1}^{s,N}\rangle \otimes |\psi_{k_2}^{s,N}\rangle = |00\rangle + e^{2\pi i k_1 s/N} |10\rangle + e^{2\pi i k_2 s/N} |10\rangle + e^{2\pi i (k_1+k_2) s/N} |11\rangle$$

- Measurement conditioned on the parity then collapses this state to

$$|\psi_{k_2+k_1}^{s,N}\rangle \qquad \text{or} \qquad |\psi_{k_2-k_1}^{s,N}\rangle$$

- We use the states $|\psi_{k_2-k_1}^{s,N}\rangle$ to cancel out the least significant bits

Drawback: We need to generate and store $2^{O(\sqrt{n})}$ states.

Regev's variant

Regev's strategy: Combine states in stages and use exhaustive search

- Given $l+4$ states of the form $|\psi_{k_1}^{s,N}\rangle, \dots, |\psi_{k_{l+4}}^{s,N}\rangle$, create the state

$$\frac{1}{2^{(l+4)/2}} \sum_{\vec{b} \in \{0,1\}^{l+4}} e^{2\pi i \cdot \langle \vec{b}, \vec{k} \rangle \cdot s/N} |\vec{b}\rangle \, |\langle \vec{b}, \vec{k} \rangle \mod 2^l \rangle$$

where $\vec{k} = (k_1, \dots, k_{l+4}) \in (\mathbb{Z}_N)^{l+4}$ are known and $\langle \vec{b}, \vec{y} \rangle = \sum_{j=1}^{n} b_j y_j$.

- Use $l+4$ states with known $\vec{k} = (k_1, \dots, k_{l+4}) \in \mathbb{Z}_N)^{l+4}$ to obtain

$$\frac{1}{\sqrt{m}} \sum_{j=1}^{m} e^{2\pi i \cdot \langle \vec{B}_j, \vec{k} \rangle \cdot s/N} |\vec{B}_j\rangle$$

where $\langle \vec{B}_j, \vec{k} \rangle = z \mod 2^l$ and do a classical search to find $\vec{B}_1, \dots, \vec{B}_m$.

- If $m \in [2, 32]$, perform a projective measurement on the subspace spanned by $\vec{B}_1$ and $\vec{B}_2$ to obtain the state (with constant probability)

Regev's variant

Regev's strategy: Combine states in stages and use exhaustive search

- Use $l+4$ states with known $\vec{k}=(k_1,\ldots,k_{l+4})\in\mathbb{Z}_N)^{l+4}$ to obtain

$$\frac{1}{\sqrt{m}}\sum_{j=1}^{m} e^{2\pi i\cdot\langle\vec{B}_j,\vec{k}\rangle\cdot s/N}\,|\vec{B}_j\rangle$$

where $\langle\vec{B}_j,\vec{k}\rangle = z \mod 2^l$ and do a classical search to find $\vec{B}_1,\ldots,\vec{B}_m$.

- If $m\in[2,32]$, perform a projective measurement on the subspace spanned by $\vec{B}_1$ and $\vec{B}_2$ to obtain the state (with constant probability)

$$e^{2\pi i\langle\vec{B}_1,\vec{y}\rangle\cdot s}\,|\vec{B}_1\rangle + e^{2\pi i\langle\vec{B}_1,\vec{y}\rangle\cdot s}\,|\vec{B}_1\rangle$$

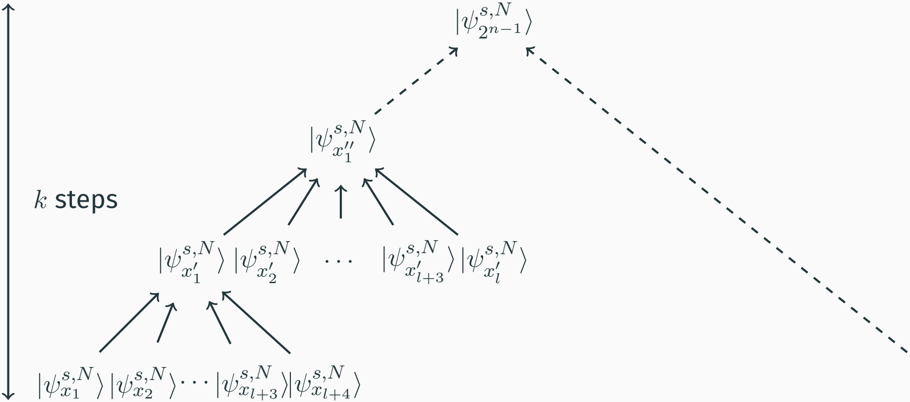
Relabelling (we know $\vec{B}_1$ and $\vec{B}_2$) and discarding qubits then gives us

$$|0\rangle + 2^{2\pi i\cdot\langle\vec{B}_2-\vec{B}_1,\vec{k}\rangle\cdot s/N}\,|1\rangle$$

$\langle\vec{B}_i,\vec{k}\rangle \bmod 2^l = z$ implies that the l least significant bits are zeroed.

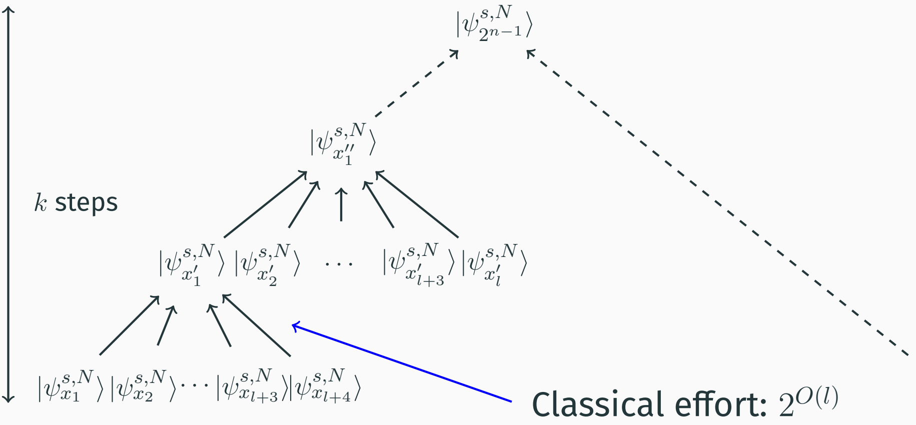
Regev's variant framework

- $n \approx k \times l$
- $\#$ calls to $\mathcal{O}_f$ is $l^{O(k)}$



Regev's variant framework

- $n \approx k \times l$
- $\#$ calls to $\mathcal{O}_f$ is $l^{O(k)}$



Our adaptation

Basic idea: $n = k \times l$ and

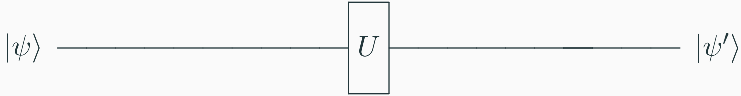
- Calls to $\mathcal{O}_f$: $2^{\tilde{O}(k)}$
- Other quantum gates: $2^{\tilde{O}(k)}$
- Classical effort: $2^{O(l)}$
- Use heuristic oracle assumptions from O_f from (Biasse-Iezzi-Jacobson 2018)

Suppose $k \approx n^\alpha$ and $l \approx n^{1-\alpha}$ for $0 < \alpha < 1/2$:

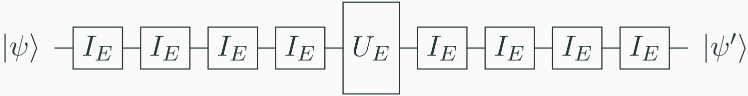
- Quantum circuit: $2^{O(n^\alpha)}$
- Classical circuit: $2^{O(n^{1-\alpha})}$

What about fault tolerance?

Quantum state is idle whilst classical-circuit with cost $2^{O(l)}$ executes



Logical quantum circuit



Quantum circuit with error-correction

- Potential disparity between cost of U_E and I_E
- Classical gates cheaper than quantum gates
- Classical search is embarassingly parallel

Conclusions and open problems

Contributions

Demonstrated how we trade quantum gates for classical gates to produce an attack on CSIDH with a quantum circuit-size of $2^{O(n^{\alpha})}$, where $0 < \alpha < 1/2$.

Open problems

1. Remove heuristics on the class group from (Biasse-Iezzi-Jacobson 2018) for evaluation of $\mathcal{O}_f$
2. Concrete gate counts (in various models)

References i

- Andrew Childs, David Jao, and Vladimir Soukharev, Constructing elliptic curve isogenies in quantum subexponential time, Journal of Mathematical Cryptology **8** (2014), no. 1, 1–29.
- Greg Kuperberg, A subexponential-time quantum algorithm for the dihedral hidden subgroup problem, 2003.
- Greg Kuperberg, Another subexponential-time quantum algorithm for the dihedral hidden subgroup problem, 2013.
- National Institute of Standards and Technology., Submission requirements and evaluation criteria for the post-quantum cryptography standardization process., 2016.
- Oded Regev, A subexponential time algorithm for the dihedral hidden subgroup problem with polynomial space, 2004.