

Going quantum-resistant: preparing IKEv2 for the quantum era

Tobias Heider, Stefan-Lukas Gazdag

The logo for 'genja' is written in a purple, lowercase, sans-serif font. The letters are connected, with the 'g' and 'e' sharing a common baseline and the 'n' and 'j' also connected to each other.

Shor's Algorithm

The end of hidden-subgroup cryptography

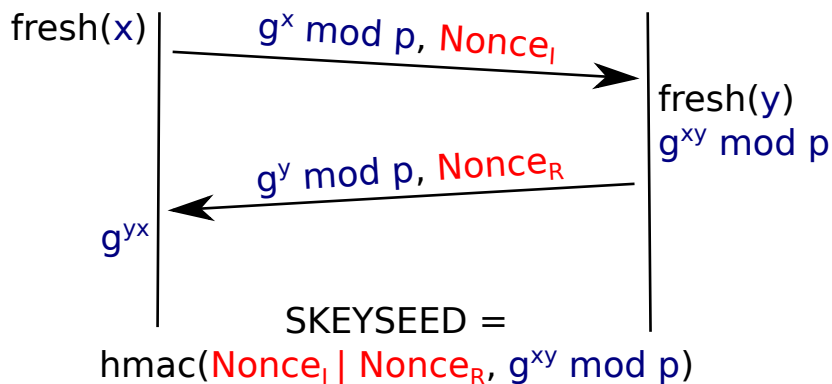
Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor[†]

Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

IKE SA INIT



Massive Mission Data Repository

NSA's Utah Datacenter



NIST PQC Competition

CRYSTALS-KYBER

FrodoKEM

LAC

NewHope

NTRU

NTRU Prime

Round5

SABER

Three Bears

BIKE

Classic McEliece

HQC

LEDACrypt

NTS-KEM


ROLLO

RQC

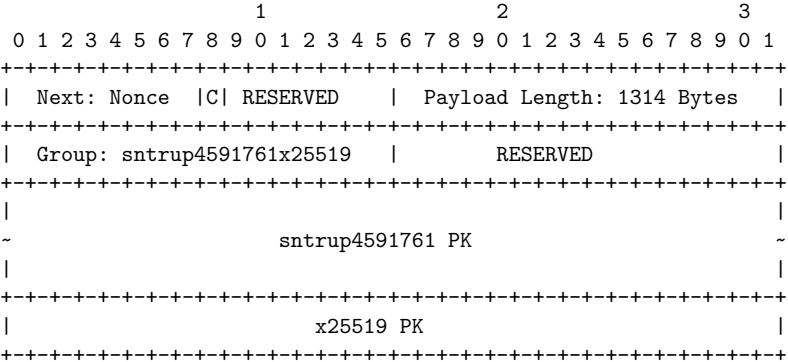
SIKE

 Lattice

 Code

 Isogeny

Combined KE: An Example



PQC IKEv2: IPv6 MTU

CRYSTALS-KYBER

FrodoKEM

LAC

NewHope

NTRU

NTRU Prime

Round5

SABER

Three Bears

BIKE

Classic McEliece

HQC

LEDACrypt

NTS-KEM


ROLLO

RQC

SIKE

 Lattice

 Code

 Isogeny

PQC IKEv2: IPv4 MTU

CRYSTALS-KYBER

FrodoKEM

LAC

NewHope

NTRU

NTRU Prime

Round5

SABER

Three Bears

BIKE

Classic McEliece

HQC

LEDACrypt

NTS-KEM

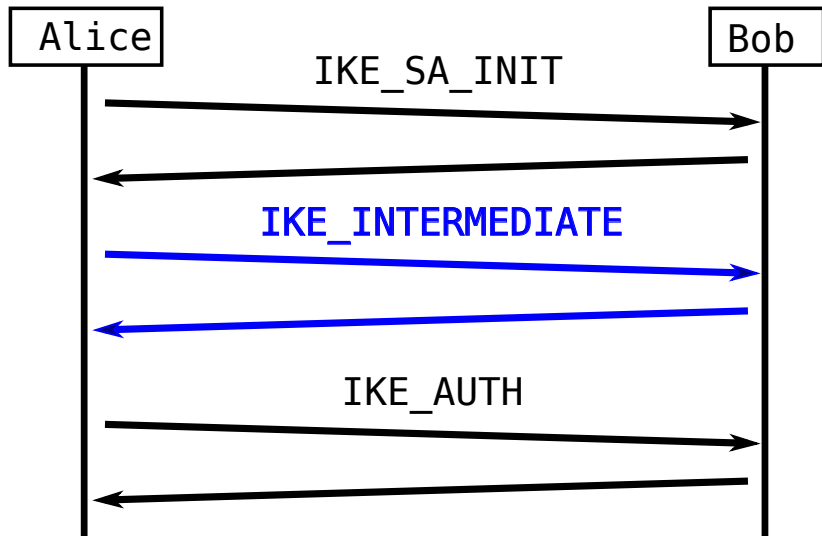
ROLLO

RQC

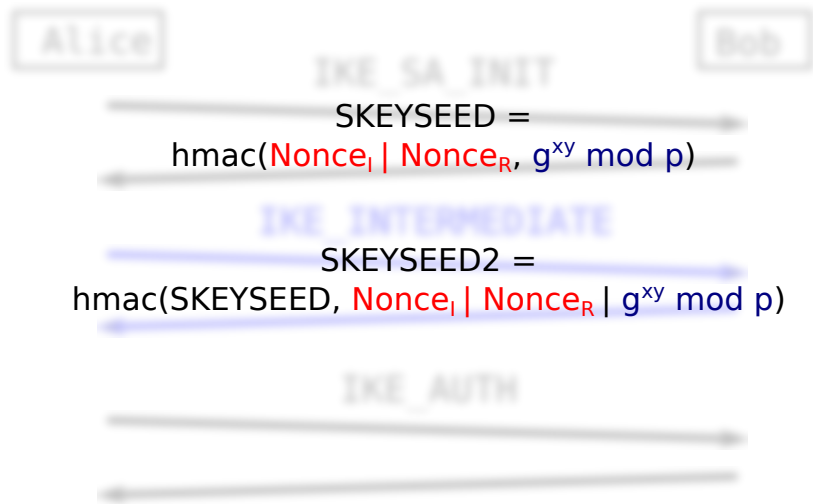
SIKE

-  Lattice
-  Code
-  Isogeny

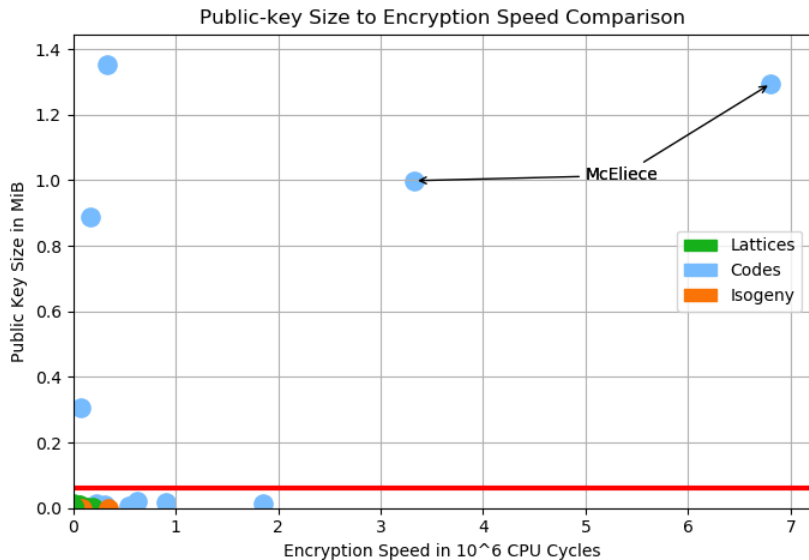
Quantum-Resistant IKEv2



Quantum-Resistant IKEv2



Hybrid PQKE: Unresolved problems



Ongoing work

- Implementations
- Expert Review
- Formal Verification
- NIST Standardization Process

Resources

IETF draft: [draft-tjhai-ipsecme-hybrid-qske-ikev2](#)
Implementation: github.com/tobhe/iked
Plots: github.com/tobhe/pqplot