Getting Ready for the Post-Quantum Transition

Brian A. LaMacchia, Ph.D.
Distinguished Engineer
Microsoft Research Security & Cryptography

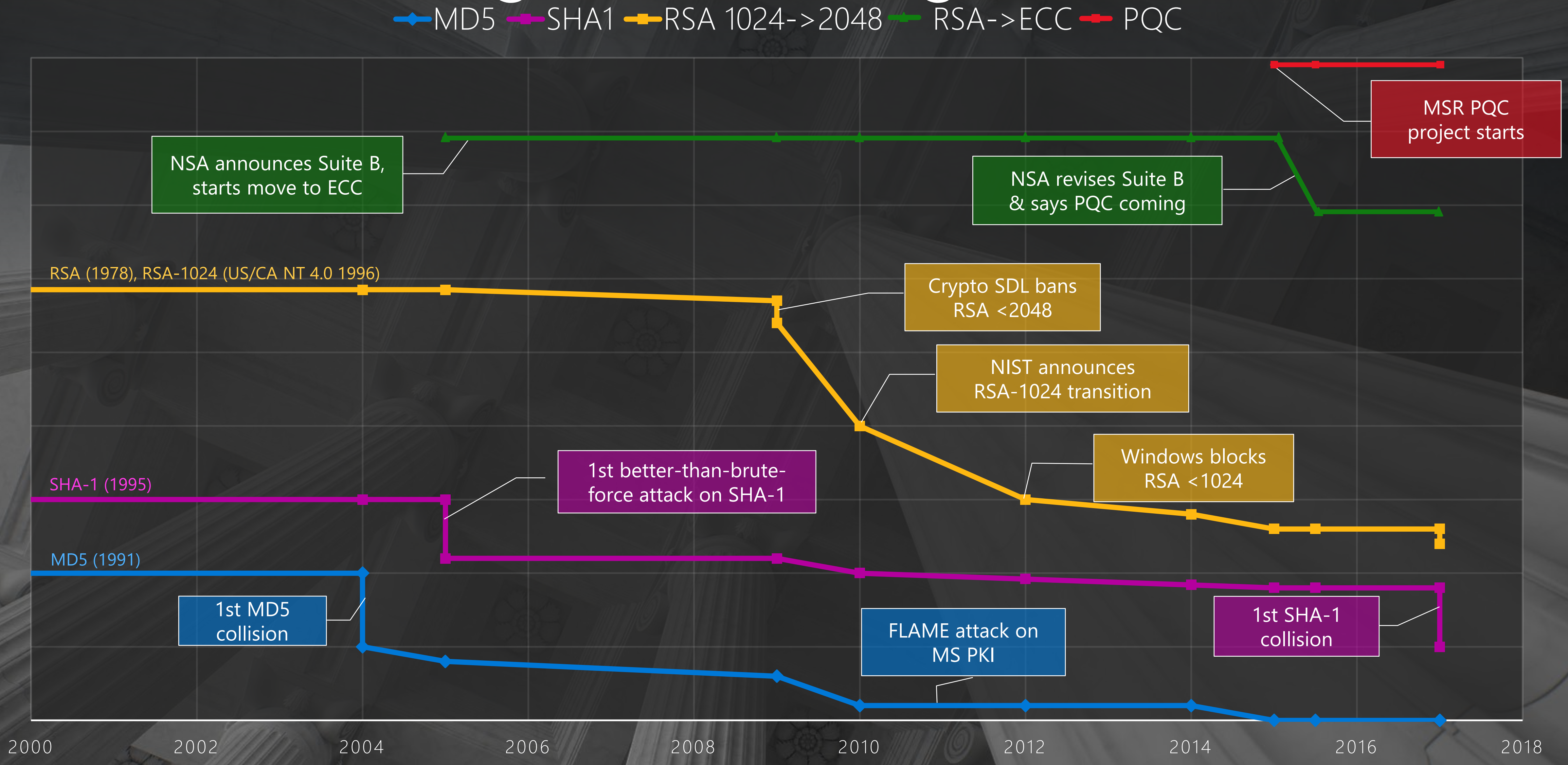
2020 / VIRTUAL
ISO ACADEMY

a.k.a. How to Prepare for Certain Catastrophe

Brian A. LaMacchia, Ph.D.
Distinguished Engineer
Microsoft Research Security & Cryptography

2020 / VIRTUAL
ISO ACADEMY

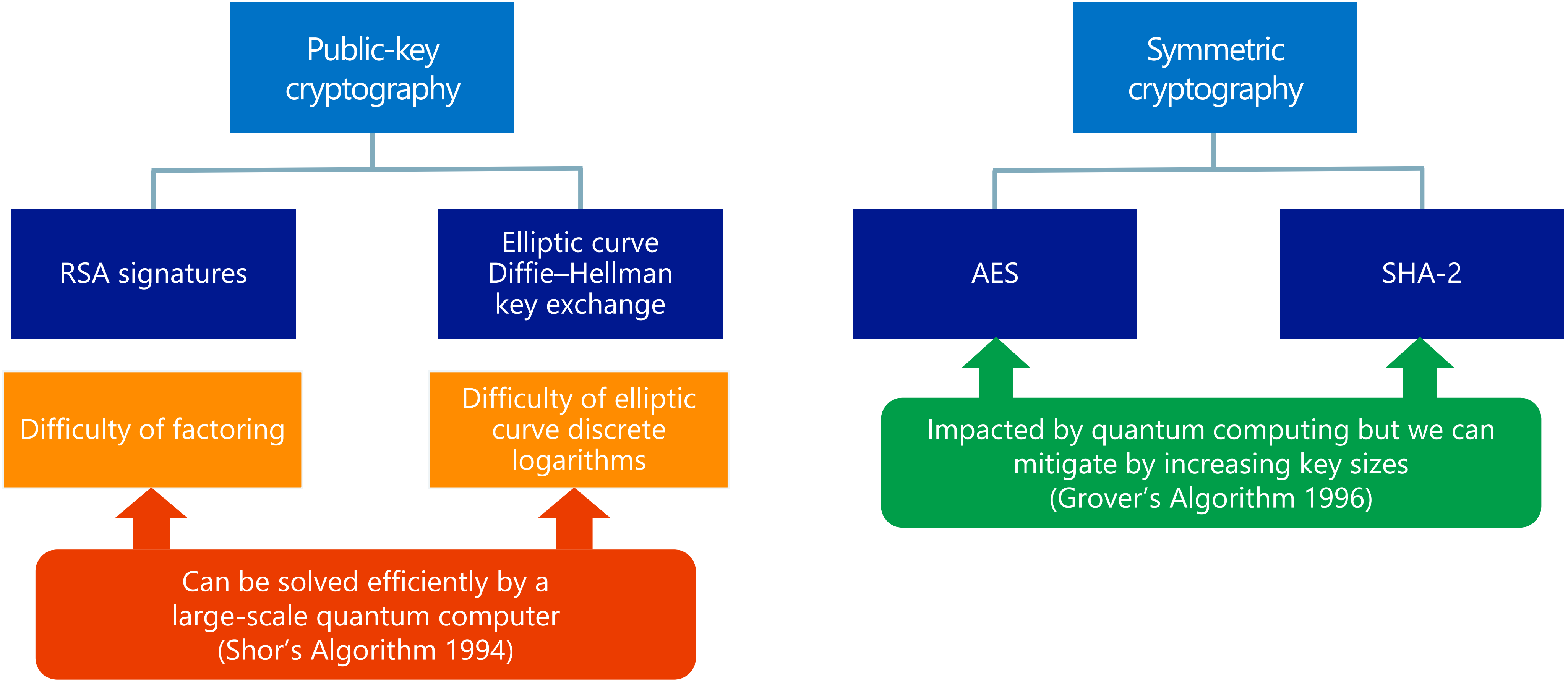
Relative Algorithm Strength Over Time



Quantum is coming

Contemporary Cryptography

TLS-ECDHE-RSA-AES128-GCM-SHA256

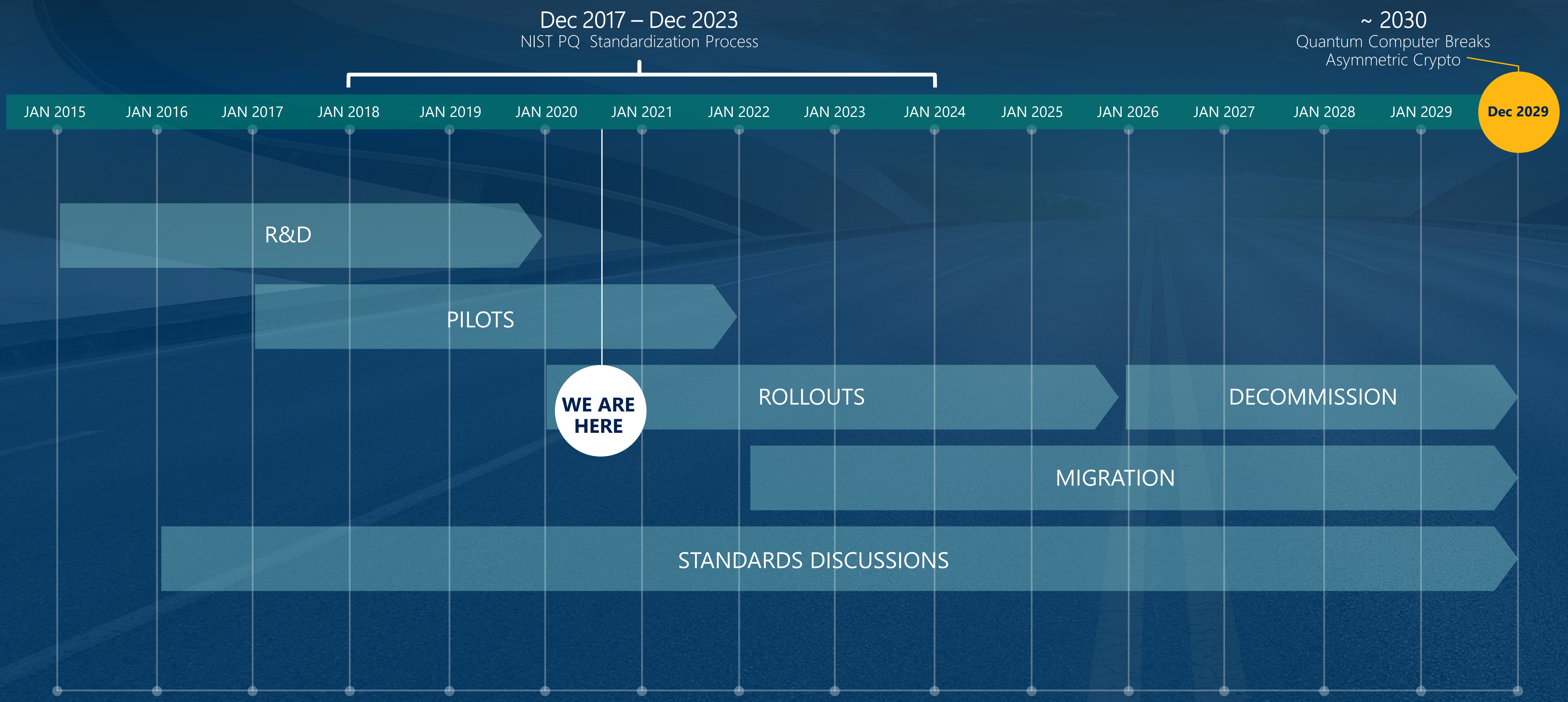


Resource Estimates for Shor's Algorithm

ECDLP in $E(\mathbb{F}_p)$ simulation results					Factoring of RSA modulus N interpolation from [21]		
$\lceil \log_2(p) \rceil$ bits	#Qubits	#Toffoli gates	Toffoli depth	Sim time sec	$\lceil \log_2(N) \rceil$ bits	#Qubits	#Toffoli gates
110	1014	$9.44 \cdot 10^9$	$8.66 \cdot 10^9$	273	512	1026	$6.41 \cdot 10^{10}$
160	1466	$2.97 \cdot 10^{10}$	$2.73 \cdot 10^{10}$	711	1024	2050	$5.81 \cdot 10^{11}$
192	1754	$5.30 \cdot 10^{10}$	$4.86 \cdot 10^{10}$	1 149	–	–	–
224	2042	$8.43 \cdot 10^{10}$	$7.73 \cdot 10^{10}$	1 881	2048	4098	$5.20 \cdot 10^{12}$
256	2330	$1.26 \cdot 10^{11}$	$1.16 \cdot 10^{11}$	3 848	3072	6146	$1.86 \cdot 10^{13}$
384	3484	$4.52 \cdot 10^{11}$	$4.15 \cdot 10^{11}$	17 003	7680	15362	$3.30 \cdot 10^{14}$
521	4719	$1.14 \cdot 10^{12}$	$1.05 \cdot 10^{12}$	42 888	15360	30722	$2.87 \cdot 10^{15}$

Source: *Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms*, Roeteller et al., Asiacrypt 2017.

Hypothetical 15-Year View for PQ Crypto



Future Quantum Computers are a Threat Today

- Even if a cryptographically-relevant quantum computer is a decade away…
- Record now, exploit later
  - Today's non-PQ encryption will break in the future
  - What is the security lifetime of the data you and your customers are transmitting and storing?
- Authentication, code-signing, and digital signatures
  - If I can break the algorithm and determine the private key, I can impersonate
  - For example, the Windows Update channel
  - What happens if an adversary can "update" the firmware on your processor?
- We're creating more legacy every day

Post-Quantum Cryptography at Microsoft
Three Parallel Workstreams

- Algorithms: 4 submissions to the NIST PQC standardization process. Ongoing work on high-performance implementations and cryptanalysis of our submissions.
- Protocols: Make commonly-used security protocols “PQ-enabled”.
- Systems: Integrate PQC into exemplary “high-value/high-risk” engineering systems and processes.

NIST Post-Quantum Standardization Project

- “Competition” launched Nov 30, 2017
- Research teams from around the world responded
- 70 submissions accepted into Round 1
- Four candidates submitted by Microsoft & collaborators
- NIST & crypto community now engaged in cryptanalysis
- NIST expected to pick multiple “winning” algorithms

NIST PQC Round 3 Expected Shortly

- NIST announced algorithms selected for Round 2 on January 30, 2019.
  - 17 key encipherment (encryption) algorithms
  - 9 digital signature algorithms
  - After being selected for Round 2, each team was allowed to “tweak” their submissions in response to recent research results.
- All four MSR co-submitted proposals advanced to Round 2.
  - All of our proposals were tweaked for Round 2.
  - We have announced some post-Round 2 tweaks, too, which we would apply in Round 3.
- NIST is expected to announce soon which algorithms will advance to Round 3
- NIST has previous said they hope to conclude the selection process by the end of 2022 and have the corresponding FIPS issued by the end of 2023.

BREAKING NEWS
NIST Announced
Round 3 yesterday

NIST PQC Round 3

- 15 algorithms selected for Round 3
  - 7 “Finalists” (4 encryption, 3 digital signature)
  - 8 “Alternates” (5 encryption, 3 digital signature)
- NIST said they expect to pick at most 2 encryption & 2 signature algorithm Finalists for standardization at the end of Round 3
- But…NIST also announced a Round 4 and the likely standardization of at least some of the Alternates at the end of Round 4
- ANALYSIS: We will see at least two waves of PQC algorithm standards from NIST, which makes having **cryptographic agility** in deployed systems even more important

Our Proposals to NIST

"FrodoKEM"
Learning With Errors
Key Encipherment

"SIKE"
Supersingular Isogeny
Key Encipherment

"Picnic"
Post-Quantum
Signatures

"qTESLA"
Post-Quantum
Signatures

FrodoKEM: Learning With Errors Key Encipherment

- Collaboration among
  Microsoft (Craig Costello, Karen Easterbrook, Brian LaMacchia, Patrick Longa, Michael Naehrig)
  Facebook (Ilya Mironov)
  Google (Ananth Raghunathan)
  NXP (Joppe Bos)
  CWI (Leo Ducas)
  Ondokuz Mayıs University (Erdem Alkim)
  Stanford University (Valeria Nikolaenko)
  University of Michigan (Chris Peikert)
  University of Waterloo (Douglas Stebila)
- Lattice-based encryption based on the “learning with errors” problem
- Efficiency: Fast, but relatively large keys.

SIKE: Supersingular Isogeny Key Encipherment

- Collaboration among
  Microsoft (Craig Costello, Brian LaMacchia, Patrick Longa, Michael Naehrig)
  LinkedIn Corporation (Amir Jalali)
  Amazon (Matt Campagna)
  IBM Zürich (Luca DeFeo)
  InfoSec Global (Basil Hess, Vladimir Soukharev)
  Texas Instruments (Brian Koziel)
  Radboud University (Joost Renes)
  Florida Atlantic University (Reza Azarderakhsh)
  University of Waterloo (David Jao)
  University of Toronto (David Urbanik)
- Elliptic curve-based KEM, based on the “supersingular isogeny” problem
- Efficiency: Small keys, but relatively slow

Picnic Post-Quantum Digital Signature Scheme

- Collaboration among
  Microsoft (Melissa Chase, Greg Zaverucha)
  DFINITY (David Derler)
  Aarhus University (Claudio Orlandi)
  Austrian Institute of Technology (Sebastian Ramacher, Daniel Slamanig)
  Cornell Tech (Steven Goldfeder)
  George Mason University (Jonathan Katz)
  Georgia Tech (Vladimir Kolesnikov)
  Graz University of Technology (Daniel Kales, Christian Rechberger)
  Northwestern University (Xiao Wang)

  Signature scheme based on efficient zero-knowledge proofs
- Hard problems: Hash collision and preimage, block cipher key recovery
- Efficiency: Small keys, large signatures

NIST Round 2 Public Key & Signature Sizes
Security Level 1

Signature Algorithm	pk (bytes)	signature (bytes)
CRYSTALS-Dilithium	1,184	2,044
Falcon	897	652
Rainbow	149,000	48
GeMSS	352,190	33
LUOV	11,500	239
MQDSS	46	20,854
Picnic	32	12,850
qTESLA	14,880	2,592
Sphincs+	32	8,080

Bringing PQ to Industry Crypto Protocols

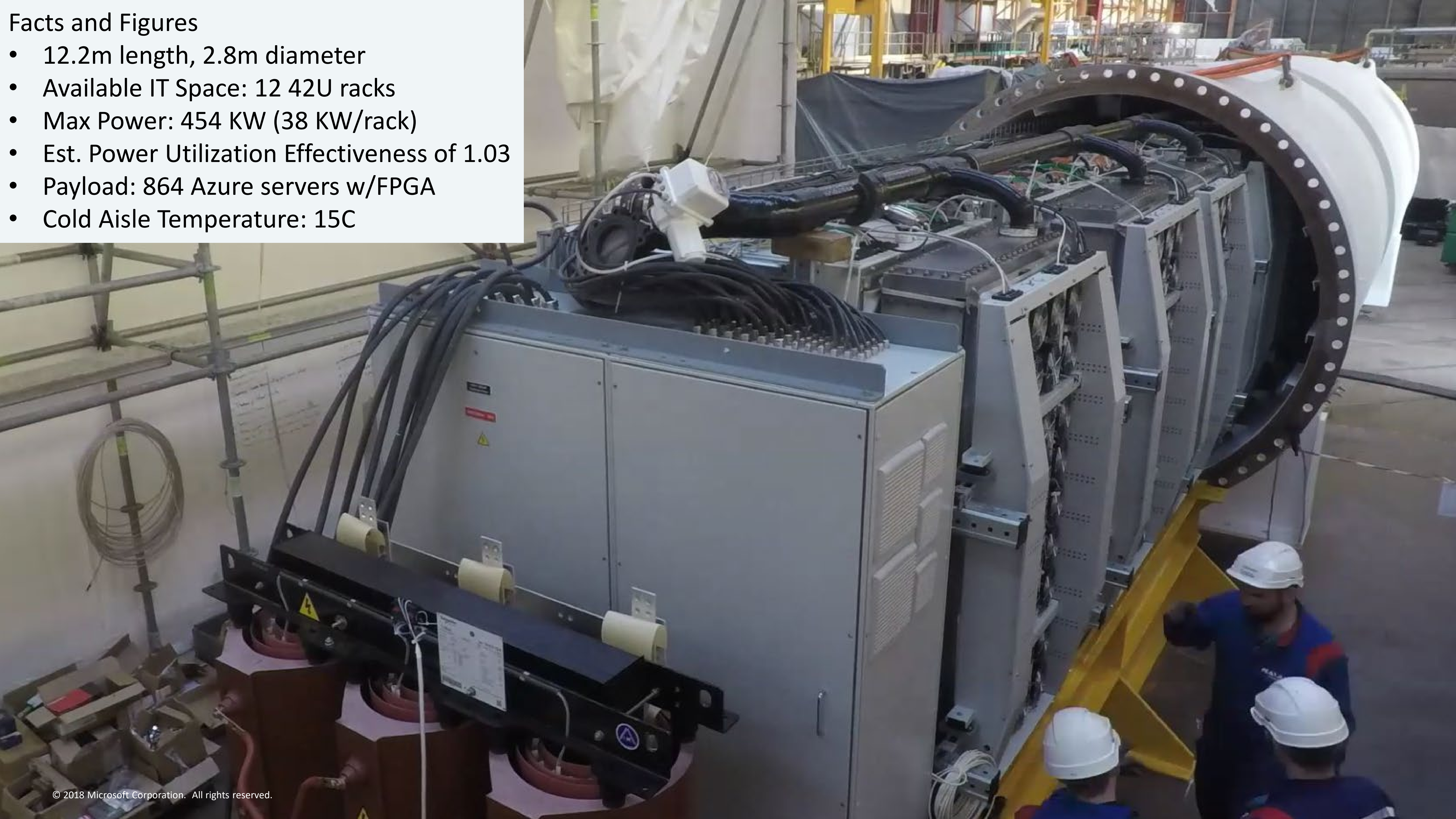
- The Open Quantum Safe (OQS) project provides a common API for testing and prototyping with post-quantum crypto algorithms
  - Multi-org OQS dev team includes University of Waterloo, Microsoft, Amazon, SRI International
  - Includes LIBOQS, an open source C library for PQ Crypto algorithms (with C++/C#/Python wrappers)
- This lets us access and test any PQ algorithm in an OQS-enlightened protocol
  - To date, we have integrated Frodo/FrodoKEM, SIDH/SIKE, qTESLA, and Picnic into OQS
- https://openquantumsafe.org/

PQC Protocol Integrations using OQS

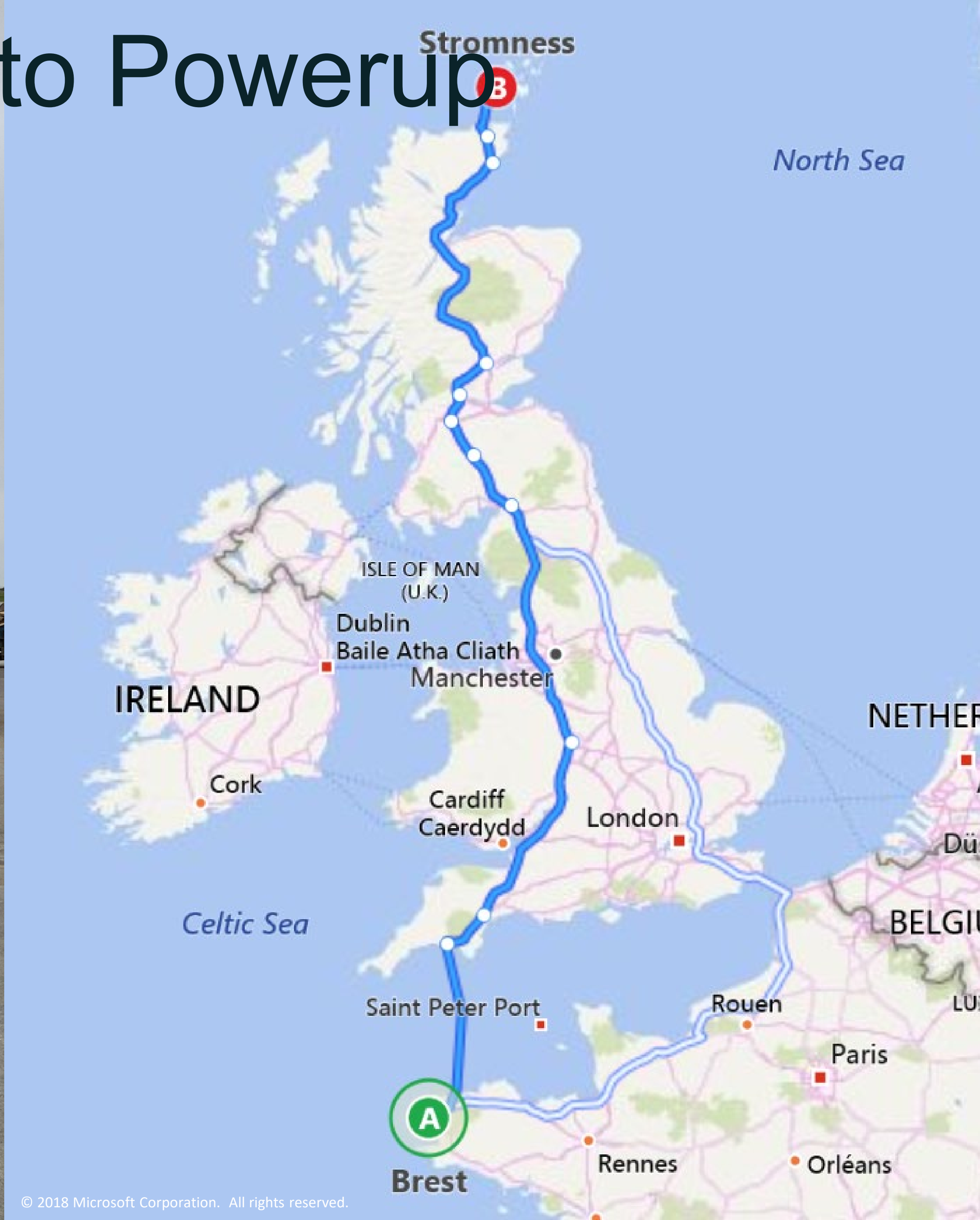
- We integrated the OQS library into protocols to provide PQC and hybrid ciphersuites
  - Hybrid: keep your FIPS or otherwise approved crypto, add PQ protection
  - For more on hybrid PKI, see Bindel et al. 2017: https://eprint.iacr.org/2017/460.pdf
- OpenSSL, with TLS 1.2 and 1.3 support
  - https://github.com/open-quantum-safe/openssl
- OpenSSH
  - https://github.com/open-quantum-safe/openssh-portable
- OpenVPN: For securing links against “record now/exploit later” attacks.
  - https://github.com/Microsoft/PQCrypto-VPN

Facts and Figures

- 12.2m length, 2.8m diameter
- Available IT Space: 12 42U racks
- Max Power: 454 KW (38 KW/rack)
- Est. Power Utilization Effectiveness of 1.03
- Payload: 864 Azure servers w/FPGA
- Cold Aisle Temperature: 15C



30 Days: Factory to Powerup

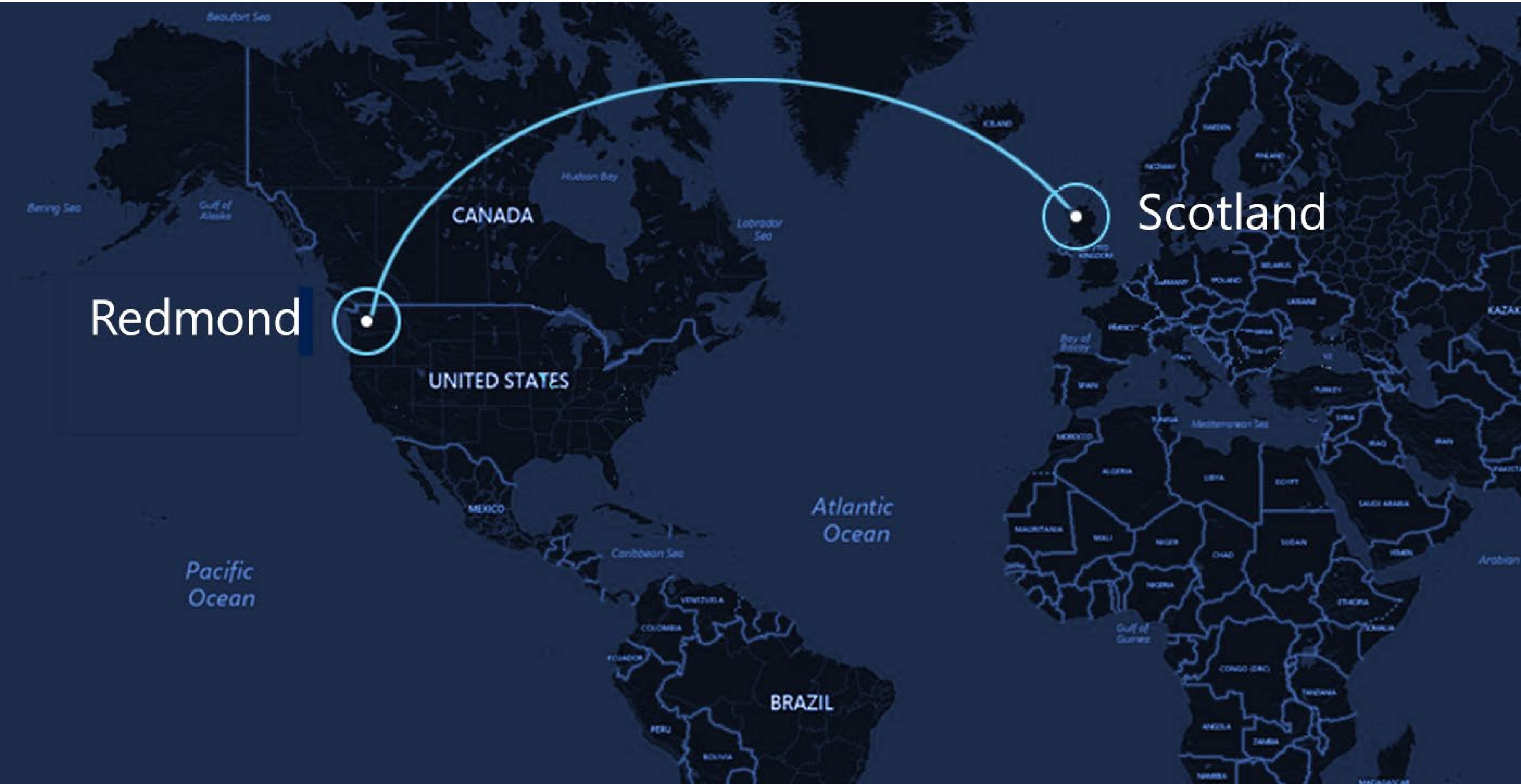


Site Information

- Location: European Marine Energy Centre, Scotland
- Electricity: 100% locally sourced renewable


700T. SWL

Securing the link (>6900km) with a Post-Quantum VPN



Systems: Key Scenarios for Microsoft

- Public Key Infrastructure (PKI)
  - Both corporate and externally-facing
- Code signing for Microsoft products and services
  - Authenticode (e.g. Windows DLLs)
  - UWP (Microsoft Store) applications
  - XBOX
- Azure Cloud Computing
  - Key Vault

PQC & Hybrid Certs with an HSM

- We added support for the Picnic algorithm to an Utimaco HSM
  - Where possible, we replaced functions in MS software with calls to Utimaco firmware: RNG, SHA-3, ASN.1 utilities
- Demonstrated key PKI CA operations:
  - HSM generates & stores new PQ CA key and issues self-signed cert
  - HSM generates & stores new PQ EE key, CA issues cert for EE key
  - CA issues PQ cert for externally-generated CSR for (legacy) RSA public key.
  - All PQ operations use Picnic keys and signatures
- More recently: working with DigiCert and Utimaco, we demonstrated using an HSM to issue (RSA/ECDSA)-PQ hybrid certificates
  - X.509v3 certificates with a new “hybrid” signature OID
  - Signature blob is concatenation of “classic” and PQ signatures

PQ Open Source Releases

Libraries:

- https://github.com/Microsoft/PQCrypto-LWEKE
- https://github.com/Microsoft/PQCrypto-SIKE
- https://github.com/microsoft/qTESLA-Library
- https://github.com/Microsoft/Picnic

Protocol Integrations:

- https://openquantumsafe.org/
- https://github.com/open-quantum-safe/openssl
- https://github.com/open-quantum-safe/openssh-portable
- https://github.com/Microsoft/PQCrypto-VPN

Overall project site:

- https://www.microsoft.com/en-us/research/project/post-quantum-cryptography/

Summary – Preparing for a PQ future

- Quantum computers are coming – maybe not for a decade or more, but within the protection lifetime of data we are generating and encrypting today
  - We need to start planning the transition to post-quantum cryptographic algorithms now.
- To prepare for the PQ transition, all our systems need cryptographic agility
  - Hybrid solutions combining classical and post-quantum primitives look promising; they provide both traditional cryptographic guarantees as well as some PQ resistance
- Practical engineering options exist today for deploying PQ
  - But it is going to take a long time to update our software stacks…
- We may already be late to transition
  - Some of our customers have data with a protection lifespan of 15-20 years or more.
  - IoT and critical infrastructure have devices that won't be updated for 15+ years.

Open Q&A

Brian A. LaMacchia, Ph.D.

Distinguished Engineer

Microsoft Research Security & Cryptography