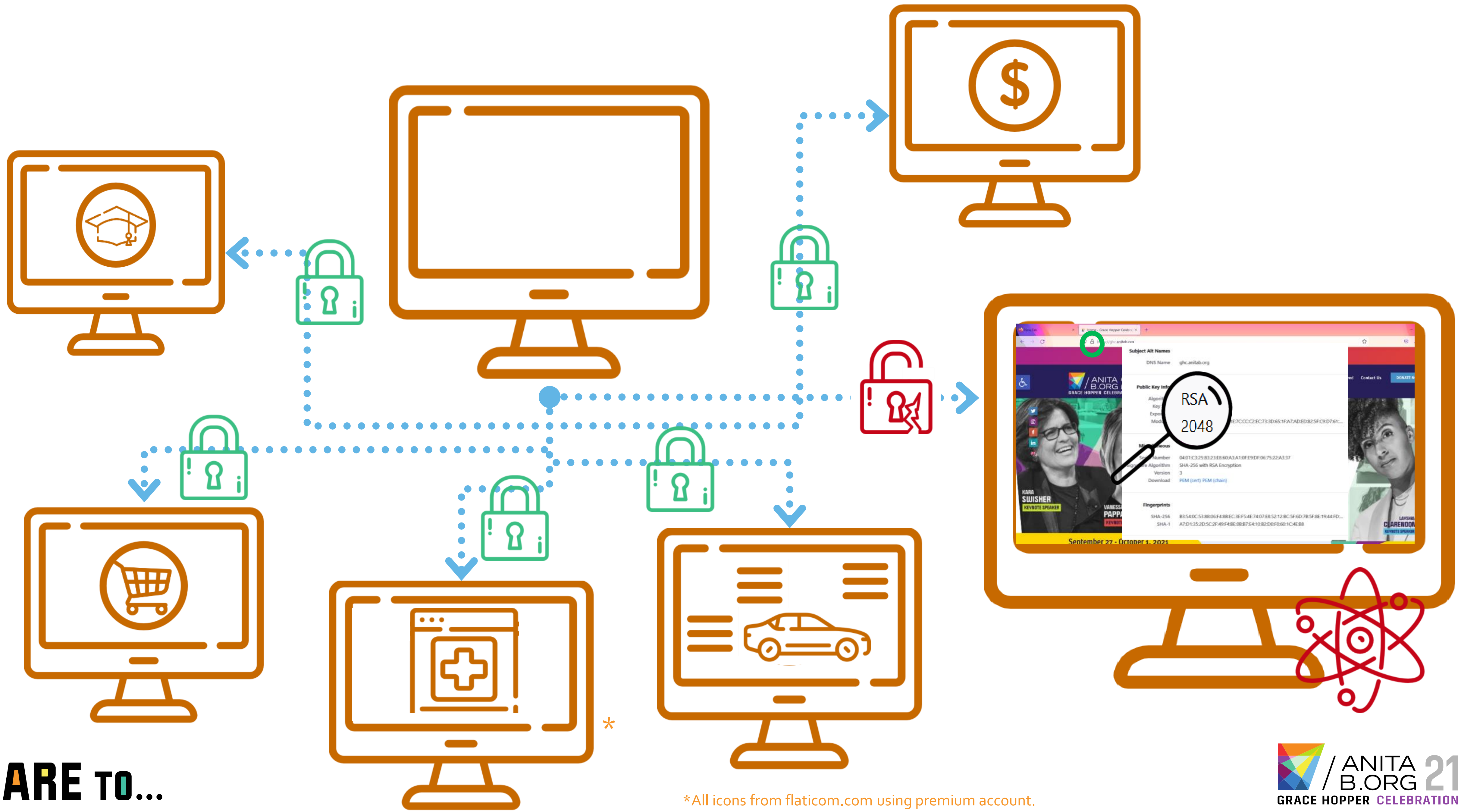
From Transparency to Security, or How to Prepare for the Quantum Threat

Nina Bindel
University of Waterloo and IQC, Canada
Kristen Csenkey
Balsillie School of International Affairs, Canada



*

DARE TO...

*All icons from flaticom.com using premium account.

ANITA B.ORG 21
GRACE HOPPER CELEBRATION

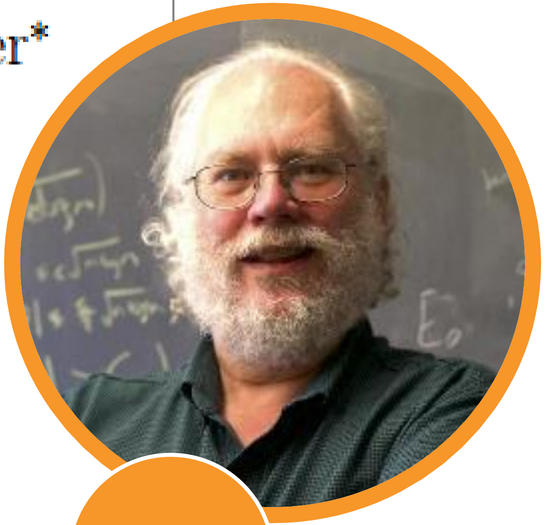
Shor's quantum algorithm

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

Peter W. Shor†

Abstract

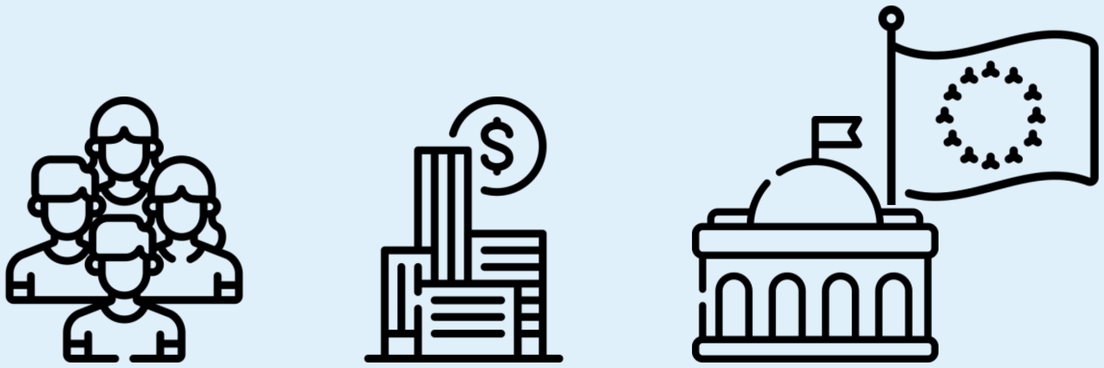
A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. 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.

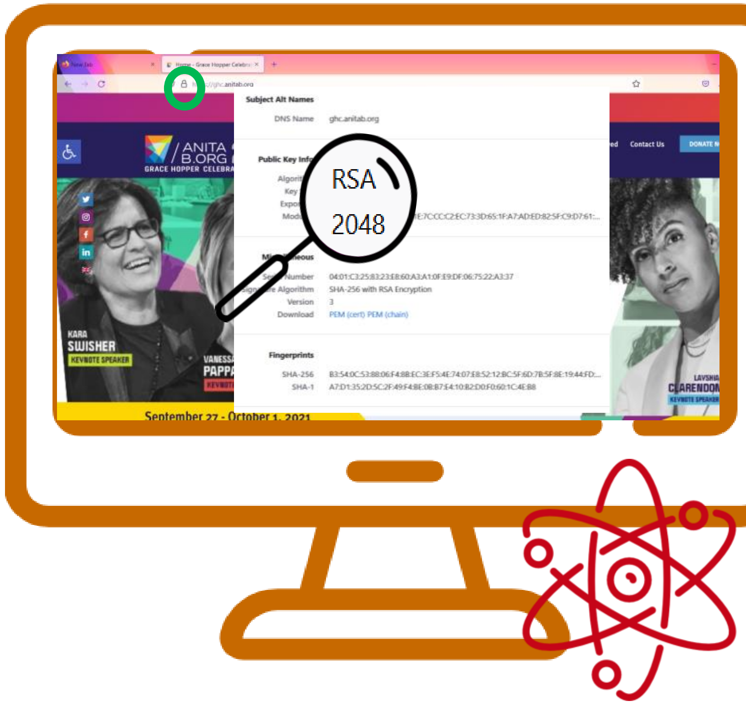


1997

Shor's quantum algorithm

- Recover secret key info
- Decrypt any RSA-🔒
- Threaten the health, safety, and economic well-being of ordinary people, corporations, and governments





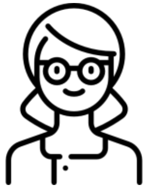
Outline

- Short Introduction to Cryptography
- State-of-the-Art Quantum Computer
- Perceptions of the Quantum Threat
- Overview of Sources & Strategies
- Standardization of Quantum-Resistant Cryptography
- So what? – Key Takeaways and Conclusion

Short Introduction to Cryptography

Symmetric and Asymmetric

Symmetric Crypto



Alice

Cipher text
LBDVY

Bob

5-13-15-3-20 =

= 5-13-15-3-20

Message
GOOSE

Encryption

Cipher text
LBDVY

Cipher text
LBDVY

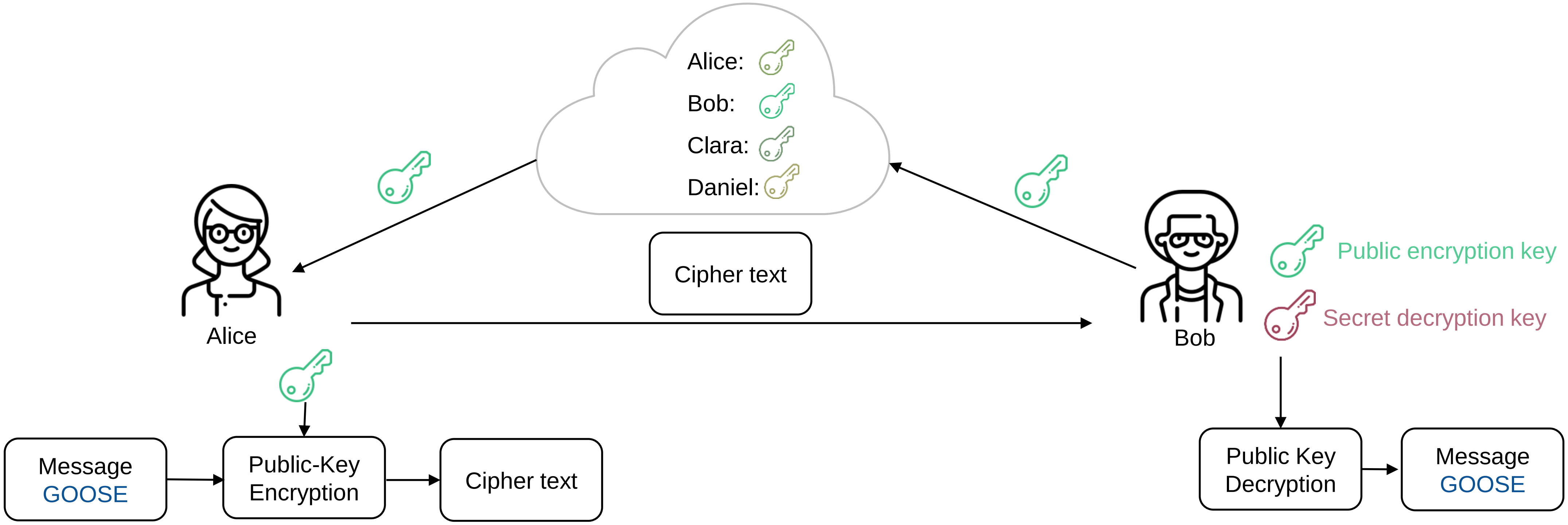
Decryption

Message
GOOSE

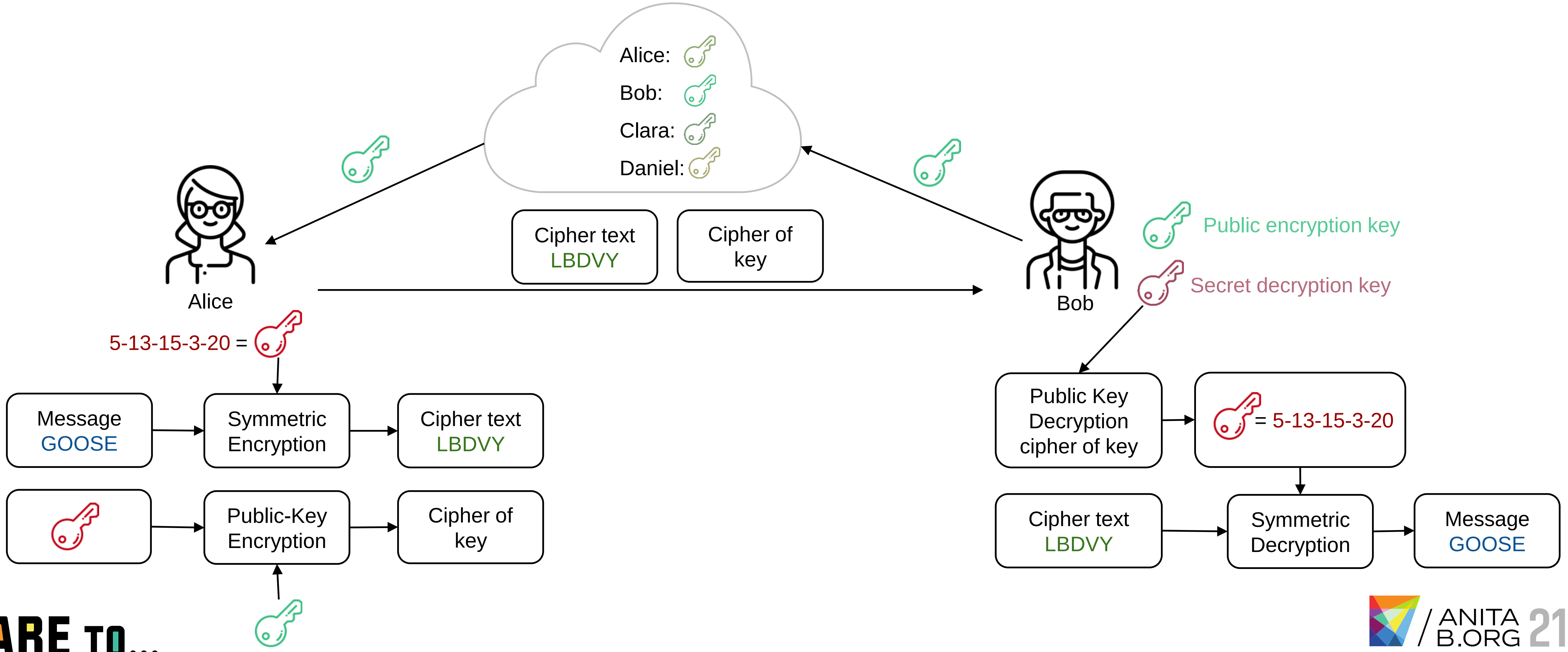
https://twitter.com/uwaterlooARTS/status/1337034359749005312?s=20

L	B	D	V	Y
5	13	15	3	20
G	O	O	S	E
4	23	12	7	11
H	E	R	O	N
9	10	3	8	20
C	R	A	N	E

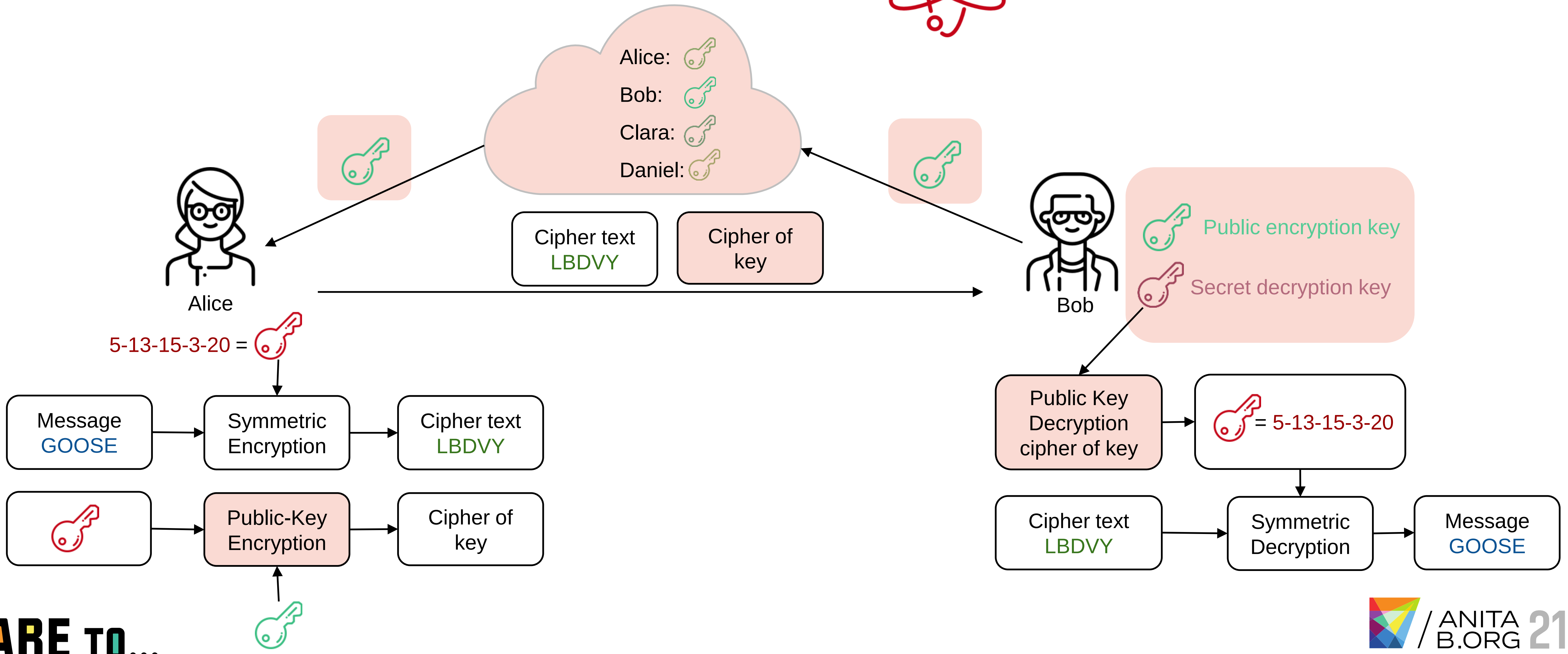
Asymmetric Crypto



Asymmetric and Symmetric Crypto in Practice



Asymmetric Crypto Broken by Quantum Computers



State-of-the-Art Quantum Computers

Jul. 2017 — 51 qubits, HARVARD UNIVERSITY

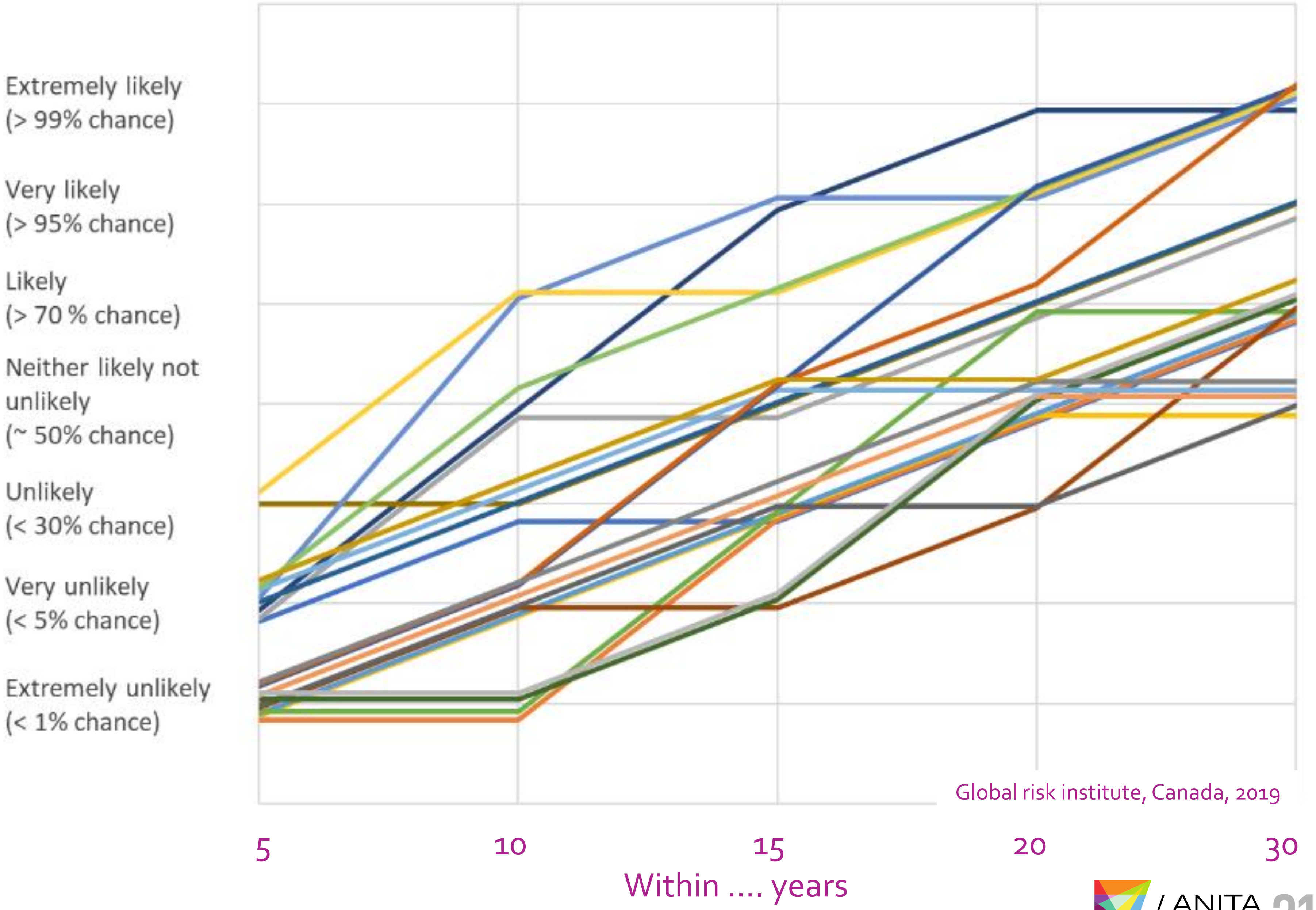
Feb. 2018 — 72 qubits, Google

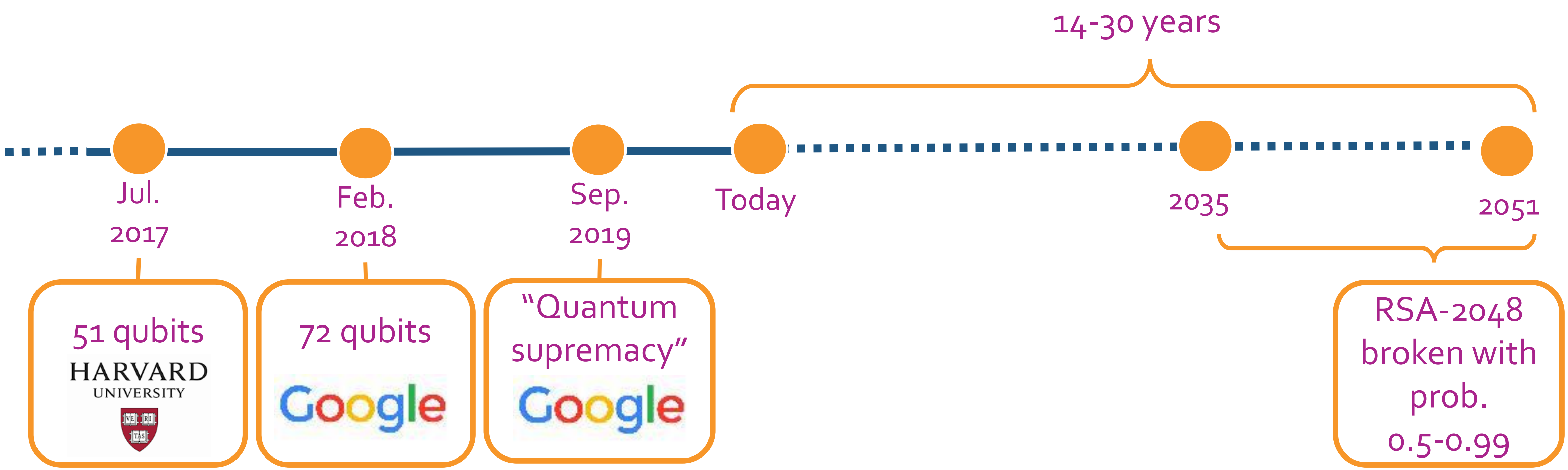
Sep. 2019 — "Quantum supremacy", Google

Today

20 million qubits
needed to break RSA-2048
[GK19]

Expert opinions about likelihood of a quantum computer able to break RSA-2048 in 24 hours

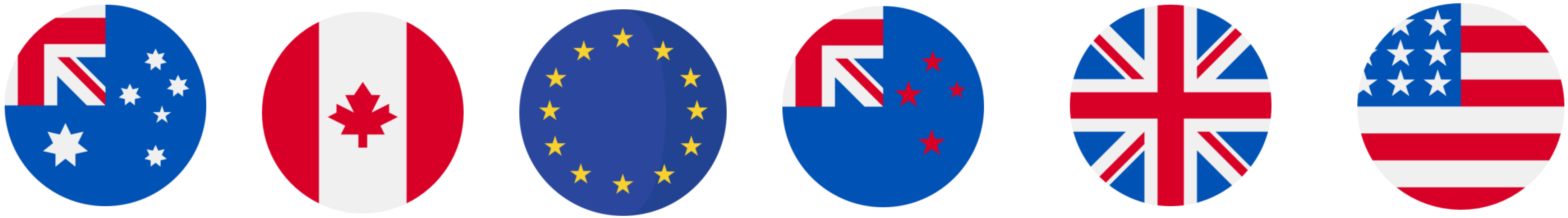



14-30 years
Jul. 2017
Feb. 2018
Sep. 2019
Today
2035
2051
51 qubits
HARVARD UNIVERSITY
72 qubits
Google
"Quantum supremacy"
Google
RSA-2048 broken with prob. 0.5-0.99

Historically, it has taken almost two decades to deploy our modern public key cryptography infrastructure. Therefore, regardless of whether we can estimate the exact time of the arrival of the quantum computing era, we must begin now to prepare our information security systems to be able to resist quantum computing.

US-American National Institute for Standards and Technology (NIST), 2017

Cooperating Allies

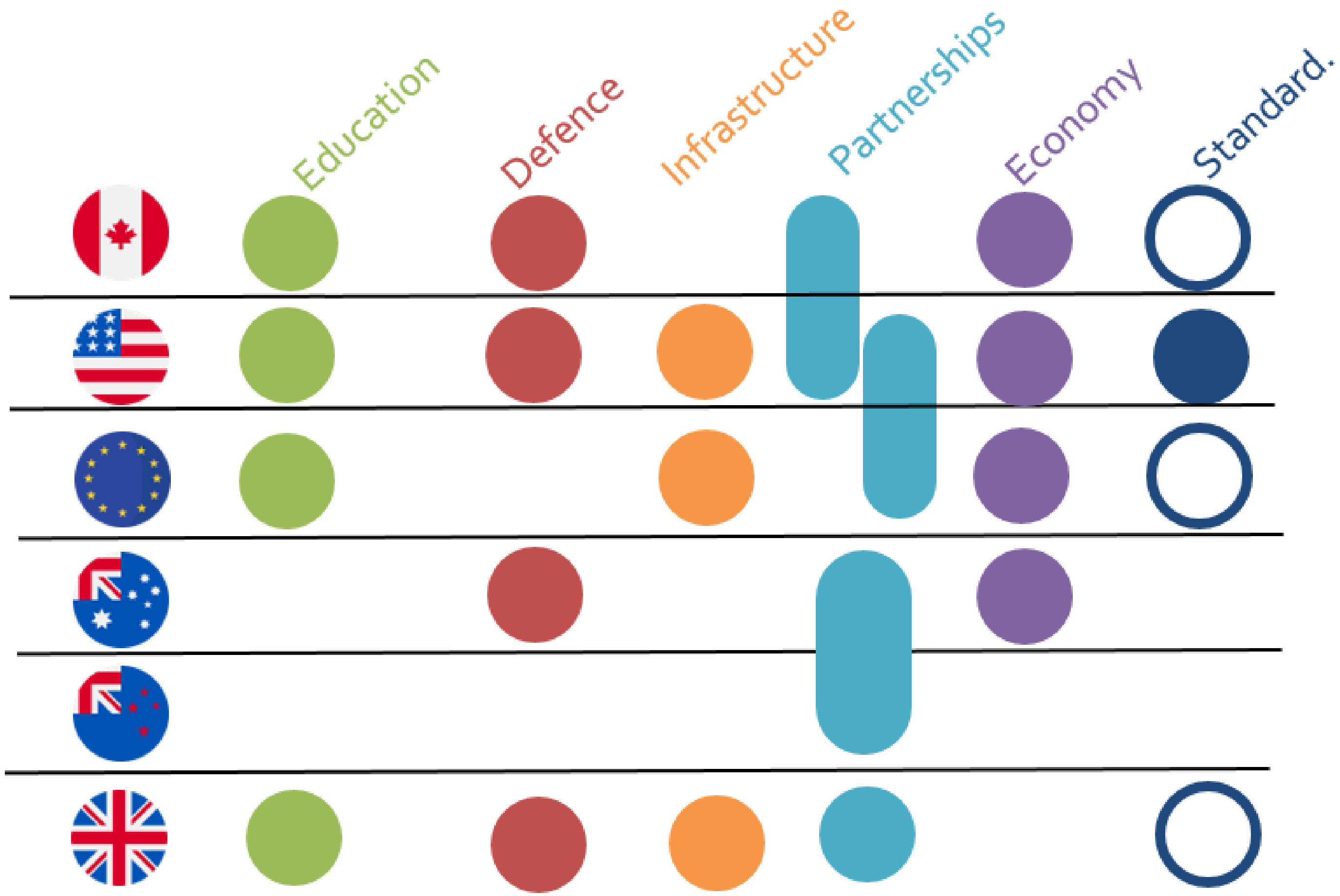


How to Address the Quantum Threat

Main Strategies to Prepare Against the Quantum Threat

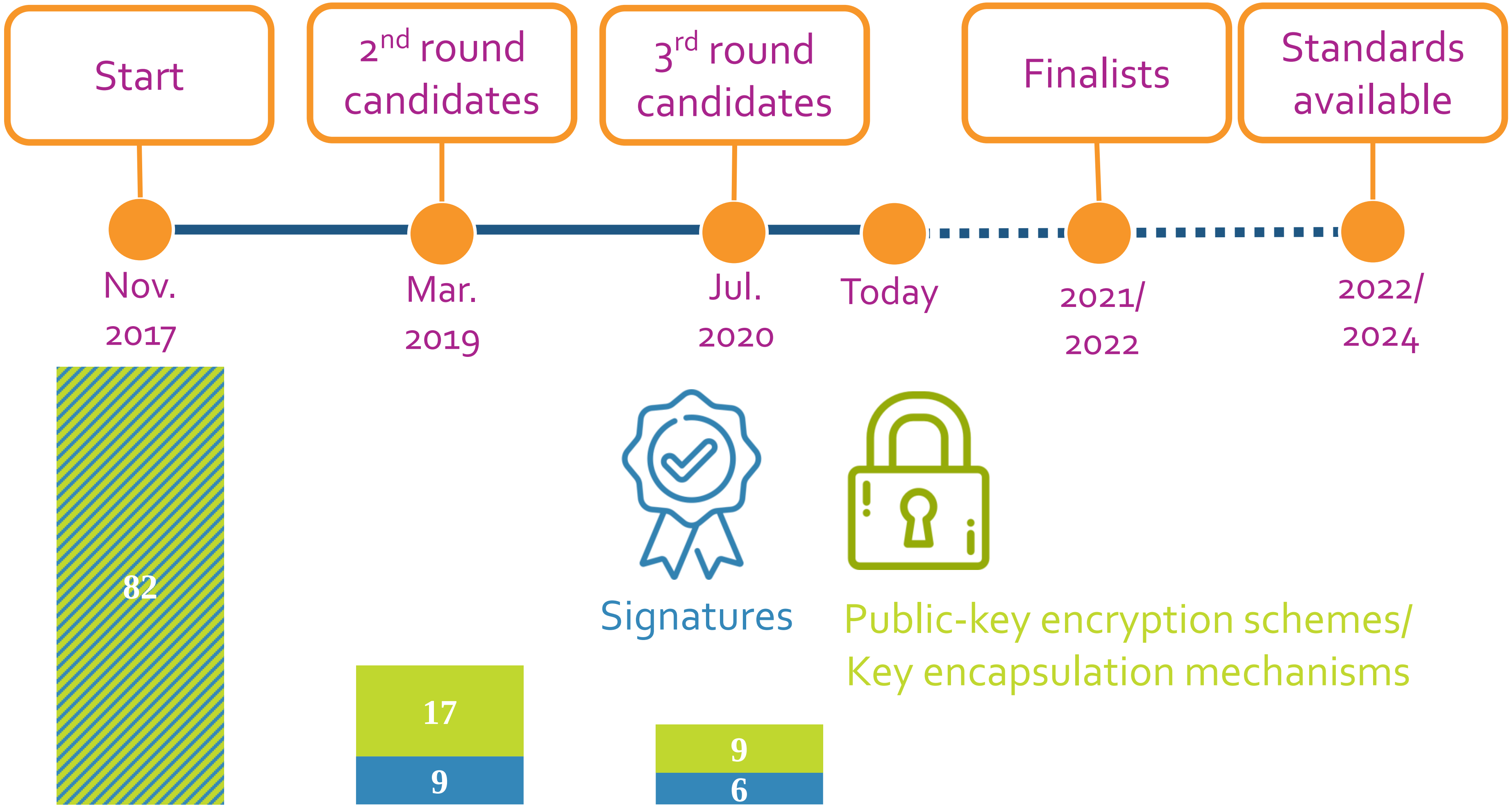
1. Economy
2. Education
3. Defence
4. Infrastructure
5. Partnerships
6. Standardization

Post-Quantum Strategies Matrix

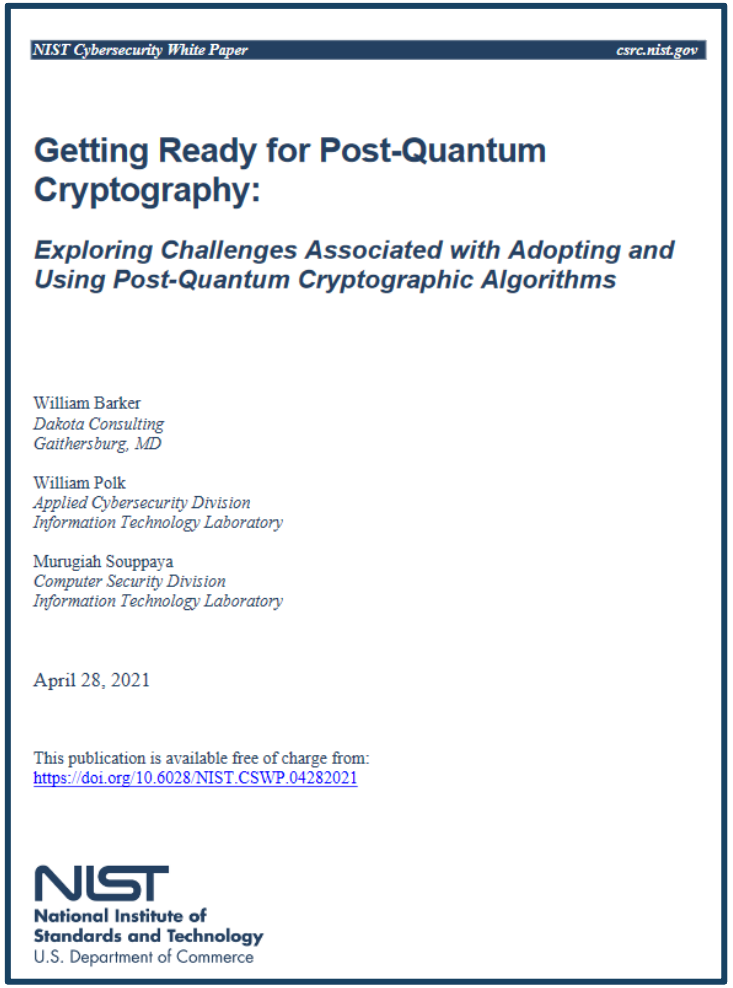


Standardization of Quantum-Resistant Cryptography

NIST post-quantum standardization



PQ Transition


NIST Cybersecurity White Paper csrc.nist.gov

Getting Ready for Post-Quantum Cryptography:

Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms

William Barker
Dakota Consulting
Gaithersburg, MD

William Polk
Applied Cybersecurity Division
Information Technology Laboratory

Murugiah Souppaya
Computer Security Division
Information Technology Laboratory

April 28, 2021

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.04282021

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

- Outreach to standardization agencies raising awareness of necessary changes
- Determine what government publications needs to be updated
- Assist organizations to identify how public-key cryptography is being used
    - Update used standards
    - Inventory and prioritize standards for PQ transition
    - Develop configuration guidelines
    - Develop implementation strategies

Classical-PQ Hybrid Approach

Suggested by most standardization agencies, e.g. NIST, ETSI, IETF

S_1 - PQ

$sk_1, pk_1,$

S_2 - RSA

$sk_2, pk_2,$

$S = C[S_1, S_2]$

$sk = (sk_1, sk_2)$

$pk = (pk_1, pk_2),$

S is secure if S_1 or S_2 is secure.

Hybrid Approach in Application

Certificates:
X.509
[**B**HM+17,KPD+18]

Secure channels:
TLS
[**B**HM+17,**B**BF+19,
SKD20, PST20]

Secure email:
S/MIME
[**B**HM+17]

Secure vehicle
communication
[**B**MRT**21**]

2015 Announced switch to PQ algorithms for NSA B-suite

2017 Start NIST PQ standardization for signatures, public-key encryption

2018 using 72 qubits Google

2019 ETSI Standard proposal for ID-based encryption

2020 ETSI Recommendation for combination of PQ and ECDH key exchang

2021 NIST PQ transition white paper

Today

2024 NIST PQ Standards expected for signatures, public-key encryption

11 - 36 years

2035 -2050 RSA-2048 broken, expected

[...] it appears that a transition to post-quantum cryptography will not be simple as there is unlikely to be a simple "drop-in" replacement for our current public-key cryptographic algorithms.

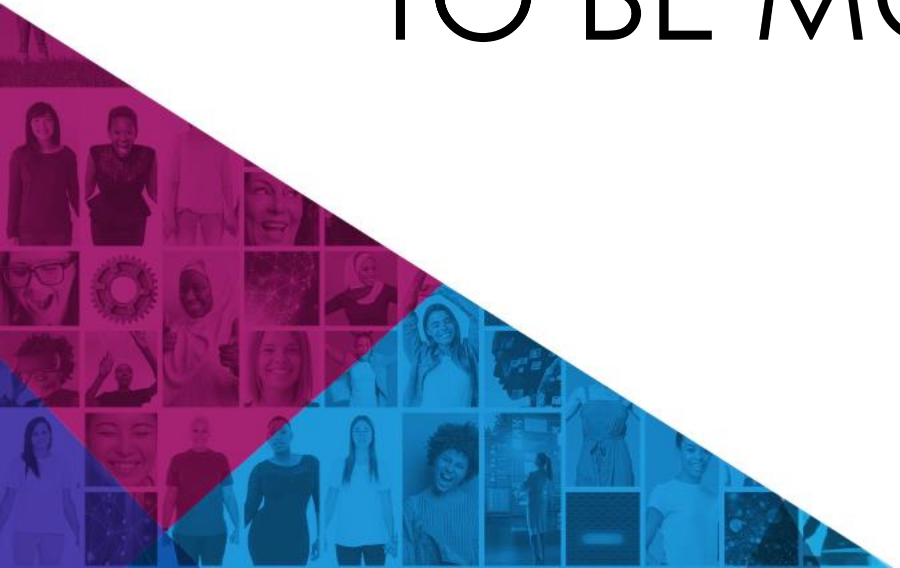
NIST, Call for submissions, 2017

So What? & Lessons Learned

Cooperation between allies

Leverage:
- expertise
- existing pathways, and
- building trusted new ones

BE MORE OPEN,
TO BE MORE EFFICIENT,
TO BE MORE SECURE



Thank You

ninabindel.de
https://www.balsillieschool.ca/kristen-csenkey/

nina.bindel@uwaterloo.ca
kcsenkey@balsillieschool.ca

@NinaBindel
@KCsenkey

nbindel
kristen-csenkey