Quantum circuits for the CSIDH: optimizing quantum evaluation of isogenies

Daniel J. Bernstein

Tanja Lange

Chloe Martindale

Lorenz Panny

quantum.isogeny.org

Key bits where all known attacks take 2^λ operations (naive serial attack metric, ignoring memory cost):

	pre-quantum	post-quantum
SIDH, SIKE	$(24 + o(1))\lambda$	$(36 + o(1))\lambda$
compressed	$(14 + o(1))\lambda$	$(21 + o(1))\lambda$
CRS, CSIDH	$(4 + o(1))\lambda$	superlinear

Key bits where all known attacks take 2^λ operations (naive serial attack metric, ignoring memory cost):

	pre-quantum	post-quantum
SIDH, SIKE	$(24 + o(1))\lambda$	$(36 + o(1))\lambda$
compressed	$(14 + o(1))\lambda$	$(21 + o(1))\lambda$
CRS, CSIDH	$(4 + o(1))\lambda$	superlinear

For which λ does this cross $(21 + o(1))\lambda$?

Key bits where all known attacks take 2^λ operations (naive serial attack metric, ignoring memory cost):

	pre-quantum	post-quantum
SIDH, SIKE	$(24 + o(1))\lambda$	$(36 + o(1))\lambda$
compressed	$(14 + o(1))\lambda$	$(21 + o(1))\lambda$
CRS, CSIDH	$(4 + o(1))\lambda$	superlinear

For which λ does this cross $(21 + o(1))\lambda$?

Subexp 2010 Childs–Jao–Soukharev attack, using 2003 Kuperberg or 2004 Regev or 2011 Kuperberg.

Key bits where all known attacks take 2^λ operations (naive serial attack metric, ignoring memory cost):

	pre-quantum	post-quantum
SIDH, SIKE	$(24 + o(1))\lambda$	$(36 + o(1))\lambda$
compressed	$(14 + o(1))\lambda$	$(21 + o(1))\lambda$
CRS, CSIDH	$(4 + o(1))\lambda$	superlinear

For which λ does this cross $(21 + o(1))\lambda$?

Subexp 2010 Childs–Jao–Soukharev attack, using 2003 Kuperberg or 2004 Regev or 2011 Kuperberg.

- How many queries do these attacks perform?

Key bits where all known attacks take 2^λ operations (naive serial attack metric, ignoring memory cost):

	pre-quantum	post-quantum
SIDH, SIKE	$(24 + o(1))\lambda$	$(36 + o(1))\lambda$
compressed	$(14 + o(1))\lambda$	$(21 + o(1))\lambda$
CRS, CSIDH	$(4 + o(1))\lambda$	superlinear

For which λ does this cross $(21 + o(1))\lambda$?

Subexp 2010 Childs–Jao–Soukharev attack, using 2003 Kuperberg or 2004 Regev or 2011 Kuperberg.

- How many queries do these attacks perform?
- How expensive is each CSIDH query?

Key bits where all known attacks take 2^λ operations (naive serial attack metric, ignoring memory cost):

	pre-quantum	post-quantum
SIDH, SIKE	$(24 + o(1))\lambda$	$(36 + o(1))\lambda$
compressed	$(14 + o(1))\lambda$	$(21 + o(1))\lambda$
CRS, CSIDH	$(4 + o(1))\lambda$	superlinear

For which λ does this cross $(21 + o(1))\lambda$?

Subexp 2010 Childs–Jao–Soukharev attack, using 2003 Kuperberg or 2004 Regev or 2011 Kuperberg.

- How many queries do these attacks perform?
- How expensive is each CSIDH query?
  Our 56-page paper: see `quantum.isogeny.org`.

Key bits where all known attacks take 2^λ operations (naive serial attack metric, ignoring memory cost):

	pre-quantum	post-quantum
SIDH, SIKE	$(24 + o(1))\lambda$	$(36 + o(1))\lambda$
compressed	$(14 + o(1))\lambda$	$(21 + o(1))\lambda$
CRS, CSIDH	$(4 + o(1))\lambda$	superlinear

For which λ does this cross $(21 + o(1))\lambda$?

Subexp 2010 Childs–Jao–Soukharev attack, using 2003 Kuperberg or 2004 Regev or 2011 Kuperberg.

- How many queries do these attacks perform?
- How expensive is each CSIDH query?
  Our 56-page paper: see `quantum.isogeny.org`.
- What about memory, using parallel *AT* metric?

Case study: attacking CSIDH-512

CSIDH-512 query, uniform over $\{-5, \ldots, 5\}^{74}$, failure chance $<2^{-32}$ (maybe ok), nonlinear bit ops: $\approx 2^{51}$ by 2018 Jao–LeGrow–Leonardi–Ruiz-Lopez.

Case study: attacking CSIDH-512

CSIDH-512 query, uniform over $\{-5, \ldots, 5\}^{74}$,
failure chance $<2^{-32}$ (maybe ok), nonlinear bit ops:
$\approx 2^{51}$ by 2018 Jao–LeGrow–Leonardi–Ruiz-Lopez.
$1118827416420 \approx 2^{40}$ by our Algorithm 7.1.

Case study: attacking CSIDH-512

CSIDH-512 query, uniform over $\{-5, \ldots, 5\}^{74}$,
failure chance $<2^{-32}$ (maybe ok), nonlinear bit ops:
$\approx 2^{51}$ by 2018 Jao–LeGrow–Leonardi–Ruiz-Lopez.
$1118827416420 \approx 2^{40}$ by our Algorithm 7.1.
$765325228976 \approx 0.7 \cdot 2^{40}$ by our Algorithm 8.1.

Generic conversion to quantum computation:
$\approx 2^{43.3}$ T-gates using $\approx 2^{40}$ qubits.

Case study: attacking CSIDH-512

CSIDH-512 query, uniform over $\{-5,\ldots,5\}^{74}$, failure chance $<2^{-32}$ (maybe ok), nonlinear bit ops:
$\approx 2^{51}$ by 2018 Jao–LeGrow–Leonardi–Ruiz-Lopez.
$1118827416420 \approx 2^{40}$ by our Algorithm 7.1.
$765325228976 \approx 0.7 \cdot 2^{40}$ by our Algorithm 8.1.

Generic conversion to quantum computation:
$\approx 2^{43.3}$ T-gates using $\approx 2^{40}$ qubits.
Can do $\approx 2^{45.3}$ T-gates using $\approx 2^{20}$ qubits.

Case study: attacking CSIDH-512

CSIDH-512 query, uniform over $\{-5, \ldots, 5\}^{74}$, failure chance $<2^{-32}$ (maybe ok), nonlinear bit ops:
$\approx 2^{51}$ by 2018 Jao–LeGrow–Leonardi–Ruiz-Lopez.
$1118827416420 \approx 2^{40}$ by our Algorithm 7.1.
$765325228976 \approx 0.7 \cdot 2^{40}$ by our Algorithm 8.1.

Generic conversion to quantum computation:
$\approx 2^{43.3}$ T-gates using $\approx 2^{40}$ qubits.
Can do $\approx 2^{45.3}$ T-gates using $\approx 2^{20}$ qubits.
Total gates (T+Clifford): $\approx 2^{46.9}$.

Case study: attacking CSIDH-512

CSIDH-512 query, uniform over $\{-5, \ldots, 5\}^{74}$,
failure chance $<2^{-32}$ (maybe ok), nonlinear bit ops:
$\approx 2^{51}$ by 2018 Jao–LeGrow–Leonardi–Ruiz-Lopez.
$1118827416420 \approx 2^{40}$ by our Algorithm 7.1.
$765325228976 \approx 0.7 \cdot 2^{40}$ by our Algorithm 8.1.

Generic conversion to quantum computation:
$\approx 2^{43.3}$ T-gates using $\approx 2^{40}$ qubits.
Can do $\approx 2^{45.3}$ T-gates using $\approx 2^{20}$ qubits.
Total gates (T+Clifford): $\approx 2^{46.9}$.

BS18 claim only $\approx 2^{2}$ lattice overhead per query.
BS18 claim only $\approx 2^{32.5}$ queries using $\approx 2^{31}$ qubits.

Case study: attacking CSIDH-512

CSIDH-512 query, uniform over $\{-5,\ldots,5\}^{74}$, failure chance $<2^{-32}$ (maybe ok), nonlinear bit ops:
$\approx 2^{51}$ by 2018 Jao–LeGrow–Leonardi–Ruiz-Lopez.
$1118827416420 \approx 2^{40}$ by our Algorithm 7.1.
$765325228976 \approx 0.7 \cdot 2^{40}$ by our Algorithm 8.1.

Generic conversion to quantum computation:
$\approx 2^{43.3}$ T-gates using $\approx 2^{40}$ qubits.
Can do $\approx 2^{45.3}$ T-gates using $\approx 2^{20}$ qubits.
Total gates (T+Clifford): $\approx 2^{46.9}$.

BS18 claim only $\approx 2^{2}$ lattice overhead per query.
BS18 claim only $\approx 2^{32.5}$ queries using $\approx 2^{31}$ qubits.
If these claims are correct: $\approx 2^{81.4}$ total gates.

Case study: attacking CSIDH-512

CSIDH-512 query, uniform over $\{-5, \ldots, 5\}^{74}$,
failure chance $<2^{-32}$ (maybe ok), nonlinear bit ops:
$\approx 2^{51}$ by 2018 Jao–LeGrow–Leonardi–Ruiz-Lopez.
$1118827416420 \approx 2^{40}$ by our Algorithm 7.1.
$765325228976 \approx 0.7 \cdot 2^{40}$ by our Algorithm 8.1.

Generic conversion to quantum computation:
$\approx 2^{43.3}$ T-gates using $\approx 2^{40}$ qubits.
Can do $\approx 2^{45.3}$ T-gates using $\approx 2^{20}$ qubits.
Total gates (T+Clifford): $\approx 2^{46.9}$.

BS18 claim only $\approx 2^{2}$ lattice overhead per query.
BS18 claim only $\approx 2^{32.5}$ queries using $\approx 2^{31}$ qubits.
If these claims are correct: $\approx 2^{81.4}$ total gates.
BS18 claim 2^{71} total gates. We explain gap.