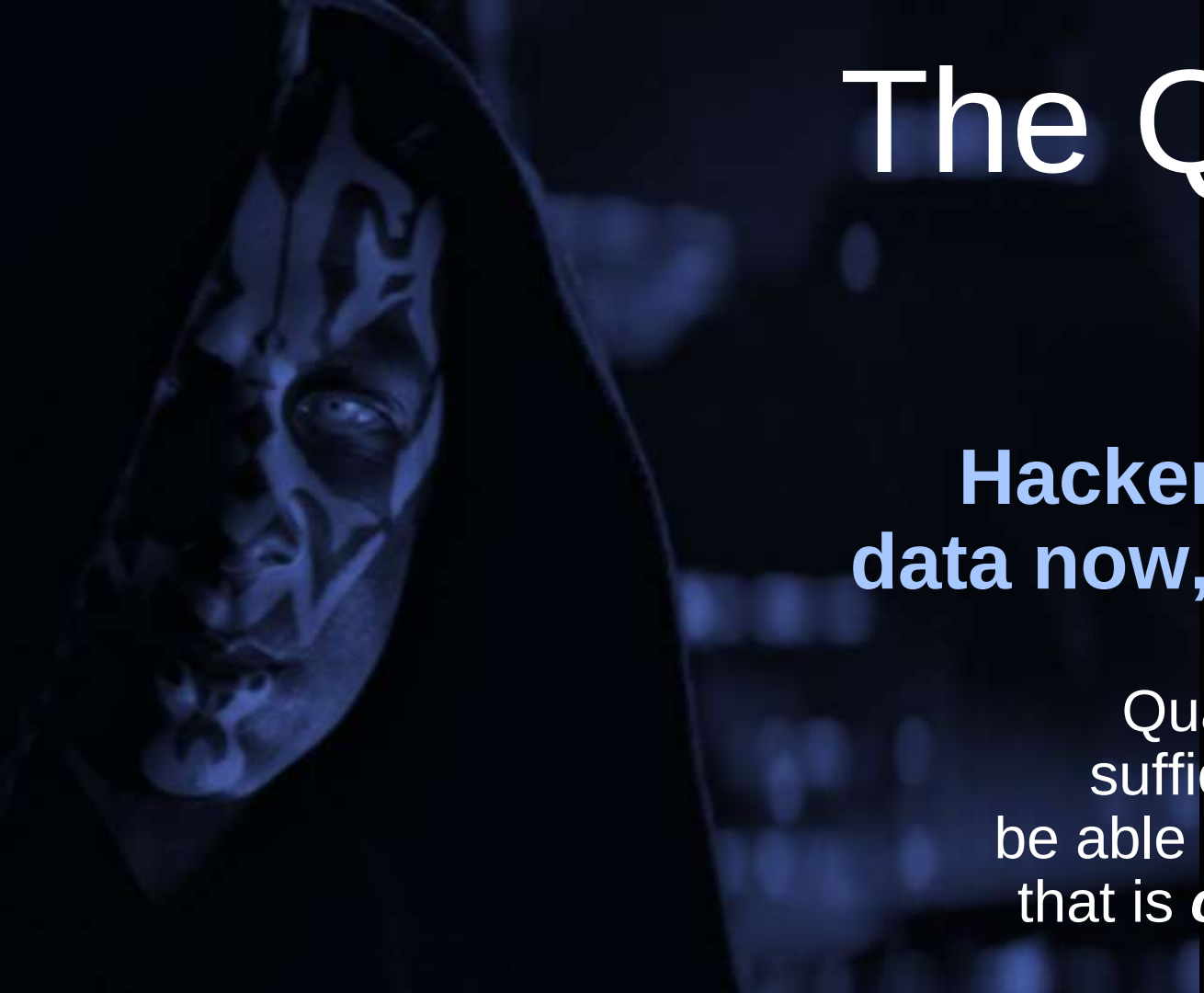
An Introduction to Quantum-Safe

Securing today's data and systems against tomorrow's computers

Dwaine Snow
WW Technology Sales Enablement
Cyber Resiliency
dwsnow@us.ibm.com



The Quantum Menace

Hackers are stealing data now, *to crack later*

Quantum computers of sufficient scale will likely be able to compromise data that is ***currently*** protected

Quantum computers

Can perform certain mathematical computations exponentially faster than today's computers – making current encryption standards obsolete

With quantum computers, hackers will be able to forge transactions and change legal history by manipulating data that they gained access to using forged digital signatures

Quantum-safe is **NOT** just about the data

Ensure that the system (i.e. firmware, OS, VM, container, application) has not been hacked, altered, updated, damaged, or modified in any way since it was created by the manufacturer, installed, and/or started

Quantum-safe

is about protecting
data and systems
from the advent of
quantum computers
and the power
they will provide

System level security

Workloads, VMs, and containers

OS security

Hardware and firmware security

Secure VMs & Containers

Signed images and files

Runtime verification of workload files

OS, LPAR, VM, container isolation

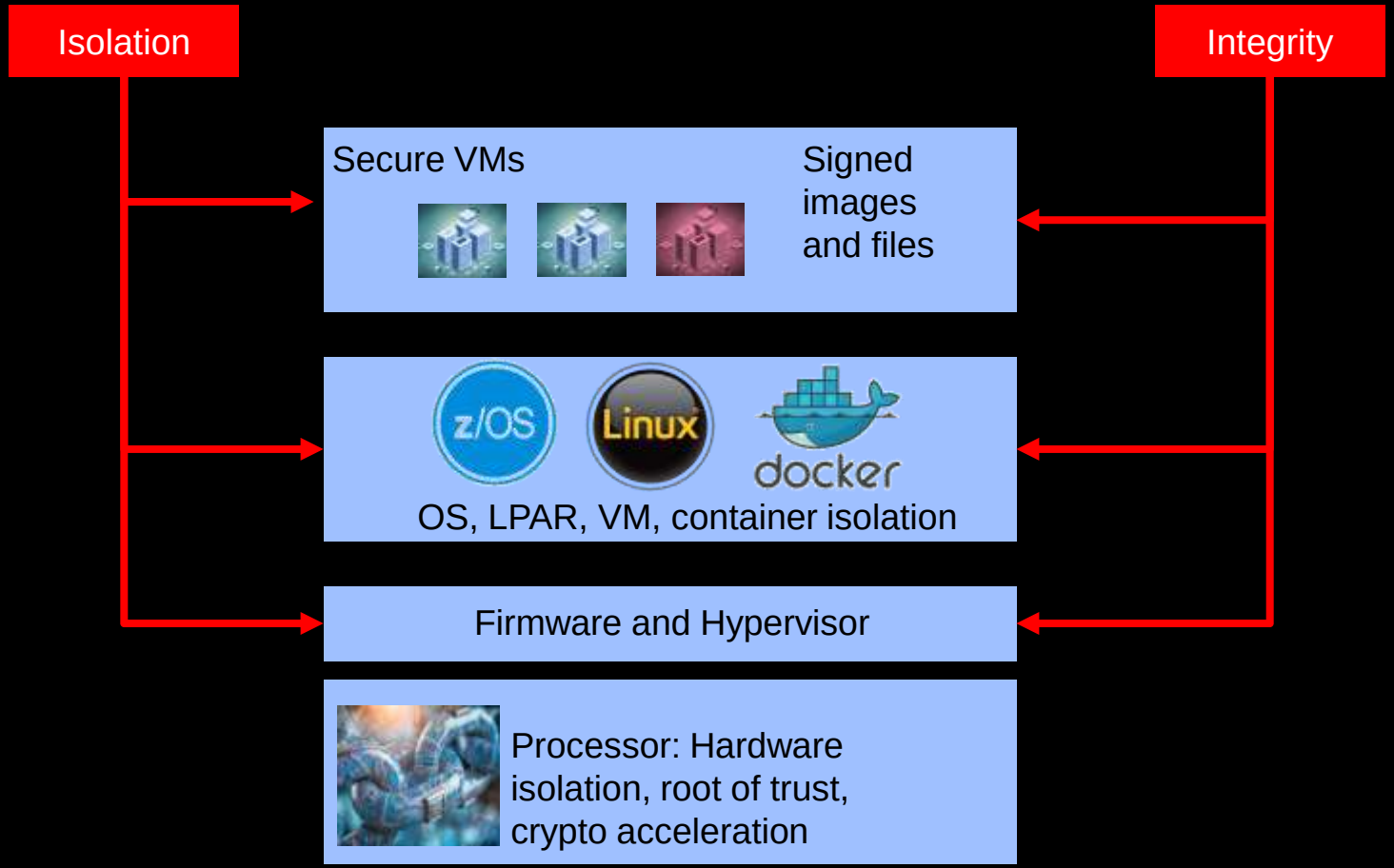
Runtime verification of OS files

Firmware and Hypervisor

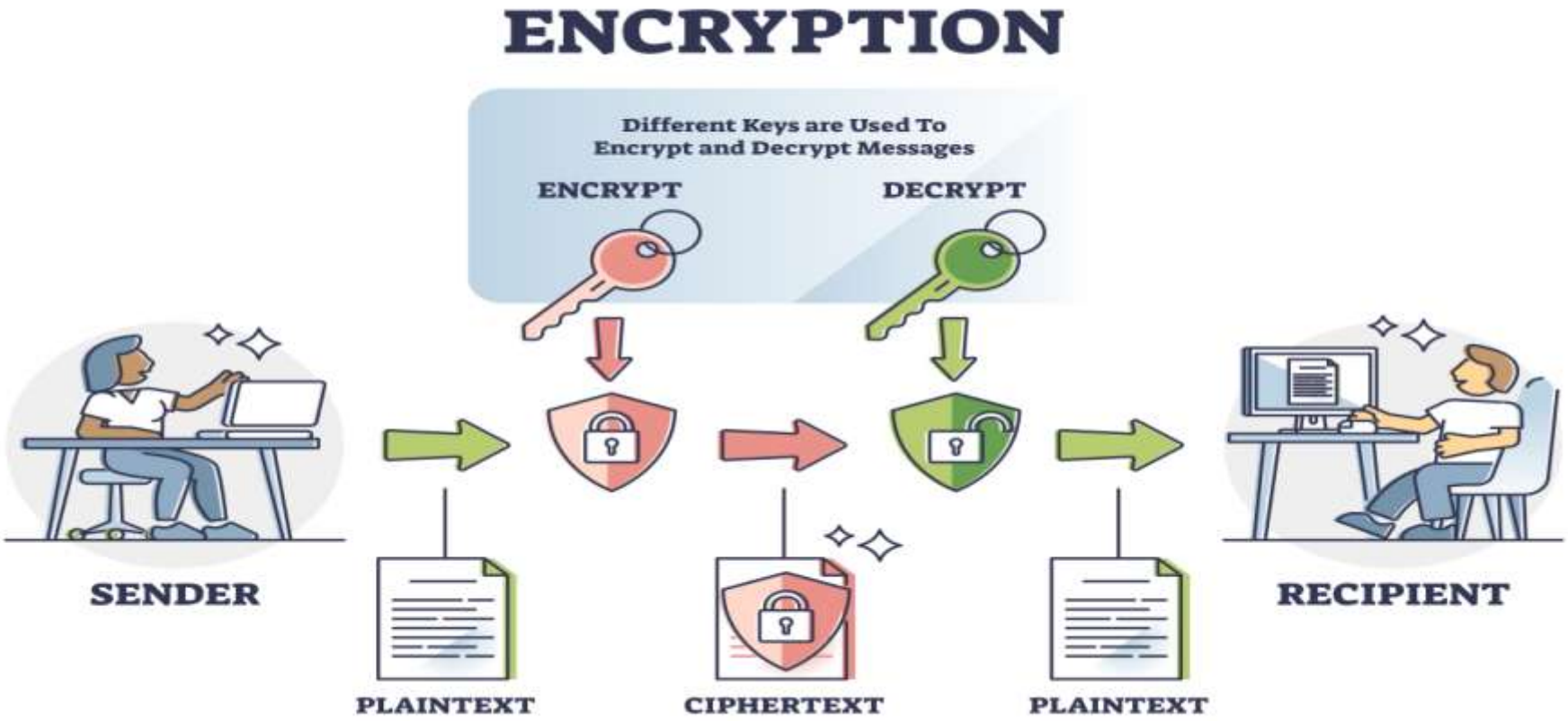
Processor: Hardware isolation, root of trust, crypto acceleration

Boot time Integrity

System level security must provide



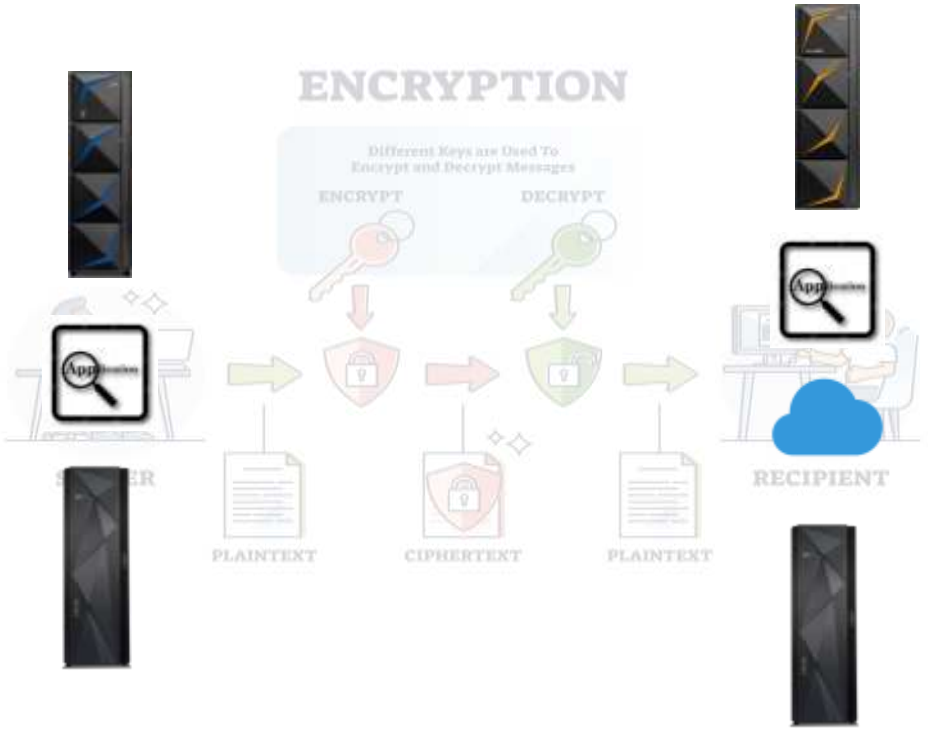
Data security is all about encryption



Data need not be sent from one person to another to be stolen

- Server to storage
- Server to server
- App to app
- Server to cloud
- Storage to cloud

- Data can also be stored on disk/tape, or even in the cloud, and “stolen” by a hacker



The KEY(s) to the kingdom

The secret or encryption key grants clear access to the file/data

So that the contents can be read, shared, sold, held for ransom, …

Encryption Keys

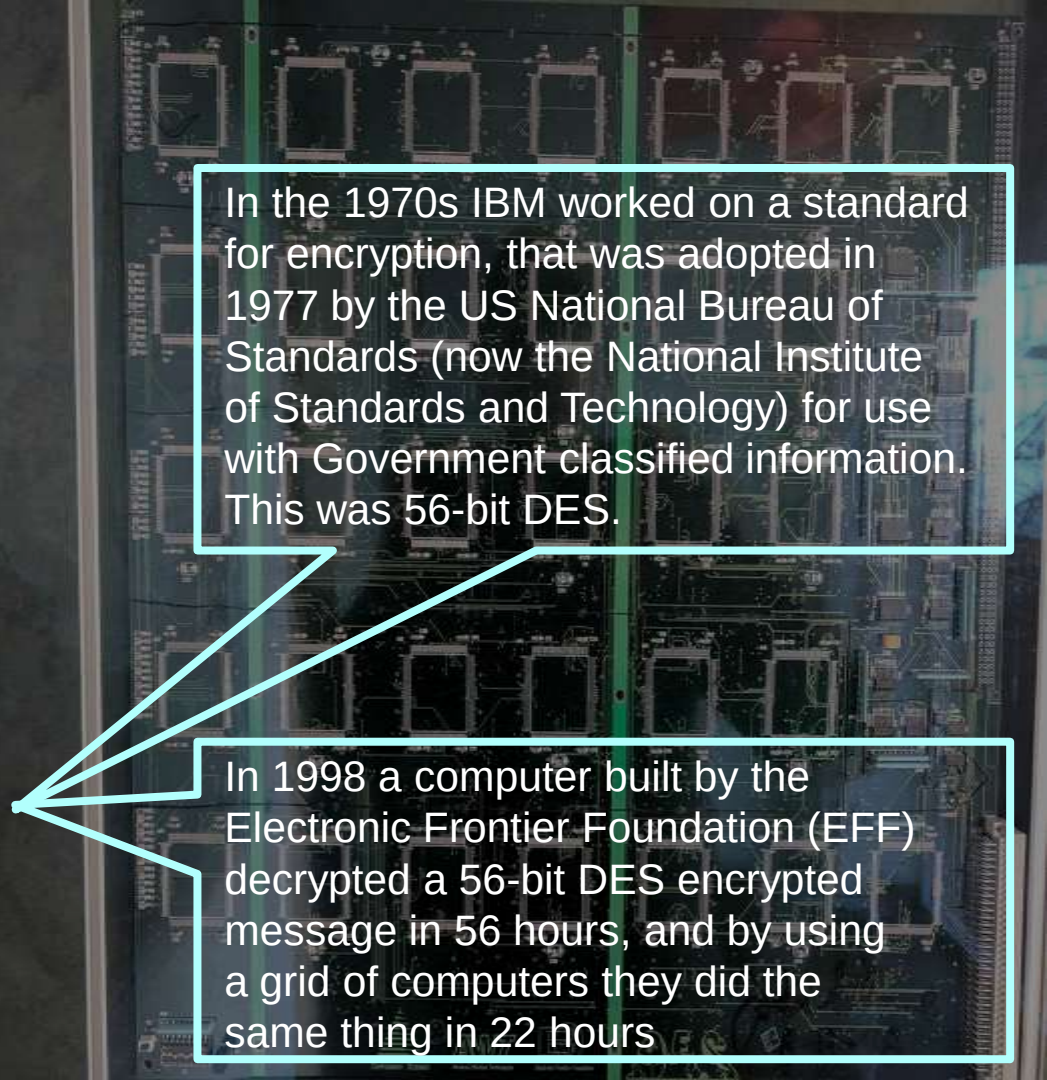
The key length determines the number of possible "combinations" and ultimately the time to break it

Number of bits	Distinct patterns
1	0 1
2	00 01 10 11
3	000 001 010 011 100 101 110 111

Key Size	Possible combinations
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	4.2×10^{9}
56-bit (DES)	7.2×10^{16}
64-bit	1.8×10^{19}
128-bit (AES)	3.4×10^{38}
192-bit (AES)	6.2×10^{57}
256-bit (AES)	1.1×10^{77}

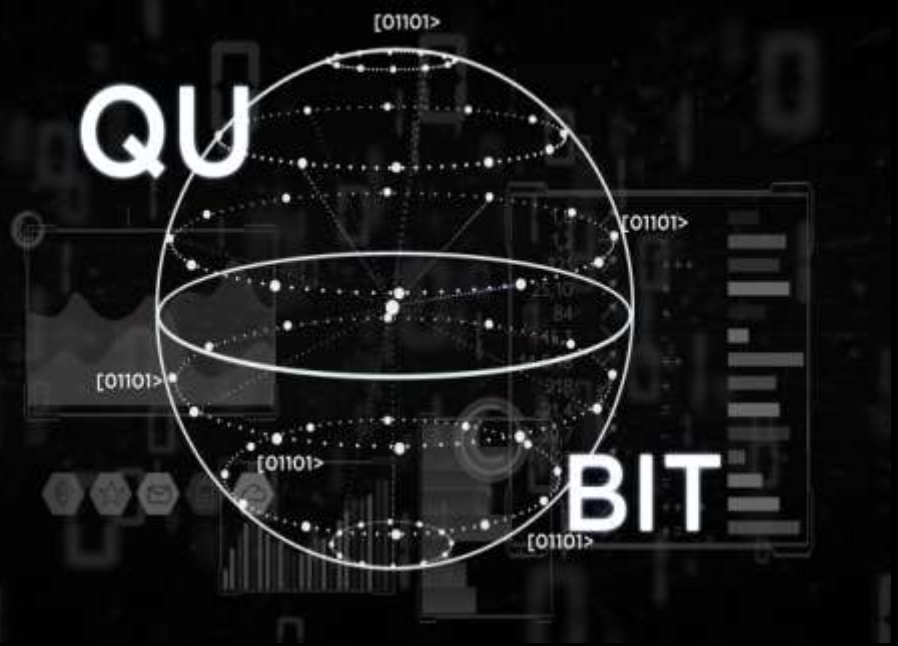
Encryption Keys

Key Size	Possible combinations
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	4.2×10^{9}
56-bit (DES)	7.2×10^{16}
64-bit	1.8×10^{19}
128-bit (AES)	3.4×10^{38}
192-bit (AES)	6.2×10^{57}
256-bit (AES)	1.1×10^{77}



In the 1970s IBM worked on a standard for encryption, that was adopted in 1977 by the US National Bureau of Standards (now the National Institute of Standards and Technology) for use with Government classified information. This was 56-bit DES.

In 1998 a computer built by the Electronic Frontier Foundation (EFF) decrypted a 56-bit DES encrypted message in 56 hours, and by using a grid of computers they did the same thing in 22 hours



Traditionally, a bit is either a 0 or a 1

There are two possible values

A Qubit can be all possible values, at the same time

For a bit wise value, it can be both a 0 AND a 1

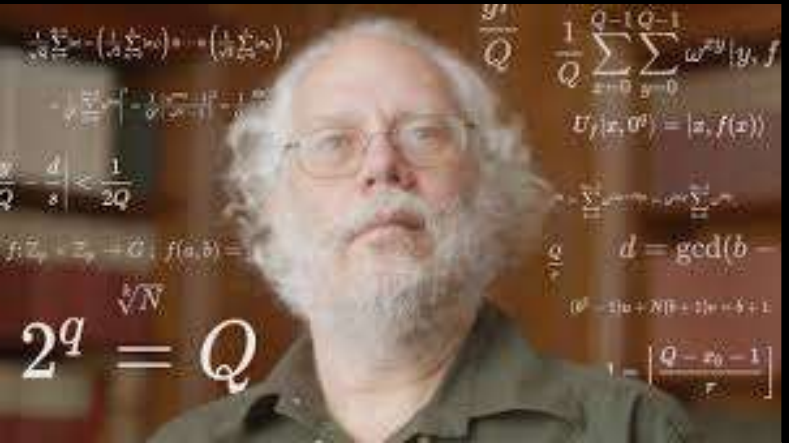
Two Qubits can be 00, 01, 10, and 11- all at the same time

The current IBM 127 Qubit system, can have 2^{127} possible bit combinations – all at the same time!

Breaking 2048 bit encryption in 8 hours…

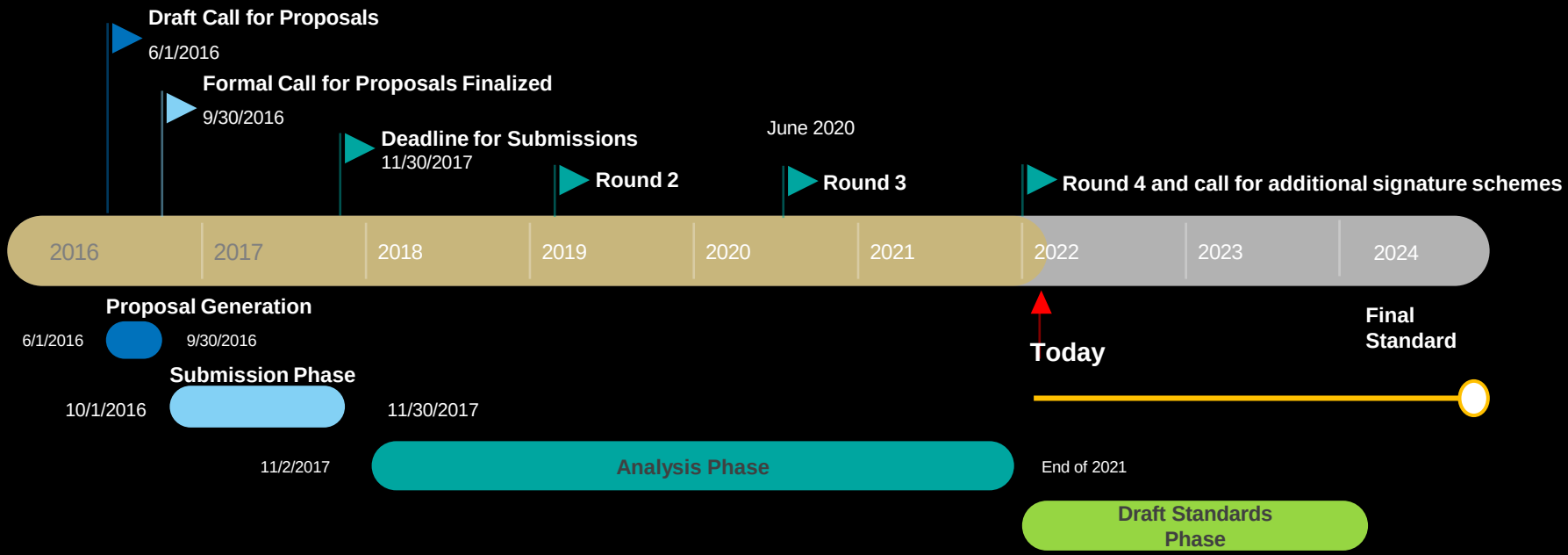
.

In 1994 Peter Shor created a quantum algorithm that efficiently solves integer factorization problems, all it needs is a powerful enough quantum computer to run it



Without quantum-safe cryptography,
all information, whether transmitted
on public channels or stored
on premises,is at risk!

NIST Standardization for Quantum-Safe / Post Quantum Cryptography



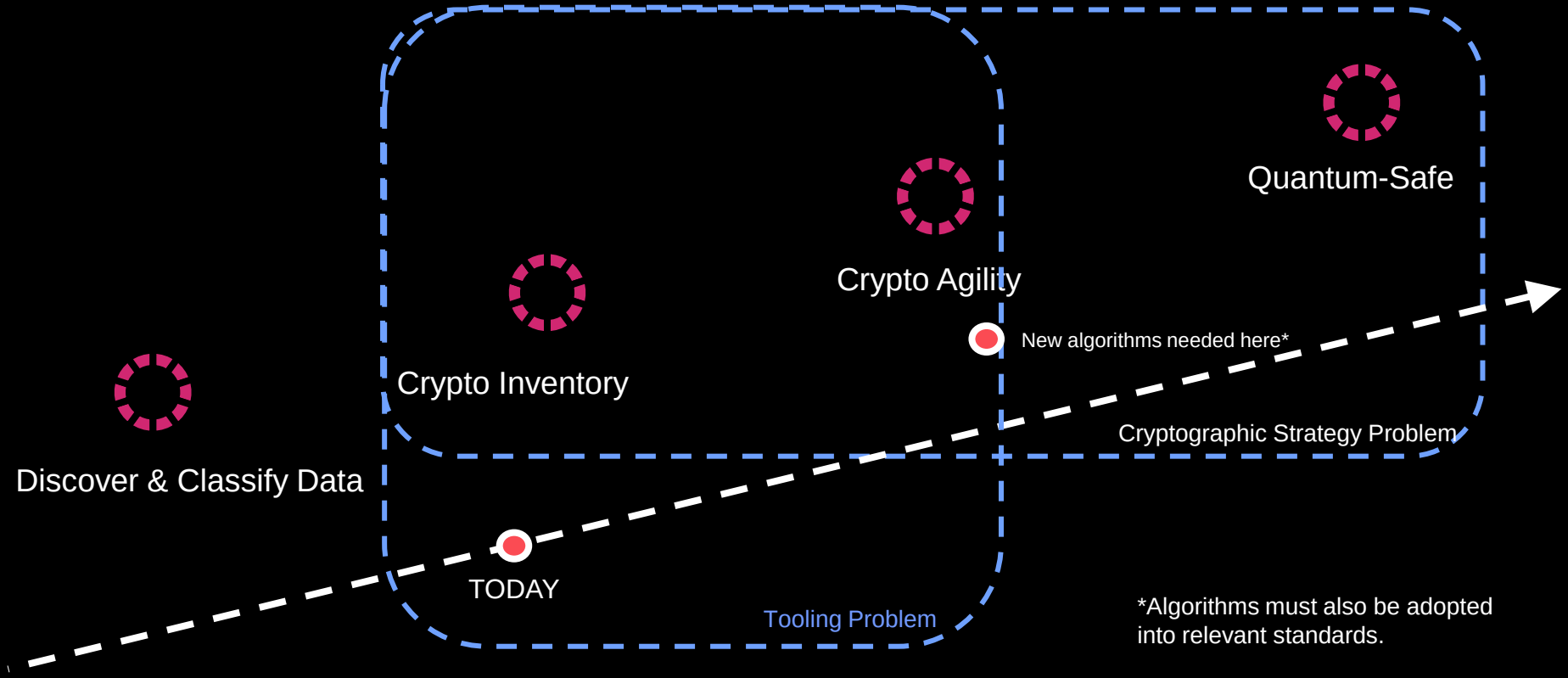
Start now!

- Critical to begin planning for the replacement of hardware, software, and services that use public-key algorithms now
- Be ready to adopt and implement the new algorithms at the end of the standardization process
- 5 to 15 or more years following, standardization to replace most of the vulnerable public-key systems currently in use

- The protection of long-lasting secrets makes it urgent that actions be taken now or as soon as possible
- BSI is not waiting for NIST to come out with a standard to issue technical guidance
- In high security applications, hybrid schemes (use classical algorithms + quantum-safe algorithm) are required by BSI

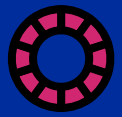
https://www.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography

Milestones on the way to Quantum-Safe Cryptography



Source: IBM Research Security Forum / Nov. 10-12, 2020

Milestones on the way to Quantum-Safe Cryptography



Discover and classify data

- Classify the value of your data and identify your “Crown Jewels”
- Identify locations of your data
- Understand your compliance requirements
- Create and manage your data inventory with defined ownership

Crypto inventory

- Identify how your data is encrypted
- Create your cryptography inventory (containing certificates, encryption protocols, algorithms, key lengths, etc.)
- Manage your cryptography inventory and the lifecycle of certificates, encryption keys, etc.

Crypto agility

- Define and implement processes to update/replace cryptography with well-defined lead-times
- Take all dimensions of crypto agility into account
- Test your crypto agility

Quantum-safe

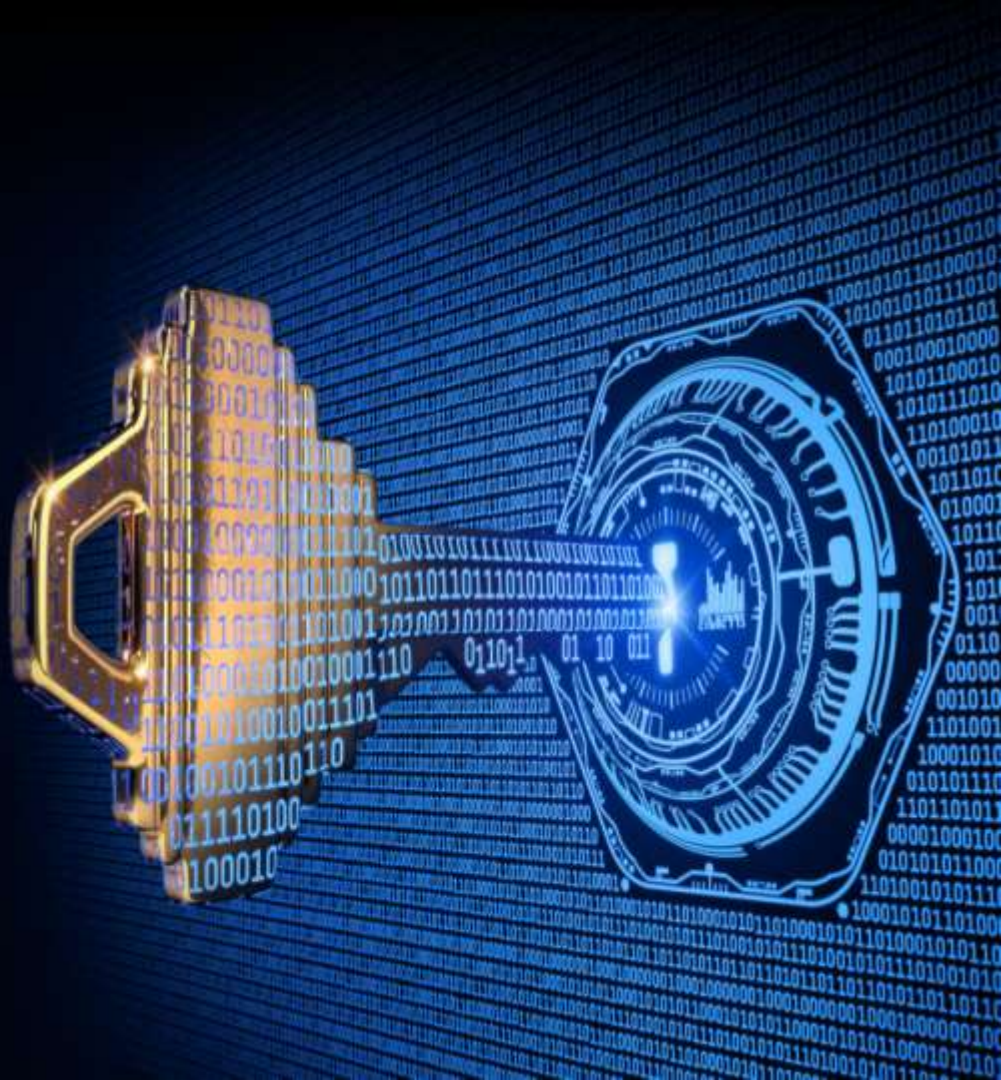
- Implement quantum-safe cryptography algorithms
- Understand the performance impact of quantum-safe crypto on the business

Next generation systems must

Leverage quantum-safe technology throughout

- From basic HW initialization, through multiple layers of firmware, quantum-safe cryptographic technology protections need to be leveraged
- The system must provide the capabilities with which the system layers such as operating system, virtualization, middleware, and applications can make themselves quantum-safe over time

Your future needs to be Quantum-safe



IBM Quantum-Safe benefits

Provide core infrastructure technology necessary to prepare your business to resist quantum attacks

Provide tooling to aid in crypto discovery and crypto application and ecosystem modernization

Protect keys and applications using hybrid schemes as recommended by industry organizations

Provide the quantum-safe capabilities needed to protect long lasting secrets

#LetsCreate

Safety and security in the quantum era


IBM