

Going quantum-resistant: preparing IKEv2 for the quantum era

Tobias Heider, Stefan-Lukas Gazdag

genua

Shor's Algorithm

The end of hidden-subgroup cryptography

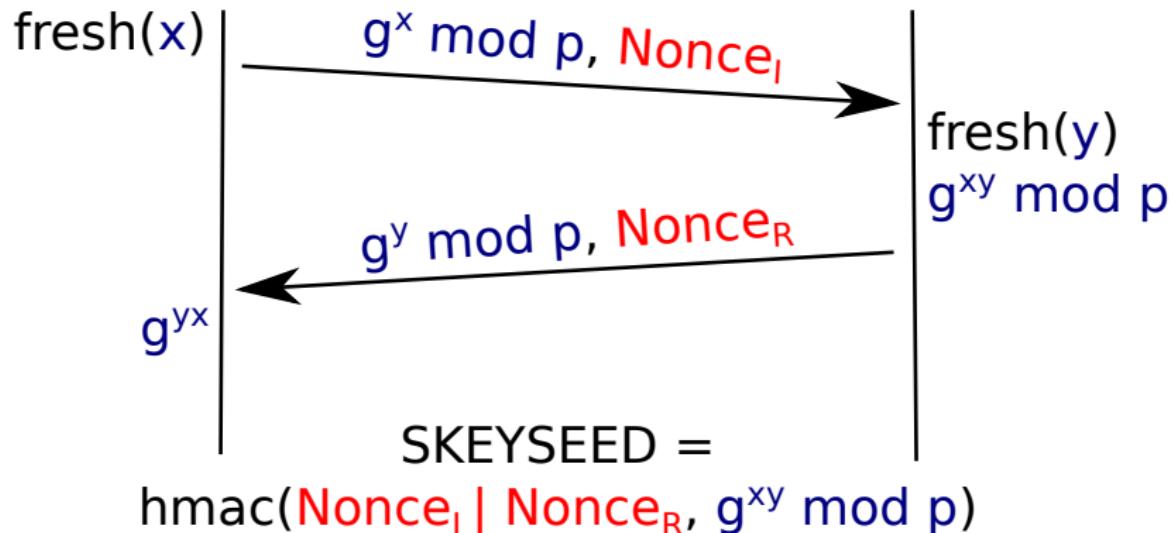
Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

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

1	2	3
0 1 2 3 4 5 6 7 8 9 0	1 2 3 4 5 6 7 8 9 0	1 2 3 4 5 6 7 8 9 0 1
+++++ Next: Nonce C RESERVED Payload Length: 1314 Bytes +++++		
Group: snstrup4591761x25519 RESERVED +++++		
~ snstrup4591761 PK ~ 		
+++++ x25519 PK +++++		

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

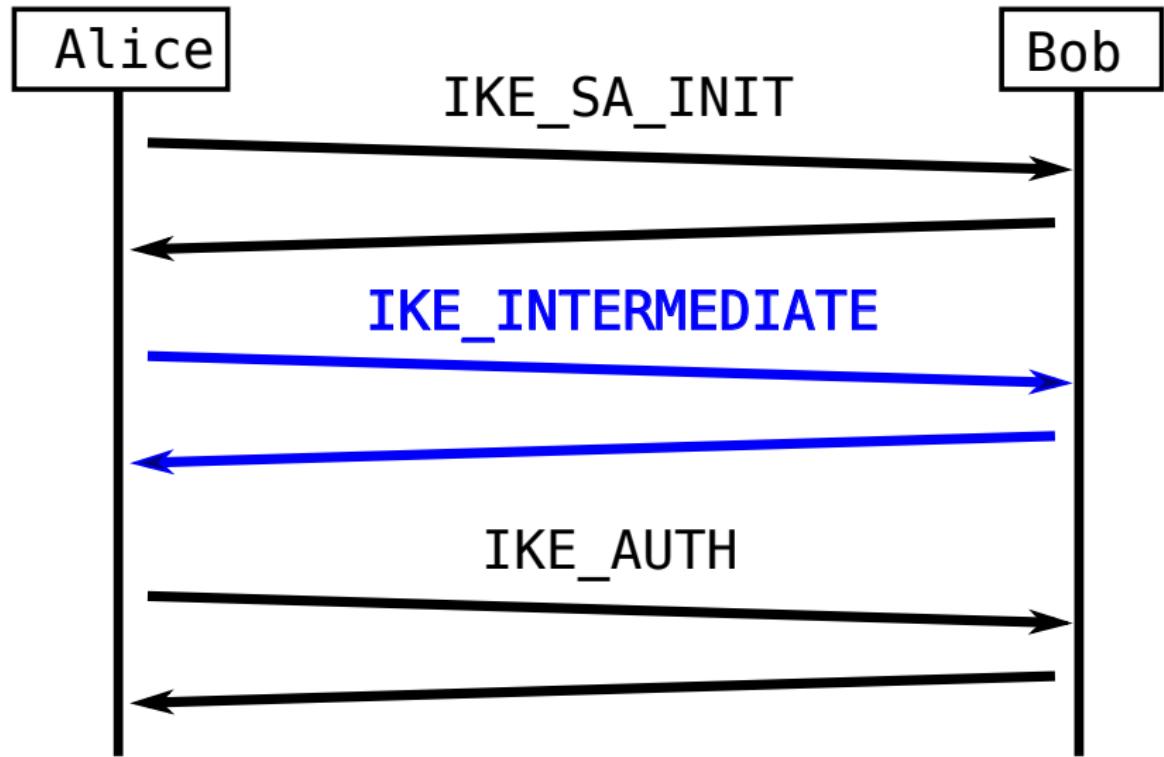


Code



Isogeny

Quantum-Resistant IKEv2



Quantum-Resistant IKEv2

ALICE

Bob

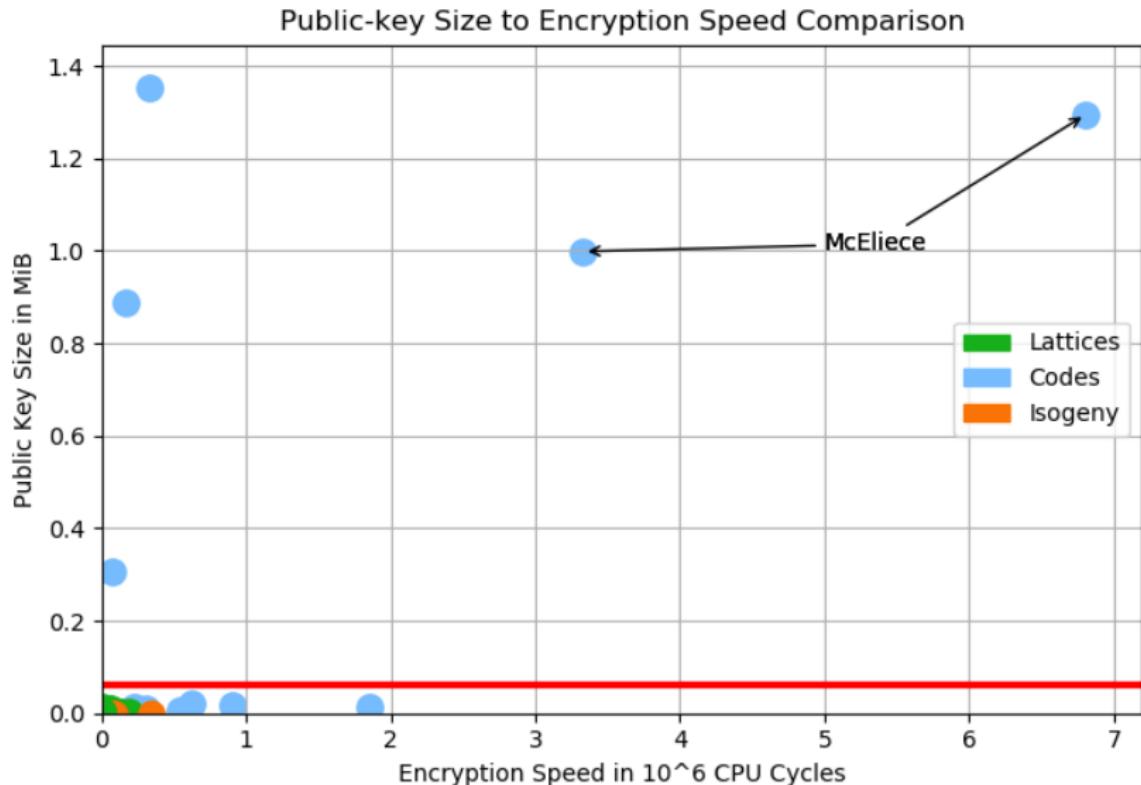
SKEYSEED =

hmac($\text{Nonce}_L \mid \text{Nonce}_R, g^{xy} \bmod p$)

SKEYSEED2 =

hmac(SKEYSEED, $\text{Nonce}_L \mid \text{Nonce}_R \mid g^{xy} \bmod p$)

Hybrid PQKE: Unresolved problems



Ongoing work

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

Resources

IETF draft: [draft-tjhai-ipsecme-hybrid-qske-ikev2](https://datatracker.ietf.org/doc/draft-tjhai-ipsecme-hybrid-qske-ikev2)
Implementation: github.com/tobhe/iked
Plots: github.com/tobhe/pqplot