Quantum circuits for the CSIDH: optimizing quantum evaluation of isogenies

Daniel J. Bernstein

Tanja Lange

Chloe Martindale

Lorenz Panny

quantum.isogeny.org

Non-interactive key exchange

Alice: secret a, public aG. Bob: secret b, public bG.
Shared secret $a(bG) = (ab)G = (ba)G = b(aG)$.

Non-interactive key exchange

Alice: secret a, public aG. Bob: secret b, public bG.
Shared secret $a(bG) = (ab)G = (ba)G = b(aG)$.

DH: 1976 Diffie–Hellman.
ECDH: 1985 Miller, 1987 Koblitz.
Cost poly(λ) for pre-quantum security level 2^λ
(*assuming* that the best attacks known are optimal).

Non-interactive key exchange

Alice: secret a, public aG. Bob: secret b, public bG.
Shared secret $a(bG) = (ab)G = (ba)G = b(aG)$.

DH: 1976 Diffie–Hellman.
ECDH: 1985 Miller, 1987 Koblitz.
Cost poly(λ) for pre-quantum security level 2^λ
(*assuming* that the best attacks known are optimal).
Fast addition of public keys $\rightarrow$ post-quantum break.

Non-interactive key exchange

Alice: secret a, public aG. Bob: secret b, public bG.
Shared secret $a(bG) = (ab)G = (ba)G = b(aG)$.

DH: 1976 Diffie–Hellman.
ECDH: 1985 Miller, 1987 Koblitz.
Cost poly(λ) for pre-quantum security level 2^λ
(*assuming* that the best attacks known are optimal).
Fast addition of public keys $\rightarrow$ post-quantum break.

CRS: 2006 Rostovtsev–Stolbunov, 2006 Couveignes.
CSIDH: 2018 Castryck-Lange-Martindale-Panny-Renes.
Cost poly(λ) for pre-quantum security level 2^λ.

Non-interactive key exchange

Alice: secret a, public aG. Bob: secret b, public bG.
Shared secret $a(bG) = (ab)G = (ba)G = b(aG)$.

DH: 1976 Diffie–Hellman.
ECDH: 1985 Miller, 1987 Koblitz.
Cost poly(λ) for pre-quantum security level 2^λ
(*assuming* that the best attacks known are optimal).
Fast addition of public keys $\to$ post-quantum break.

CRS: 2006 Rostovtsev–Stolbunov, 2006 Couveignes.
CSIDH: 2018 Castryck-Lange-Martindale-Panny-Renes.
Cost poly(λ) for pre-quantum security level 2^λ.
Cost poly(λ) for post-quantum security level 2^λ.

Encryption systems with small public keys

PKE doesn't require NIKE: e.g., 2011 SIDH/SIKE.

Encryption systems with small public keys

PKE doesn't require NIKE: e.g., 2011 SIDH/SIKE.
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
ECDH	$(2+o(1))\lambda$	exponential

Encryption systems with small public keys

PKE doesn't require NIKE: e.g., 2011 SIDH/SIKE.
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
ECDH	$(2 + o(1))\lambda$	exponential

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

Major questions

What CSIDH key sizes are needed for
post-quantum security level 2^{64}? 2^{96}? 2^{128}?

Major questions

What CSIDH key sizes are needed for
post-quantum security level 2^{64}? 2^{96}? 2^{128}?

Subexp attack: many quantum CSIDH queries.

- How many queries do these attacks perform?
  2011 Kuperberg supersedes previous papers.

Major questions

What CSIDH key sizes are needed for post-quantum security level 2^{64}? 2^{96}? 2^{128}?

Subexp attack: many quantum CSIDH queries.

- How many queries do these attacks perform? 2011 Kuperberg supersedes previous papers.
- How is attack affected by occasional errors and non-uniform distributions over the group?

Major questions

What CSIDH key sizes are needed for
post-quantum security level 2^{64}? 2^{96}? 2^{128}?

Subexp attack: many quantum CSIDH queries.

- How many queries do these attacks perform? 2011 Kuperberg supersedes previous papers.
- How is attack affected by occasional errors and non-uniform distributions over the group?
- How expensive is each CSIDH query? **See our paper**—full 56-page version online, with detailed analysis and many optimizations.

Major questions

What CSIDH key sizes are needed for post-quantum security level 2^{64}? 2^{96}? 2^{128}?

Subexp attack: many quantum CSIDH queries.

- How many queries do these attacks perform? 2011 Kuperberg supersedes previous papers.
- How is attack affected by occasional errors and non-uniform distributions over the group?
- How expensive is each CSIDH query? **See our paper**—full 56-page version online, with detailed analysis and many optimizations.
- What about memory, using parallel AT metric?

Verifying quantum costs on your laptop

We provide software to compute CSIDH group action using bit operations. Automatic tallies of nonlinear ops (AND, OR), linear ops (XOR, NOT).

Verifying quantum costs on your laptop

We provide software to compute CSIDH group action using bit operations. Automatic tallies of nonlinear ops (AND, OR), linear ops (XOR, NOT).

Generic conversions:
sequence of bit ops with $\leq B$ nonlinear ops
$\Rightarrow$ sequence of *reversible* ops with $\leq 2B$ Toffoli ops

Verifying quantum costs on your laptop

We provide software to compute CSIDH group action using bit operations. Automatic tallies of nonlinear ops (AND, OR), linear ops (XOR, NOT).

Generic conversions:
sequence of bit ops with $\leq B$ nonlinear ops
$\Rightarrow$ sequence of *reversible* ops with $\leq 2B$ Toffoli ops
$\Rightarrow$ sequence of *quantum* gates with $\leq 14B$ T-gates.

Verifying quantum costs on your laptop

We provide software to compute CSIDH group action using bit operations. Automatic tallies of nonlinear ops (AND, OR), linear ops (XOR, NOT).

Generic conversions:
sequence of bit ops with $\le B$ nonlinear ops
$\Rightarrow$ sequence of *reversible* ops with $\le 2B$ Toffoli ops
$\Rightarrow$ sequence of *quantum* gates with $\le 14B$ T-gates.

Building confidence in correctness of output:
1. Compare output to Sage script for CSIDH.
2. Generating-function analysis of *exact* error rates.
Compare to experiments with noticeable error rates.

Case study: one CSIDH-512 query

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

Case study: one CSIDH-512 query

CSIDH-512 query, uniform over $\{-5,\ldots,5\}^{74}$,
error rate $<2^{-32}$ (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: one CSIDH-512 query

CSIDH-512 query, uniform over $\{-5, \ldots, 5\}^{74}$,
error rate $<2^{-32}$ (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.

Case study: one CSIDH-512 query

CSIDH-512 query, uniform over $\{-5, \ldots, 5\}^{74}$,
error rate $<2^{-32}$ (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.

$\Rightarrow \approx 2^{43.3}$ T-gates using $\approx 2^{40}$ qubits.

Case study: one CSIDH-512 query

CSIDH-512 query, uniform over $\{-5, \ldots, 5\}^{74}$,
error rate $<2^{-32}$ (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.

$\Rightarrow \approx 2^{43.3}$ T-gates using $\approx 2^{40}$ qubits.
Can do $\approx 2^{45.3}$ T-gates using $\approx 2^{20}$ qubits.

Case study: one CSIDH-512 query

CSIDH-512 query, uniform over $\{-5,\ldots,5\}^{74}$,
error rate $<2^{-32}$ (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.

$\Rightarrow \approx 2^{43.3}$ 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: one CSIDH-512 query

CSIDH-512 query, uniform over $\{-5,\ldots,5\}^{74}$,
error rate $<2^{-32}$ (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.

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

Variations in 512, $\{-5,\ldots,5\}$, 2^{-32}: see paper.

Case study: full CSIDH-512 attack

Important issues from other layers of attack:

- CSIDH-512 user has inputs $\{-5, \ldots, 5\}^{74}$ but attack seems to need wider range of inputs. BS18 claim$_1$: $\approx 2^2$ overhead to handle this issue.
- Attack has big outer loop, many queries. BS18 claim$_2$: $\approx 2^{32.5}$ queries using $\approx 2^{31}$ qubits.

BS18 = 2018 Bonnetain–Schrottenloher.

Case study: full CSIDH-512 attack

Important issues from other layers of attack:

- CSIDH-512 user has inputs $\{-5, \ldots, 5\}^{74}$ but attack seems to need wider range of inputs. BS18 claim$_1$: $\approx 2^2$ overhead to handle this issue.
- Attack has big outer loop, many queries. BS18 claim$_2$: $\approx 2^{32.5}$ queries using $\approx 2^{31}$ qubits.

BS18 = 2018 Bonnetain–Schrottenloher.

If claim$_1$ and claim$_2$ are correct: $\approx 2^{81.4}$ total gates. (Presumably larger cost in AT metric. Big circuit!)

Case study: full CSIDH-512 attack

Important issues from other layers of attack:

- CSIDH-512 user has inputs $\{-5, \ldots, 5\}^{74}$ but attack seems to need wider range of inputs. BS18 claim$_1$: $\approx 2^2$ overhead to handle this issue.
- Attack has big outer loop, many queries. BS18 claim$_2$: $\approx 2^{32.5}$ queries using $\approx 2^{31}$ qubits.

BS18 $=$ 2018 Bonnetain–Schrottenloher.

If claim$_1$ and claim$_2$ are correct: $\approx 2^{81.4}$ total gates. (Presumably larger cost in AT metric. Big circuit!)

BS18 claim$_3$: 2^{71} total gates. Our paper explains gap.