Going quantum-resistant: preparing IKEv2 for the quantum era

Tobias Heider
tobias_heider@genua.de

genua GmbH

genua
A Bundesdruckerei Company

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.

The State of Quantum Computing

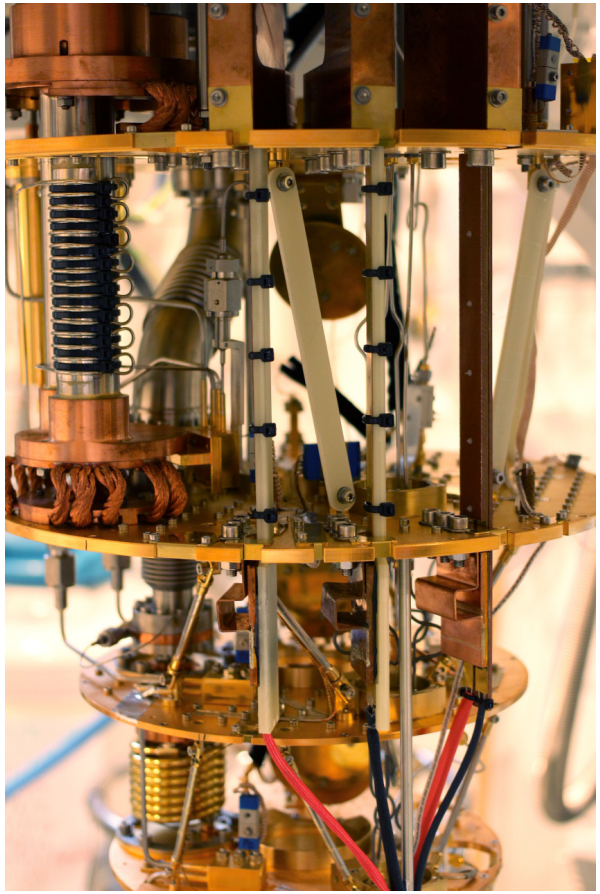


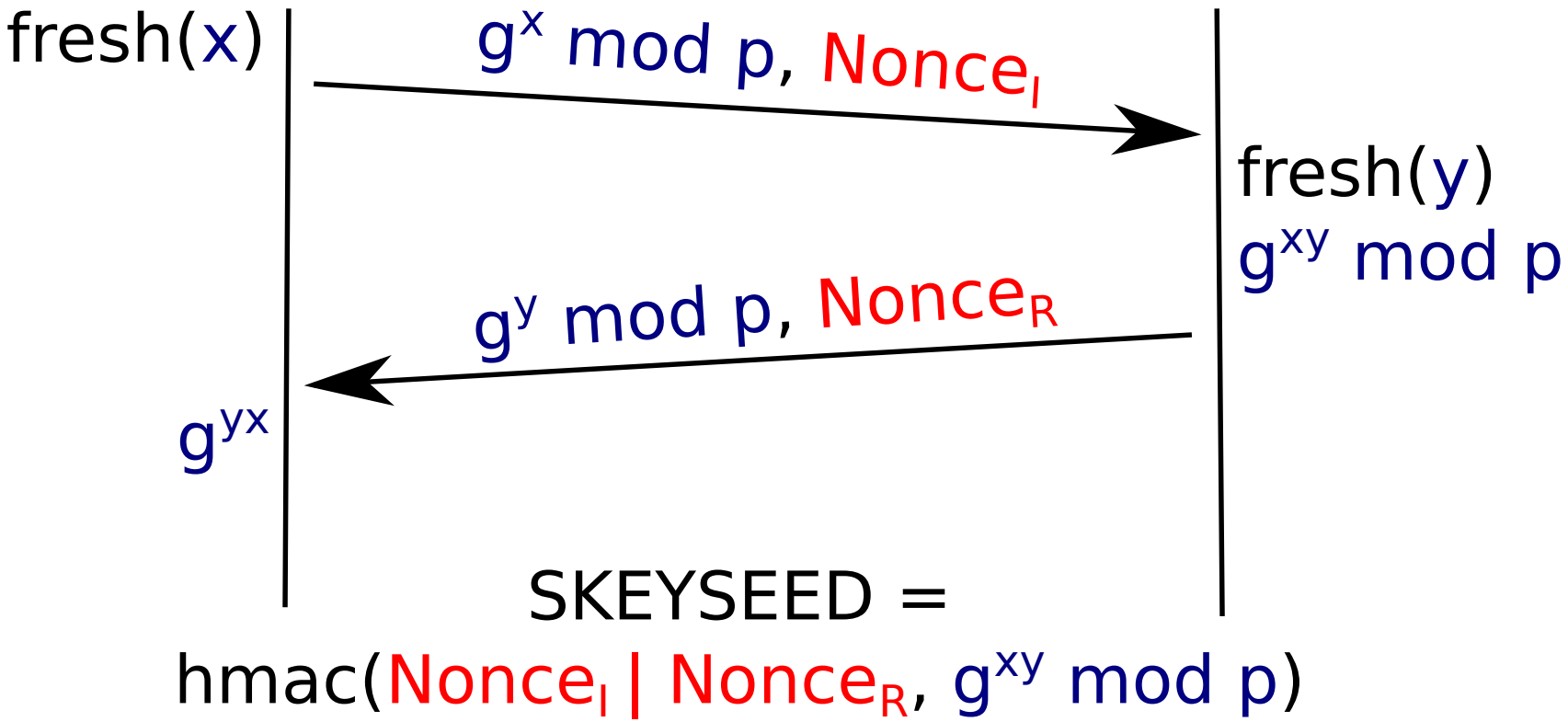
Figure: `https://commons.wikimedia.org/wiki/File:Quantum_refrigerator_at_UCL_(17626619658).jpg`

~~Massive~~ Mission Data Repository

NSA's Utah Datacenter

Figure: `https://www.eff.org/deeplinks/2014/07/releasing-public-domain-image-nsas-utah-data-center`

IKE SA INIT


fresh(x)
$g^x \bmod p$, $Nonce_I$
fresh(y)
$g^{xy} \bmod p$
$g^y \bmod p$, $Nonce_R$
g^{yx}
SKEYSEED =
hmac($Nonce_I$ | $Nonce_R$, $g^{xy} \bmod p$)

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

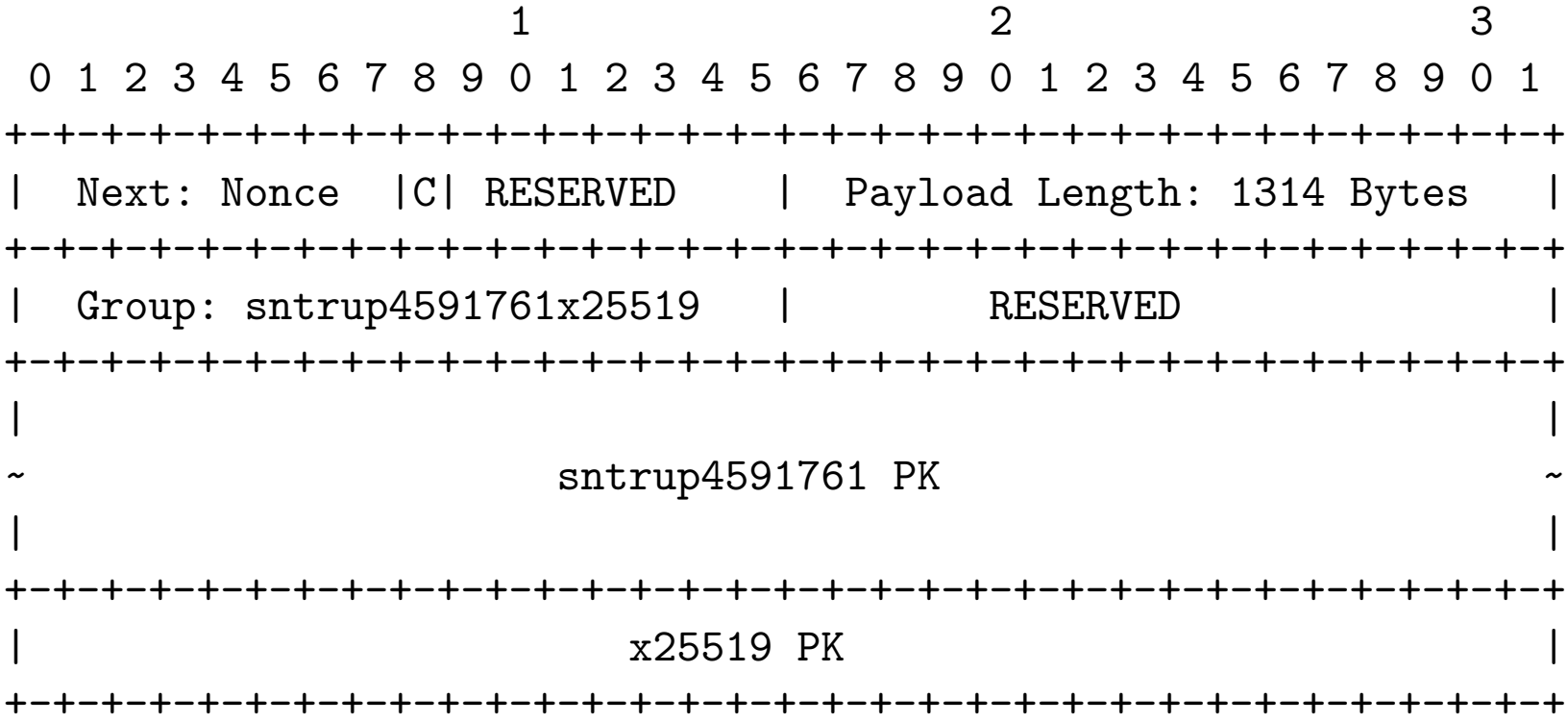
Lattice
Code
Isogeny

Combined KE: A trivial solution

$$g^x = g_{PQ}{}^x \bmod q \mid g^x \bmod p$$

$$g^{xy} = \text{hash}(g_{PQ}{}^{xy} \bmod q \mid g^{xy} \bmod p)$$

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: 500 Byte MTU

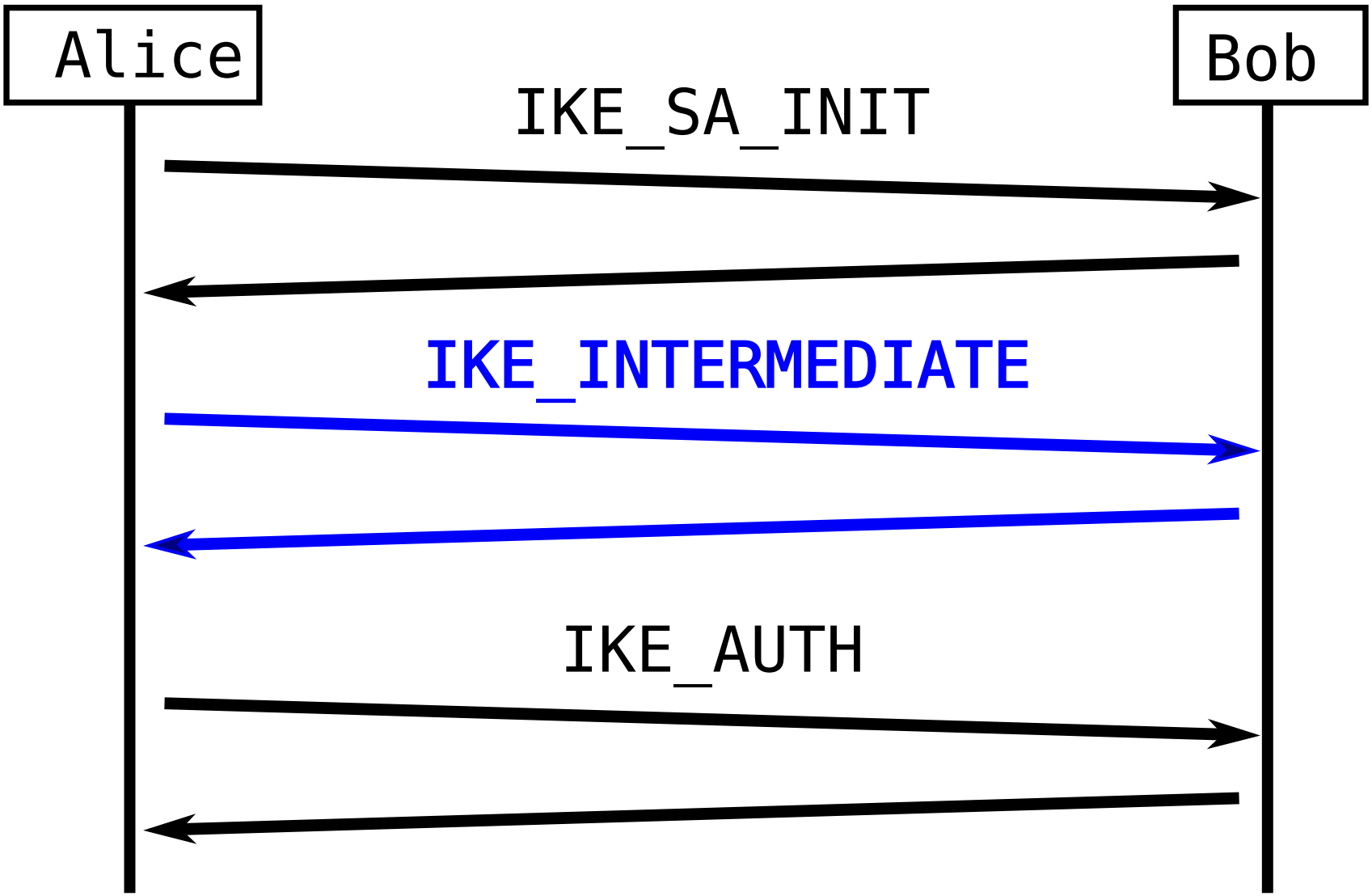
CRYSTALS-KYBER
FrodoKEM
LAC
NewHope
NTRU
NTRU Prime
Round5
SABER
Three Bears

BIKE
Classic McEliece
HQC
LEDAcrypt
NTS-KEM
ROLLO
RQC

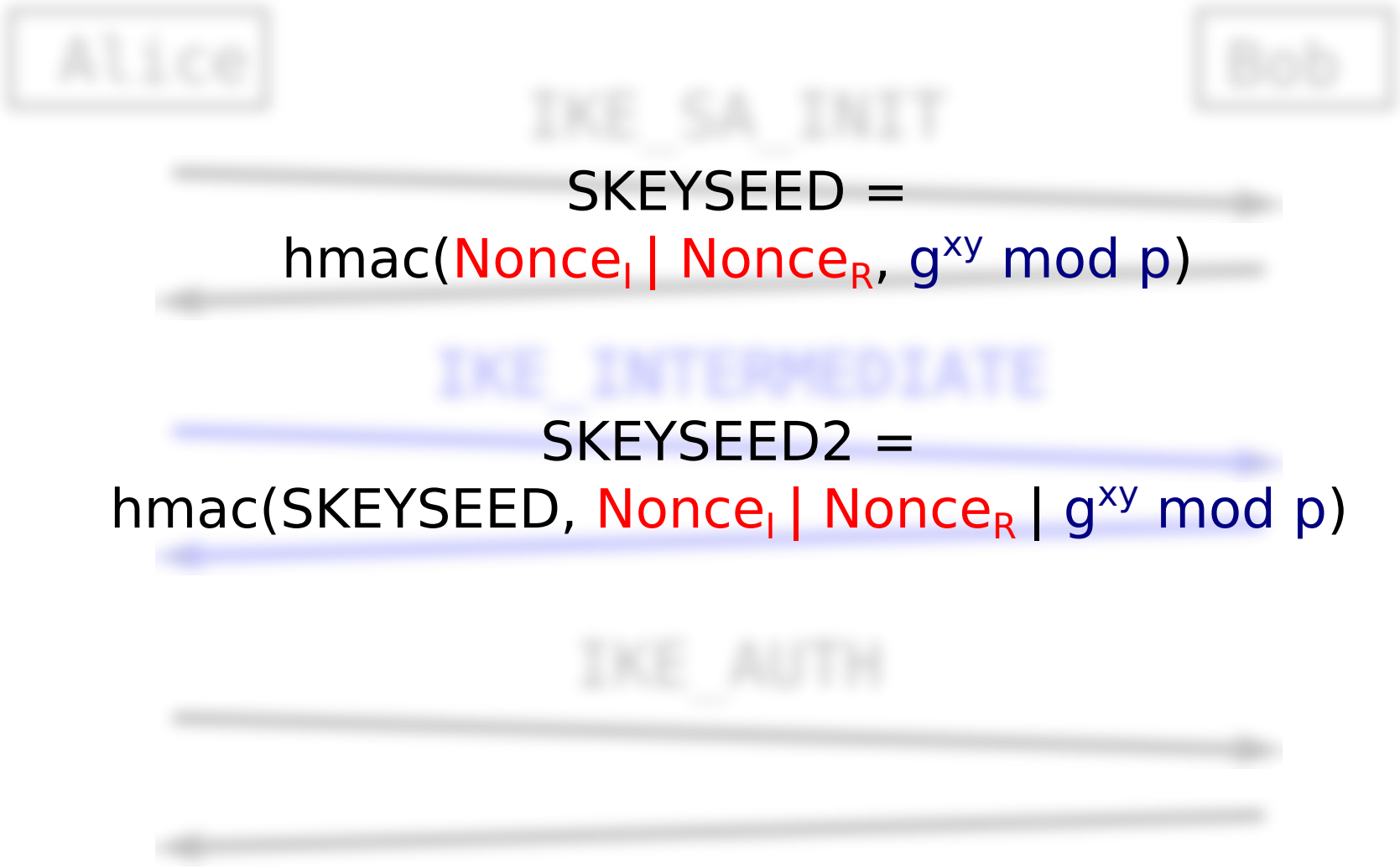
SIKE

Lattice
Code
Isogeny

Quantum-Resistant IKEv2



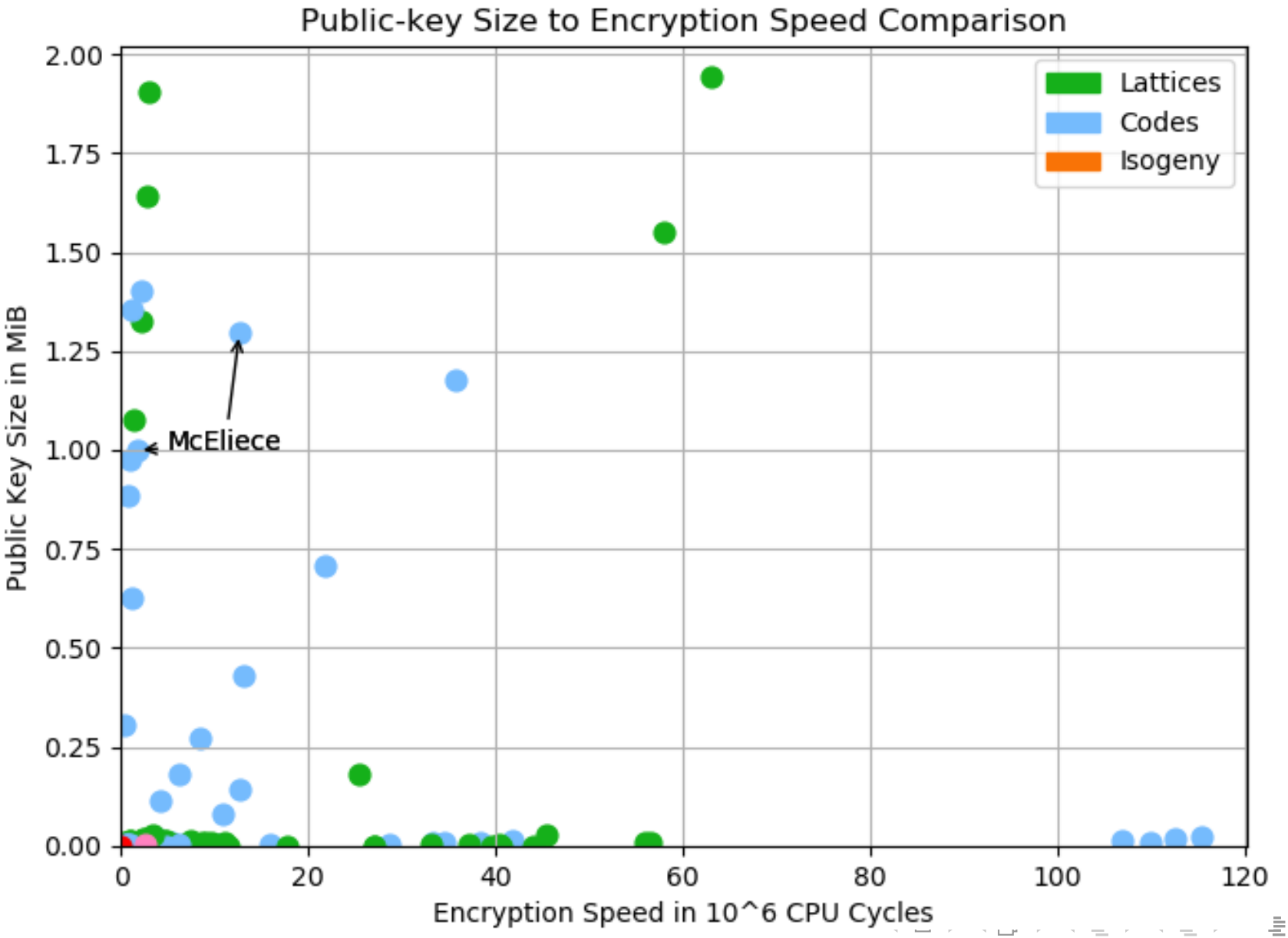
Quantum-Resistant IKEv2



$$SKEYSEED = hmac(Nonce_I \mid Nonce_R, g^{xy} \bmod p)$$

$$SKEYSEED2 = hmac(SKEYSEED, Nonce_I \mid Nonce_R \mid g^{xy} \bmod p)$$

Hybrid PQKE: Unresolved problems



Ongoing work

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

Resources

IETF draft:
draft-tjhai-ipsecme-hybrid-qske-ikev2

Reference Implementation (for OpenBSD):
`https://github.com/tobhe/openbsd-src/tree/PQKE_IKED`

Plots:
`https://github.com/tobhe/pq-plot`