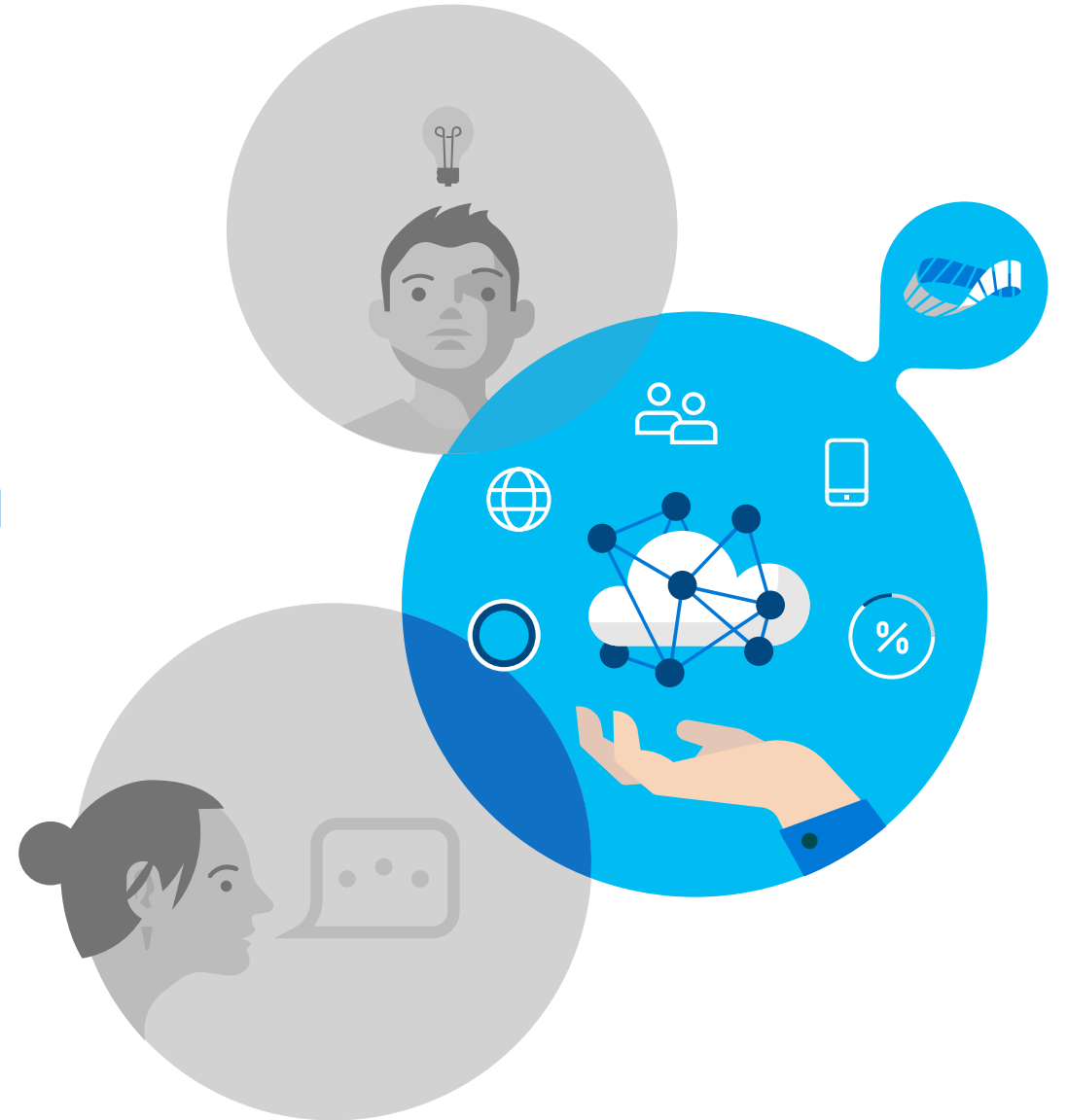


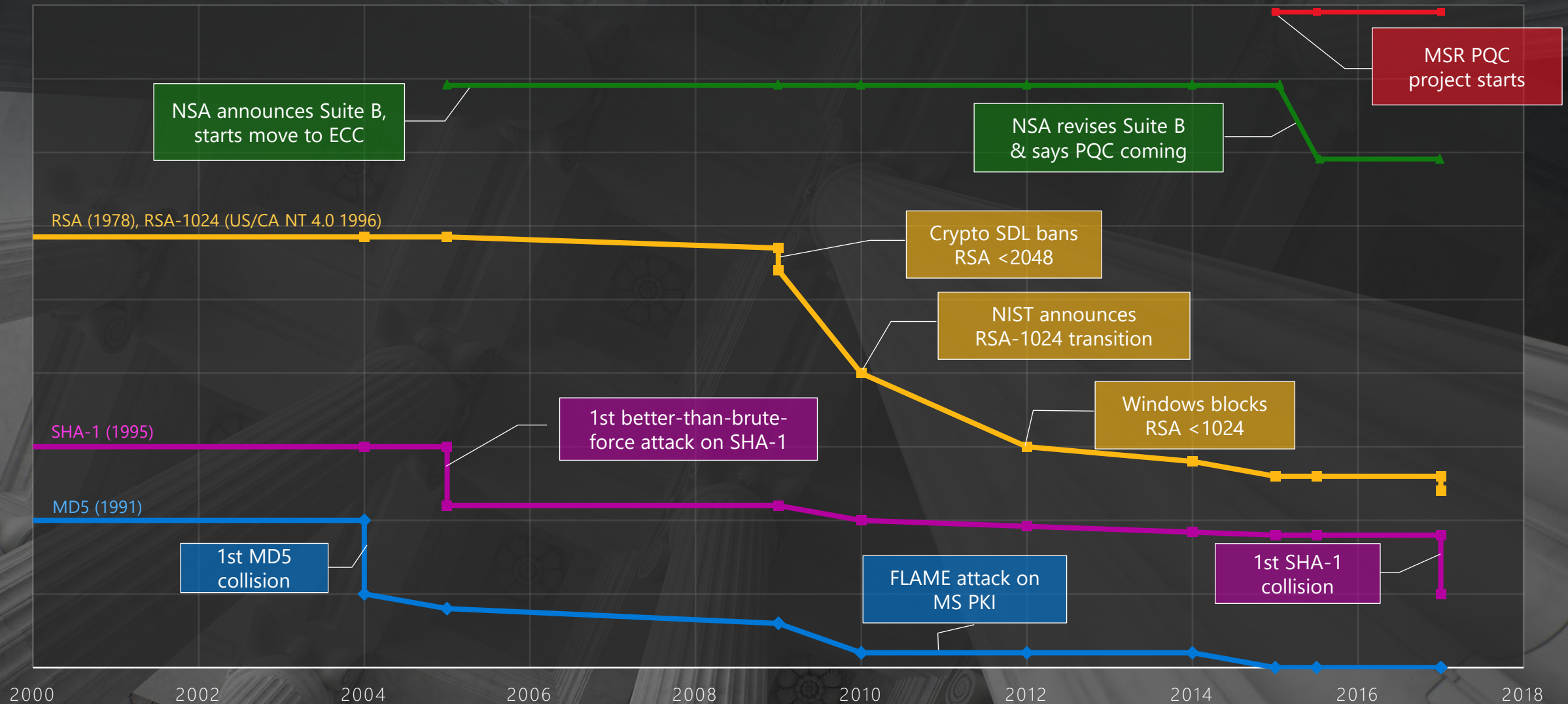
Getting Ready for the Post-Quantum Transition

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



Relative Algorithm Strength Over Time

— MD5 — SHA1 — RSA 1024->2048 — RSA->ECC — PQC

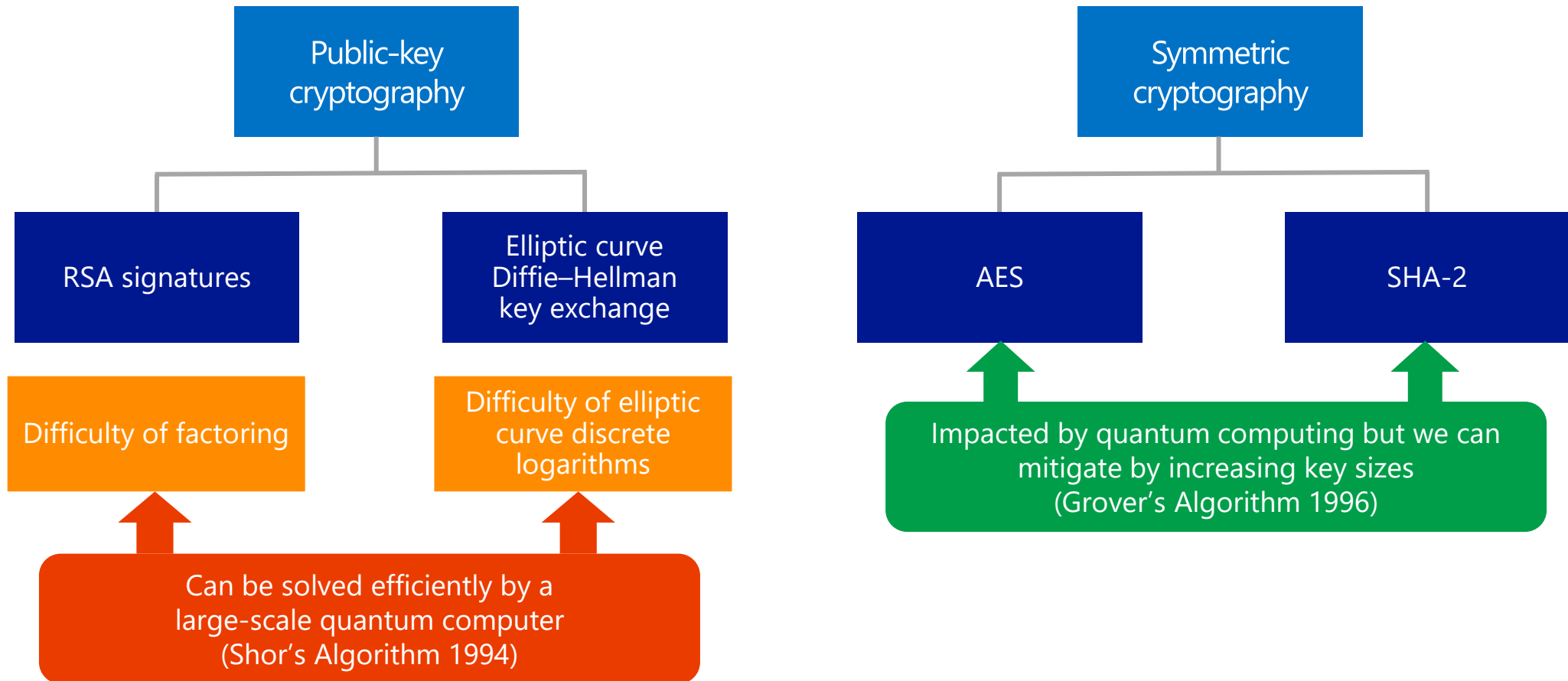


Quantum is coming



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*, Roettler et al., Asiacrypt 2017.

Hypothetical 15-Year View for PQ Crypto

NSA
Suite B
Update

Dec 2017 – Dec 2023
NIST PQ Standardization Process

~ 2030
Quantum Computer Breaks
Asymmetric Crypto
(>2400 logical qubits)



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.

Our NIST Round 3 Candidates

"FrodoKEM"
Learning With Errors
Key Encipherment

"SIKE"
Supersingular Isogeny
Key Encipherment

"Picnic"
Post-Quantum
Signatures

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 likely 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

Predictions: “Cascades” and “Long Tails”

- 2025: likely ~2-4 NIST PQ encryption algorithms and ~1-3 NIST PQ signature algorithms
- 2025-2030: standards bodies will begin updating for PQC (having waited for FIPS)
 - Expect at least a year per standard, likely longer based on past experience
- Cascade of crypto/protocol standards dependencies will extend transition times
- Long tail of security protocols with small implementor communities
 - These protocols won't migrate to PQC as quickly as TLS, SSH, OpenVPN, IPSec, etc., and they will likely be harder to update
- 2030: likely to still be “PQ-messy” in terms of updates to standards

Bringing PQ to Industry Crypto Protocols

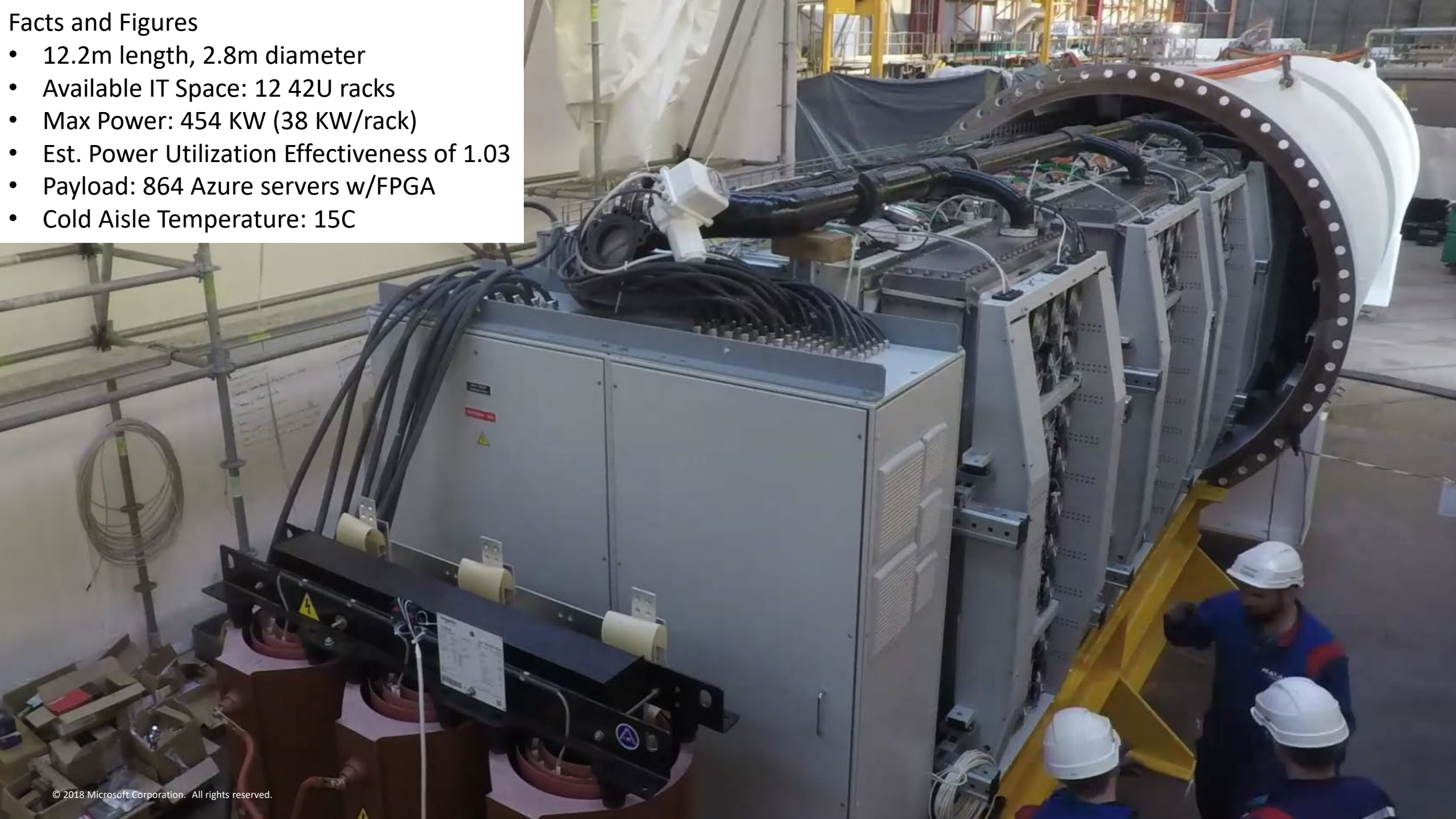
- The Open Quantum Safe (OQS) project provides a common API for testing and prototyping with post-quantum crypto algorithms
 - Multi-org OQS dev team includes University of Waterloo, Microsoft, Amazon, SRI International
 - Includes LIBOQS, an open source C library for PQ Crypto algorithms (with C++/C#/Python 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

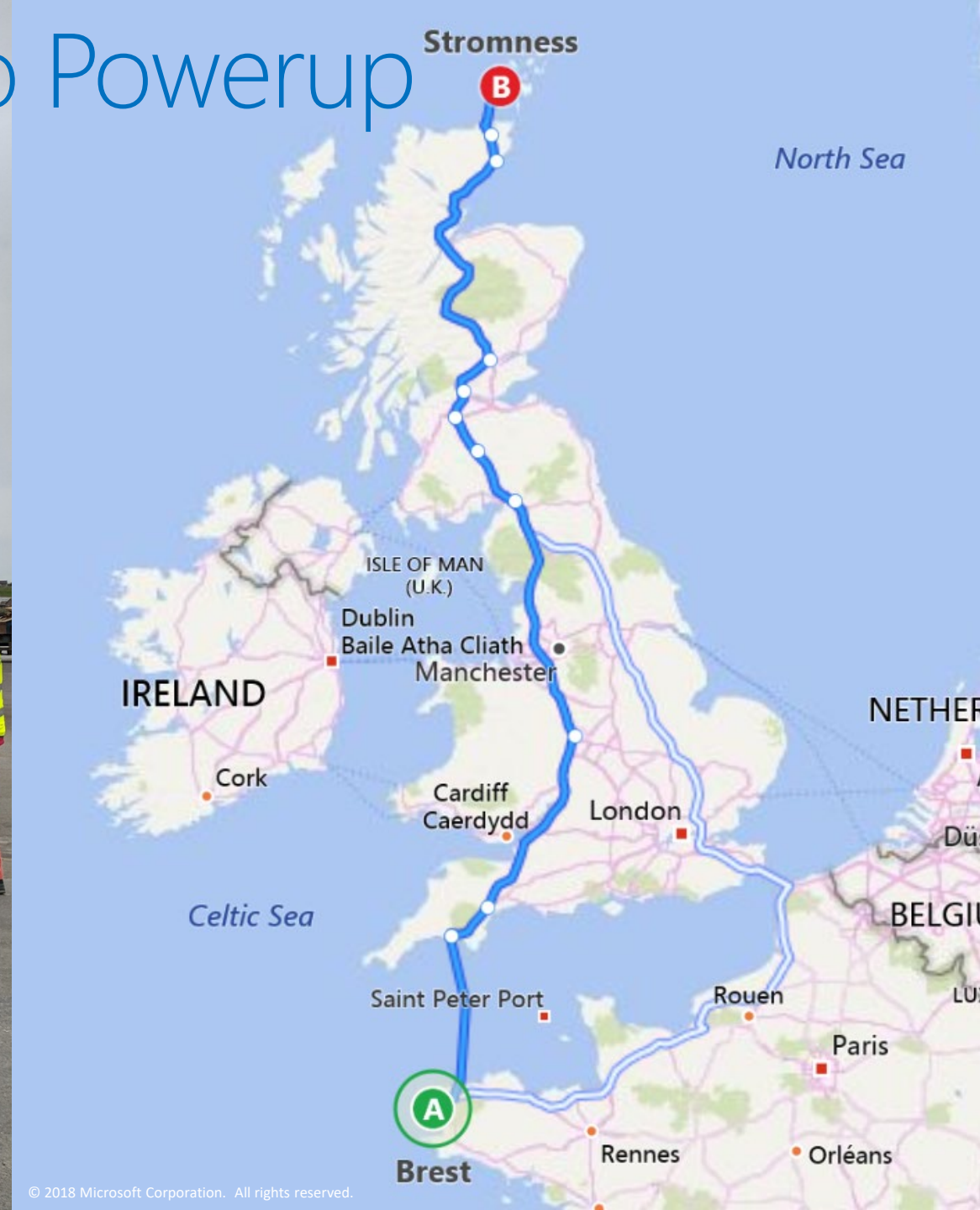


30 Days: Factory to Powerup



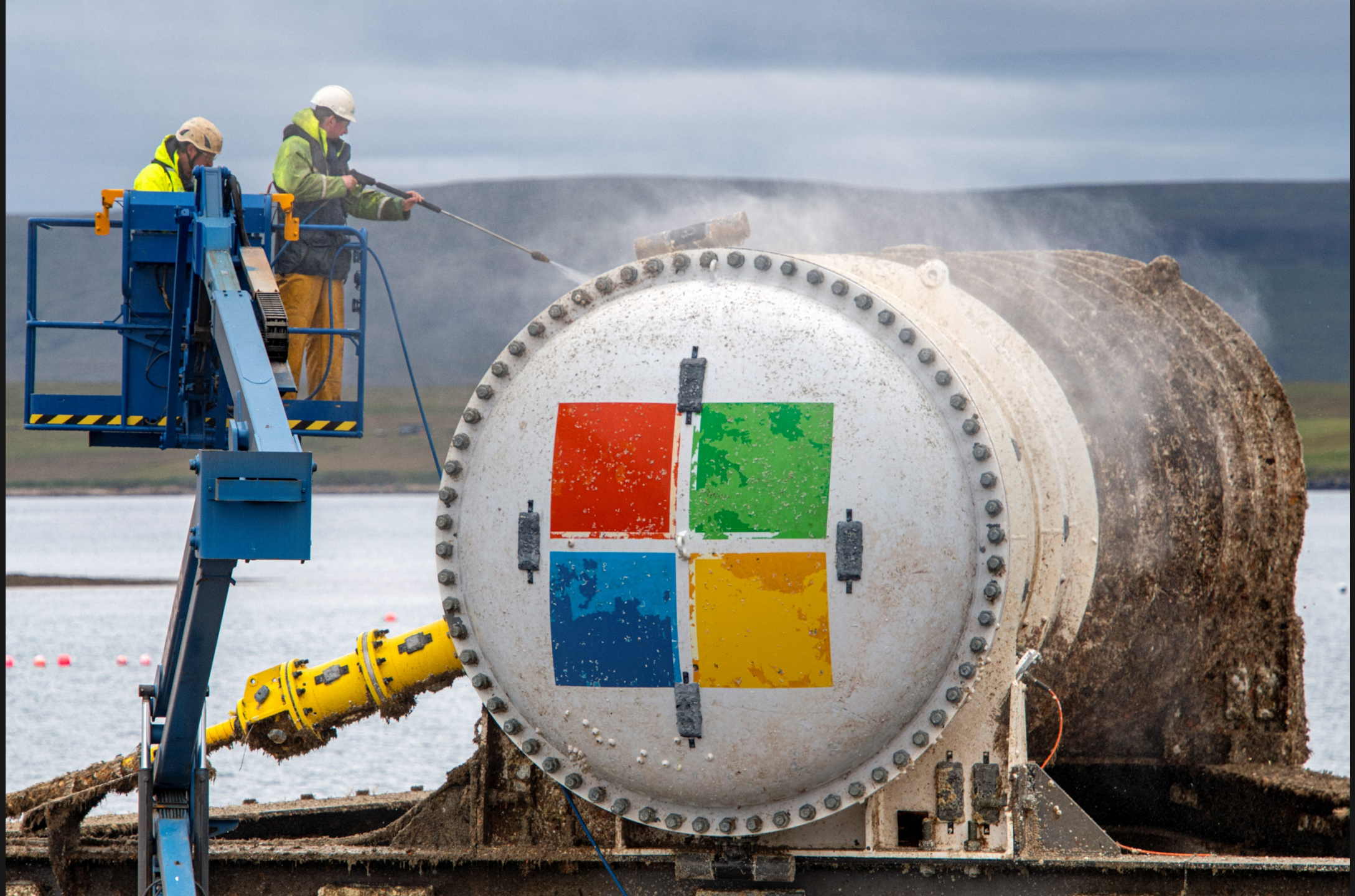
Site Information

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

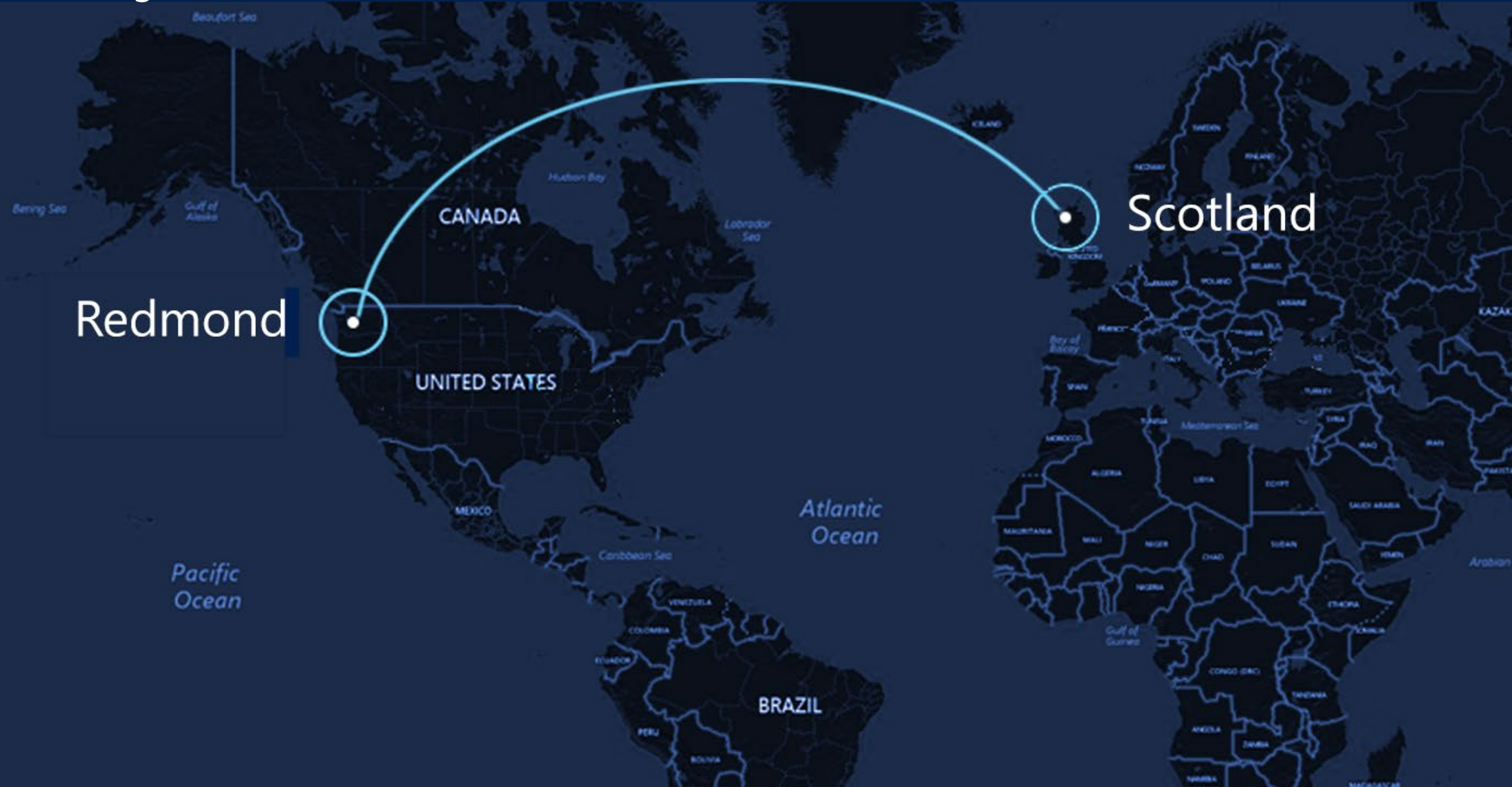








Securing the link (>6900km) with a Post-Quantum VPN



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

Upgrading to PQC Means Larger Keys, Ciphertexts, Signatures

NIST Round 3 Candidates -- Public Key & Signature Sizes for L1

Signature Algorithm	pk (bytes)	signature (bytes)
CRYSTALS-DILITHIUM (L2)	1312	2420
Falcon	897	666
Rainbow	157800	66
SPHINCS+	32	7856
Picnic	34	13802
GeMSS	352190	32

RSA-2048: pk 256 bytes, signatures 256 bytes

ECC-P256: pk 32 bytes, signatures 64 bytes

Looking Forward...

Past Algorithm Transitions Have Taken Years

PQC Will Be No Different

- ECC (starting in 2005) is the closest model to the PQC transition
- Adding base level of ECC support to Windows took 4.5 years
 - Three releases (Vista, Vista SP1, Win7) from NSA's Suite B announcement
- 15 years later, parts of the ecosystem still working on ECC parity
- Transitioning to a new algorithm takes more time, is more complicated, and impacts more functions and features than you expect
- Long-term support requirements slow algorithm decommissioning
- Start planning your migration now
 - Draft NCCoE white paper: [Getting Ready for Post-Quantum Cryptography](#)
 - CRA Quad Paper: [Post Quantum Cryptography: Readiness Challenges and the Approaching Storm](#)

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.

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>

PQ-VPN to Project Natick:

- <https://www.microsoft.com/en-us/research/project/post-quantum-crypto-tunnel-to-the-underwater-datacenter/>

Overall project site:

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

Questions?