An Introduction to Quantum Key Distribution (QKD) and Quantum-Resistant Cryptography

TOSHIBA

Robert Woodward & Andy Simpkins

2023-11-26, Debian Miniconf – Cambridge UK

TOSHIBA

Outline

1. Background: Why care about “Quantum”?
2. Introduction to Quantum Key Distribution (QKD)
3. QKD Deployments & Quantum Networks
4. Quantum-Resistant Cryptography
5. Impact within Debian

TOSHIBA

Communications in the Age of Quantum Computing

Background

00

Quantum at Toshiba

Toshiba in Cambridge:

- 1991: founded ***Cambridge Research Laboratory (CRL)*** in Cambridge Science Park
- Pioneered quantum technology research, particularly quantum communications, for decades

- 2020: new commercial division formed, launching QKD as a commercial product for quantum-safe communications

- 2023: Toshiba opened a 2nd site, the ***Quantum Technology Centre (QTC)*** housing the Development and Production facility

What is 'Quantum Technology'?

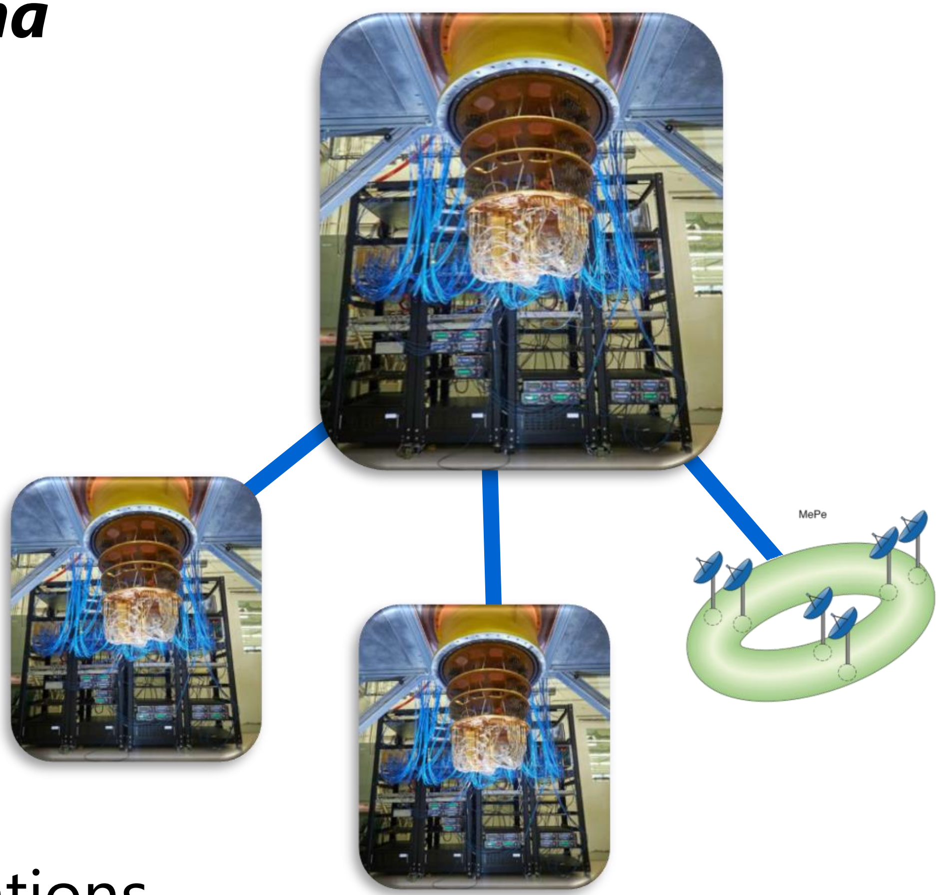
Broadly, "using quantum mechanical phenomena for new / augmented technologies, spanning computing, communications, sensing etc."

Quantum 1.0, 1900s

- Concepts: wave-particle duality & quantized atomic energy levels
- Enables lasers, transistors etc.

Quantum 2.0, 2000s

- Concepts: superposition, entanglement
- Enables quantum computing, secure communications etc.



Dowling & Milburn, Quantum technology: the second quantum revolution, DOI:10.1098/rsta.2003.1227; https://phys.org/news/2020-08-google-largest-chemical-simulation-quantum.html; Pezzè et al. Nat. Photonics 15, 74 (2021)

We are entering the age of quantum computing...

2019

NEWSLETTERS
Sign up to read our regular email newsletters

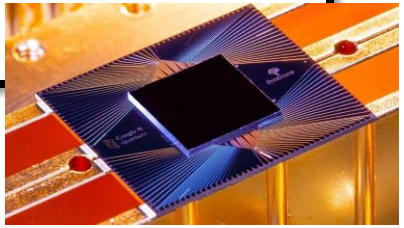
NewScientist

SUBSCRIBE AND SAVE 72%

News Podcasts Video Technology Space Physics Health More Shop Courses Events Tours Jobs Sign In Search

It's official: Google has achieved quantum supremacy

PHYSICS 23 October 2019



2021

NEWSLETTERS
Sign up to read our regular email newsletters

NewScientist

News Podcasts Video Technology Space Physics Health More Shop Courses Events

2021 in review: Jian-Wei Pan leads China's quantum computing successes

In July, the University of Science and Technology of China announced it had surpassed Google's claimed quantum supremacy achievement. China's ambitious quantum computing efforts are all under the oversight of one man, Jian-Wei Pan

2022

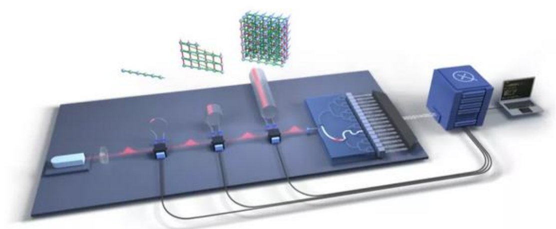
XANADU

Quantum Chip Brings 9,000 Years of Compute Down to Microseconds

By Francisco Pires published 15 days ago

Claiming quantum computational advantage over the classic-bit technologies of the world.

Comments (4)



2023

ALL ABOUT CIRCUITS

LOG IN JOIN

ARTICLES FORUMS EDUCATION TOOLS VIDEOS DATASHEETS GIVEAWAYS TECH COMMUNITIES

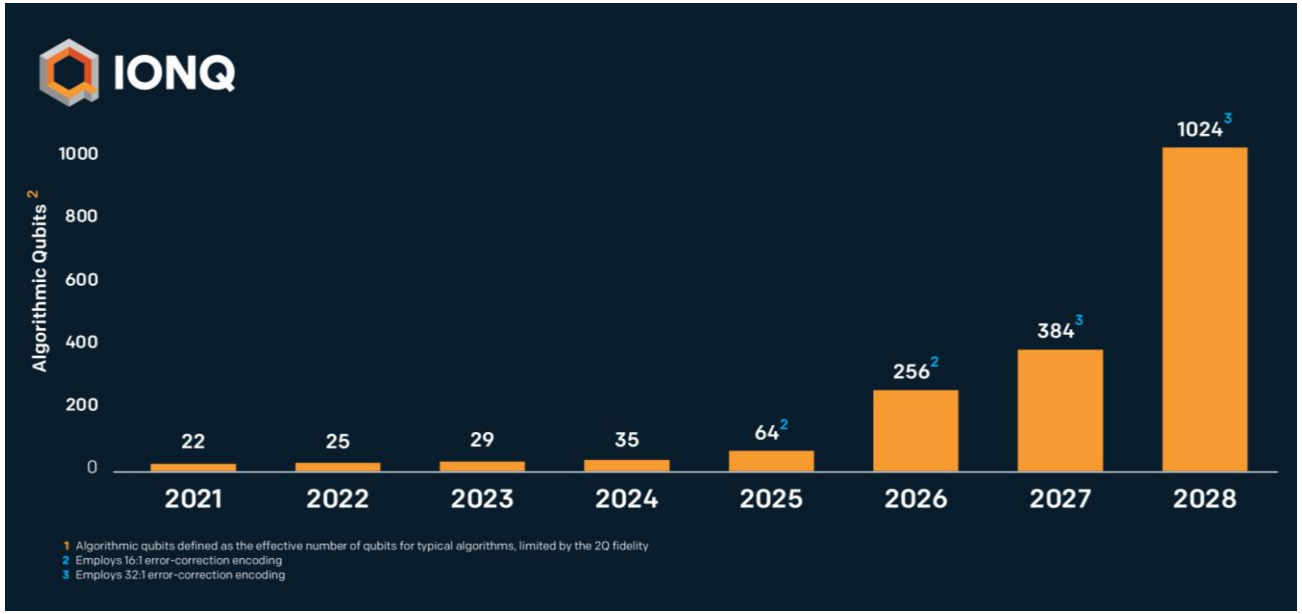
Home > News > Exclusive—IBM Shares Details of Its 400+ Qubit Quantum Processor

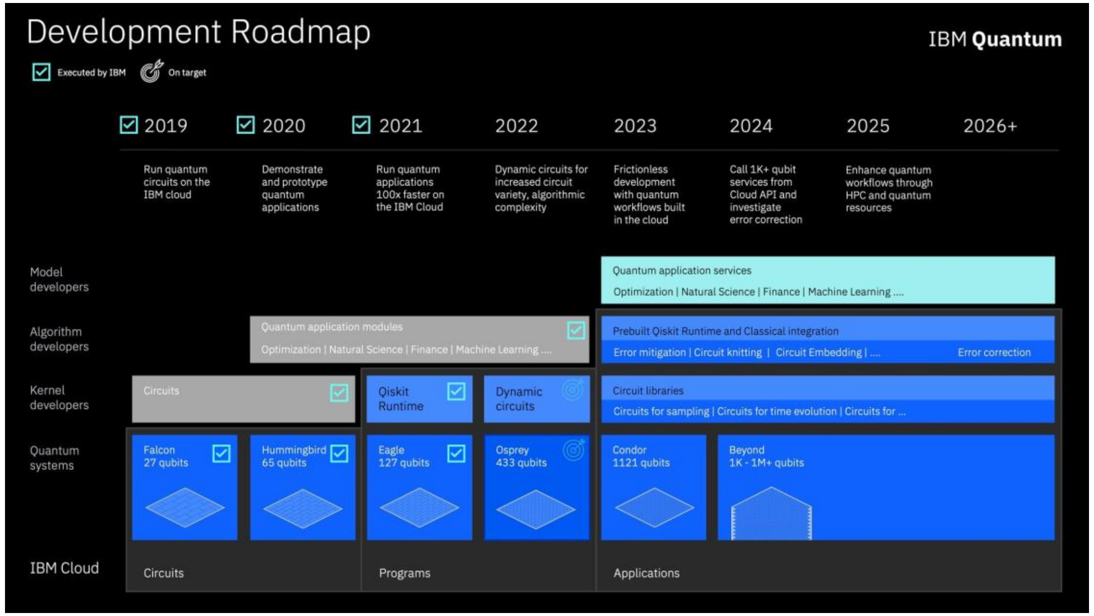
NEWS

Exclusive—IBM Shares Details of Its 400+ Qubit Quantum Processor

January 23, 2023 by Ingrid Fadelli

Progress towards large-scale quantum computers keeps accelerating





What does this actually mean?

- Quantum computers <u>are not</u> simply 'faster' computers
- Quantum computers <u>do not</u> simply perform many tasks in parallel

- Quantum computers <u>do</u> enable new types of computation, which can <u>exponentially speed-up certain tasks</u>.

BUT…

Today's cryptographic key exchange based on **public key (a.k.a. asymmetric) crypto** – assumes **limited computational power** for an eavesdropper.

Approaches like **RSA, elliptic-curve crypto etc. are "broken"** by Shor's algorithm.

reduces exponential-time computation to polynomial-time (no longer "hard" to crack)

Threat Assessment in 2023

Current ***asymmetric cryptography*** (e.g. public key exchange) is **broken** by quantum computers, since *integer factorization* & *discrete-log problem* no longer "hard"

Current ***symmetric cryptography*** (e.g. AES encryption) is **weakened** by quantum computers, but not broken (need to use longer keys).

Can we just ignore this until quantum computers become widely available?

No.

Data sent that is encrypted using current public key exchanged keys can be stored for many years, then decrypted in future. **"Harvest-now-decrypt-later" attack.**

Much data has decades-long security requirements (medical, government records etc.)

TOSHIBA

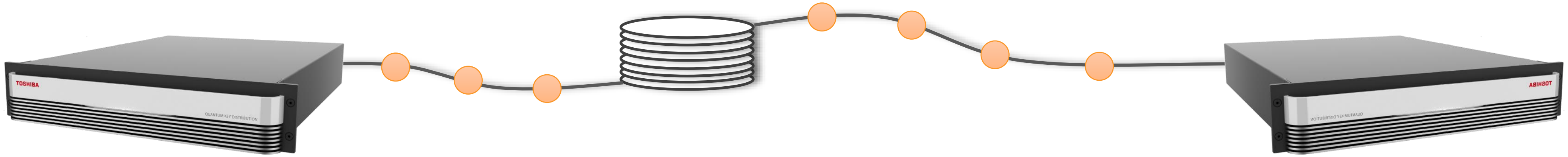
Securing point to point communications

Introduction to Quantum Key Distribution (QKD) Technology

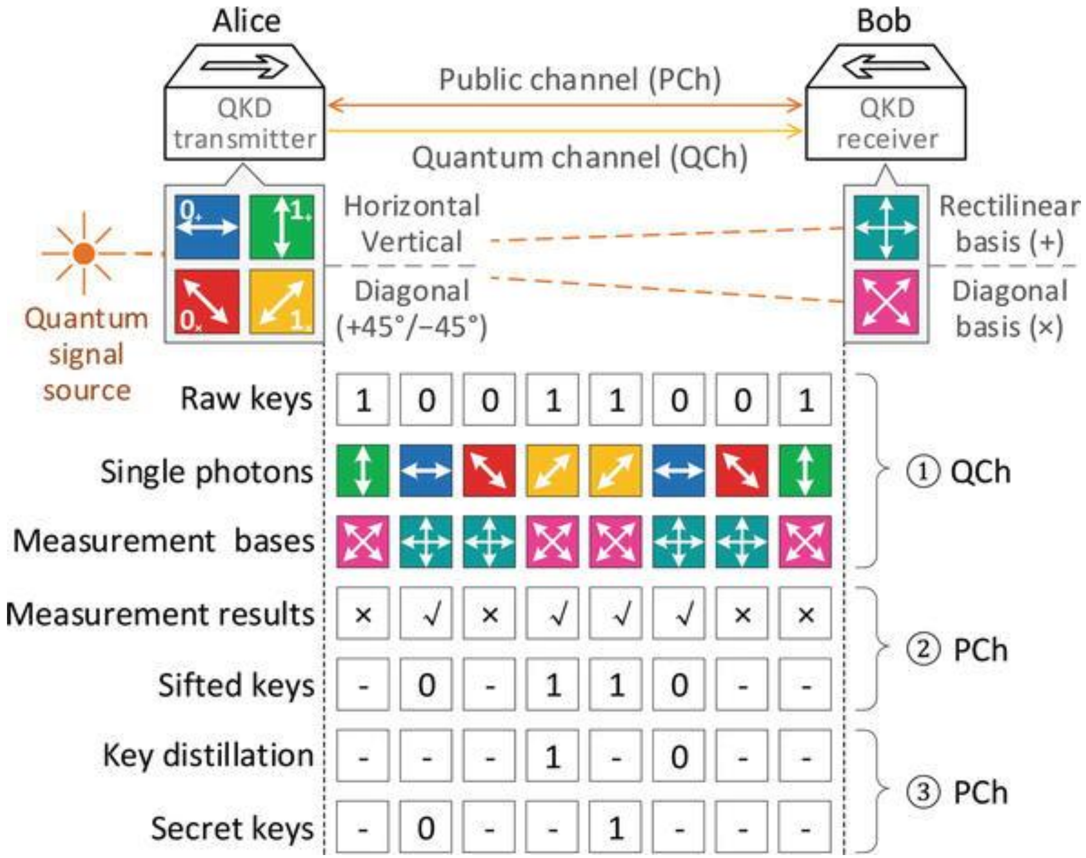
01

Introducing Quantum Key Distribution (QKD)

Quantum cryptography, specifically, quantum key distribution (QKD) is a solution.



- Exploits quantum mechanics to offer **mathematically proven** secure communication
- Encode each bit on a single photon (in superposition state of 2 bases)
- An eavesdropper observing the photon unavoidably alters the state
- Altered states are detected, identifying when an eavesdropper is present.
- Practically: eavesdropping on fibre equates to measurable noise in the quantum channel
- Provable (quantified) security, **"information theoretically secure"**



[BB84] Bennett & Brassard, 1984. Image: "Quantum Cryptography in Advanced Networks" Ed. O. Morozov (2019).

Securing communications using keys – i.e. how to use QKD?

QKD **distributes keys** between 2 remote nodes with **information-theoretic security.**

(no assumptions on attacker's computational power!)

These keys are often then used for data encryption.

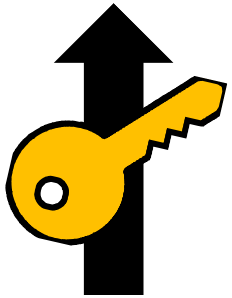
User Data

Encryptor

"Quantum-Safe"
Encrypted Data

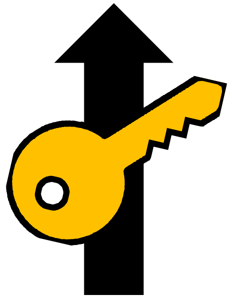
Encryptor

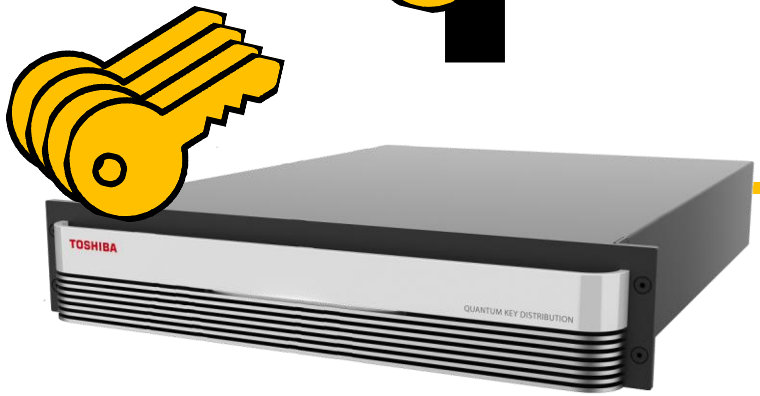
User Data



Which encryption algorithm to use?

- One-time pad (information-theoretic secure)
- AES (quantum safe *for now*)
- etc.





Communication Channel

Requirements for "Practical" QKD

To become a useful widespread technology, QKD systems need to satisfy:

- High secure bit rate
  - ✓ high system clock rate e.g. GHz
- "Practical" size, weight and power
  - ✓ no cryo cooling, use avalanche photodiodes (APDs)
- Integration into existing fibre networks
  - ✓ robustness against real-world fibre fluctuations
  - ✓ phase encoding, not polarisation encoding

Encode information in phase between 2 pulses:
Basis 1: Phase difference = 0 or π
Basis 2: Phase difference = π/2 or 3π/2

Encode information in polarisation state:
Basis 1: Polarisation = H or V
Basis 2: Polarisation = D or A

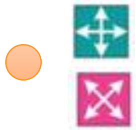
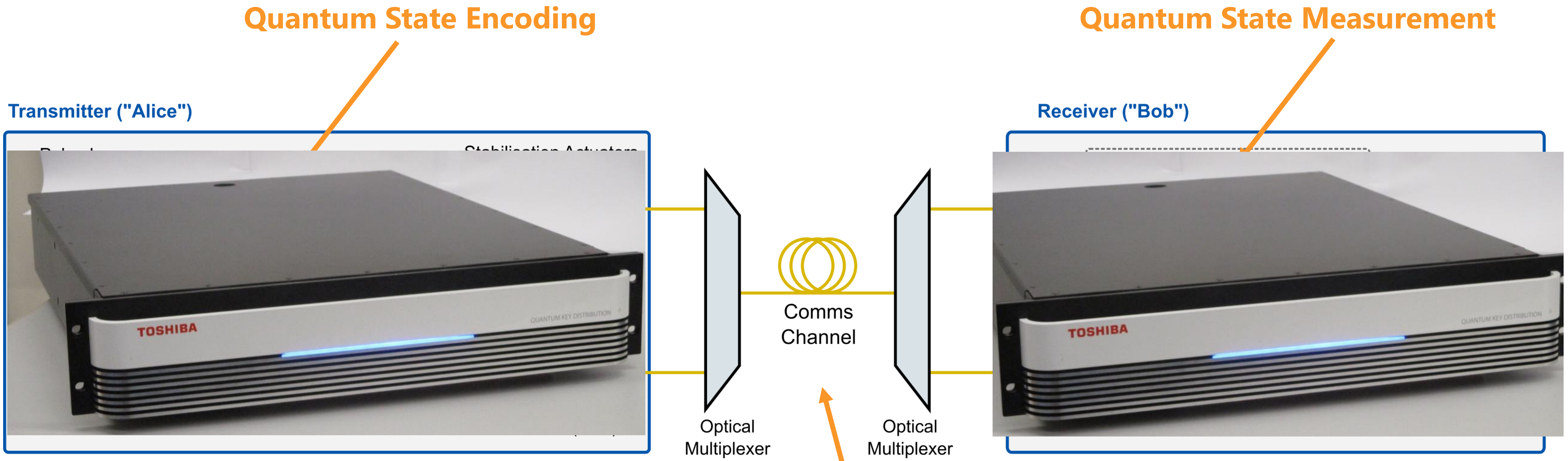


Image: https://www.cryofab.com

A Complete QKD System



Maximum Range?
Commercial Product: 150 km range
Lab Research: >600 km

Most quantum technologies need **classical communication** to actually run **quantum protocols.**
(can use any standard comms approach)

All optical signals (quantum + classical) multiplexed onto comms channel

Yuan et al., "10 Mb/s quantum key distribution", J. Lightwave Technol. **36**, 3427 (2018)

Software for QKD

The QKD protocol requires classical processing following quantum measurements.

1. "Sifting"

- Alice & Bob communicate what "basis" they sent/measured in.
- Discard bits when basis choices don't match.

2. "Error Correction"

- Correct differences in sent and received bit strings
- (these may be from hardware imperfections OR an eavesdropper attacking)
- Can't use forward error correction (information doesn't really exist until measured!)
- Instead, use novel protocol such as "Cascade"

3. "Privacy Amplification"

- Based on quantum science / information theory proofs and using measured stats, compute maximum number of secure bits that can be distilled from the measurements
- Perform "randomness extraction" to extract uniformly random bits from sources of potentially biased and correlated bits → provably secure correlated randomness (i.e. a key)

Real World Examples

QKD Deployments & Networks

02

Not Just Hype: Global QKD Deployments

PoC for financial blockchain with Ciena & **JPMorgan Chase & Co.**
(February 2022)

QKD trial in smart manufacturing with NCC, CFMS and **BT**
(since October 2020)

Proximus Belgium
Developing Quantum Safe networks
(2023)

EU Open QKD testbeds in six European countries
(since 2019)

QKD & PQC based secure optical transport network demo with **NTT**
(November 2021)

Orange France

QKD network deployment & evaluation

QKD trial by **Verizon**
(since September 2020)

Very long distance hybrid QKD network demo and QoS assessment with **KT**
(March 2022)

Quantum Network Testbed with **CQE**
(since April 2022)

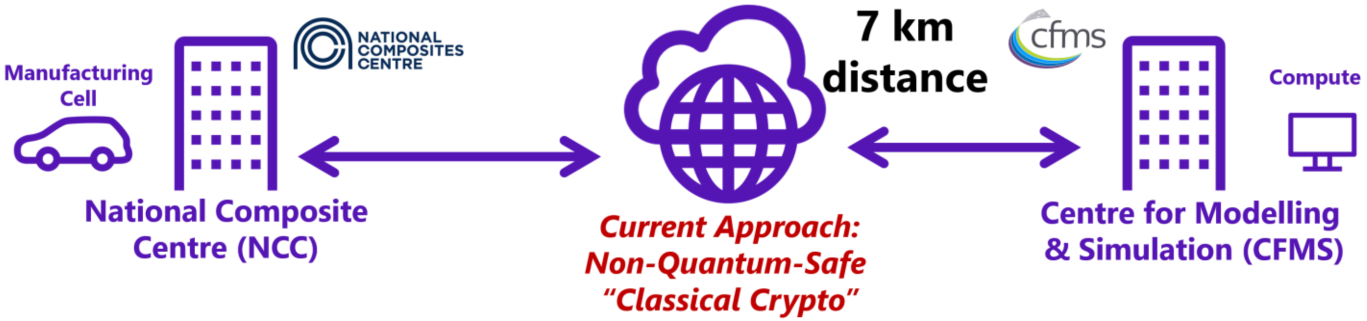
CHICAGO
QUANTUM
EXCHANGE

Commercial quantum-secured metro network trial in London with **BT**
(since April 2022)

QKD collaboration for Singapore and SE Asia region with **SpeQtral**
(since August 2021)

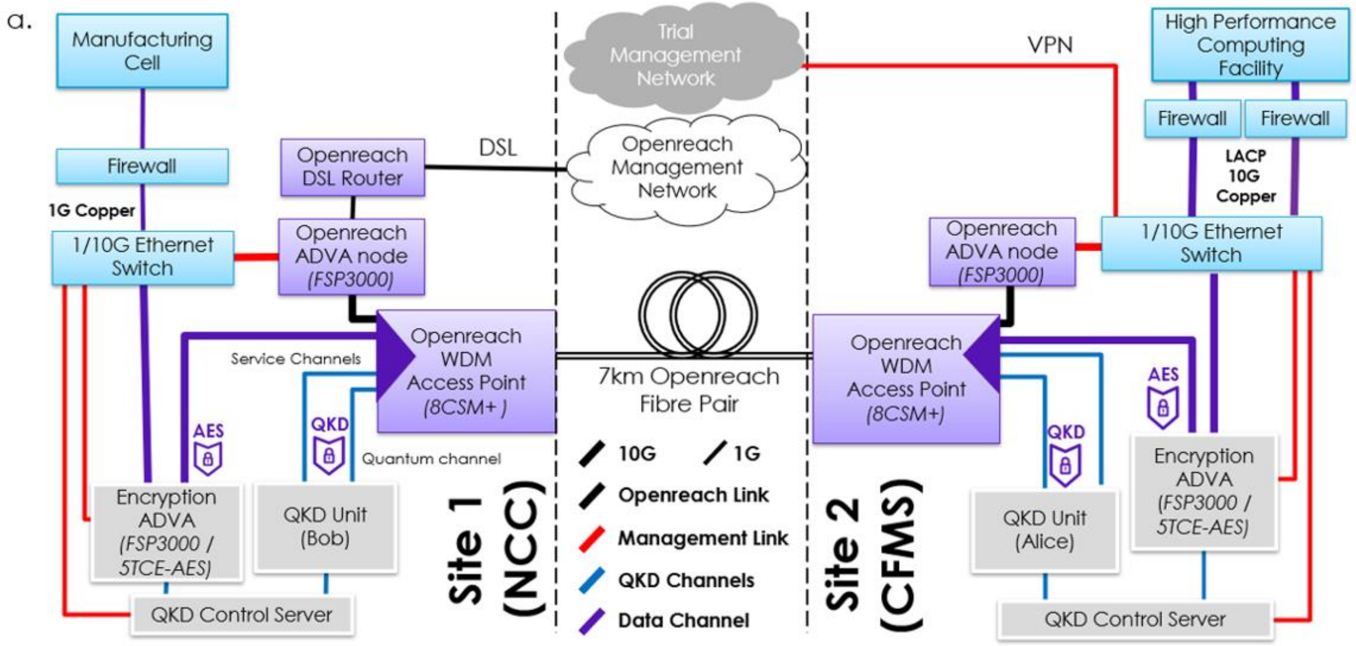
Deployment Example in Bristol, UK (Point-to-Point Link)

Quantum-safe link required between a manufacturing site and modelling facility to share data.



To operate QKD practically:
wavelength division multiplex
quantum and classical channels.

Quantum technologies need to co-exist with classical approaches in the real world.



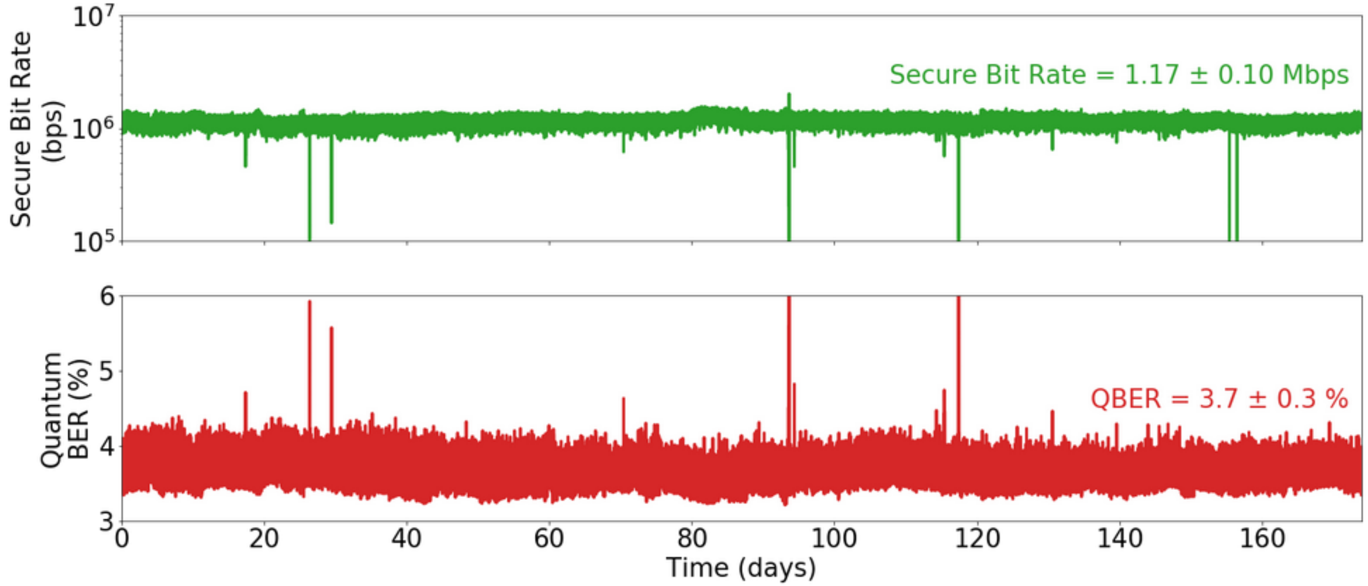
https://ieeexplore.ieee.org/abstract/document/9489683

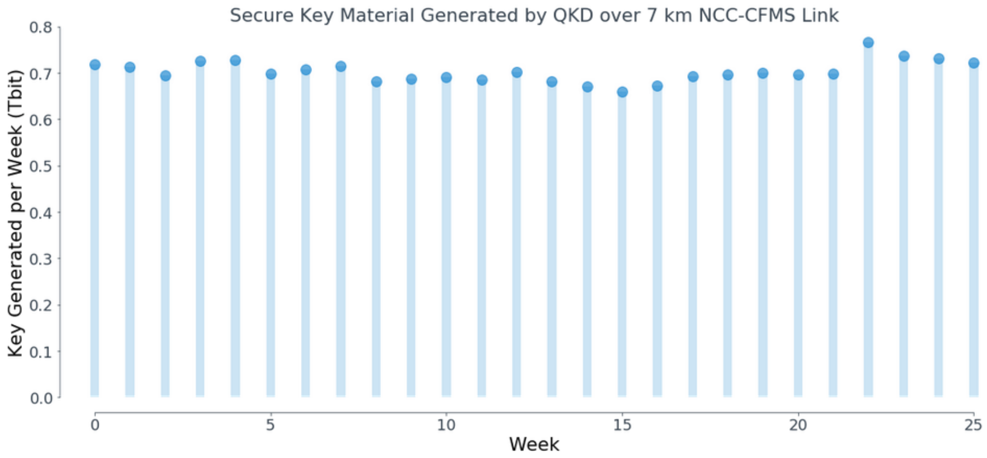
Deployment Example in Bristol, UK (Point-to-Point Link)

- All equipment installed in standard 19” racks

- Plug & play installation

- Stable operation for >6 months at >1 Mbps quantum secure bit rate (>4500 AES-256 keys a second)



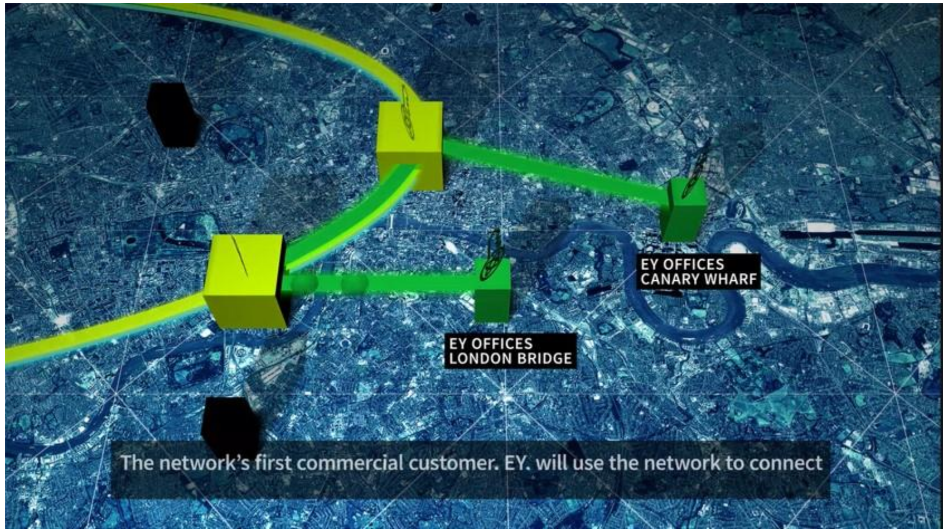


London Quantum-Secure Network

Aim: scalable network that offers door-to-door quantum-secured links for users

Current QKD networks perform "trusted node key relaying" (c.f. packet switching)

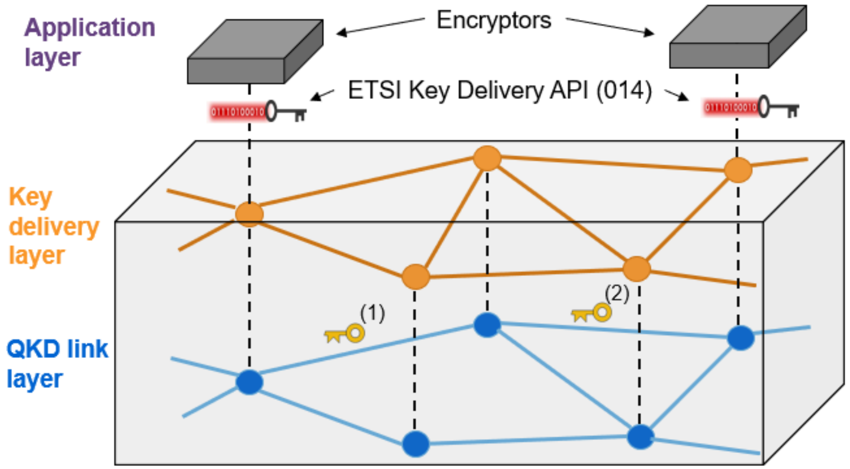
Solution:
- ***Core network*** (3-node ring) connecting strategically important locations (major data centres)
- "***Access tails***" added from nearest main node to each customer site



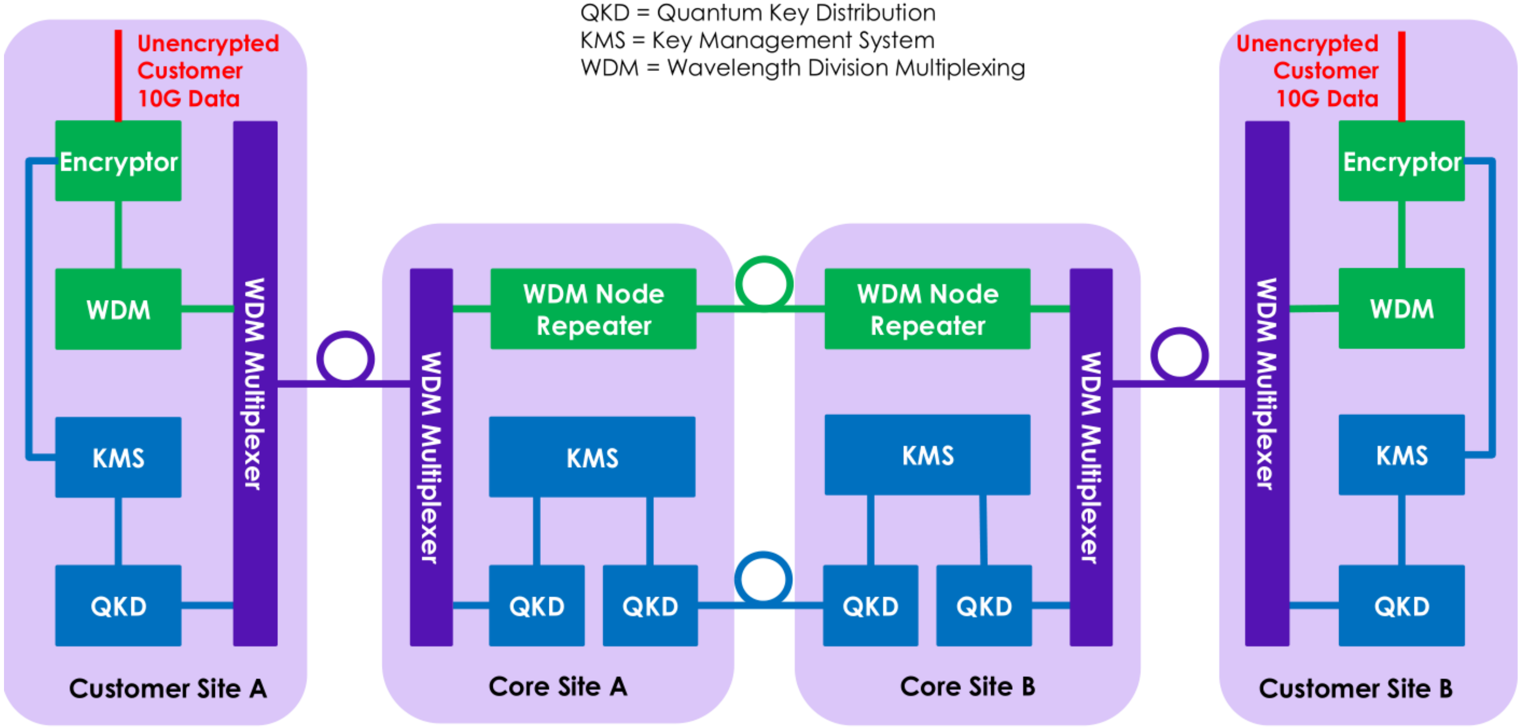
London Quantum-Secure Network

Trusted-node relaying network:

- each node has a key management system (KMS) for key relay
- customer nodes have 10G encryptors which pull keys from KMS using ETSI 014 standard
- encrypted traffic MUXed with QKD



QKD = Quantum Key Distribution
KMS = Key Management System
WDM = Wavelength Division Multiplexing



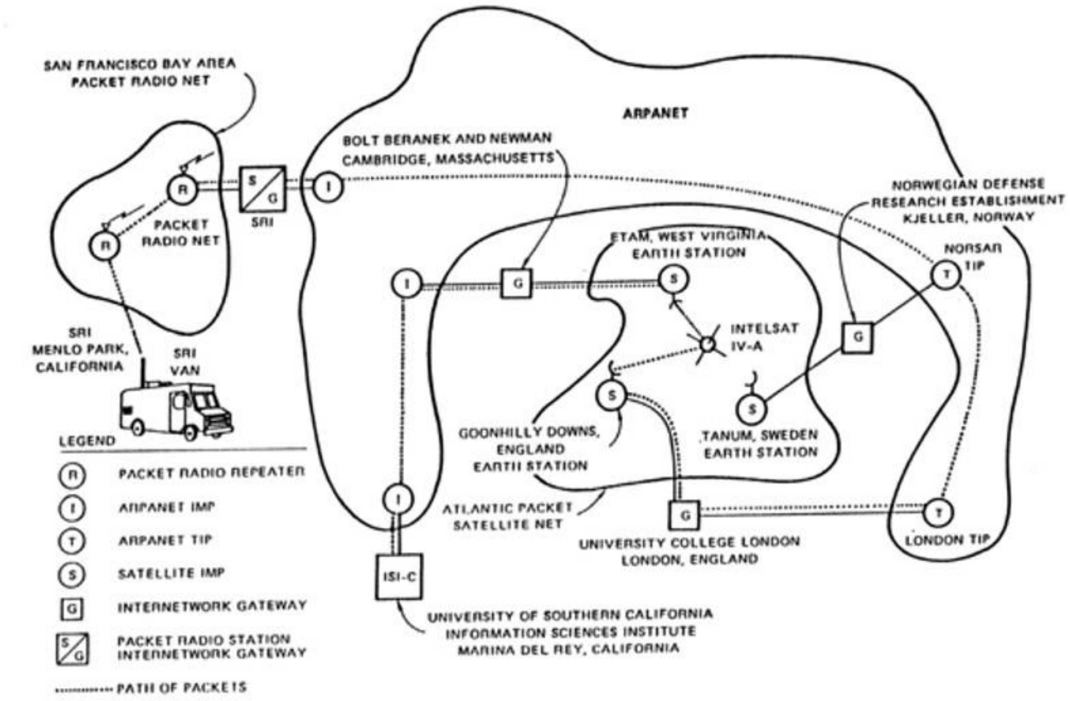
AES Encryptors are an off-the-shelf technology, already widely used in telecom (using non quantum safe key exchange)

Many vendors now support the ETSI 014 REST API for QKD key pull, enabling QKD-keyed AES encryption.

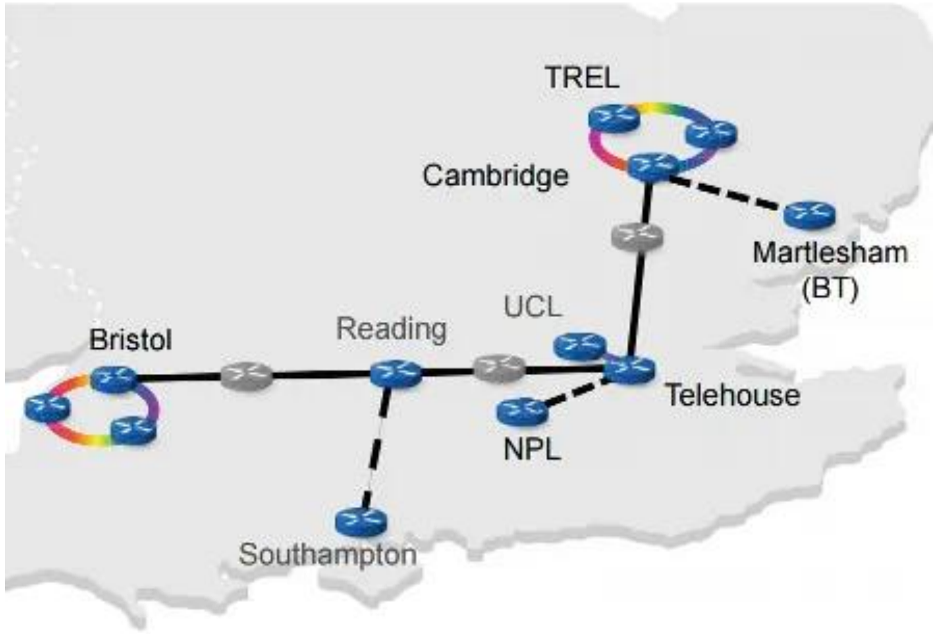
Inter-Quantum-Networking

Next, we need to build networks of networks.

1977: classical inter-networking



202X: UK quantum network



TOSHIBA

Introducing Post Quantum Cryptography

Quantum-Resistant Cryptography

03

Recap: Threat Assessment

Current ***asymmetric cryptography*** (e.g. public key exchange) is **broken** by quantum computers, since *integer factorization* & *discrete-log problem* no longer "hard"

Current ***symmetric cryptography*** (e.g. AES encryption) is **weakened** by quantum computers, but not broken (need to use longer keys).

PQC

Post-quantum cryptography (PQC) (sometimes referred to as **quantum-proof**, **quantum-safe** or **quantum-resistant**) is the development of cryptographic algorithms (usually public-key algorithms) that are thought to be secure against a cryptanalytic attack by a quantum computer. [0]

WHILST QKD IS MATHEMATICALLY PROVEN ("INFORMATION THEORETICALLY SECURE"), PQC SECURITY HAS NOT BEEN PROVEN MATHEMATICLY

"NSA expects transition to QR algorithms for NSS to be complete by 2035" [1]

"The first sets of these standards are expected to be released publicly by [NIST/NSA] 2024" [1]

"NCSC advice remains that the best mitigation against the threat of quantum computers to traditional PKC is post-quantum cryptography (PQC)" [2]

[0] https://en.wikipedia.org/wiki/Post-quantum_cryptography
[1] https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/
[2] https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

NIST Shortlisted Algorithms

For key exchange

CRYSTALS-Kyber

For digital signatures

CRYSTALS-Dilithium
FALCON
SPHINCS+

Other standards organisations may recommend other algorithms.....

[0] https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

Hybrid keys could be the answer (for now)

- Secure material with both existing key algorithm and a PQC key in series

- Encryption / authentication is only as secure as the more secure of the two keys used

- Protects against harvest now, decrypt later

  Even if you do not trust PQC hybrid keys mean that no security is lost

- Protects against earlier than anticipated Viable Quantum Computer

Impact within Debian

all to arms....

This is a private opinion not associated or endorsed by my employer...

Infrastructure 1

Debian depends on PKI for authentication of packages

- apt and friends
- Installation images

Apt -> GPGV (part of GPG) -> LibG-Crypt (GPG's crypto library)

DAK index hashes

Di -> apt, u-debs -> ??

update the libraries Apt depends on, don't change to a different library.

Otherwise this adds to the 'set of essential packages'

Need UPSTREAM POINT RELEASES of GNU-PG to include PQC Hybrid

Currently we have 2.4.0, I haven't looked at the release notes

We need to wait for GPG 2.6? To make it into Debian if 2.4 doesn't support H/PQC

Infrastructure 2

Debian depends on PKI for authentication of developers and infra

- *Keyring*
- *Debian servers (Salsa, build boxes, porter boxes etc.)*

We use stable for internal infrastructure

If we need features before those then....
What can we do?

Infrastructure 3

Packages depend on PKI themselves

- *Effects almost all internet facing software (and more)*

users depend on SSH TLS etc.

OpenSSH v9 (April '22) introduced Hybrid keys:
"use the hybrid Streamlined NTRU Prime + x25519 key exchange method by default" [0]
Unfortunately, this was not included in first NIST release [1] even though NTRU NOT shown to be broken
but at least upstream of THIS project is aware of the problem

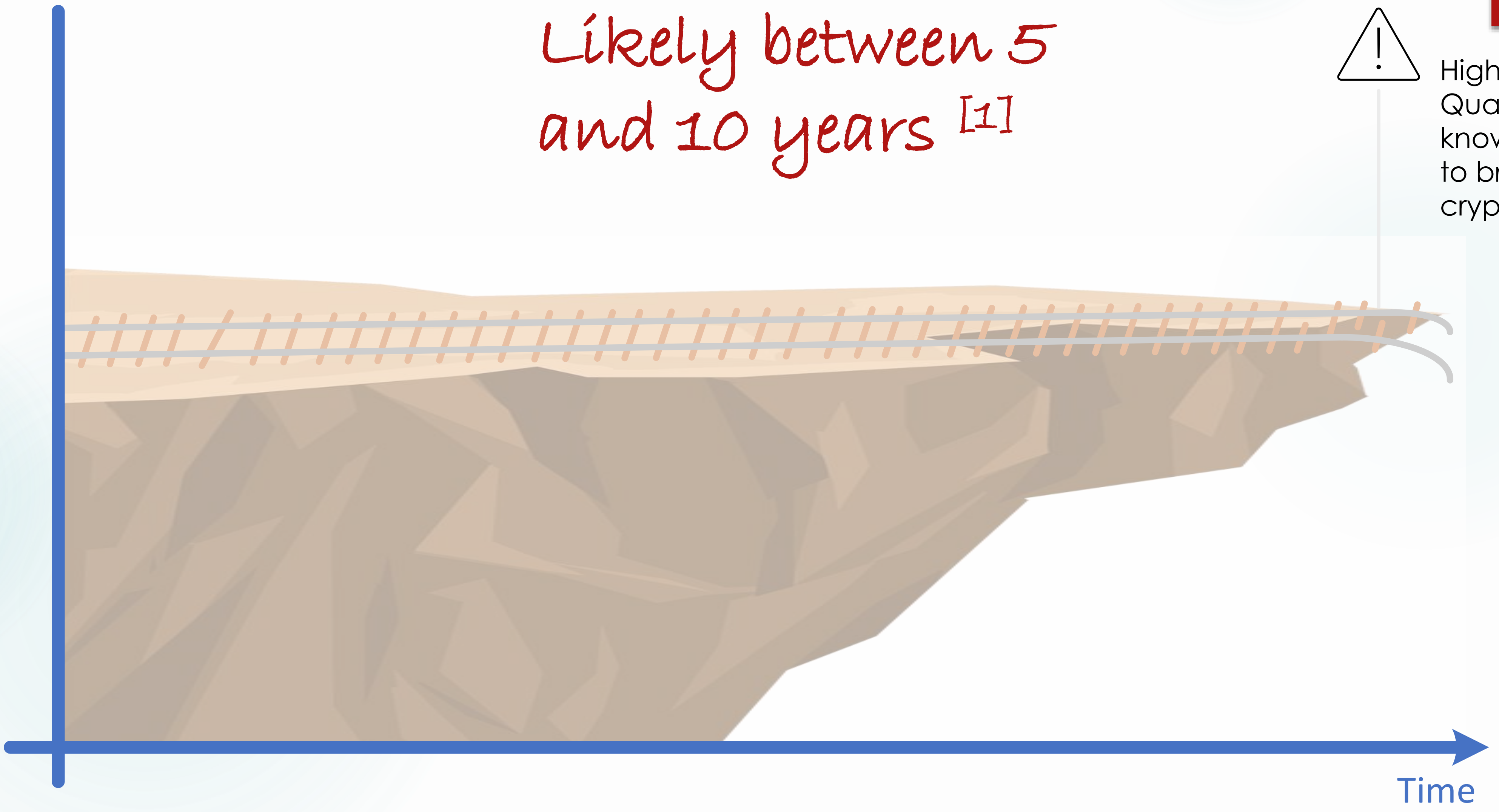
[0] openssh.com/txt/release-9.0
[1] The NSA, NIST and Crypto in Court | by Prof Bill Buchanan OBE | ASecuritySite: When Bob Met Alice | Medium

Timeline

Likely between 5 and 10 years [1]

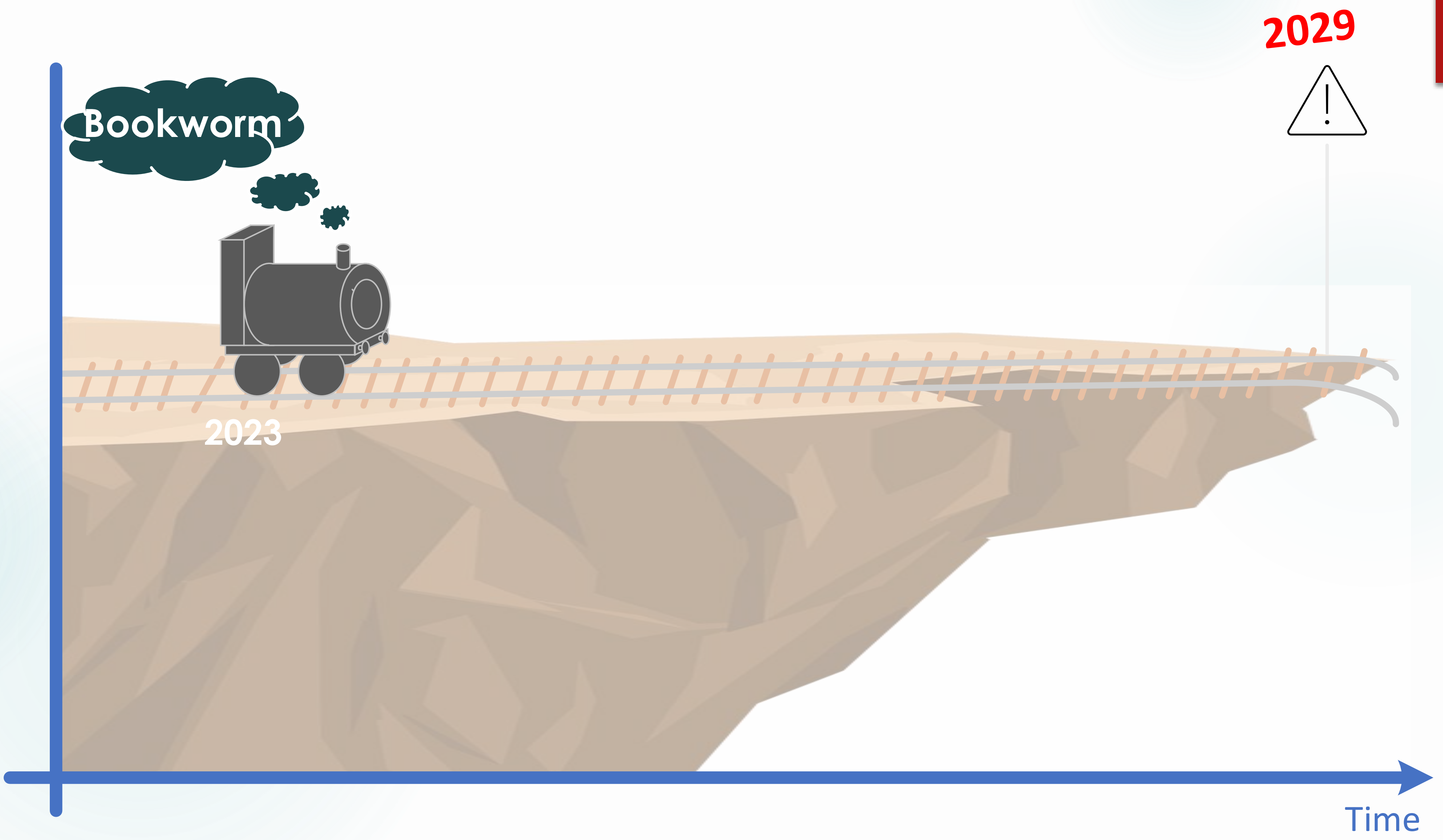
2029

High performance Quantum computer known to exist able to break existing PKI cryptography

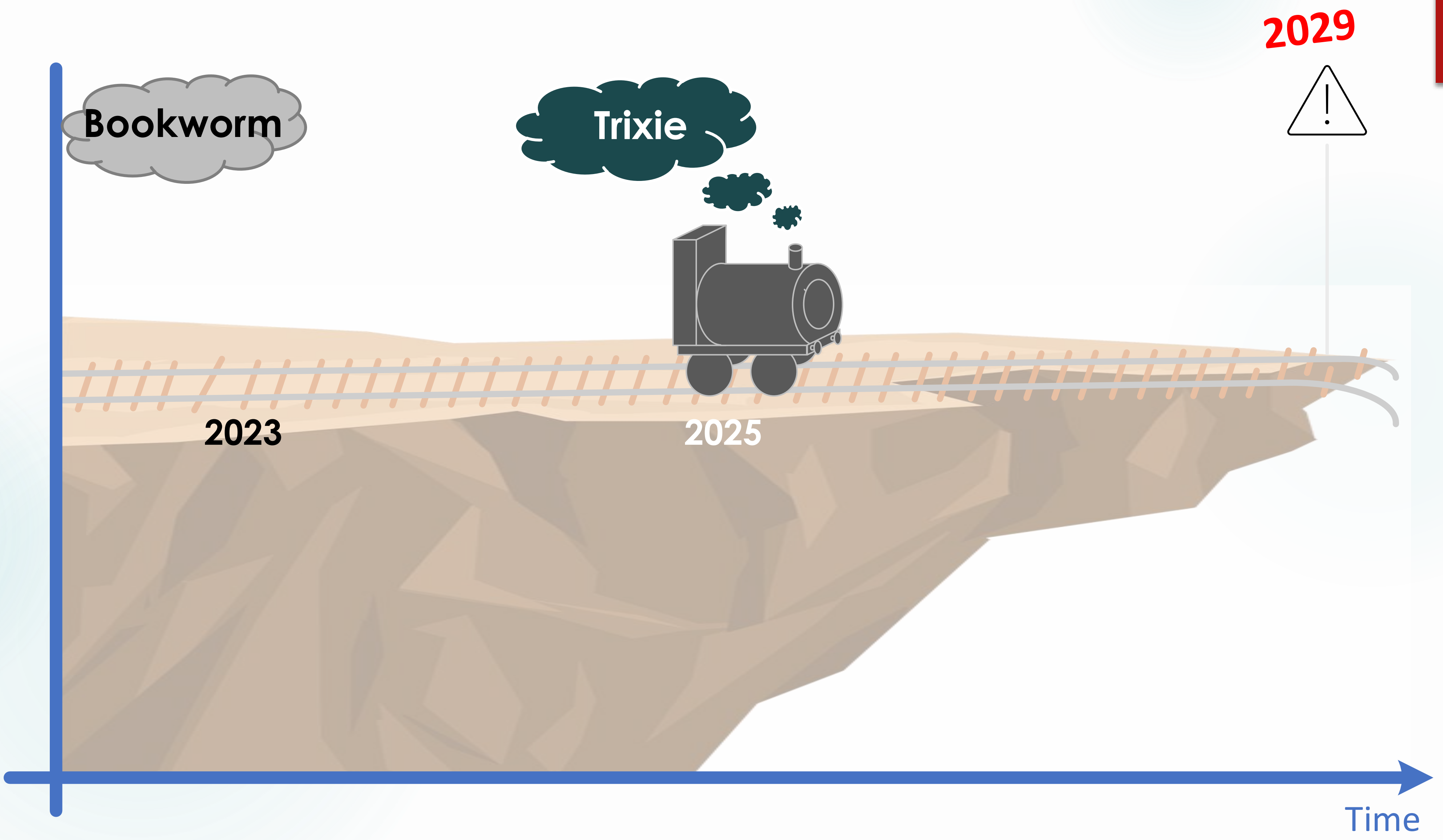


[1] Quantum Threat Timeline Research Report 2022 - Publication (evolutionq.com)

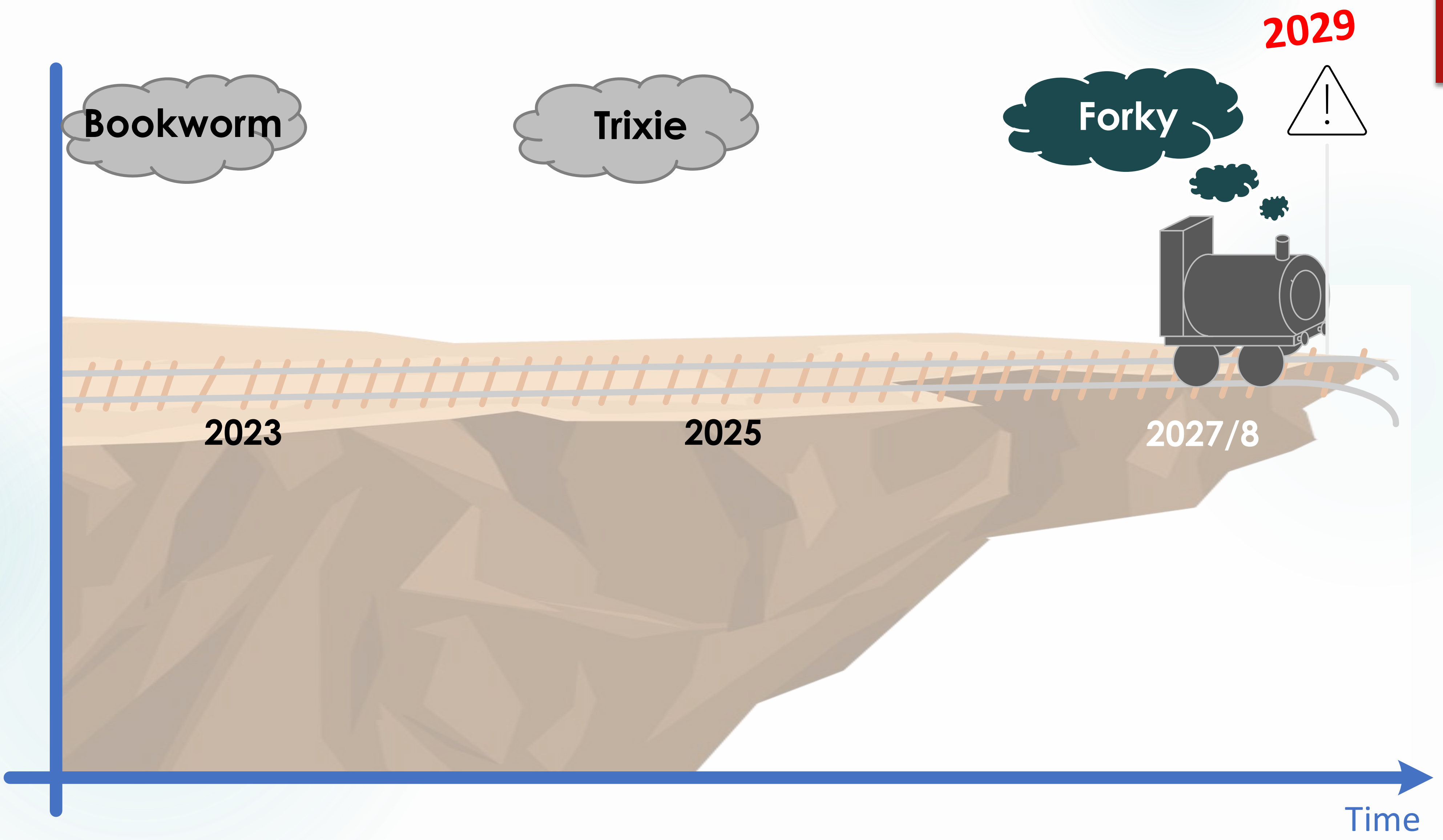
Timeline



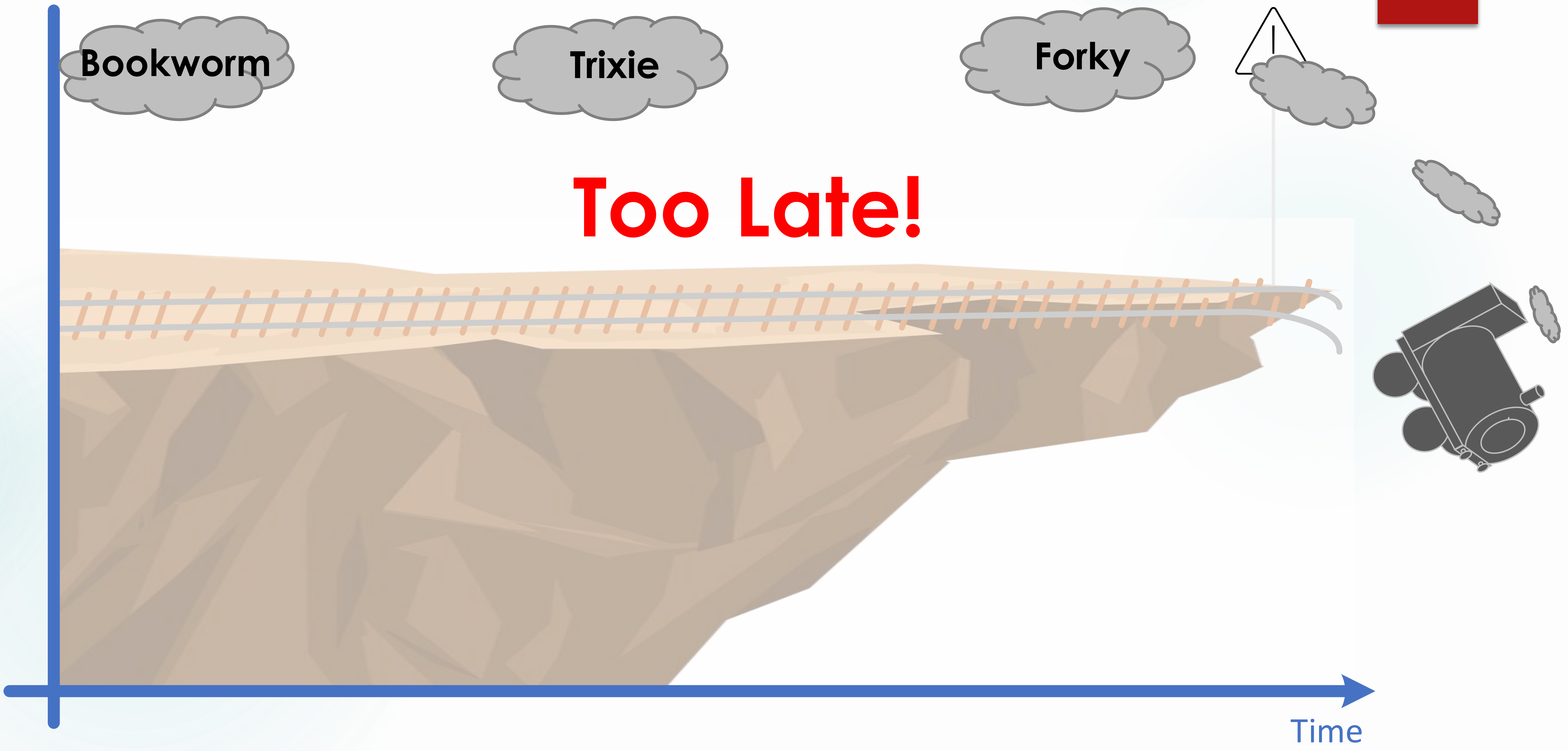
Timeline



Timeline



Timeline



Debian Infrastructure

probably

We can ^secure our infrastructure quickly if needed.

1. Our servers must at least support Hybrid keys

Does this mean that Hybrid key support needs to exist in 'Stable' before we can turn it on for our own infrastructure?

2. Run hybrid keys in parallel on our infrastructure, turning this on server by server

3. Require developers to support hybrid keys

4. Run only hybrid keys on Debian infrastructure

Can we start updating our own keys today?

Packages in archive

Introduce PQC across several release cycles

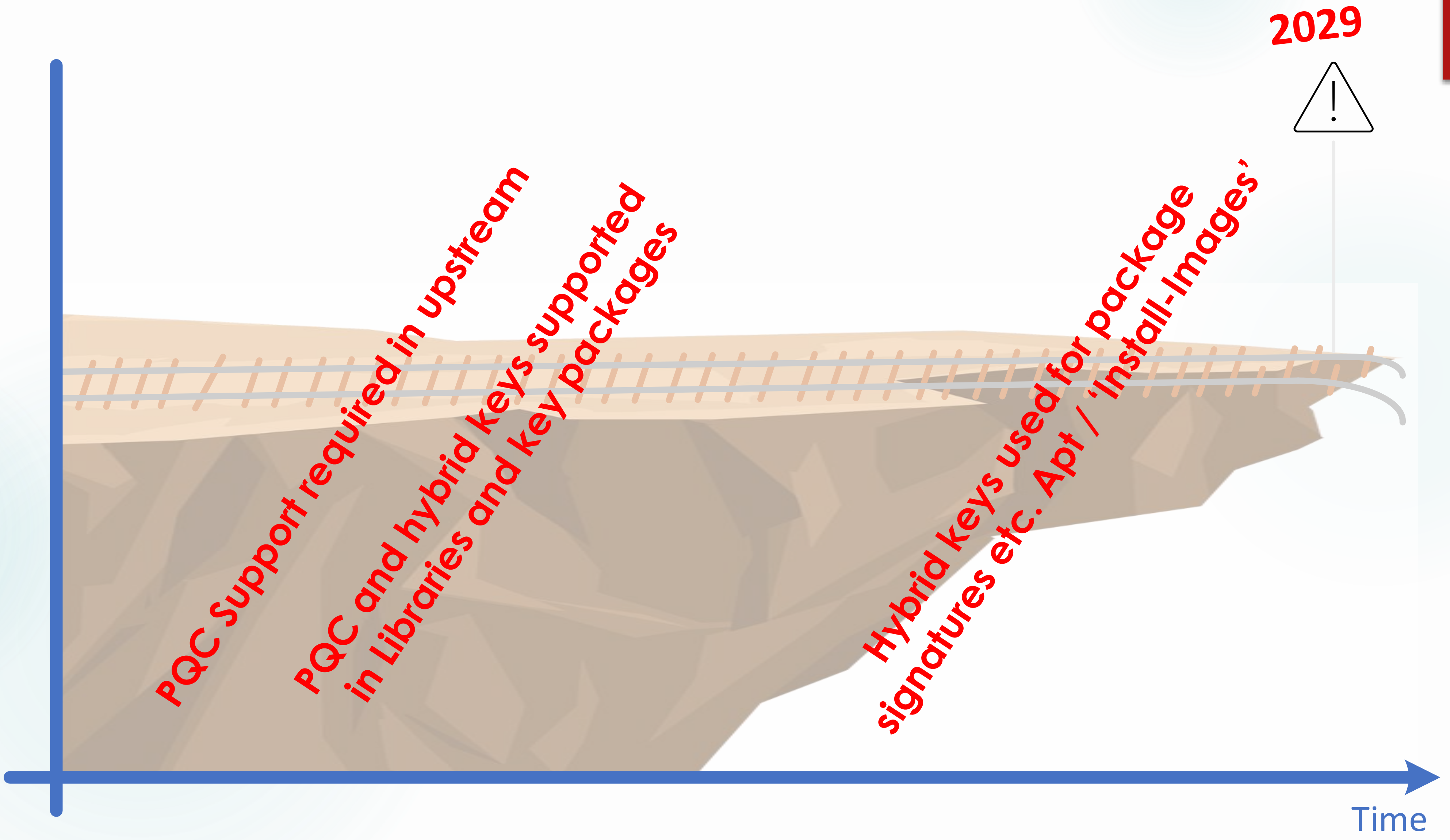
Do we need a GR?
Can this be a release goal for several releases?

1. Get the project to agree this needs to be done
2. Introduce support for both PQC and hybrid key systems
3. Require use of hybrid keys
4. Deprecate non PQC

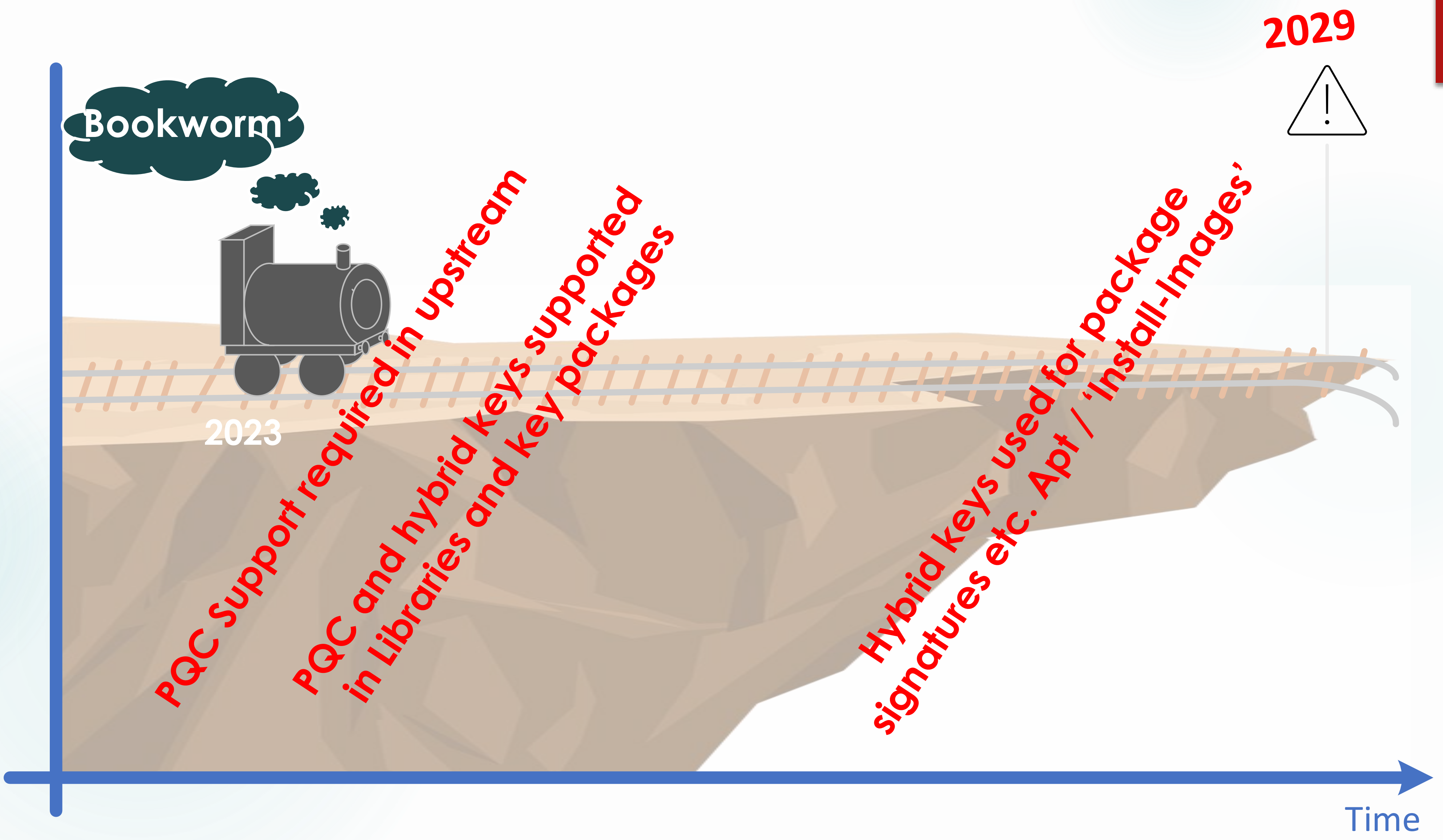
Can this be achieved across just 2 releases?

What if we need to stagger requirements?
i.e. core / library packages 1 release ahead of leaf packages

Timeline

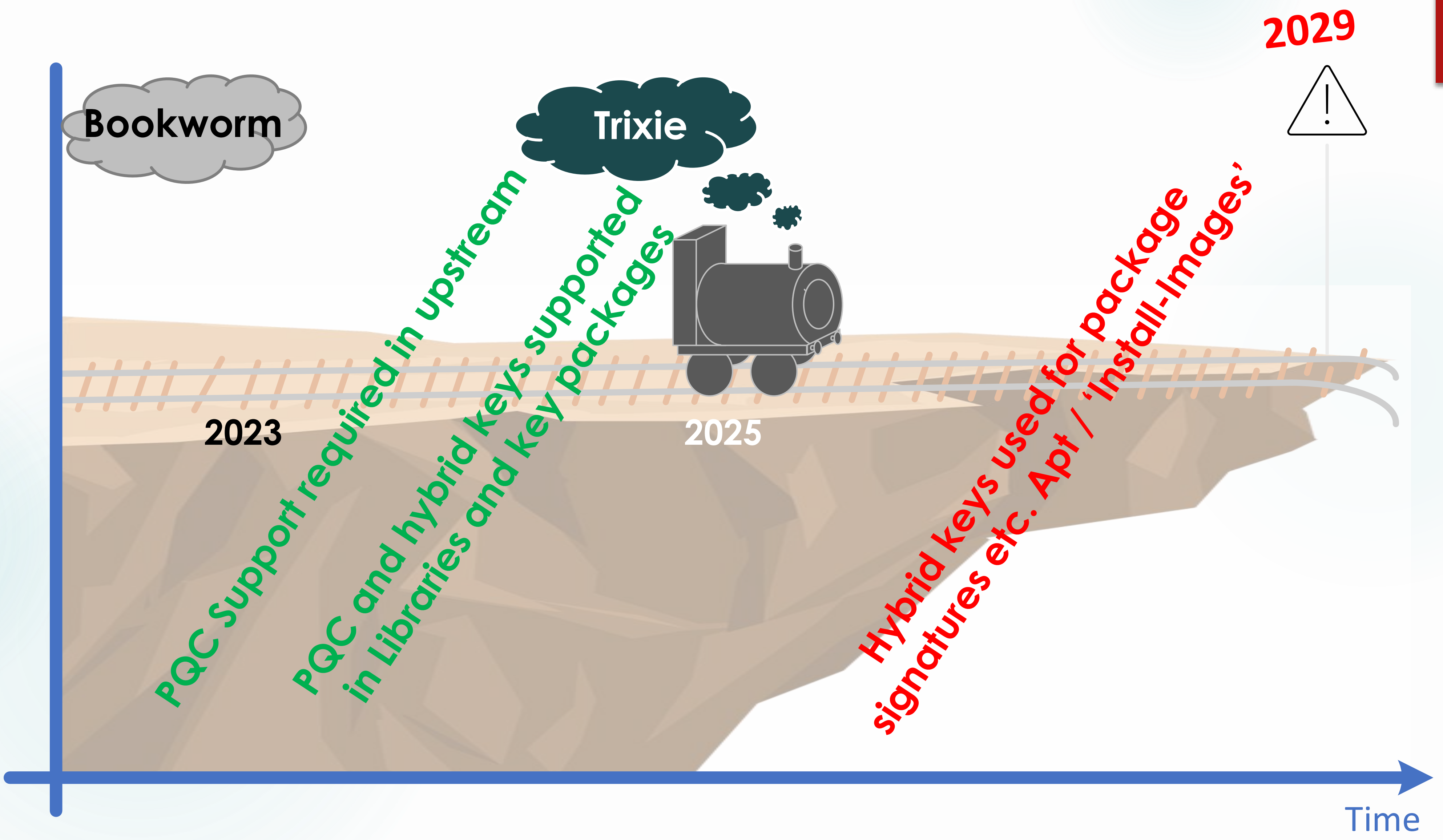

2029
PQC Support required in upstream
PQC and hybrid keys supported in Libraries and key packages
Hybrid keys used for package signatures etc. Apt / 'Install-Images'
Time

Timeline



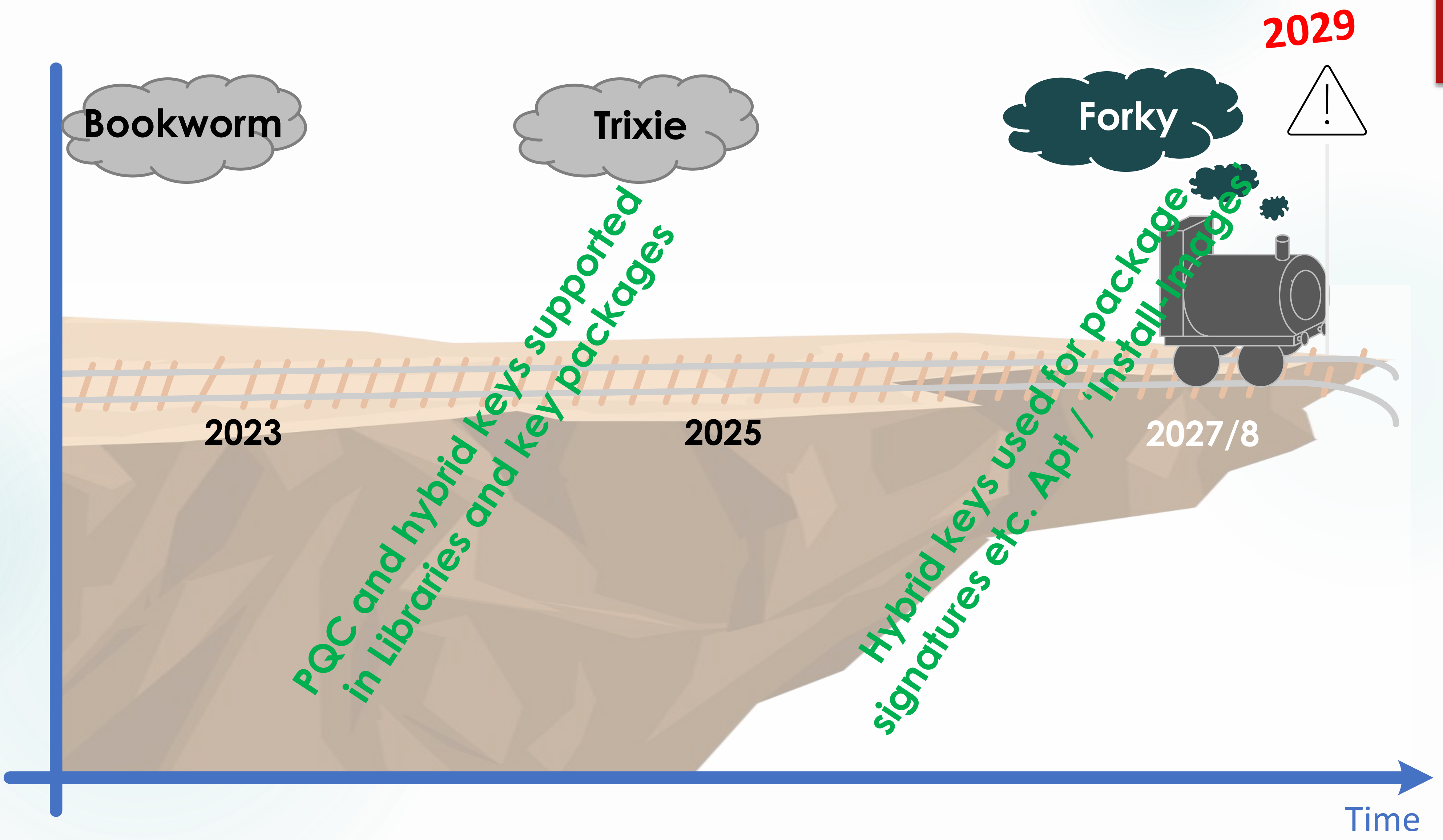
Bookworm
2023
PQC Support required in upstream
PQC and hybrid keys supported in Libraries and key packages
Hybrid keys used for package signatures etc. Apt / 'Install-Images'
2029
Time

Timeline

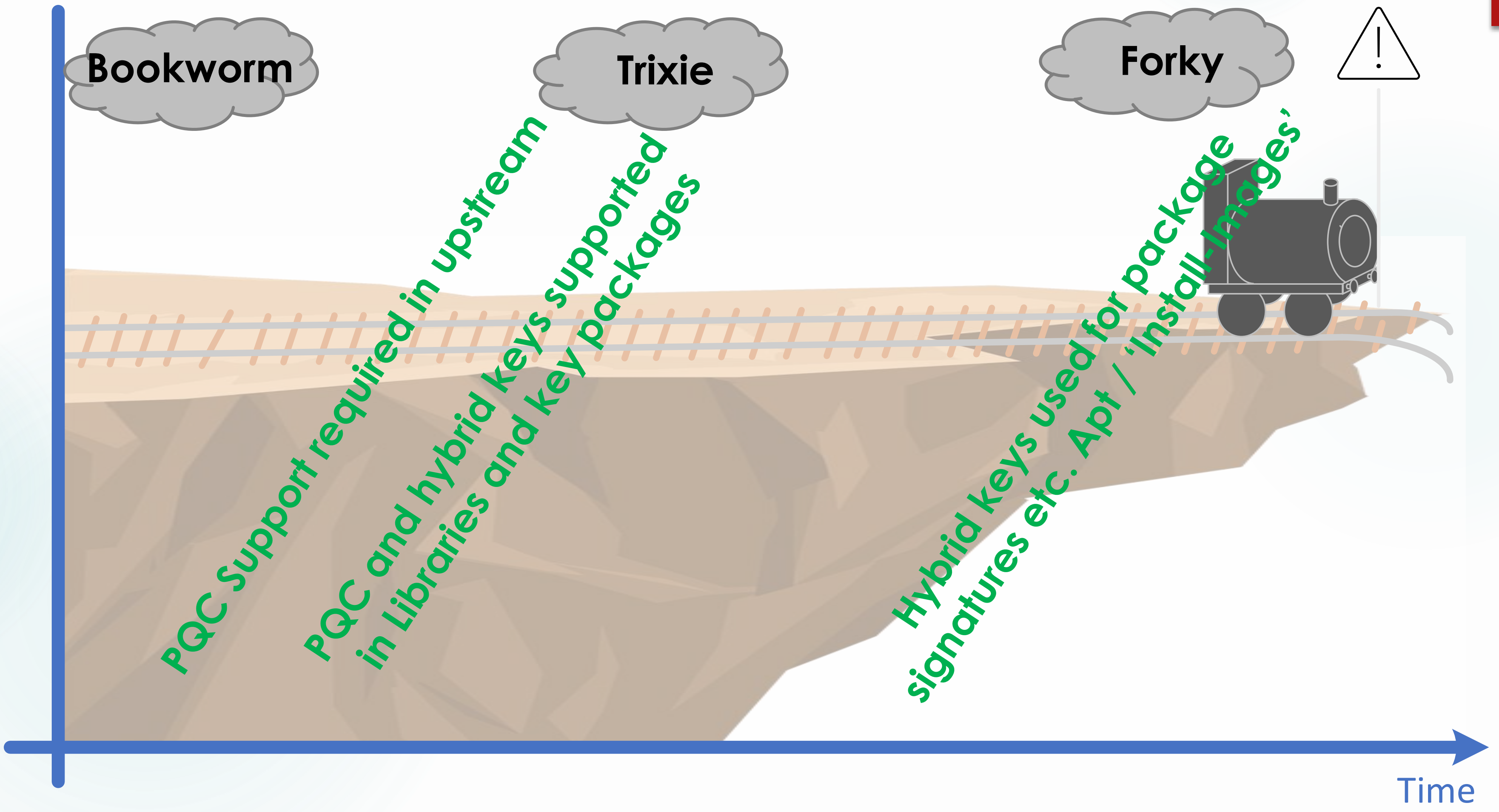


Bookworm
Trixie
2029
2023
2025
PQC Support required in upstream
PQC and hybrid keys supported
in Libraries and key packages
Hybrid keys used for package
signatures etc. Apt / 'Install-Images'
Time

Timeline

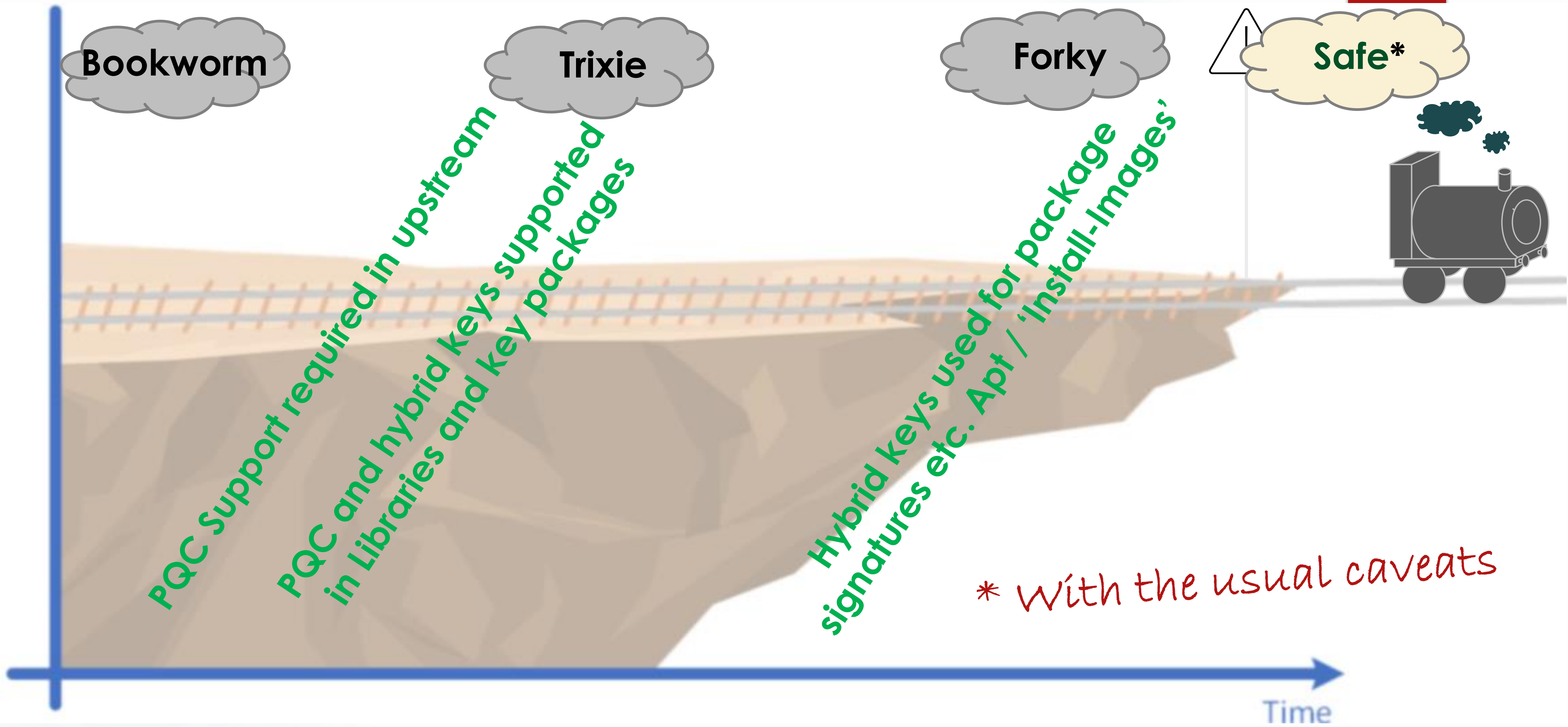

Bookworm
Trixie
Forky
2029
2023
2025
2027/8
PQC and hybrid keys supported
in Libraries and key packages
Hybrid keys used for package
signatures etc. Apt / 'Install-Images'
Time

Timeline



Bookworm
Trixie
Forky
PQC Support required in upstream
PQC and hybrid keys supported in Libraries and key packages
Hybrid keys used for package signatures etc. Apt / 'Install-Images'
Time

Timeline


Bookworm
Trixie
Forky
Safe*
PQC Support required in upstream
PQC and hybrid keys supported in Libraries and key packages
Hybrid keys used for package signatures etc. Apt / 'Install-Images'
* With the usual caveats
Time

Questions…

Robert Woodward

robert.woodward@toshiba.eu

Andy Simpkins

andy.simpkins@toshiba.eu

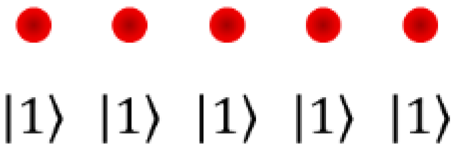
TOSHIBA

Extra Slides

Laser Sources in QKD

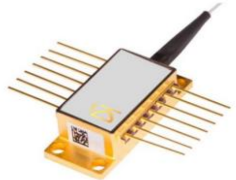
How to generate & encode **single photons** at high speed?

☒ GHz-clocked single-photon sources not yet practically available



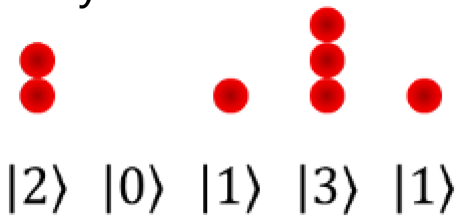
Fock states

Instead, use attenuated telecom-grade semiconductor pulsed lasers: "**weak coherent pulses**" (need to be phase randomized)



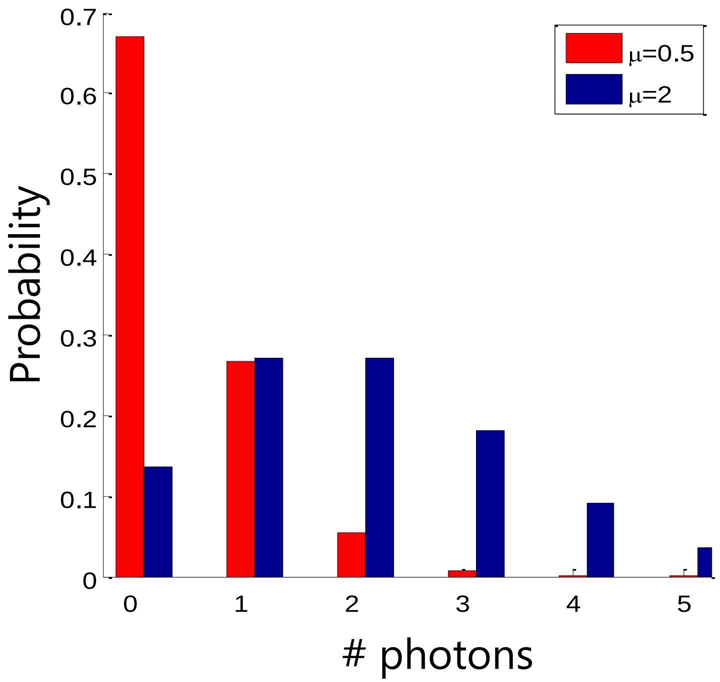
Pulses:

Reality:



Coherent states represent **distribution** of Fock states.

(Poisson distribution with mean photon number **μ**)



We choose μ < 1 to maximize single photon probability, while minimizing multiphoton events.

Multi-photon pulses break security. Circumvent this by occasionally modulating the mean photon number during QKD → "**<u>decoy state QKD</u>**"

Hwang, Physical Review Letters **91,** 057901 (2003)