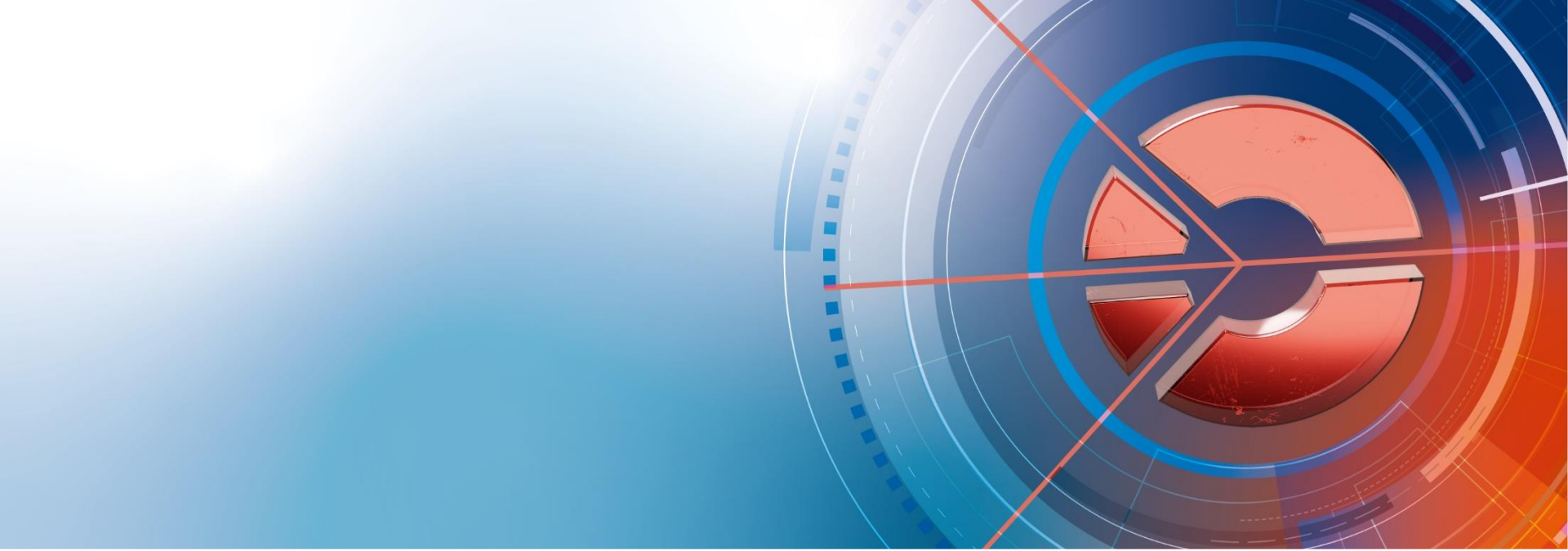


Post-quantum Cryptography and Standardization Efforts

Helmut Grießer, ADVA Optical Networking

Symposium on Quantum Communications, ECOC, Basel, Sept. 21st 2022

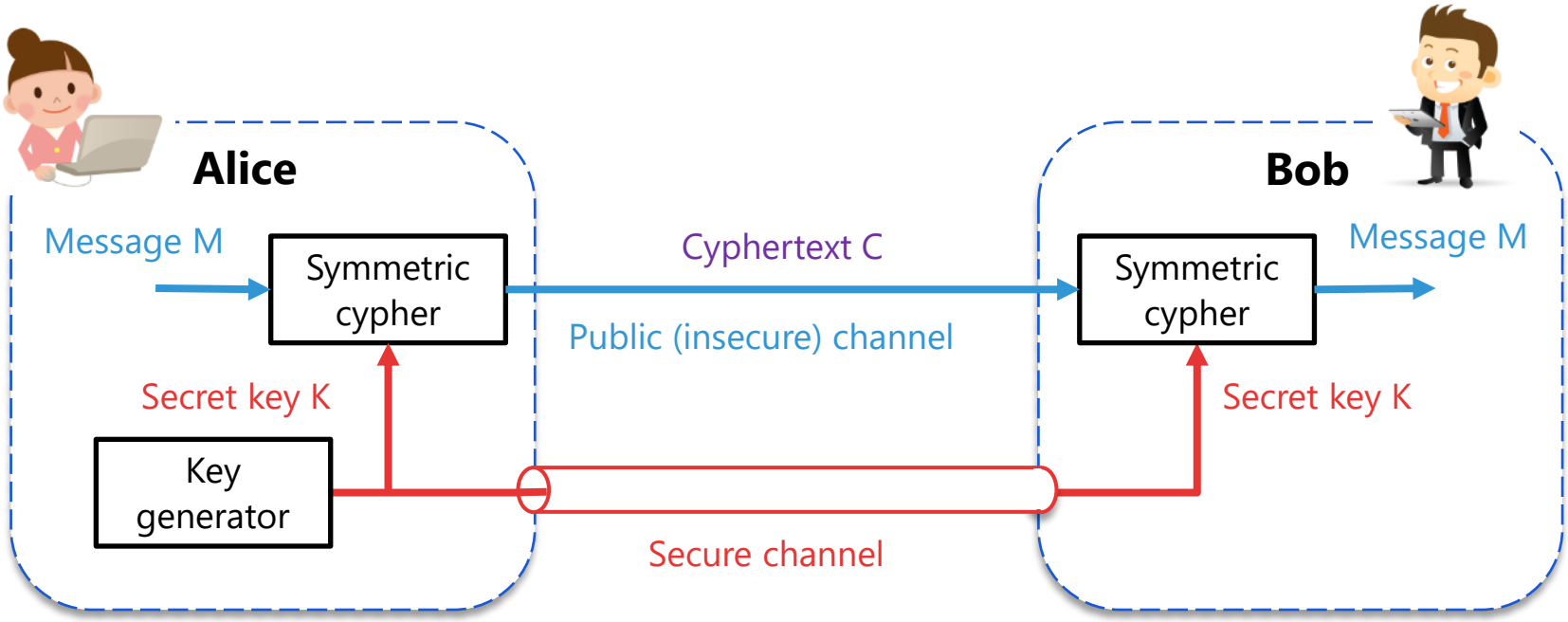
OPEN QKD

ADVA

What is Post-quantum Cryptography?
(… and what not)

- **NOT** a successor of quantum cryptography
- classical (modern) cryptography,
  assuming attacks with classical and **quantum algorithms**
- computational security

Confidentiality: Symmetric Cryptography

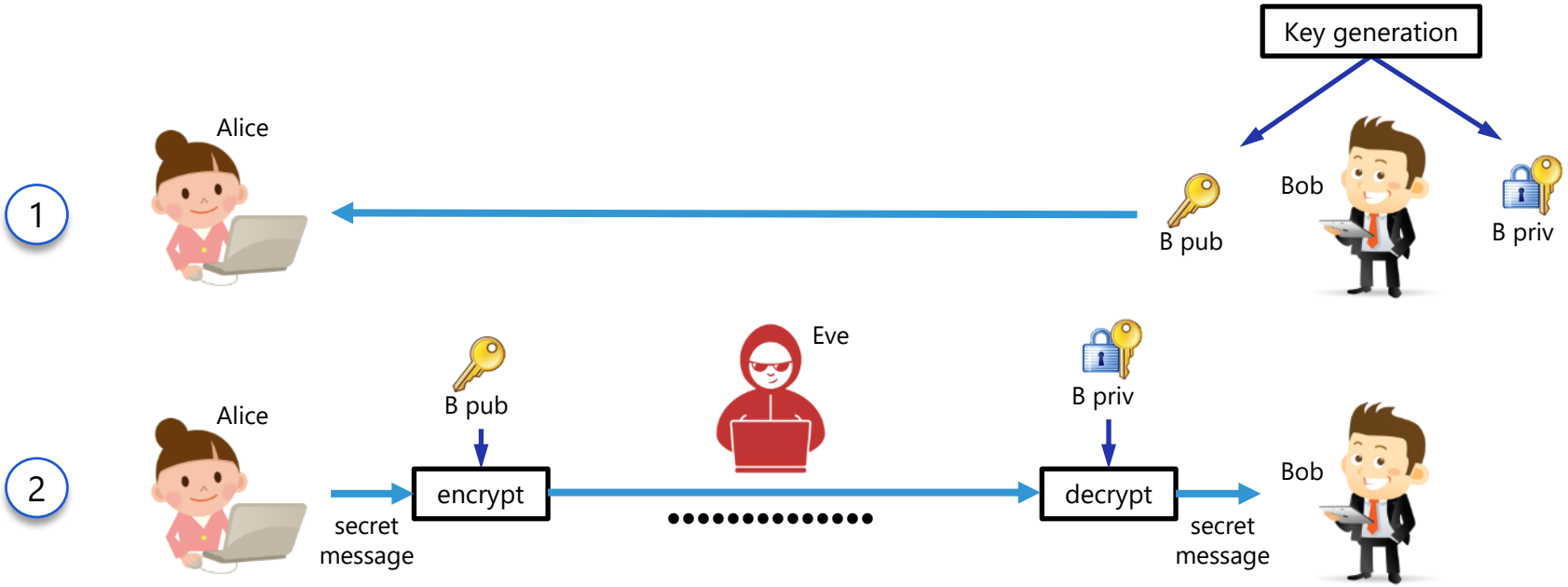


Problem: No secure channel, key exchange over a public channel

Public-key cryptography: allows to exchange *secure* key over *insecure* channel

Public key cryptography (e.g. RSA)

One-way (or trap door) function based on prime factors.



RSA

Trap door is based on two large primes: Multiplication is easy, factorizing the product not

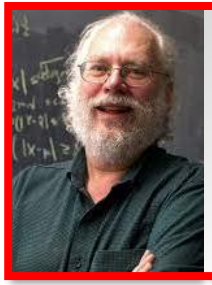
Calculating the private key from the public one would require the factorization

Cryptographic protocols …

… and some relevant quantum algorithms

Public key cryptography

Application: key exchange, signature, PKI



Shor's algorithm:

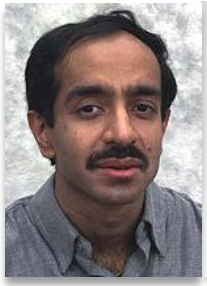
Polynomial solution of

- Integer factoring (RSA)
- Discrete logarithm (DH)
- Elliptic curve discrete logarithm (ECDH)

?

Symmetric cryptography

Application: encryption



Grover's algorithm

Quadratic speed up of brute-force search

- Reduces effective key length of AES by a factor of two

Simon's algorithm

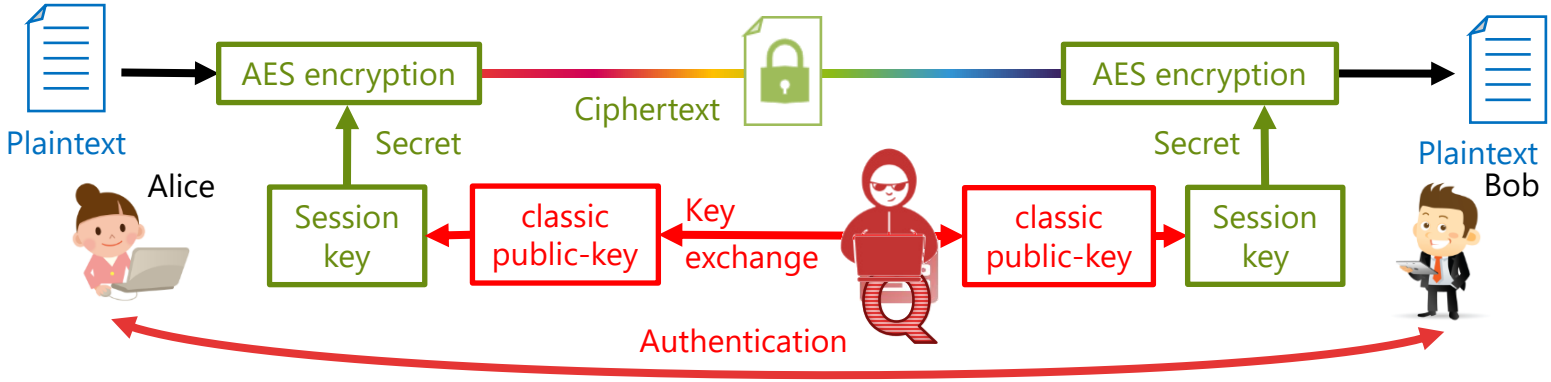
Linear solution of Simon's problem

- Find s such that f(x)=f(x+s)
- exp-2.5 speedup of some symmetric structures

Shor [1]: Why haven't more quantum algorithms been found?

[1] P. W. Shor, "Why haven't more quantum algorithms been found?," *Journal of the ACM (JACM)*, vol. 50, no. 1, Art. no. 1, 2003.

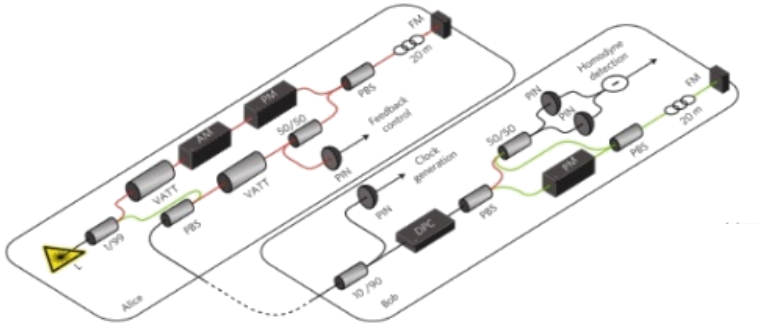
Quantum-safe high-speed encryption

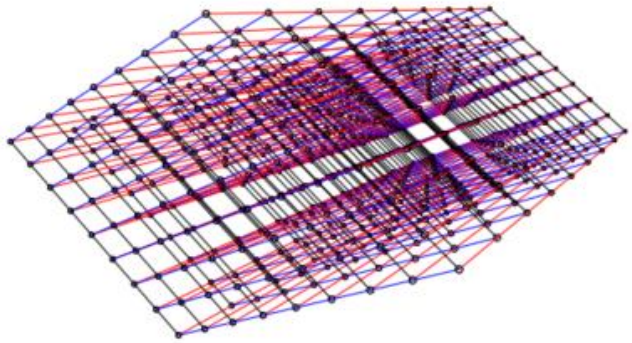


- Large and reliable quantum computers do not exist yet
- Harvesting attack on key exchange: store now, decrypt later
- Risk for data that needs to be secure for a long time

Action needed for key exchange – authentication, signatures less urgent

Quantum Key Distribution vs Post-Quantum Cryptography





Quantum Key Distribution (QKD)

- Provides information-theoretic security
- Needs optical channel (fiber or space)
- Needs access to the phys. Infrastructure
- Depends on optical link performance

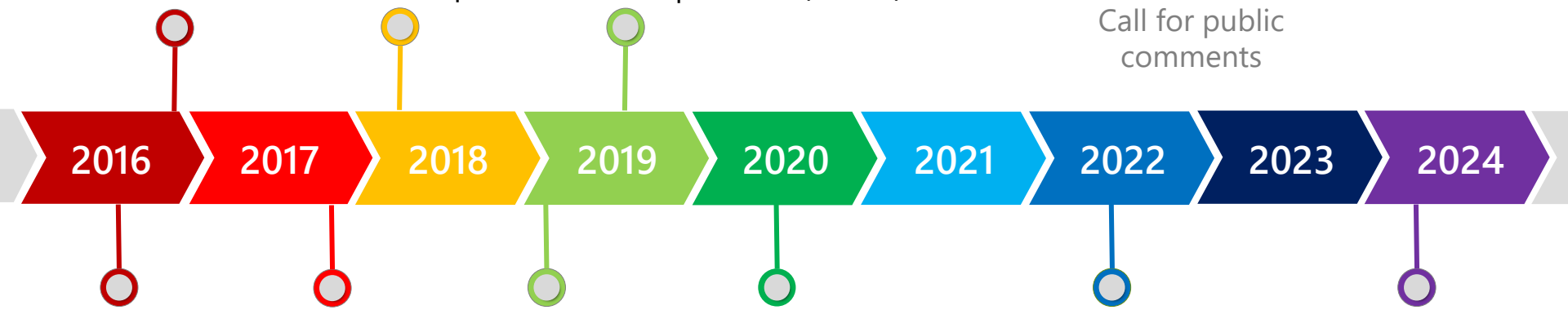
Post-Quantum Cryptography (PQC)

- Provides computational security
- Based on hardened of math problems
- Independent of communication channel
- Requires endpoint protocol access only

Complementary techniques – PQC (Standard) & QKD (Add-on)

NIST Post-quantum Cryptography Project

NIST National Institute of Standards and Technology



Dec 2016
Final requirements and criteria

April 2018
1st NIST PQC workshop

Aug 2019
2nd NIST PQC workshop

2020-2021
Round 3 seminars (virtual)

2022-2023
Release draft standards
Call for public comments

Aug 2016
Draft submission requirements & evaluation criteria

Nov 2017
DL for submissions

Jan 2019
2nd round started

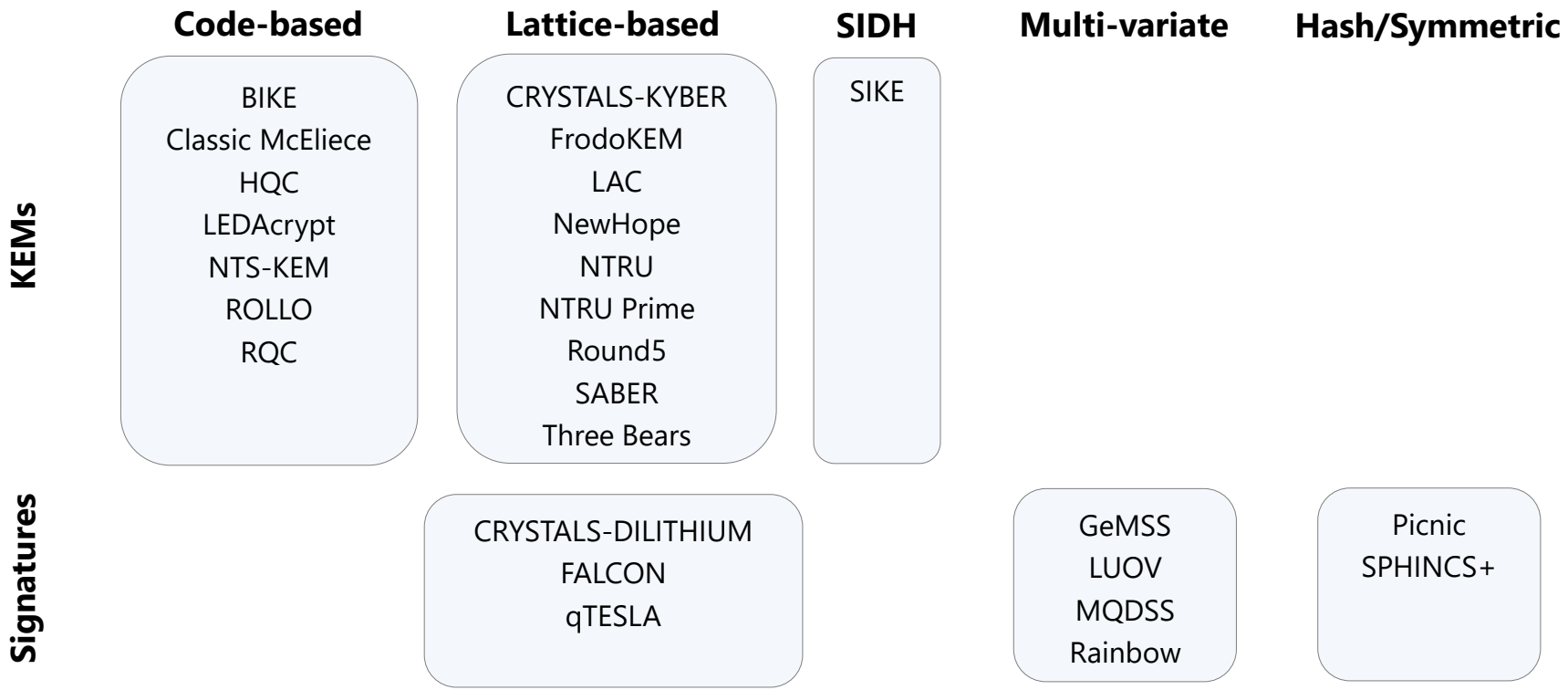
July 2020
Selected finalists and alternate candidates

July 2022
Announced finalists to be standardized and candidates for 4th round

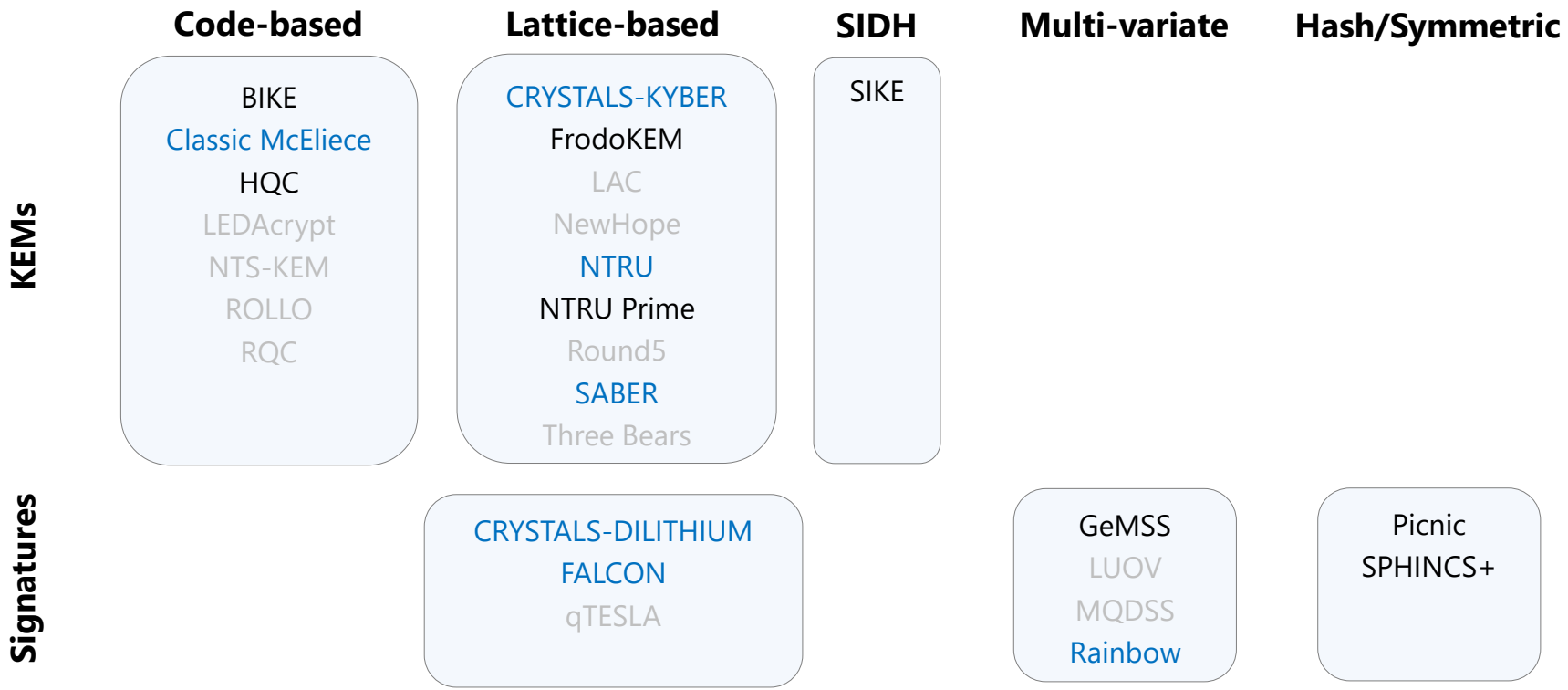
~2024
Final standards ready

ADVA

Second Round Candidates: 17 (KEM) + 9 (Signature)



Third Round Finalists and Alternate Candidates



Classical Attack on Alternate Signature Candidates

Breaking Rainbow Takes a Weekend on a Laptop

Ward Beullens

IBM Research, Zurich, Switzerland
wbe@zurich.ibm.com

Abstract. This work introduces new key recovery attacks against the Rainbow signature scheme, which is one of the three finalist signature schemes still in the NIST Post-Quantum Cryptography standardization project. The new attacks outperform previously known attacks for all the parameter sets submitted to NIST and make a key-recovery practical for the SL 1 parameters. Concretely, given a Rainbow public key for the SL 1 parameters of the second-round submission, our attack returns the corresponding secret key after on average 53 hours (one weekend) of computation time on a standard laptop.

Classical Attack on Alternate KEM Candidate

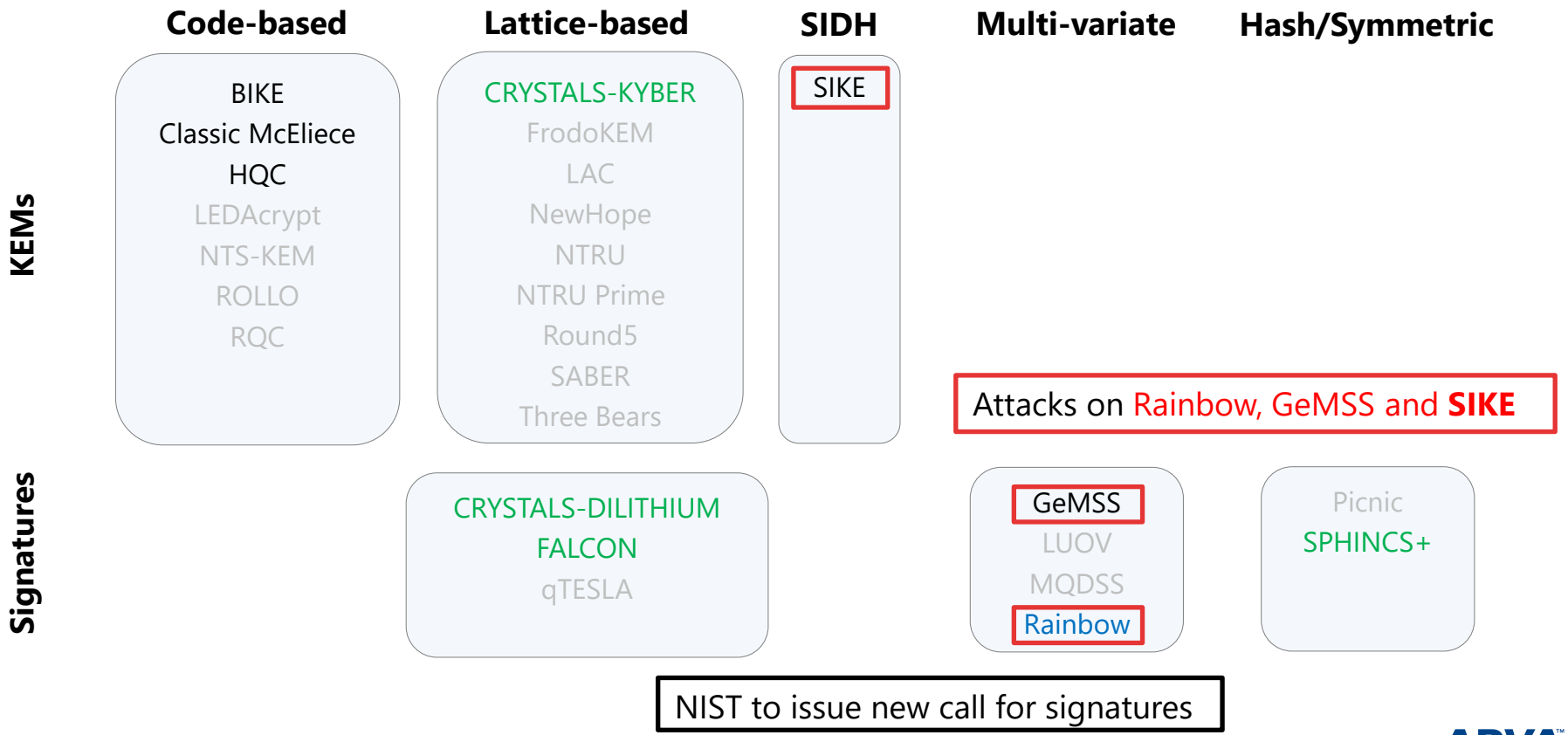
AN EFFICIENT KEY RECOVERY ATTACK ON SIDH
(PRELIMINARY VERSION)

WOUTER CASTRYCK AND THOMAS DECRU

imec-COSIC, KU Leuven

ABSTRACT. We present an efficient key recovery attack on the Supersingular Isogeny Diffie–Hellman protocol (SIDH), based on a "glue-and-split" theorem due to Kani. Our attack exploits the existence of a small non-scalar endomorphism on the starting curve, and it also relies on the auxiliary torsion point information that Alice and Bob share during the protocol. Our Magma implementation breaks the instantiation SIKEp434, which aims at security level 1 of the Post-Quantum Cryptography standardization process currently ran by NIST, in about one hour on a single core. This is a preliminary version of a longer article in preparation.

Algorithms to be standardized and Fourth Round Candidates



Post-Quantum Cryptography

- Classic public key algorithms will no longer be secure
  if large, useful quantum computers can be build
- PQC standardization is a long process not necessarily free of setbacks
- PQC will be an important building block for secure networks
- PQ key exchange can be supplemented by QKD
  for applications with increased security requirements
- Crypto agility is required (i.e. primitives and protocols can be updated)

Thank you

hgriesser@adva.com