Quantum resource estimates for computing elliptic curve discrete logarithms

Martin Roetteler, Michael Naehrig, Krysta M. Svore, Kristin Lauter

Proc. ASIACRYPT 2017 | December 2017
Published by Springer
Lecture Notes in Computer Science
View Publication | DOI
Download BibTex

We give precise quantum resource estimates for Shor's algorithm to compute discrete logarithms on elliptic curves over prime fields. The estimates are derived from a simulation of a Toffoli gate network for controlled elliptic curve point addition, implemented within the framework of the quantum computing software tool suite LIQUi|〉. We determine circuit implementations for reversible modular arithmetic, including modular addition, multiplication and inversion, as well as reversible elliptic curve point addition. We conclude that elliptic curve discrete logarithms on an elliptic curve defined over an n -bit prime field can be computed on a quantum computer with at most 9n+2⌈log_2(n)⌉+10 qubits using a quantum circuit of at most 448 n^3 log_2(n)+4090 n^3 Toffoli gates. We are able to classically simulate the Toffoli networks corresponding to the controlled elliptic curve point addition as the core piece of Shor's algorithm for the NIST standard curves P-192, P-224, P-256, P-384 and P-521. Our approach allows gate-level comparisons to recent resource estimates for Shor's factoring algorithm. The results also support estimates given earlier by Proos and Zalka and indicate that, for current parameters at comparable classical security levels, the number of qubits required to tackle elliptic curves is less than for attacking RSA, suggesting that indeed ECC is an easier target than RSA.

Download PDF

Groups

Security and Cryptography

Microsoft Quantum - Redmond (QuArC)

Projects

Post-quantum Cryptography

Language-Integrated Quantum Operations: LIQUi|>

Research Areas

Quantum computing

Research Labs

Microsoft Quantum: Research

Follow us:

Share this page:

What's new

NEW Surface Pro 6

NEW Surface Laptop 2

NEW Surface Go

Xbox One X

Xbox One S

VR & mixed reality

Windows 10 apps

Office apps

Microsoft Store

Account profile

Download Center

Microsoft Store support

Returns

Order tracking

Store locations

Buy online, pick up in store

Education

Microsoft in education

Office for students

Office 365 for schools

Deals for students & parents

Microsoft Azure in education

Enterprise

Microsoft Azure

Microsoft Industry

Data platform

Find a solution provider

Microsoft partner resources

Microsoft AppSource

Health

Financial services

Developer

Microsoft Visual Studio

Windows Dev Center

Developer Network

TechNet

Microsoft developer program

Channel 9

Office Dev Center

Microsoft Garage

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Security