



NTNU

Norwegian University of
Science and Technology

Quantum-Safe Electronic Voting: Status and Challenges

Tjerand Silde @ Trustworthy Evidence-Based Elections

The Quantum Threat

Quantum computers are not better; they are different

They will generally be worse, but do specific things better

In theory, they can break public key encryption and digital signatures based on factoring and discrete log assumptions

There are many recent developments in quantum computing

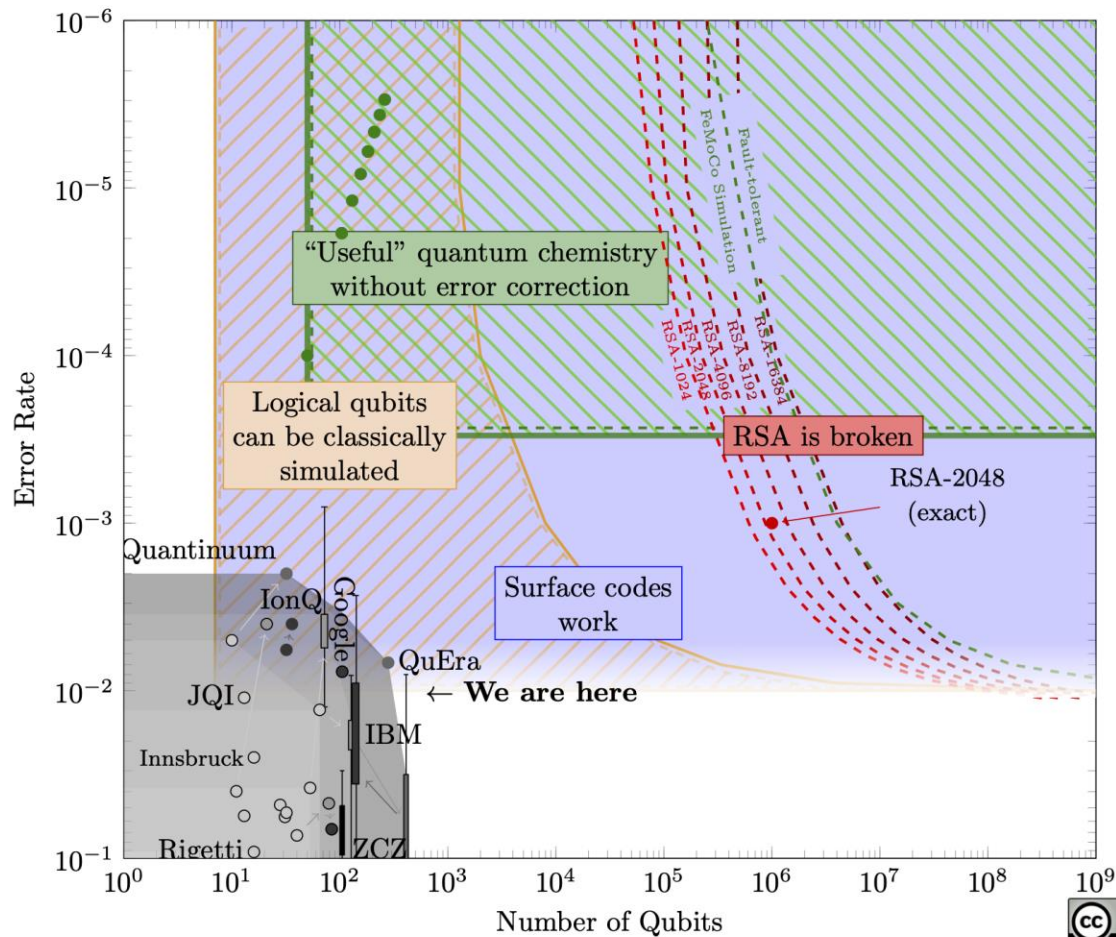
How to factor 2048 bit RSA integers with less than a million noisy qubits

Craig Gidney

Google Quantum AI, Santa Barbara, California 93117, USA

June 9, 2025

Planning the transition to quantum-safe cryptosystems requires understanding the cost of quantum attacks on vulnerable cryptosystems. In Gidney+Ekerå 2019, I co-published an estimate stating that 2048 bit RSA integers could be factored in eight hours by a quantum computer with 20 million noisy qubits. In this paper, I substantially reduce the number of qubits required. I estimate that a 2048 bit RSA integer could be factored in less than a week by a quantum computer with less than a million noisy qubits. I make the same assumptions as in 2019: a square grid of qubits with nearest neighbor connections, a uniform gate error rate of 0.1%, a surface code cycle time of 1 microsecond, and a control system reaction time of 10 microseconds.



FIPS 203

Federal Information Processing Standards Publication

Module-Lattice-Based Key-Encapsulation Mechanism Standard

Category: Computer Security

Subcategory: Cryptography

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

FIPS 204

Federal Information Processing Standards Publication

Module-Lattice-Based Digital Signature Standard

Category: Computer Security

Subcategory: Cryptography

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

Lattice Assumptions

Three main lattice assumptions: SIS, LWE, and NTRU

Have shown to be very expressive and quantum-secure

Hard to set parameters for correctness and security

(Learning With Errors)

$$\begin{bmatrix} \text{10x10 grid} \end{bmatrix} \begin{bmatrix} \text{10x1 orange vector} \end{bmatrix} + \begin{bmatrix} \text{10x1 yellow vector} \end{bmatrix} = \begin{bmatrix} \text{10x1 brown vector} \end{bmatrix}$$

Small coefficients to enforce uniqueness

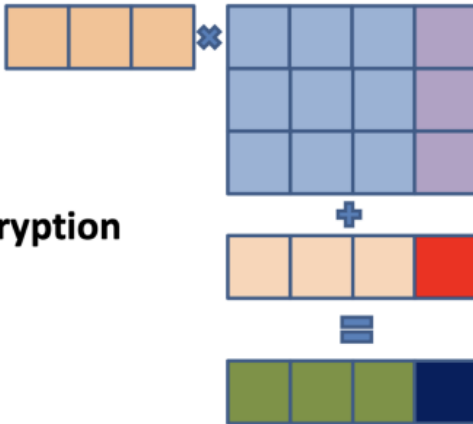
Small coefficients to enforce uniqueness

Encryption

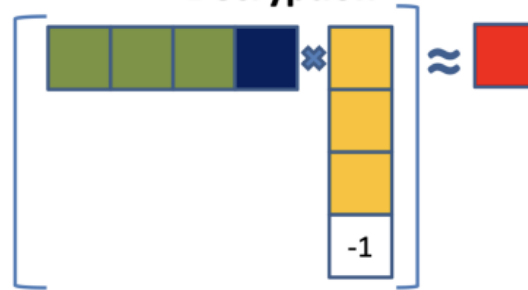


Public Key / Secret Key
Generation

Encryption



Decryption



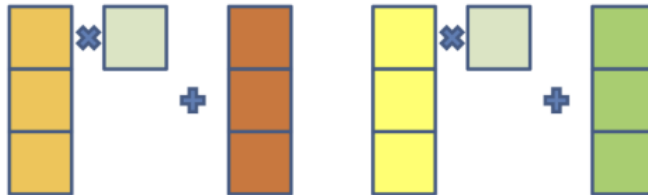
Signatures



Public Key / Secret Key
Generation



$$\text{[Green Box]} = H(\text{[Dark Purple Box]}, \mu)$$



Basic Lattice Cryptography

The concepts behind Kyber (ML-KEM) and Dilithium (ML-DSA)

Vadim Lyubashevsky

IBM Research Europe, Zurich

vad@zurich.ibm.com

Challenges with Lattices

Masking is complicated since secrets have short norms

- Must use rejection sampling or noise drowning

There exist efficient trapdoors for lattices

- Must prove that an instance is generated honestly

Homomorphic operations and challenges impact norms

- Must use specialized techniques to deal with this

Homomorphic Counting

Practical Quantum-Safe Voting from Lattices

Rafaël del Pino
IBM Research – Zurich
afe@zurich.ibm.com

Gregory Neven
IBM Research – Zurich
nev@zurich.ibm.com

Vadim Lyubashevsky
IBM Research – Zurich
vad@zurich.ibm.com

Gregor Seiler
IBM Research – Zurich
grs@zurich.ibm.com

Re-Randomization Mix-Net

More Efficient Lattice-Based Electronic Voting from NTRU

Patrick Hough^{a,1}  , Caroline Sandsbråten²   and Tjerand Silde²  



¹ University of Oxford, Mathematical Institute, Oxford, United Kingdom

² Norwegian University of Science and Technology, Department of Information Security and
Communication Technology, Trondheim, Norway

Ciphertexts of 15 KB, shuffle 115 KB, decryption 85 KB

Decryption Mix-Net

Efficient Verifiable Mixnets from Lattices, Revisited

Jonathan Bootle¹ , Vadim Lyubashevsky¹ , and
Antonio Merino-Gallardo^{1,2*} 

¹ IBM Research Europe, Zurich, Switzerland
`{jbt,vad}@zurich.ibm.com`

² Hasso-Plattner-Institute, University of Potsdam, Potsdam, Germany
`antonio@m-g.es`

Ciphertexts of ~6.5 KB, shuffle + decryption of 110 KB

(zk-)SNARKs

LaBRADOR: Compact Proofs for R1CS from Module-SIS[★]

Ward Beullens and Gregor Seiler

IBM Research Europe

Proofs of ~60-100 KB for essentially any (lattice) statement



NTNU

Norwegian University of
Science and Technology

Threshold

Olingo: Threshold Lattice Signatures with DKG and Identifiable Abort

Kamil Doruk Gur¹ , Patrick Hough² , Jonathan Katz³ ,
Caroline Sandsbråten⁴ , and Tjerand Silde⁴ 

¹ University of Maryland, dgur1@proton.me

² Universität der Bundeswehr München, patrick.hough@unibw.de

³ Google, jkatz2@gmail.com

⁴ Norwegian University of Science and Technology,
{caroline.sandsbraten, tjerand.silde}@ntnu.no

Allows for arbitrary threshold decryption and distributed setup



QROM / Online Extractability

A New Simple Technique to Bootstrap Various Lattice Zero-Knowledge Proofs to QROM Secure NIZKs

Shuichi Katsumata¹

¹AIST, Tokyo, Japan

`shuichi.katsumata@aist.go.jp`

Post-Quantum Privacy vs Integrity

Practical Non-interactive Publicly Verifiable Secret Sharing with Thousands of Parties

Craig Gentry¹, Shai Halevi¹, and Vadim Lyubashevsky²

¹ Algorand Foundation, USA

² IBM Research, Switzerland



Open-Source Implementations



The LaZer Library: Lattice-Based Zero Knowledge and Succinct Proofs for Quantum-Safe Privacy

Vadim Lyubashevsky
IBM Research Europe
Zurich, Switzerland
vad@zurich.ibm.com

Gregor Seiler
IBM Research Europe
Zurich, Switzerland
gseiler@posteo.net

Patrick Steuer
IBM Research Europe
Zurich, Switzerland
ick@zurich.ibm.com

Cryptology and Social Life Workshop

NTNU in Trondheim, on December 11 and 12

Free registration; talks, discussions, dinner

- Phil Rogaway – “Can Ethics Be Taught?”
- Rikke Bjerg Jensen – “Social Foundations of Cryptography: An Ethnography Talk”
- Jean-François Blanchette – Legislating digital signatures: Lessons from a past cryptographic utopia