HAL
archives-ouvertes.fr

Submerging CSIDH

Xavier Bonnetain, André Schrottenloher

▶ To cite this version:

Xavier Bonnetain, André Schrottenloher. Submerging CSIDH. JC2 2018 - Journées Codage et Cryptographie, Oct 2018, Aussois, France. hal-01961633

HAL Id: hal-01961633

https://hal.inria.fr/hal-01961633

Submitted on 20 Dec 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Submerging CSIDH

Xavier Bonnetain, André Schrottenloher

Inria, France

October 5, 2018

European Research Council
Established by the European Commission

Outline

One-way group action [Cou06, CLM$^+$]

Group action

A **group** G acts on a **set** X.
$h * (g * x) = (h \cdot g) * x$

Easy

- Operations in G ;
- Action $g * x$, $g \in G$, $x \in X$.

Hard

- Find g from x and $x' = g * x$.

CSIDH

In the case of CSIDH [CLM+]

Set

Montgomery curves on $\mathbb{F}_p$:

$$E_A \ : y^2 = x^3 + Ax^2 + x \ .$$

Endomorphism Ring

- $End_{p^2}(E_A)$: Order of a quaternion algebra
- $End_p(E_A) = \mathbb{Z}[\pi] = \mathbb{Z}[\sqrt{-p}]$

Group

Isogenies between those curves, which correspond exactly to $\mathcal{C}\ell\mathcal{O}$ where $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$.

Parameters rationale

The base field is $\mathbb{F}_p$ for $p = 4\ell_1 \cdots \ell_u - 1$, with $\ell_1, \ldots \ell_u$ small primes.

It turns out that each ℓ_i gives an isogeny $[\mathfrak{l}_i]$ of **small** degree ℓ_i, very easy to compute (as $[\mathfrak{l}_i]^{-1}$).

$\mathcal{C}\ell\mathcal{O}$ is spanned by products of the form:

$$\prod_{i=1}^{u} [\mathfrak{l}_i]^{e_i}$$

for $e_i \in \{-m \ldots m\}$ and $2m + 1 \simeq p^{1/(2u)}$ ($\mathcal{C}\ell\mathcal{O}$ has $O(\sqrt{p})$ elements).

The one-way commutative group action!

Computing the action of $[\mathfrak{b}] = \prod_{i=1}^{u} [\mathfrak{l}_i]^{e_i}$:

Apply successively *um* isogenies of degree $\leq \ell_u$.

Find $[\mathfrak{b}]$ such that $[\mathfrak{b}] \cdot E = E'$:

Compute an isogeny between two curves E and E'.

Commutative group action

$$[\mathfrak{b}] \cdot E = E' \Rightarrow \forall [\mathfrak{a}] \in \mathcal{C}\ell\mathcal{O}, [\mathfrak{a}\mathfrak{b}] \cdot E = [\mathfrak{a}] \cdot E'$$

CSIDH parameters for NIST security levels

Level	$\log_2 p$	# primes	Isogeny range	Estimated quantum query cost
NIST 1	512	74	5	2^{62}
NIST 3	1024	132	7	2^{94}
NIST 5	1792	209	10	2^{129}

Hidden Shift Algorithms

Hidden Shift

$$f(x) = g(x+s), x \in \mathbb{G}. \quad \text{Find } s$$

Quantum Algorithms

- $\mathcal{O}\left(8^{\sqrt{n}}\right)$ in $\mathbb{Z}/(2^n\mathbb{Z})$ [Kup05]
- $\mathcal{O}\left(8^{\sqrt{\log_2(N)}}\right)$ in $\mathbb{Z}/(N\mathbb{Z})$ [Kup05]
- $\widetilde{\mathcal{O}}\left(3^{\sqrt{2\log_3(N)}}\right)$ in $\mathbb{Z}/(N\mathbb{Z})$, N smooth [Kup05]
- $\widetilde{\mathcal{O}}\left(2^{\sqrt{2n\log_2(n)}}\right)$ in $\mathbb{Z}/(2^n\mathbb{Z})$, polynomial memory [Reg04]
- $\widetilde{\mathcal{O}}\left(2^{\sqrt{2\log_2(N)}}\right)$ in $\mathbb{Z}/(N\mathbb{Z})$, with QRAM [Kup13]
- $\widetilde{\mathcal{O}}\left(2^{\sqrt{2\log_2(N)\log_2(\log_2(N))}}\right)$ in $\mathbb{Z}/(N\mathbb{Z})$, polynomial memory [CJS14]
- $2^{\sqrt{2\log_2(3)n}}$ in $\mathbb{Z}/(2^n\mathbb{Z})$ [BNP18]

Hidden Shift

What we have

Hidden shift algorithm for $\mathbb{Z}/(2^n\mathbb{Z})$ that costs $2^{\sqrt{2\log_2(3)n}}$

What we need

Precise cost for a hidden shift algorithm for $\mathbb{Z}/(N\mathbb{Z})$

Hidden Shift in $\mathbb{Z}/(2^n\mathbb{Z})$

Oracle

$$\mathrm{O}: \begin{array}{ccc} |0\rangle\,|x\rangle\,|0\rangle & \mapsto & |0\rangle\,|x\rangle\,|f(x)\rangle \\ |1\rangle\,|x\rangle\,|0\rangle & \mapsto & |1\rangle\,|x\rangle\,|g(x)\rangle \end{array}$$

Sampling

$$\mathrm{O}\left(\frac{1}{2^{(n+1)/2}}\sum_{i=0}^{2^n}(|0\rangle+|1\rangle)\,|i\rangle\,|0\rangle\right) = \frac{1}{2^{(n+1)/2}}\sum_{f(x)}(|0\rangle\,|x\rangle+|1\rangle\,|x+s\rangle)\,|f(x)\rangle$$

Quantum Fourier Transform

$$|\psi_\ell\rangle = |0\rangle + \exp\left(2i\pi s\frac{\ell}{2^n}\right)|1\rangle\,,\ell$$

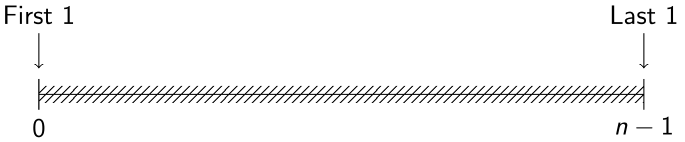
Combining the qubits

Targets

$$\begin{aligned} |\psi_{2^{n-1}}\rangle &= |0\rangle + (-1)^s |1\rangle \\ |\psi_{2^{n-2}}\rangle &= |0\rangle + (-1)^{\lfloor s/2 \rfloor} \exp\left(2i\pi \frac{s \mod 2}{4}\right) |1\rangle \\ \ldots \end{aligned}$$

Combination

$$(\ell_1, \ell_2) \mapsto \ell_1 \pm \ell_2 \mod 2^n$$



$\ell \in [0; 2^n)$

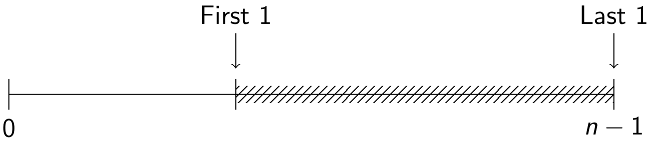
Combining the qubits

Targets

$$\begin{aligned} |\psi_{2^n-1}\rangle &= |0\rangle + (-1)^s |1\rangle \\ |\psi_{2^n-2}\rangle &= |0\rangle + (-1)^{\lfloor s/2 \rfloor} \exp\left(2i\pi \frac{s \mod 2}{4}\right) |1\rangle \\ \dots \end{aligned}$$

Combination

$$(\ell_1, \ell_2) \mapsto \ell_1 \pm \ell_2 \mod 2^n$$



$\ell \in 2^a[0; 2^{n-a})$

Combining the qubits

Targets

$$
\begin{aligned}
|\psi_{2^{n-1}}\rangle &= |0\rangle + (-1)^s\,|1\rangle \\
|\psi_{2^{n-2}}\rangle &= |0\rangle + (-1)^{\lfloor s/2 \rfloor} \exp\left(2i\pi \frac{s \mod 2}{4}\right)|1\rangle \\
&\dots
\end{aligned}
$$

Combination

$$(\ell_1, \ell_2) \mapsto \ell_1 \pm \ell_2 \mod 2^n$$

$$\ell \in 2^b[0; 2^{n-b})$$

Combining the qubits

Targets

$$
\begin{aligned}
|\psi_{2^{n-1}}\rangle &= |0\rangle + (-1)^{s} |1\rangle \\
|\psi_{2^{n-2}}\rangle &= |0\rangle + (-1)^{\lfloor s/2 \rfloor} \exp\left(2i\pi \frac{s \mod 2}{4}\right) |1\rangle \\
\ldots
\end{aligned}
$$

Combination

$$(\ell_1, \ell_2) \mapsto \ell_1 \pm \ell_2 \mod 2^n$$

$$\ell \in \{0, 2^{n-1}\}$$

Hidden Shift in $\mathbb{Z}/(N\mathbb{Z})$

Situation

Elements	$\lvert\psi_\ell\rangle = \lvert 0\rangle + \exp\left(2i\pi s\frac{\ell}{N}\right)\lvert 1\rangle$
Targets	$\bigotimes_{i=0}^{n}\lvert\psi_{2^i}\rangle \simeq QFT\lvert t\rangle,\ \frac{t}{2^n} \simeq \frac{s}{N}$
Combination	$(\ell_1, \ell_2) \mapsto \ell_1 \pm \ell_2 \mod N$

Hidden Shift in $\mathbb{Z}/(N\mathbb{Z})$

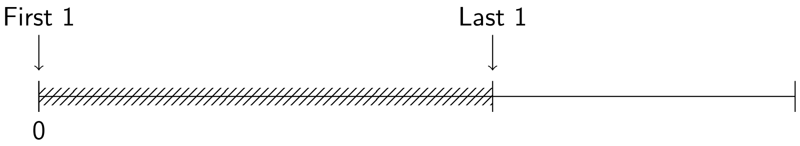
Situation

Elements	$\vert\psi_\ell\rangle = \vert 0\rangle + \exp\left(2i\pi s\frac{\ell}{N}\right)\vert 1\rangle$
Targets	$\bigotimes_{i=0}^{n}\vert\psi_{2^i}\rangle \simeq QFT\vert t\rangle, \frac{t}{2^n} \simeq \frac{s}{N}$
Combination	$(\ell_1, \ell_2) \mapsto \ell_1 \pm \ell_2$ in $\mathbb{Z}$

Hidden Shift in $\mathbb{Z}/(N\mathbb{Z})$

Situation

Elements	$\|\psi_\ell\rangle = \|0\rangle + \exp\left(2i\pi s\frac{\ell}{N}\right)\|1\rangle$
Targets	$\bigotimes_{i=0}^{n} \|\psi_{2^i}\rangle \simeq QFT\,\|t\rangle\,, \frac{t}{2^n} \simeq \frac{s}{N}$
Combination	$(\ell_1, \ell_2) \mapsto \ell_1 \pm \ell_2$ in $\mathbb{Z}$

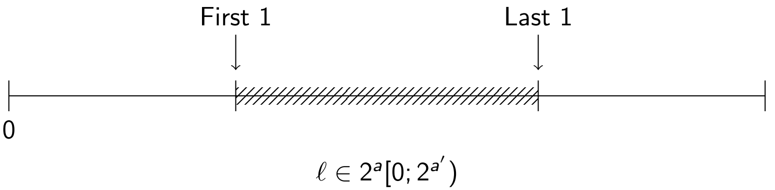


$\ell \in [0; N)$

Hidden Shift in $\mathbb{Z}/(N\mathbb{Z})$

Situation

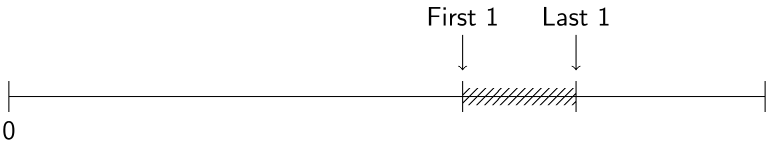
Elements	$\lvert\psi_\ell\rangle = \lvert 0\rangle + \exp\left(2i\pi s \frac{\ell}{N}\right)\lvert 1\rangle$
Targets	$\bigotimes_{i=0}^{n} \lvert\psi_{2^i}\rangle \simeq QFT \lvert t\rangle, \frac{t}{2^n} \simeq \frac{s}{N}$
Combination	$(\ell_1, \ell_2) \mapsto \ell_1 \pm \ell_2$ in $\mathbb{Z}$



Hidden Shift in $\mathbb{Z}/(N\mathbb{Z})$

Situation

Elements	$\lvert\psi_\ell\rangle = \lvert 0\rangle + \exp\left(2i\pi s\frac{\ell}{N}\right)\lvert 1\rangle$
Targets	$\bigotimes_{i=0}^{n}\lvert\psi_{2^i}\rangle \simeq QFT\lvert t\rangle,\ \frac{t}{2^n} \simeq \frac{s}{N}$
Combination	$(\ell_1, \ell_2) \mapsto \ell_1 \pm \ell_2$ in $\mathbb{Z}$



$\ell \in 2^b[0; 2^{b'})$

Hidden Shift in $\mathbb{Z}/(N\mathbb{Z})$

Situation

Elements	$\|\psi_\ell\rangle = \|0\rangle + \exp\left(2i\pi s\frac{\ell}{N}\right)\|1\rangle$
Targets	$\bigotimes_{i=0}^{n}\|\psi_{2^i}\rangle \simeq QFT\,\|t\rangle\,,\ \frac{t}{2^n} \simeq \frac{s}{N}$
Combination	$(\ell_1,\ell_2) \mapsto \ell_1 \pm \ell_2$ in $\mathbb{Z}$

$\ell \in \{0, 2^c\}$

Cost for CSIDH

Final complexity

- Around $5 \times 2^{1.8\sqrt{\log_2(N)}}$ (simulated!) queries to f and g and quantum memory
- Log. overhead for classical time and memory

Costs for CSIDH ($\log_2$)

$\log_2(p)$	n	Our Hidden Shift query cost	Query cost estimation from [CLM+]
512	256	32.5	62
1024	512	44.5	94
1792	896	57.5	129

Computing a group action

Objectives

Target

Find an **efficient** procedure to compute:

$$[\mathfrak{g}] \cdot E$$

where E is a CSIDH curve and $[\mathfrak{g}] \in \mathcal{C}\ell\mathcal{O}$, in superposition over the whole group $\mathcal{C}\ell\mathcal{O}$.

General situation

Direct computation of $[\mathfrak{g}] \cdot E$ is expensive

In CSIDH

Computing the $[\mathfrak{l}_i] \cdot E$ is cheap

Cost reduction

Strategy

- Decompose $[\mathfrak{g}] = \prod [\mathfrak{l}_i]^{e_i}$
- Ensure $(e_1, \ldots, e_k)$ is small
- Compute $\prod [\mathfrak{l}_i]^{e_i}$

In Practice

- Precompute a short basis B of $\{(e_1, \ldots, e_k) | \prod [\mathfrak{l}_i]^{e_i} = 1\}$ (BKZ-20)
- Quantumly decompose $[\mathfrak{g}]$ over $[\mathfrak{l}_i]$ (Shor)
- Reduce the size of the exponents using B (Babai)
- Compute the isogeny

Overhead between 2^5 and 2^8 theoretically, heuristically between 2 and 5.

Ordinary curves

The Couveignes–Rostovtsev–Stolbunov scheme

- In general, in the ordinary case, one can find ideal classes to span $\mathcal{C}\ell\mathcal{O}$, but they cost much more.
- Taking $u = \frac{1}{2}\frac{\log p}{\log 3}$:

$$\mathcal{C}\ell\mathcal{O} \simeq \{[\mathfrak{l}_1]^{e_1} \cdots [\mathfrak{l}_u]^{e_u}, e_i \in \{-1, 0, 1\}\} \ .$$

Two choices

- Keep this basis: the dimension increases. The approximation factor remains good in practice: 2^3 for $\log_2 p = 512$ to 2^4 for $\log_2 p = 1024$. could increase up to 2^{15} (in practice better).
- Take a smaller dimension and bigger exponents (asymptotically better) [BFJ16, BJI18].

De Feo–Kieffer–Smith's scheme [FKS18]

Intermediate situation. Products are of the form:

$$[\mathfrak{l}_1]^{e_1} \cdots [\mathfrak{l}_u]^{e_u} \cdots [\mathfrak{l}_{u+v}]^{e_{u+v}} \quad .$$

The e_i have different ranges $-m_i \ldots m_i$ and some **must be** positive.

We can adapt!

- Take the weights m_i into account in $\mathcal{L}$.
- Adapt the CVP instance to force some coordinates to be positive.

Overhead 2^5 w.r.t a classical group action (better than taking a naïve decomposition).
$\Rightarrow 2^{38}$ equivalent classical group actions for 56-bit parameters proposed in [FKS18].

Conclusion

Conclusion

We have estimated the cost of Kuperberg's algorithm.

- To reach the NIST security levels in **queries**, parameters should be multiplied by 4.

We have estimated the time to attack CSIDH.

- To reach the NIST security levels in **time**, parameters should be doubled to tripled.

Level	Original $\log_2 p$	Corrected $\log_2 p$
NIST 1	512	900
NIST 3	1024	2500
NIST 5	1792	5000

Thank you!

References I

Jean-François Biasse, Claus Fieker, and Michael J Jacobson.
Fast heuristic algorithms for computing relations in the class group of a quadratic order, with applications to isogeny evaluation.
LMS Journal of Computation and Mathematics, 19(A):371–390, 2016.

Jean-François Biasse, Michael J Jacobson, and Annamaria Iezzi.
A note on the security of CSIDH.
CoRR, 2018.

Xavier Bonnetain and María Naya-Plasencia.
Hidden shift quantum cryptanalysis and implications.
Cryptology ePrint Archive, Report 2018/432, 2018.
`https://eprint.iacr.org/2018/432`.

Andrew M. Childs, David Jao, and Vladimir Soukharev.
Constructing elliptic curve isogenies in quantum subexponential time.
J. Mathematical Cryptology, 8(1):1–29, 2014.

References II

Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes.
CSIDH: An efficient post-quantum commutative group action.
To appear in: Advances in Cryptology - ASIACRYPT 2018 - 24th Annual International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, Australia, December 02-06, 2018.

Jean-Marc Couveignes.
Hard homogeneous spaces.
Cryptology ePrint Archive, Report 2006/291, 2006.
https://eprint.iacr.org/2006/291.

Luca De Feo, Jean Kieffer, and Benjamin Smith.
Towards practical key exchange from ordinary isogeny graphs.
Cryptology ePrint Archive, Report 2018/485, 2018.
https://eprint.iacr.org/2018/485.

References III

Greg Kuperberg.
A Subexponential-Time Quantum Algorithm for the Dihedral Hidden Subgroup Problem.
SIAM J. Comput., 35(1):170–188, 2005.

Greg Kuperberg.
Another Subexponential-time Quantum Algorithm for the Dihedral Hidden Subgroup Problem.
In *8th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2013, May 21-23, 2013, Guelph, Canada*, pages 20–34, 2013.

Oded Regev.
A Subexponential Time Algorithm for the Dihedral Hidden Subgroup Problem with Polynomial Space.
CoRR, 2004.