

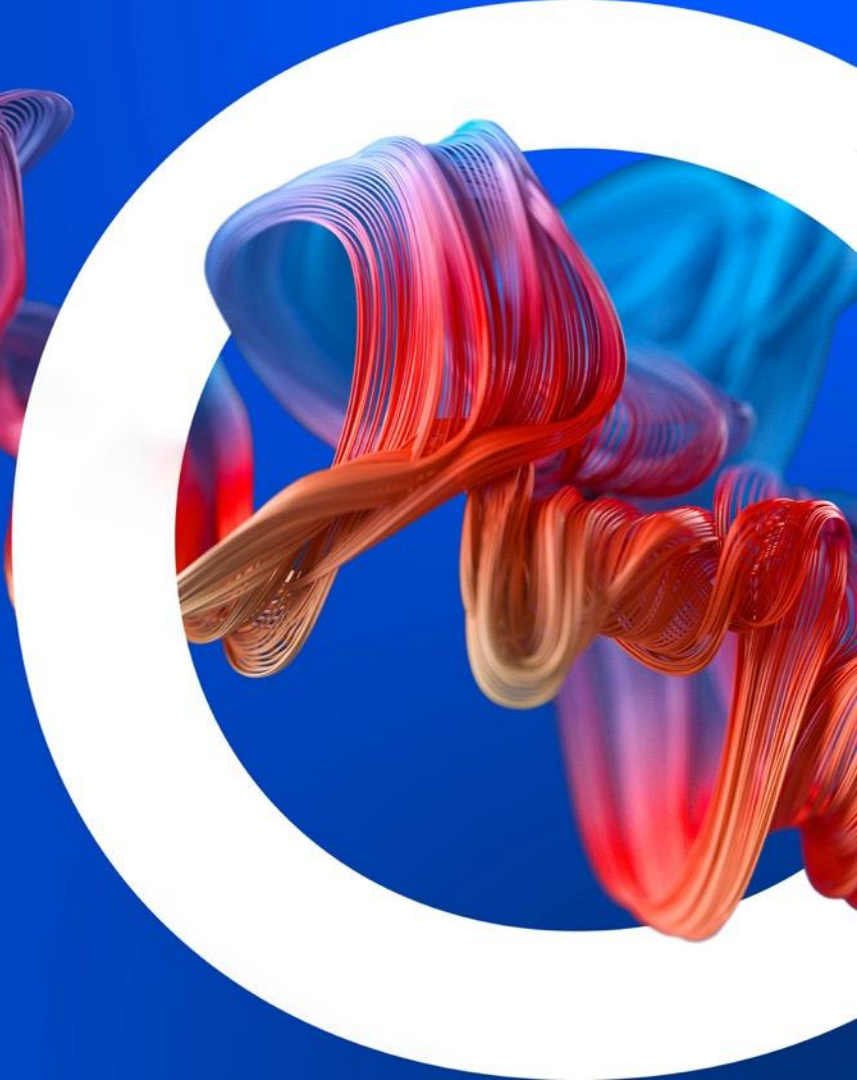


Cryptography in the Quantum Era

An IP transport perspective

Paresh Khatri

CTO IP Networks APAC



Agenda

1. Quantum computing
2. Impact of quantum computing on cryptography
3. The post-quantum future

Agenda

1. Quantum computing
2. Impact of quantum computing on cryptography
3. The post-quantum future

Quantum Technology

Quantum technology 1.0 and 2.0

Quantum Technology 1.0



Technology that exploits the *ensemble behavior* of **discrete quantum** particles, such as electrons, photons, and atoms



Transistors



LEDs/Lasers



Solar Panels



MRI

Quantum Technology 2.0



Technology that utilizes *individual quantum systems*, harnessing **quantum superposition** and **quantum entanglement**



Quantum
Computing



Quantum
Communication

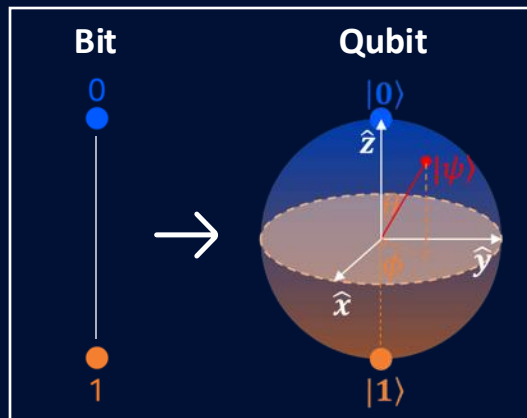


Quantum
Sensing

Qubits, superposition, and entanglement

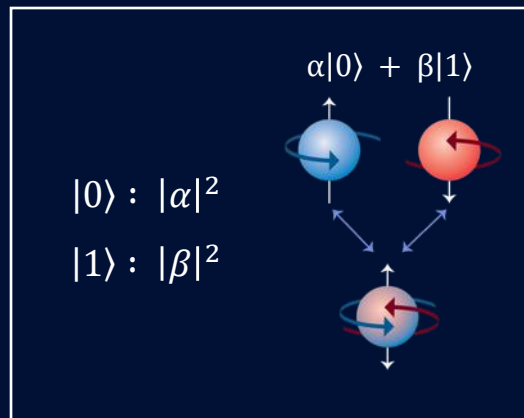
Foundation of Quantum 2.0 revolution

Qubit



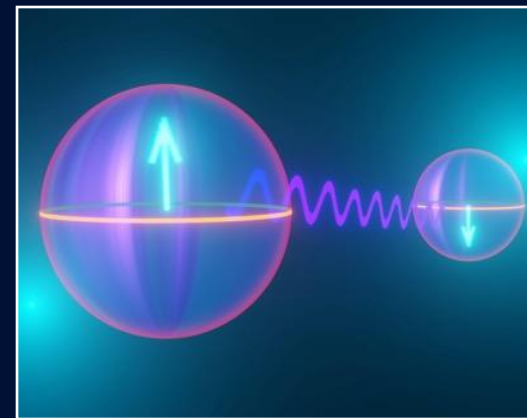
A qubit is the fundamental information container in a quantum system

Superposition



Qubits exist in multiple states at once, only collapsing to a single state when measured

Entanglement



Entangled qubits' states can't be separated. Measuring one immediately reveals the other.

Quantum computing

Computers that harness the properties of quantum mechanics, such as superposition, interference, and entanglement, to perform calculations

Quantum Computing

Classical
bit

0 1

Each bit is either
0 or 1

0 1 0 1

Each 4-bit combination is one out
of 2^4 possible permutations

Quantum bit
(qubit)

0|1

Each bit is both
0 and 1 at once

0|1 0|1 0|1 0|1

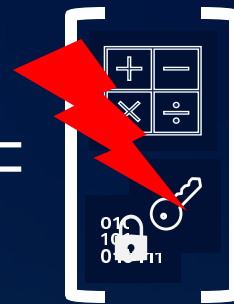
Four bits represent all of the 2^4
possible permutations

Threats



Availability of
Cryptographically
Relevant Quantum
Computer (CRQC)
[Q-Day]

=



Current
asymmetric
cryptography
(PKC)

Impacts
SSL/TLS
SSH
IPsec
Digital
signatures

Vulnerabilities

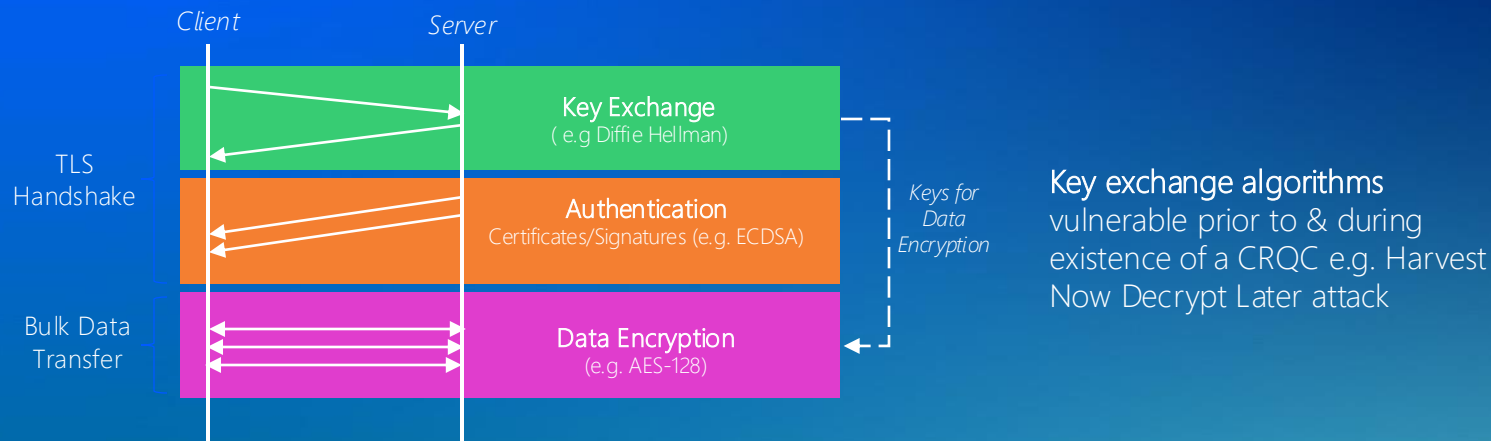


Harvest now and
decrypt later (HNDL)

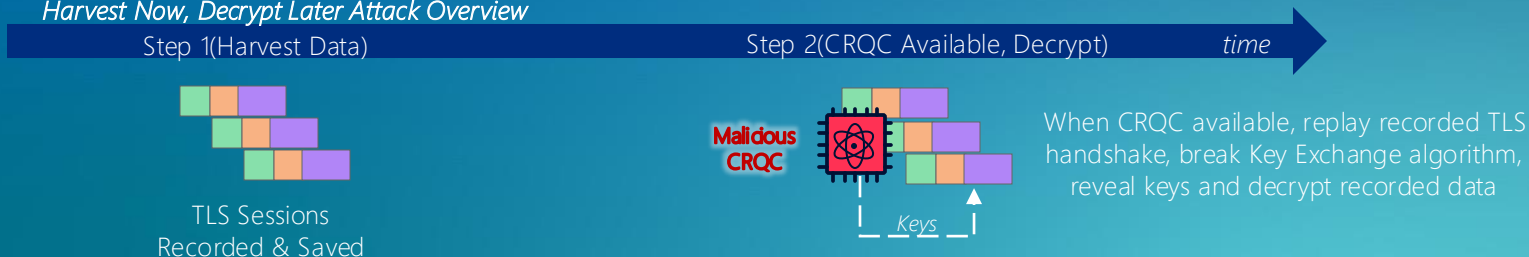


Zero-day
vulnerability

Harvest Now Decrypt Later (HNDL) attack

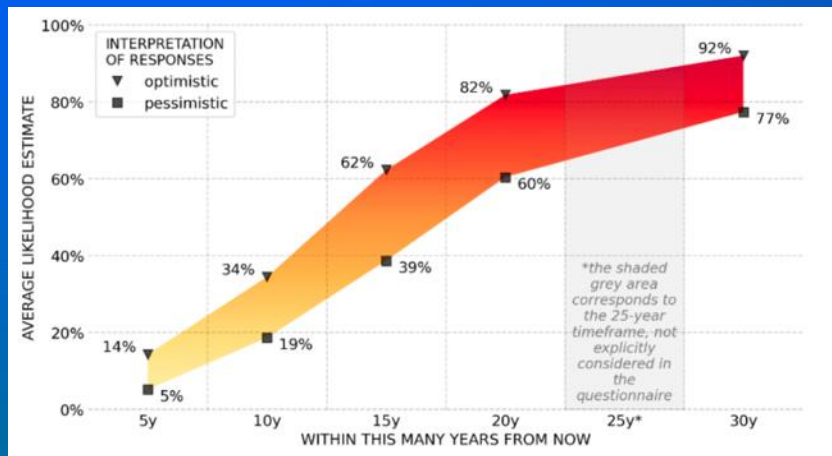


Harvest Now, Decrypt Later Attack Overview

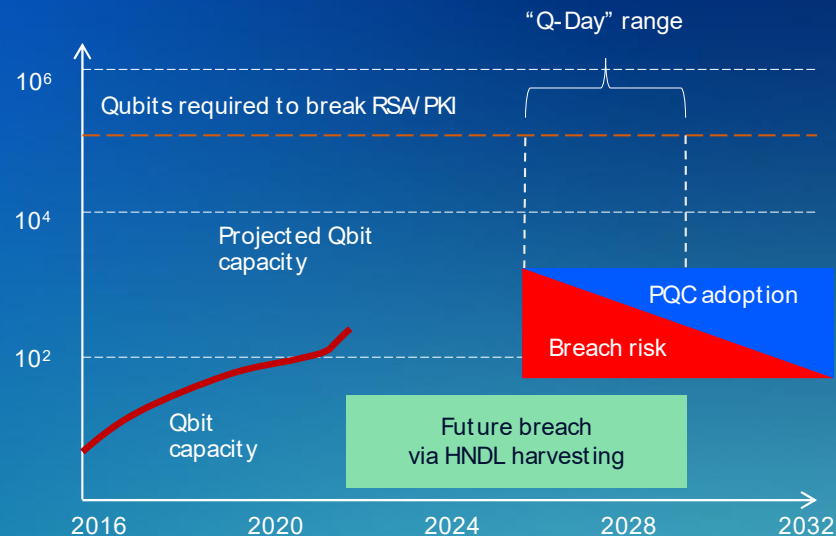


Quantum threat timeline

Likelihood of a Quantum Computer breaking RSA-2048 in 24h (2024)



Expert Survey Source: Global Risk Institute, Quantum Threat Timeline Report 2024



The key question: when is Q-Day?
Estimates vary ... some predictions of as early as 2030!

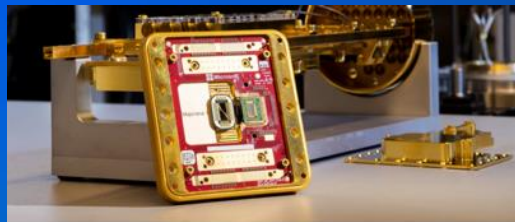
Quantum computers

Where we are today ...

Comparison Table: Leading Quantum Computers (2025)

Source: <https://makb183.com/top-10-most-powerful-quantum-computers-in-the-world/>

Rank	Company	System Name	Qubits
1	IBM	Condor	1,121
2	D-Wave	Advantage 2	7,000+
3	Google	Quantum AI	100+
4	Xanadu	X-Series	216
5	IonQ	Aria	32
6	Intel	Tunnel Falls	12
7	Rigetti	Aspen-M-3	80
8	Amazon	Braket	Various
9	Microsoft	Azure Quantum	Various
10	Baidu	Quantum Leaf	10



Microsoft's Majorana 1 chip carves new path for quantum computing

Meet Willow, our state-of-the-art quantum chip

Dec 09, 2024
4 min read

Our new chip demonstrates error correction and performance that paves the way to a useful, large-scale quantum computer

Hartmut Neven
Founder and Lead, Google Quantum AI

Read AI-generated summary

Share



We should not expect to be publicly informed about the existence of the first cryptographically relevant quantum computers (CRQCs)!

2033+

Deliver quantum-centric supercomputers with 1,000's of logical qubits.

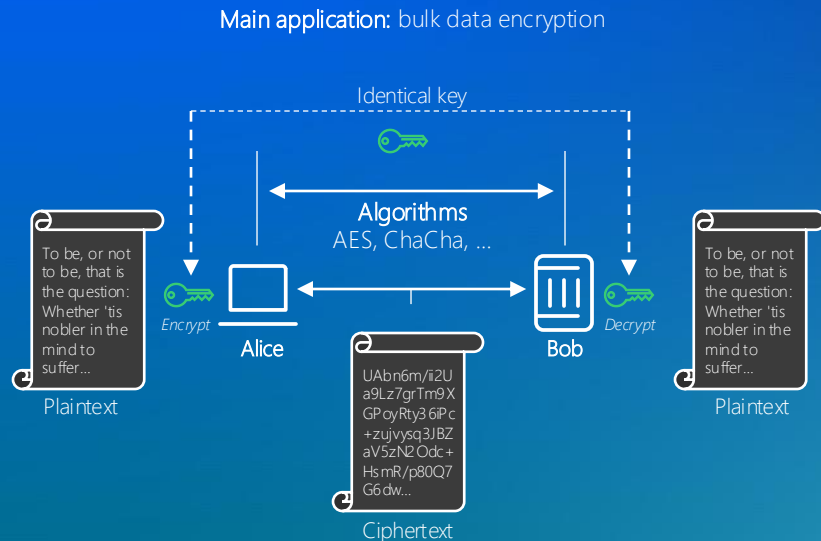
Beyond 2033, quantum-centric supercomputers will include thousands of qubits capable of running 1 billion gates, unlocking the full power of quantum computing.

Agenda

1. Quantum computing
2. Impact of quantum computing on cryptography
3. The post-quantum future

Symmetric cryptography

Overview of operation



Static applications

suitable for manual or controlled configuration



Lower scale of endpoints

limited by the need for explicit configuration



Large traffic volumes

fast encryption able to handle large amounts of data

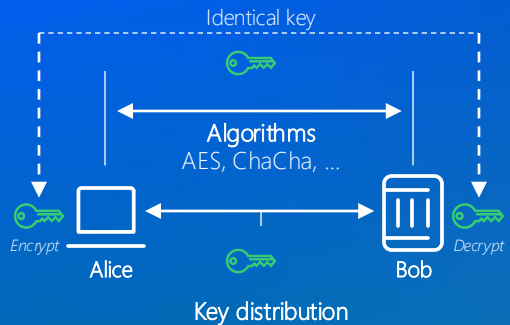


Key distribution challenge

secure key distribution is a major challenge

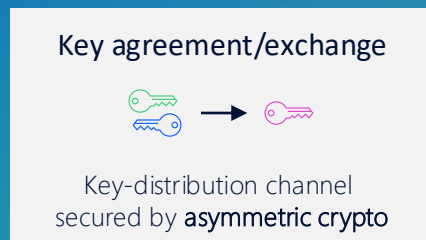
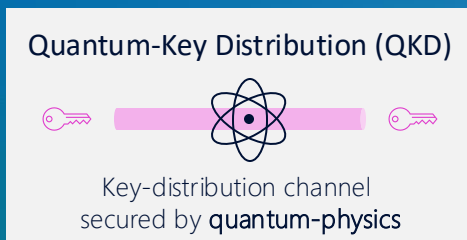
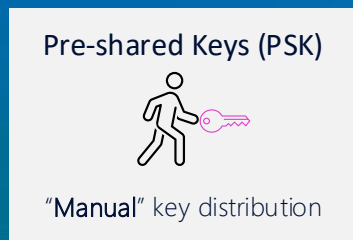
Symmetric cryptography

Key distribution, strength and cipher



Single biggest challenge

How to ensure that both of the communicating parties can securely exchange or agree on the encryption key



Key strength

Function of:

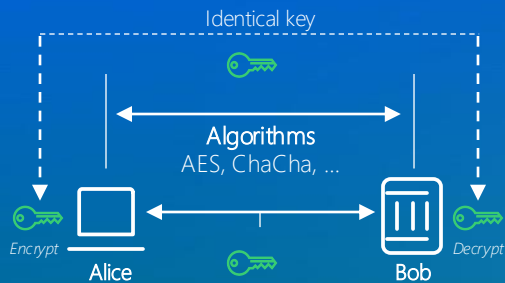
- Size of the key
- Method of key generation and resulting entropy
- Process of key exchange
- Key management

Advanced Encryption Standard (AES)

- A symmetric encryption algorithm used for securing sensitive data
- Symmetric encryption means the same secret key is used for both encryption and decryption
- AES is computationally efficient, making it suitable for a wide range of applications

Symmetric cryptography

Impact of quantum computing



The Quantum Threat

Grover's algorithm

- Devised by Luv Grover in 1996
- Also known as the quantum search algorithm
- Finds with high probability the unique input to a black box function that produces a particular output value, using $\sqrt{N}$ evaluations. In other words, it reduces time to brute-force a key from $O(N) \rightarrow O(\sqrt{N})$ i.e. provides *quadratic speedup*
- Classical computers cannot solve this in fewer than $O(N)$ as one has to check half of the domain to get a 50% chance of finding the right input



The Solution

Double the key size just to be safe!

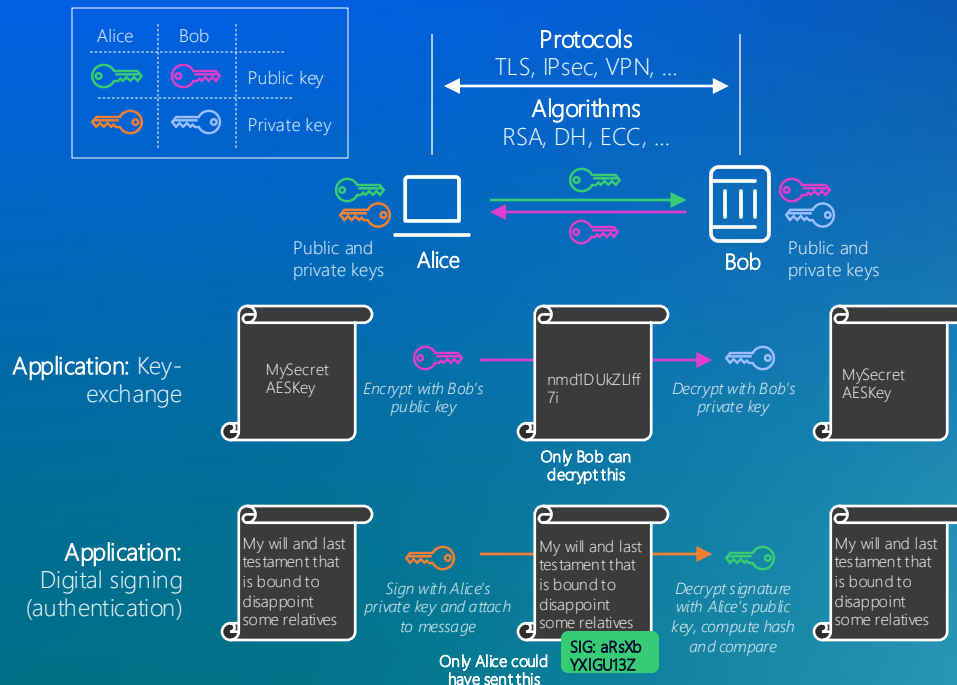
AES128 → AES256
SHA256 → SHA512

However, even this is not required since in real environments it is quite likely that Grover's algorithm will provide little or no advantage in attacking AES and AES-128 will be secure for years to come.

Asymmetric (public key) cryptography

Overview of operation

Main applications: Key-agreement, authentication



Dynamic environments
suitable for client-server applications



Larger scale of endpoints
suits dynamic, on-demand requirements



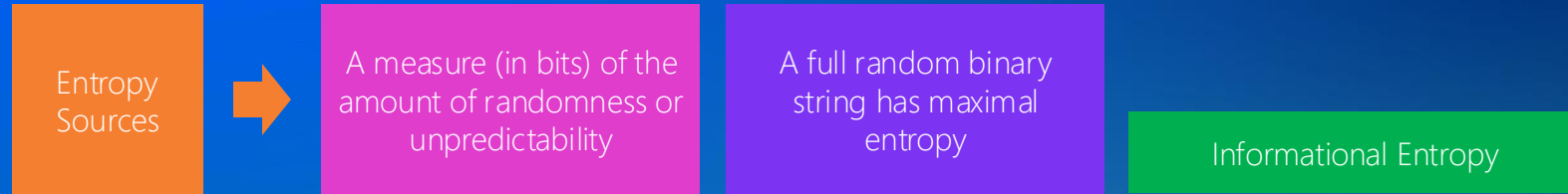
Small traffic volumes
fast encryption able to handle large amounts of data



Solves the challenge of key distribution
public/private key pair derived mathematically

Asymmetric (public key) cryptography

How it works



Informational Entropy: a function of deterministic algorithms and seed value(s) used to generate sequences of numbers that appear random

RSA → prime factorization is given by;

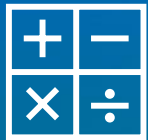
From two large prime numbers p and q , calculate $N = p \cdot q$

Then the totient T is calculated $T = (p-1) \cdot (q-1)$

Alice's Public key E_a is calculated by $T \pmod{E_a} \neq 0$

Alice's Private Key D_a is calculated by $(D_a \cdot E_a) \pmod{T} = 1$

*It's easy to work out $N = p \cdot q$.
However, given N , it is extremely difficult to determine p and q (the problem of integer factorization), provided they are sufficiently large.*



DH, ECDSA or ECDH → Discrete logarithm is given by;

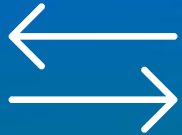
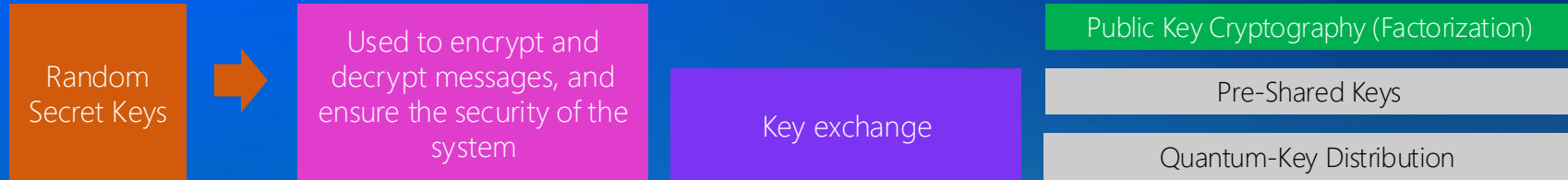
From a large prime number p , g , a generator of p and a random number X_a (Alice's private key),

Alice's Public key E_a is calculated by $E_a = g^{X_a} \pmod{p}$

Using Bob Public key E_b , the Shared Secret Session key S is calculated by $S = E_b^{X_a} \pmod{p}$

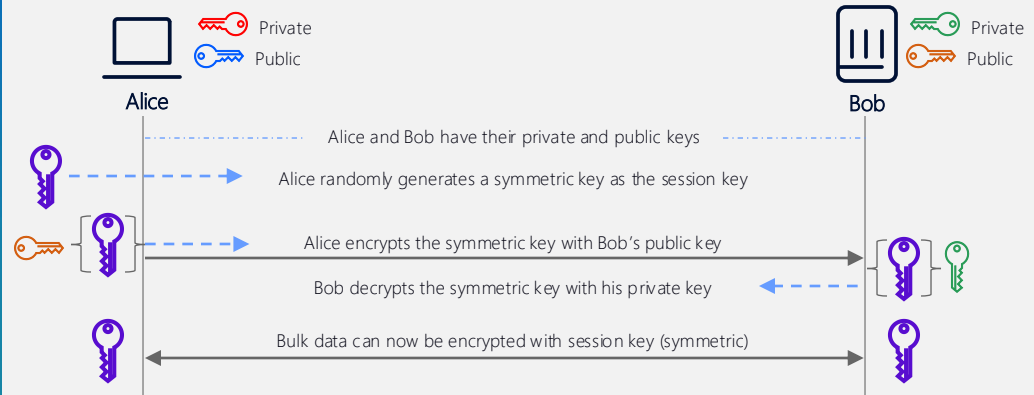
Key exchange

Asymmetric (public key) cryptography



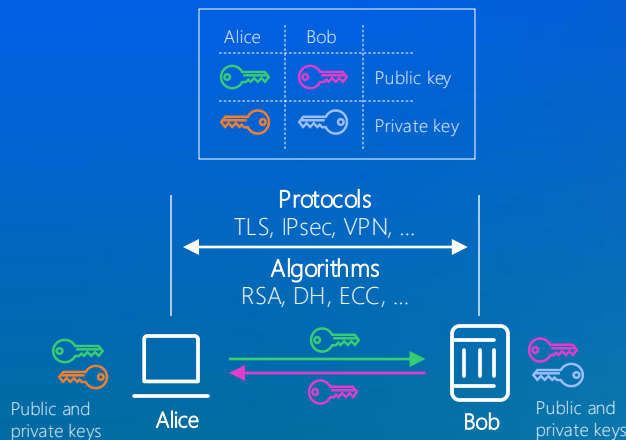
Key exchange permits the information exchange with asymmetric encryption to enable two parties with a symmetric key as session key to cipher in-flight bulk information.

Simplified example with RSA (confidentiality)



Asymmetric (public key) cryptography

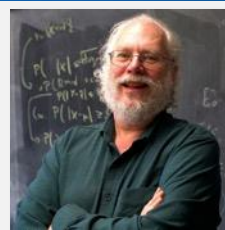
Impact of quantum computing



The Quantum Threat

Shor's algorithm

- Developed in 1994 by the American mathematician Peter Shor
- Quantum algorithm for finding the prime factors of an integer.
- RSA → prime factorization
- DH, ECDSA or ECDH → Discrete logarithm
- Estimate: to break RSA 2048, in an ideal world, one needs about 4,000 logical qubits and 100 million gates (*today: 100s of qubits and 1000s of gates*).



Breaks classical public key cryptography

The Solution

Design new quantum-resistant algorithms!

=> Post-Quantum Cryptography (PQC)

Agenda

1. Quantum computing
2. Impact of quantum computing on cryptography
3. The post-quantum future

Quantum-safe cryptography - the post-quantum future

The way forward...

Symmetric key solutions



- Based on **EXISTING** technology
- Symmetric keys & symmetric crypto
- Key distribution approach
 - Pre-shared keys (PSK)
 - Quantum Key-Distribution (QKD)
- Only encryption

Asymmetric key solutions (**PQC**)



- Based on **NEW** mathematics (Post Quantum Cryptography = PQC)
- Public Key Cryptography
- Key agreement approach (protocols)
- Authentication and encryption

QKD and PQC are seen as complementary and will co-exist
in the post-quantum cryptography toolkit

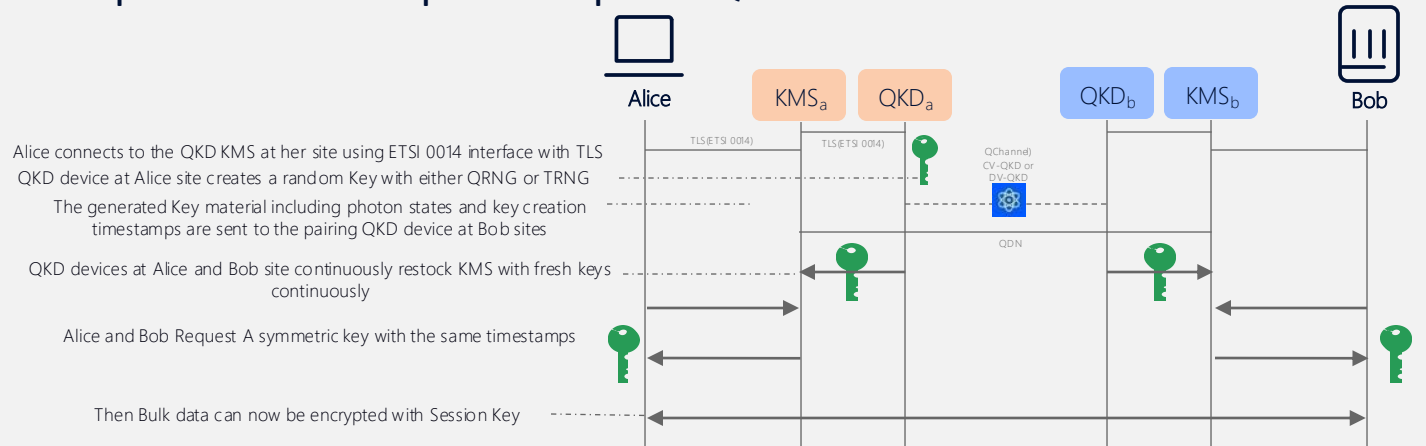
Quantum Key Distribution (QKD)

QKD: theoretically (provably) secure *without making any assumptions about the computational capability to crack it*

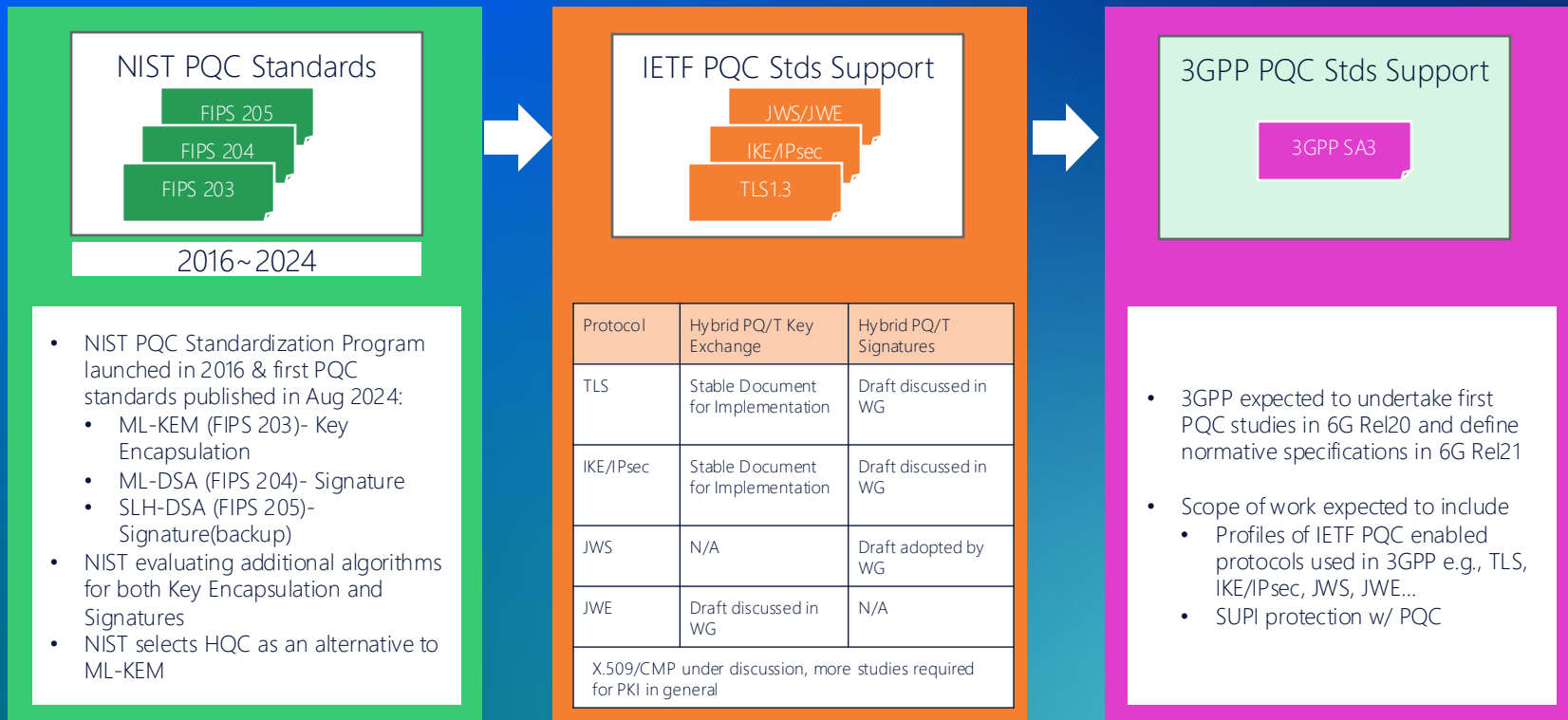
Quantum Key Distribution

- Based on principles of quantum mechanics
- Used only to produce and distribute a key (not to encrypt data itself) [can take the place of an asymmetric key exchange protocol]
- Key can then be used with a symmetric cipher
- Attempts to eavesdrop can be detected

Example of standard point-to-point QKD



PQC standardisation



Policy makers are responding to the security impact



Is your cybersecurity ready to take the quantum leap?



EU urged to prepare for quantum cyberattacks with coordinated action plan



The US is worried that hackers are stealing data today so quantum computers can crack it in a decade*



Singapore to build national quantum-safe network that provides robust cybersecurity for critical infrastructure

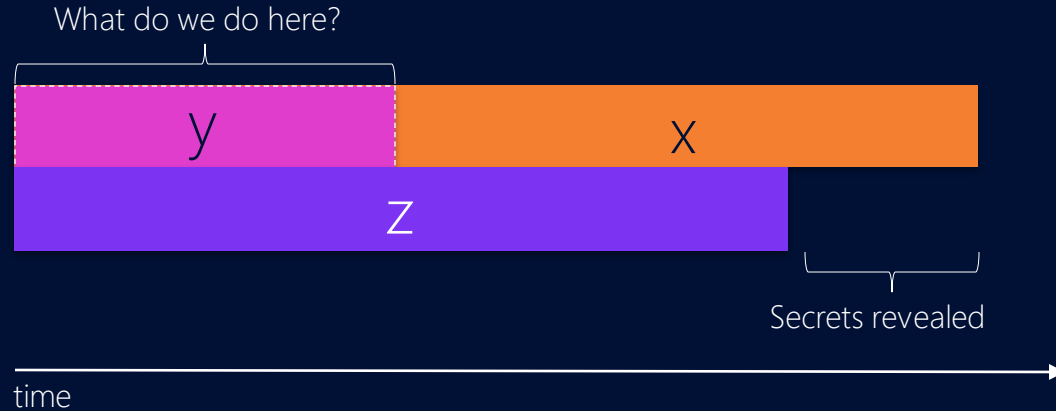


South Korea plans large scale quantum cryptography adoption

*The US government is starting a generation-long battle against the threat next-generation computers pose to encryption.

Assessing the threat

Mosca's theorem of cybersecurity in the quantum era¹



If $x + y > z$, then start worrying

x: time we want to keep our systems secure

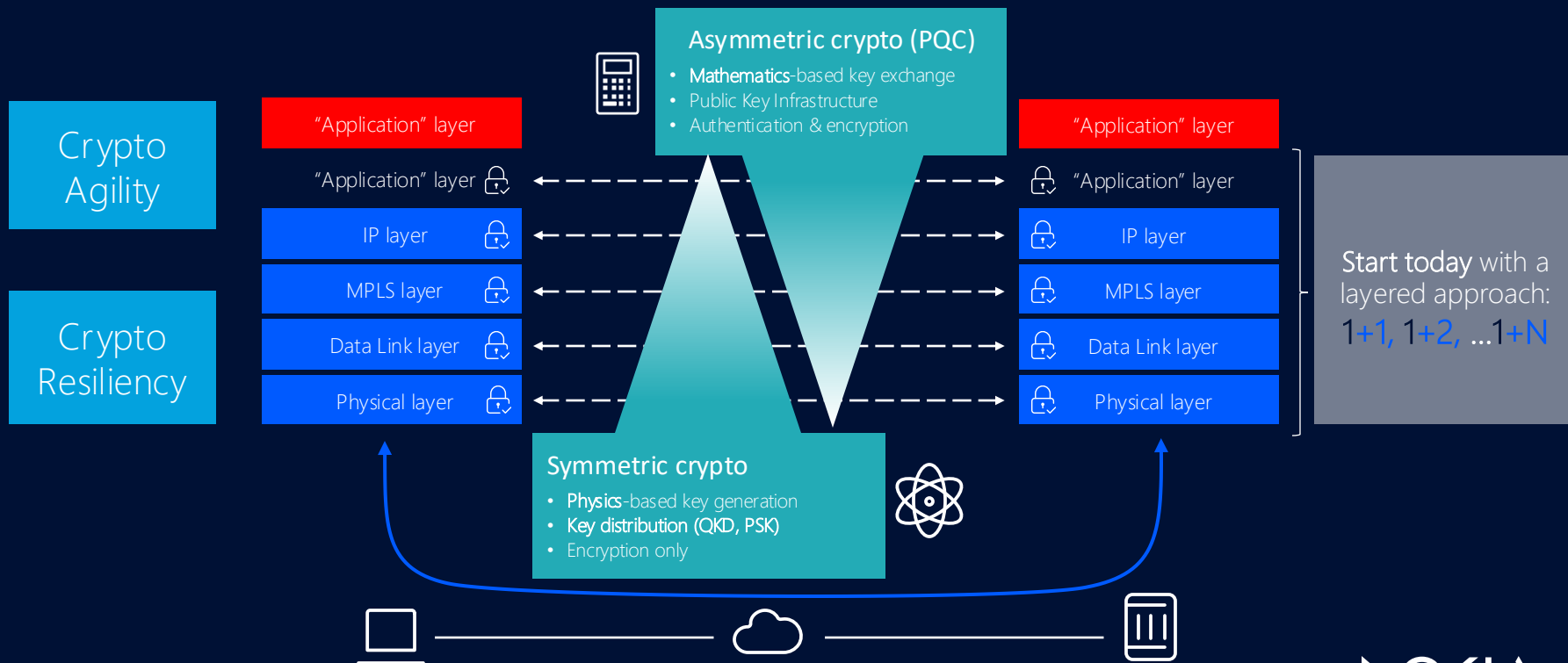
y: time to deploy a quantum-safe migration plan

z: time to build a large-scale quantum computer (2030s?)

[1] <https://eprint.iacr.org/2015/1075.pdf>

Strategy for the way forward: defense-in-depth approach

Demands multi-layered approach using asymmetric and symmetric cryptography



NOKIA