A Quantum of Safety
Rooting Trusting in a Quantum World

Mike Brown, CTO & Co-founder
December 4, 2018

THE QUANTUM RACE IS ON

Microsoft

Google

rigetti

D:wave
The Quantum Computing Company™

IBM

intel

ISARA


Quantum computing will solve today's unsolvable problems, opening up
A NEW REALM OF POSSIBILITIES.
ISARA


QUANTUM'S
NEGATIVE DISRUPTION
Quantum computing will break today's
public key encryption standards.
ISARA


“The impact of quantum on our national defense will be tremendous.
The question is whether the United States and its allies will be ready.”
- Rep. Will Hurd, WIRED, December 2017
WIRED

THE QUANTUM EFFECT ON TODAY'S CRYPTOGRAPHY

Type	Algorithm	Key Strength Classic (bits)	Key Strength Quantum (bits)	Quantum Attack
Asymmetric	RSA 2048	112	0	Shor's Algorithm
	RSA 3072	128		
	ECC 256	128		
	ECC 521	256		
Symmetric	AES 128	128	64	Grover's Algorithm
	AES 256	256	128	

WHAT'S CRYPTO AGILITY?

ISARA

SOFTWARE UPDATES ARE VULNERABLE

Embed a Root of Trust at Manufacture

- Create software update
- Digitally sign the update

Digital Signature | **Software Update**

- Receive software update
- Verify ECDSA or RSA digital signature → **broken using Shor's algorithm**
- Apply software update

ISARA

HOW ARE SECURE COMMUNICATIONS VULNERABLE?

Secure Communication Protocol

Handshake | **Data Exchange**

Shor's algorithm **breaks** current public-key algorithms

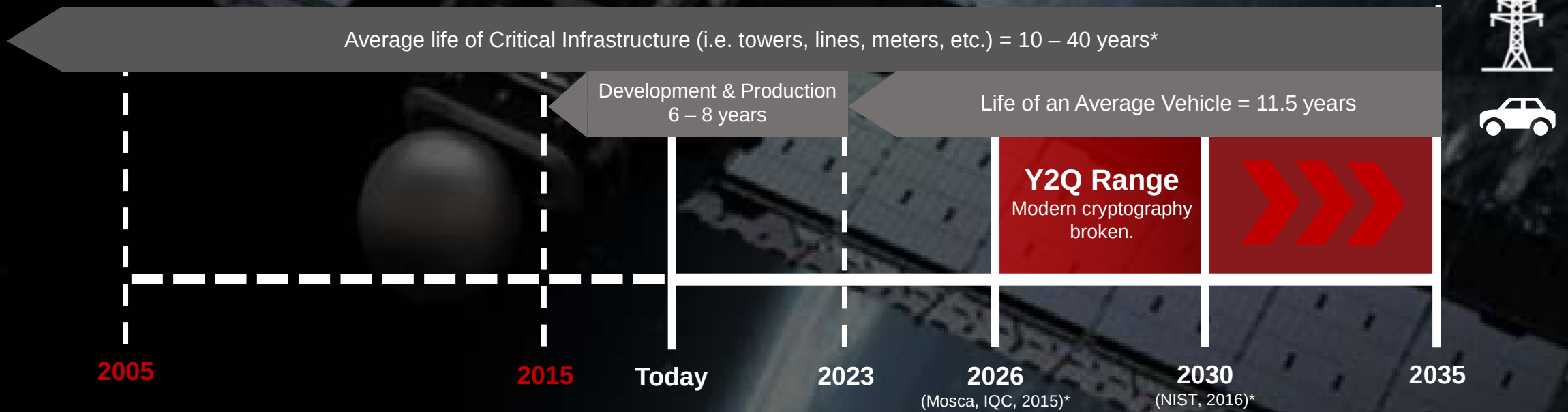
Authentication
Key Establishment

Symmetric Encryption

AES 256 → AES 128

Grover's algorithm **reduces** the effective symmetric key size to half

PRIORITIZING THE FIX
FOR TOMORROW'S THREAT

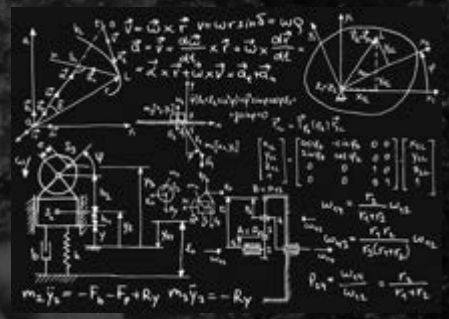


*Mosca, Michele., Institute for Quantum Computing. 2015. "Cybersecurity in an era with quantum computers: will we be ready?". https://eprint.iacr.org/2015/1075.pdf
*NIST. April 2016. "Report on Post-Quantum Cryptography". http://dx.doi.org/10.6028/NIST.IR.8105
*https://www.popsci.com/environment/article/2009-06/next-grid

ISARA

PATHWAYS TO QUANTUM SAFETY

Quantum Key Distribution



Quantum-Safe Cryptography

ISARA

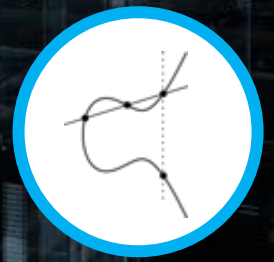
THE "NEW" MATH

Hash-based

Code-based

Lattice-based

Multivariate-based



Isogeny-based

ISARA

THE CHALLENGE

With increased connectivity, the scale of what needs to be updated also increases.

Maintain Interoperability

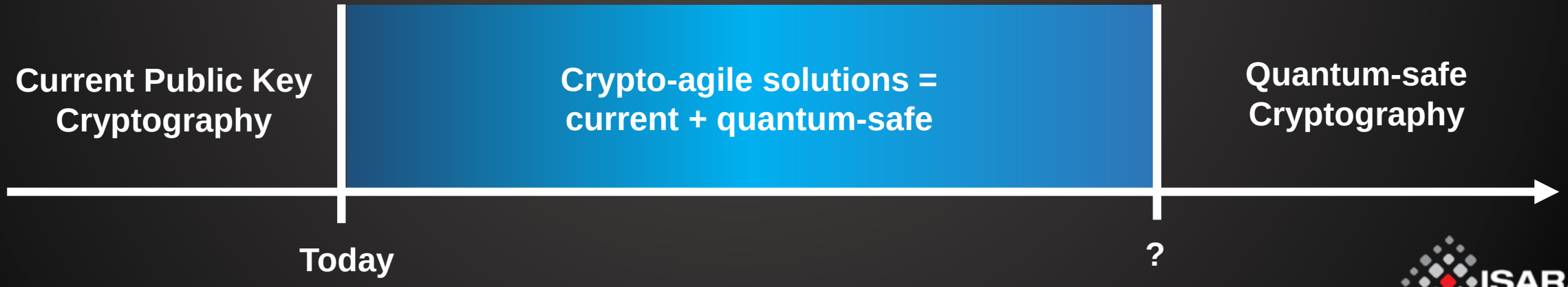
Migrate Critical Systems Faster

Reduce Switching Costs

ISARA

THE SOLUTION:
CRYPTO-AGILITY

The ability to react to cryptographic threats quickly, at a systems level it **bridges the gap** between current and quantum-safe security methods.



ISARA

SUCCESS REQUIRES STANDARDS

ISARA

CLEARING THE PATH TO QUANTUM-SAFE SECURITY

www.isara.com
quantumsafe@isara.com

Join us on social

@ISARACorp @ISARACorp @ISARA Corporation

ISARA