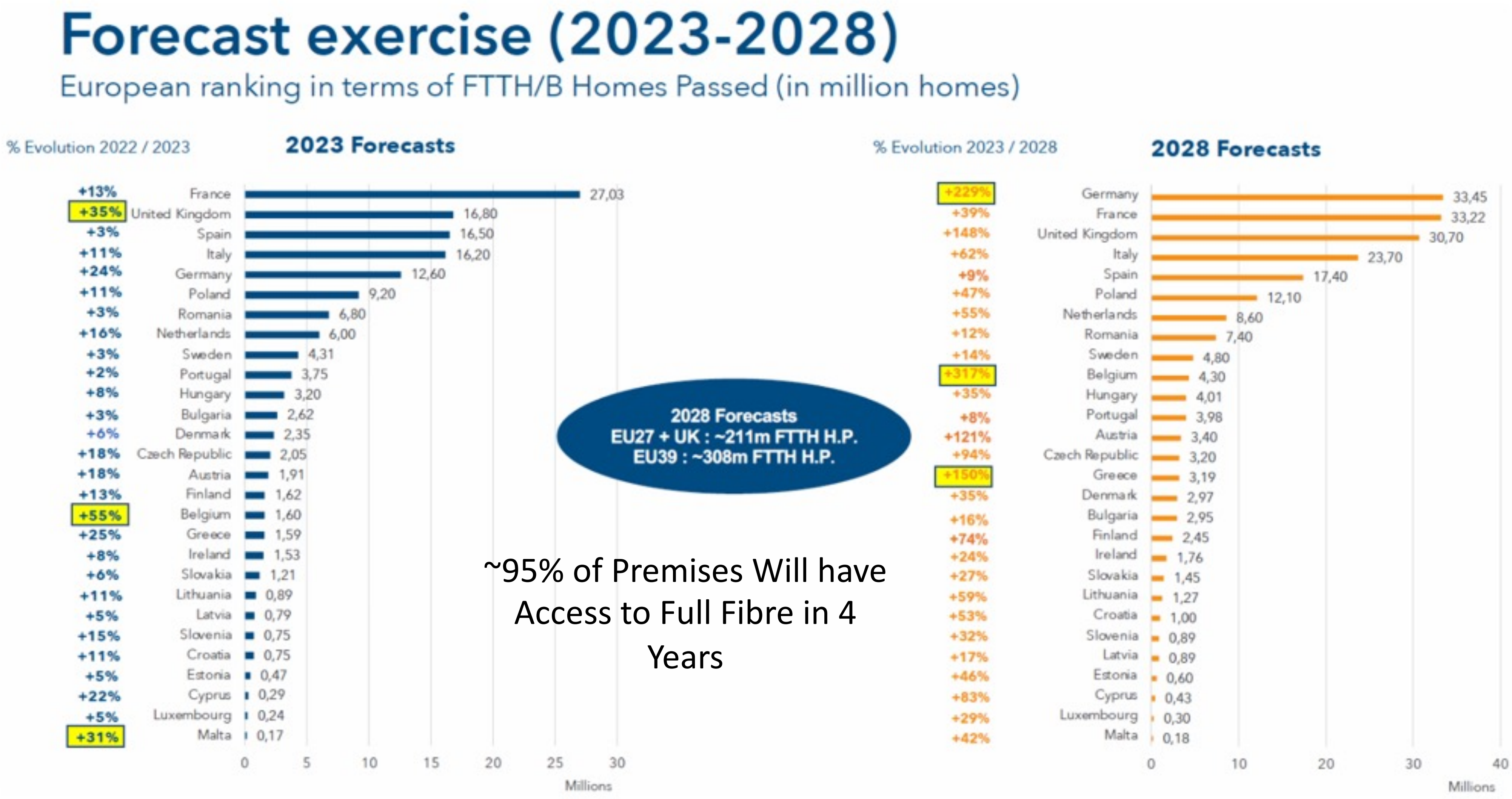
Security Considerations in a World of Bandwidth and Compute Resource Abundance

Ronan Kelly
Adtran CTO EMEA

Adtran

Status of FTTH Availability Across Europe

Fibre Ubiquity Fast Approaching



~95% of Premises Will have Access to Full Fibre in 4 Years

Status of FTTH Availability Across Europe

Cost Effectiveness of Multi-Gig Services

toob
free installation
900 Mbps
£25 per month
18 month contract then £29 per month

Community Fibre
Save £576!
1,000 Mbps Fibre Broadband
£49 £25/month

B4RN
Hyperfast
1Gbps
£33 pm

Swish fibre.
Swish 900
£39PM

iliad
€19.99
Download
up to 5 Gbit/s
divided between Wi-Fi and ethernet ports

youfibre
YOU 8000
7000 MBPS
Avg. download speed
Only
£99.99
per month
Select package

Sunrise
Up Connect XL Details
Your fastest connection
10 Gbit/s
Phone
CHF 59.90/mth ~~89.90~~
For 24 months, then 89.90/mth
24 months minimum contract duration

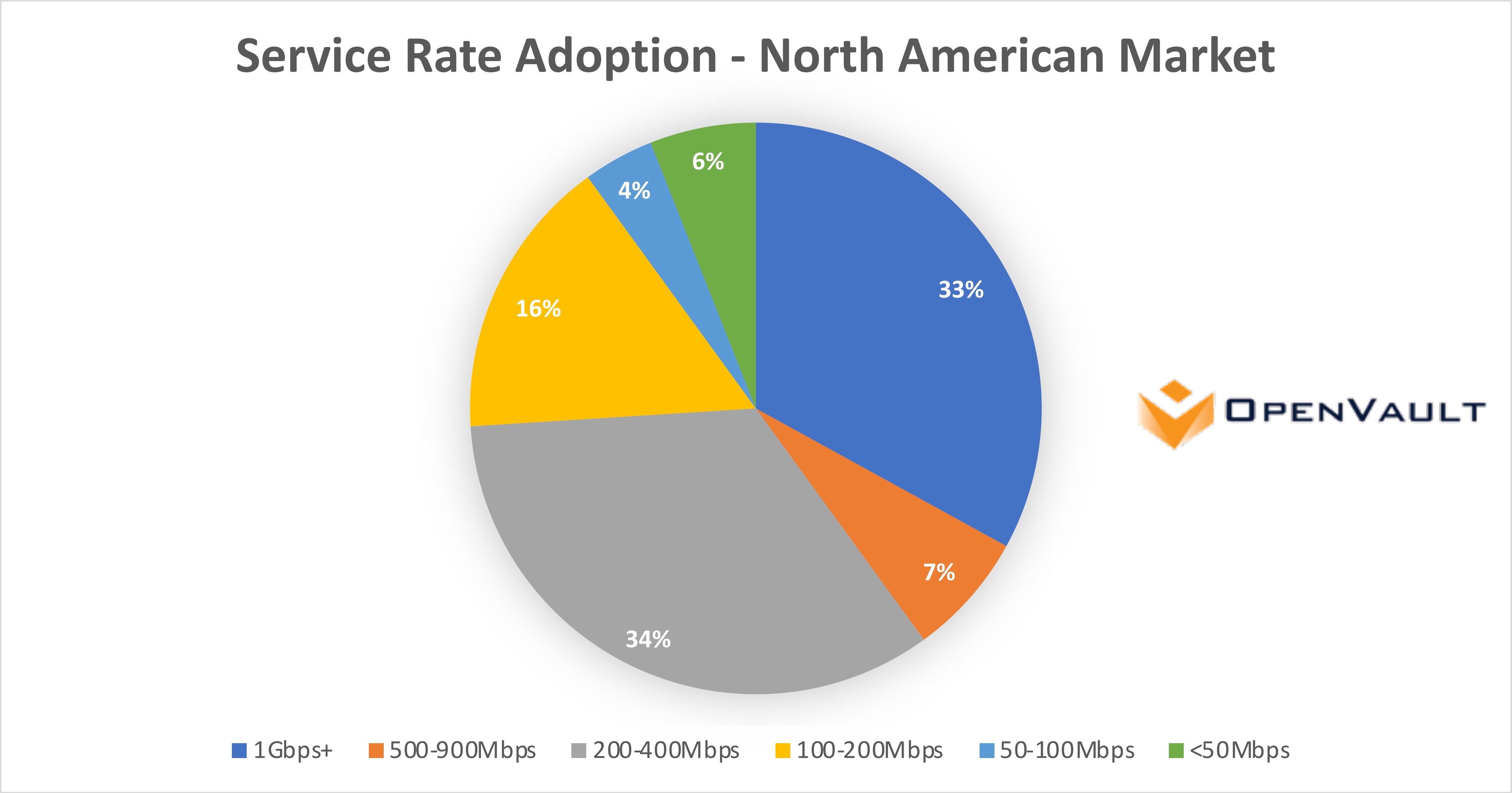
GFiber
20 Gig
Select markets*
$250/mo[1]
Symmetrical download and upload speeds up to 20 gigabits
See details

Adtran

Source: Online as of March 4th 2024

Adoption Response to Availability

Gigabit and Multi-Gigabit Beyond Lead User Status



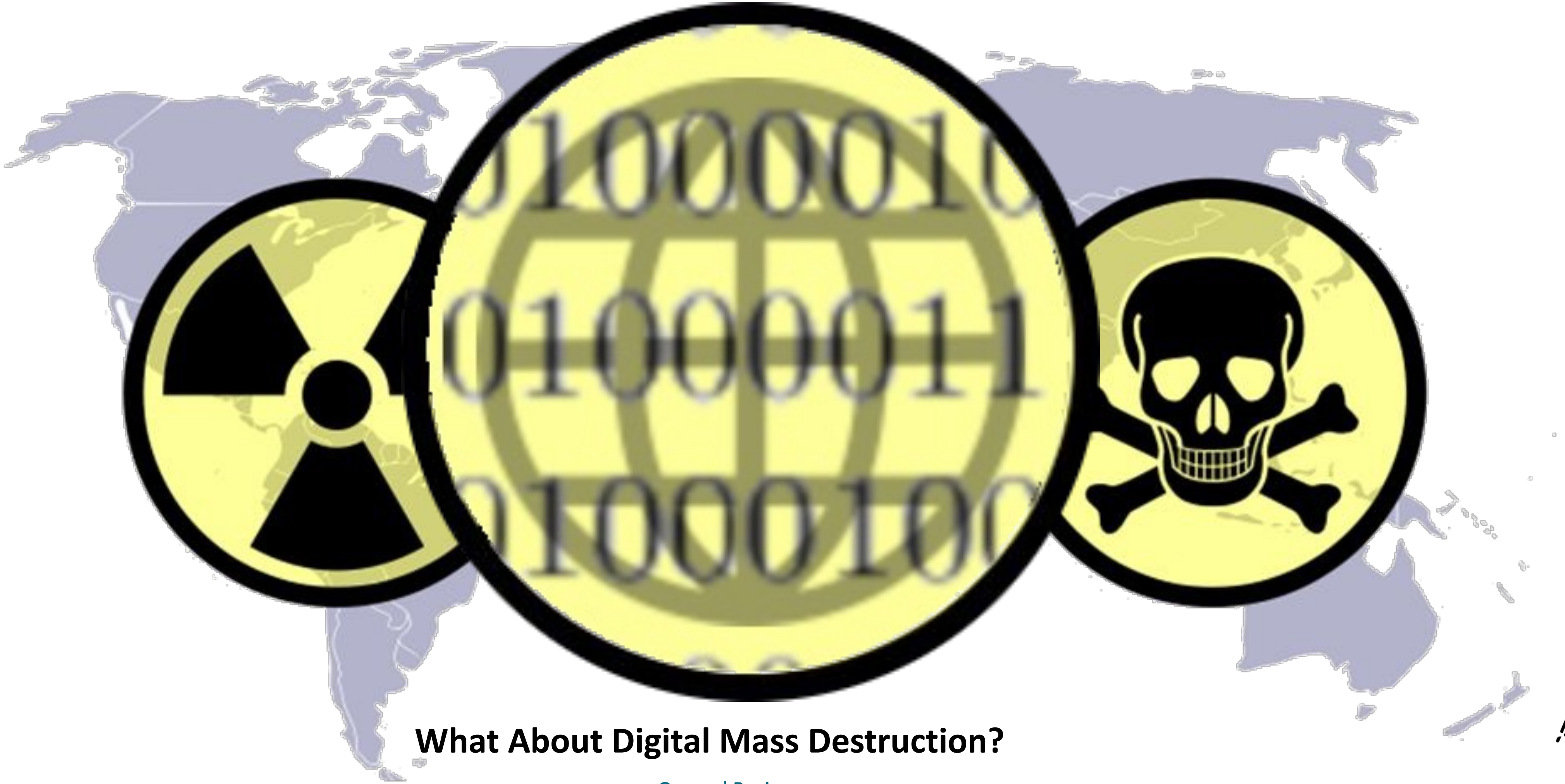
Adtran

General Business

Source: Openvault March 2024

Threat Landscape

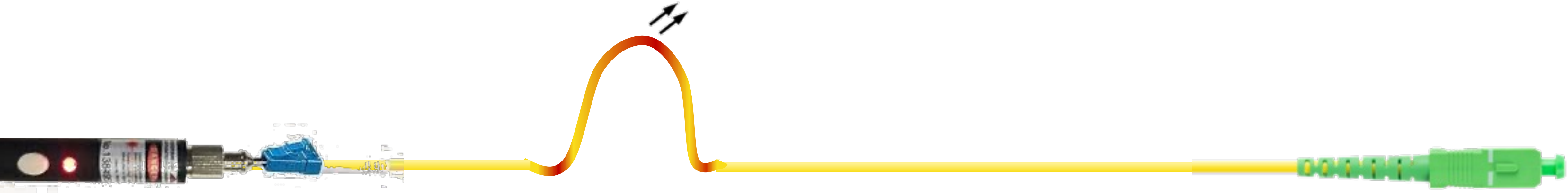
Radiological, Biological, Chemical

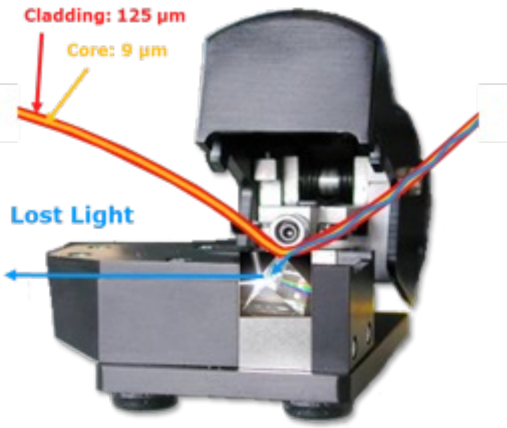


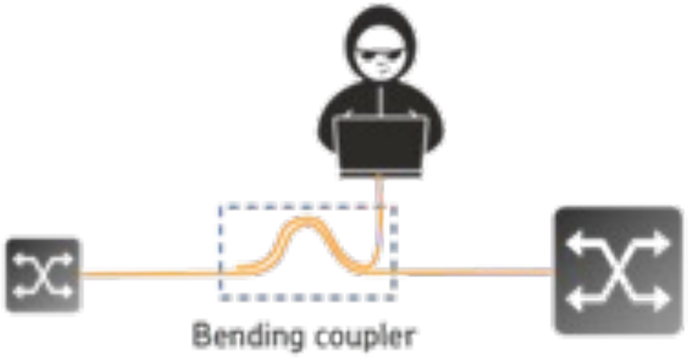
What About Digital Mass Destruction?

Adtran

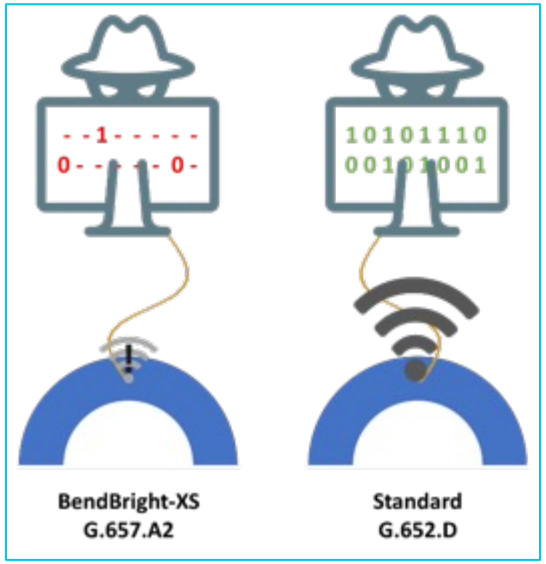
Fibre's Leaky Little Secret







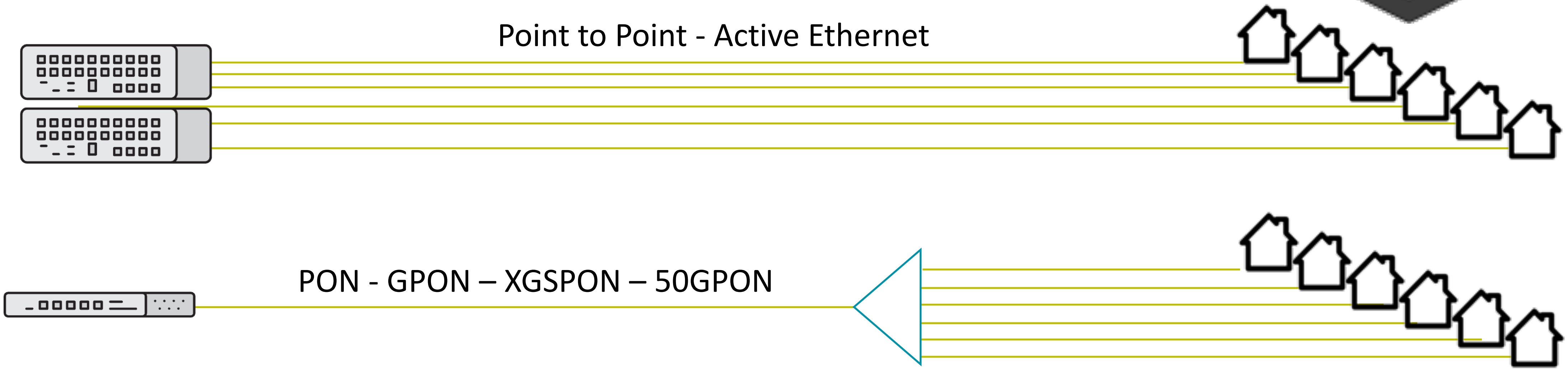
Bend Insensitive Fibre



Adtran

Securing Fibre Connections

Ethernet FE – GE – 10GE – 100GE	Natively Unencrypted
Active Ethernet	AES-128 Bi-Directional
GPON	AES-128 Downstream
XGSPON	AES-256 Bi-Directional
50G PON	AES-256 Bi-Directional

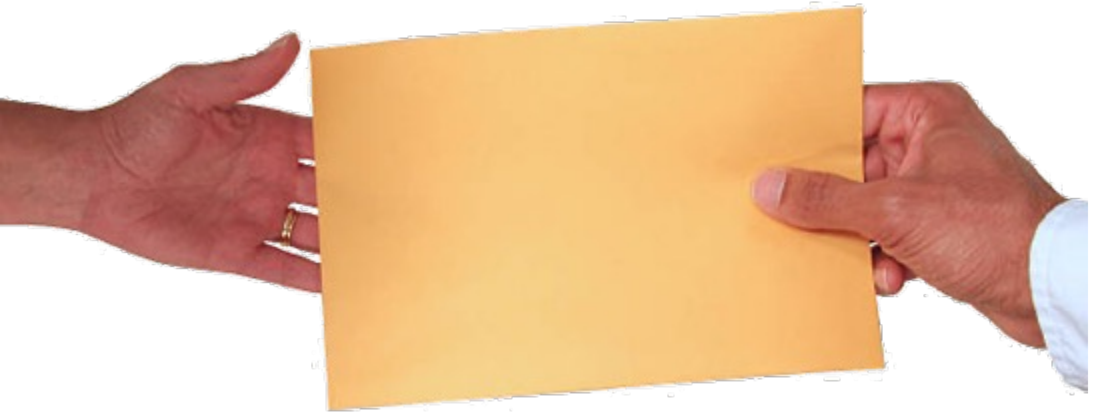


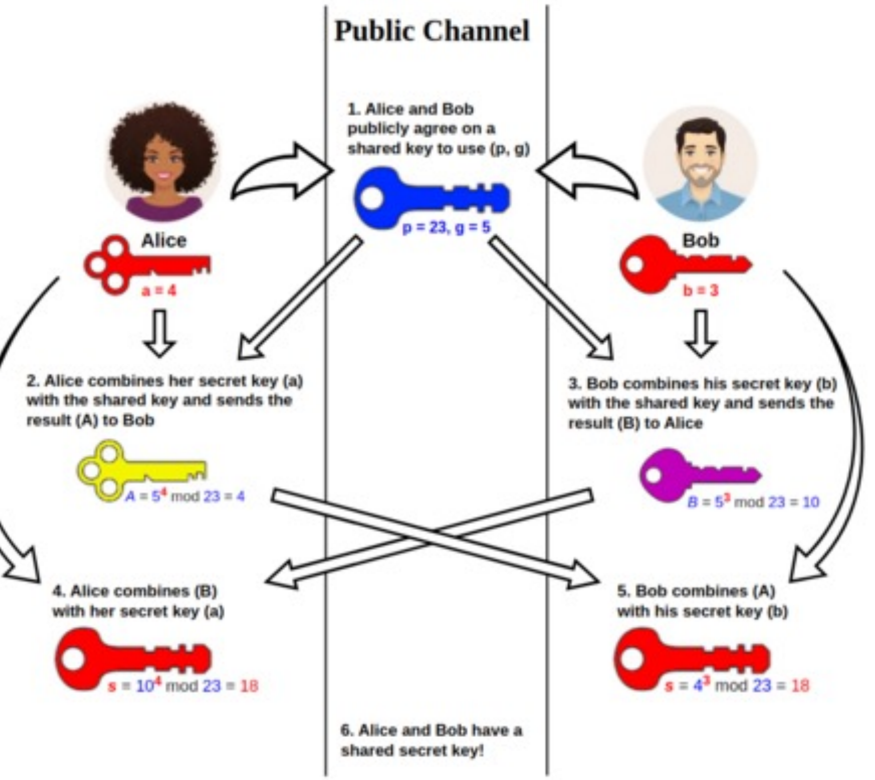
Encryption Key Exchange Mechanisms

Pre-Shared Keys

Public Key Exchange

Diffie-Hellman RSA





Public Key Exchange

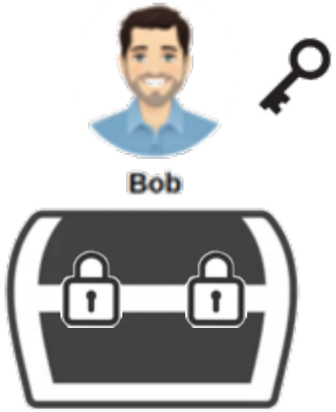
Alice has a sensitive message she wants to send to Bob

Adtran

General Business

SECURITY IMPLICATIONS

Public Key Exchange



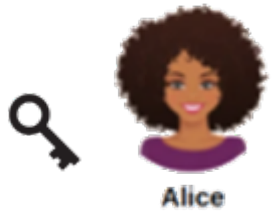
Bob returns the chest but with his lock also on it

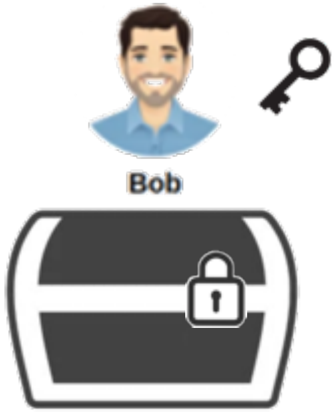
Public Key Exchange

Alice removes her lock and sends the chest back to Bob

General Business

Public Key Exchange





Bob removes his lock and reads the sensitive message

General Business

Real World Example of Primes to Make a Key

- $p =$
- 2971458192912397553811340175709686724750388804989712615528203668465542709844310552501401103762759517163627074312300265853912636278197597517576533794406803241491487790860157668289172727741435408491315121269955609950440336455795292134280100449228099671566840010364081684397099163631337274547031545503562860140817041707902804137532298861348955512618446376653439654060723569636406878004605013608944323924119875536307539941661988024079366566613068693004264183447100863184812617956794366766680110424189888441081281727916959593272856404539854080938169871021862587650885129561336897197943095174672858391041311643993907843455 9
- $q =$
- 2609203912543966574441623826039869743564840601709886444997854427162480573805938313425992696655318302051377220149644513804110037238043395102252847401736180367530090352701507591347416951209045911834751240500552004279927007879476871253684211840705737528249080071658400067934061838733136888145432891358536677962307041670917256390000904288466136745705695503949286491053230863150797994788726225314902611496553120815210253471812969971888039606870756712164088894663450500851157716280656558837830275852565791410359822928542019832310081202449335708888284023348338916840006706799317881081381849852208810358218375494042162144641 7

Factorized into two primes with 617 digits each

Adtran

A Real World Key Example

- $N = p \cdot q =$
- 77531403429078523049988340119687077029548048759850346672190025275585318721713336719288993898440300657694634560742145218730124241748829733826038031477004517606828731126814
9543742295663292645166691181035[illegible]3046435142321826042710505464762834
5917553138807968712884105599687[illegible]6959856396597061910708529414442565
6976908401424588046241791797069108332143157744689598705328768164624227834748573779946
6429770557[illegible]61062631453
2199364185950961601108509383989954266463609760139400437548746107130983414614152886086
4657796722939[illegible]595696742613691
5587251087982793730319047942684290247837937168029005694266709072999000209169509889194
7923874742058970193501315306024016667936062138529363725041845278245943874569204577896
6576515999552523983585405643139920000742186507873112890252675108406028012334471537050
6792791739260271351405730028340055756361203887336318174413457644503585933217428420582
8618205611680377987597584948629932517306030865860147025275593727055966386284032799690
1373606181123685884369021330533393228419680068904157639265770988392496177643587928979
411490167652215155315143892840077765952 5103

Factorization

Working out the original two large prime numbers that made up this number

RSA key length 4096 bit = decimal integer with 1233 digits

General Business

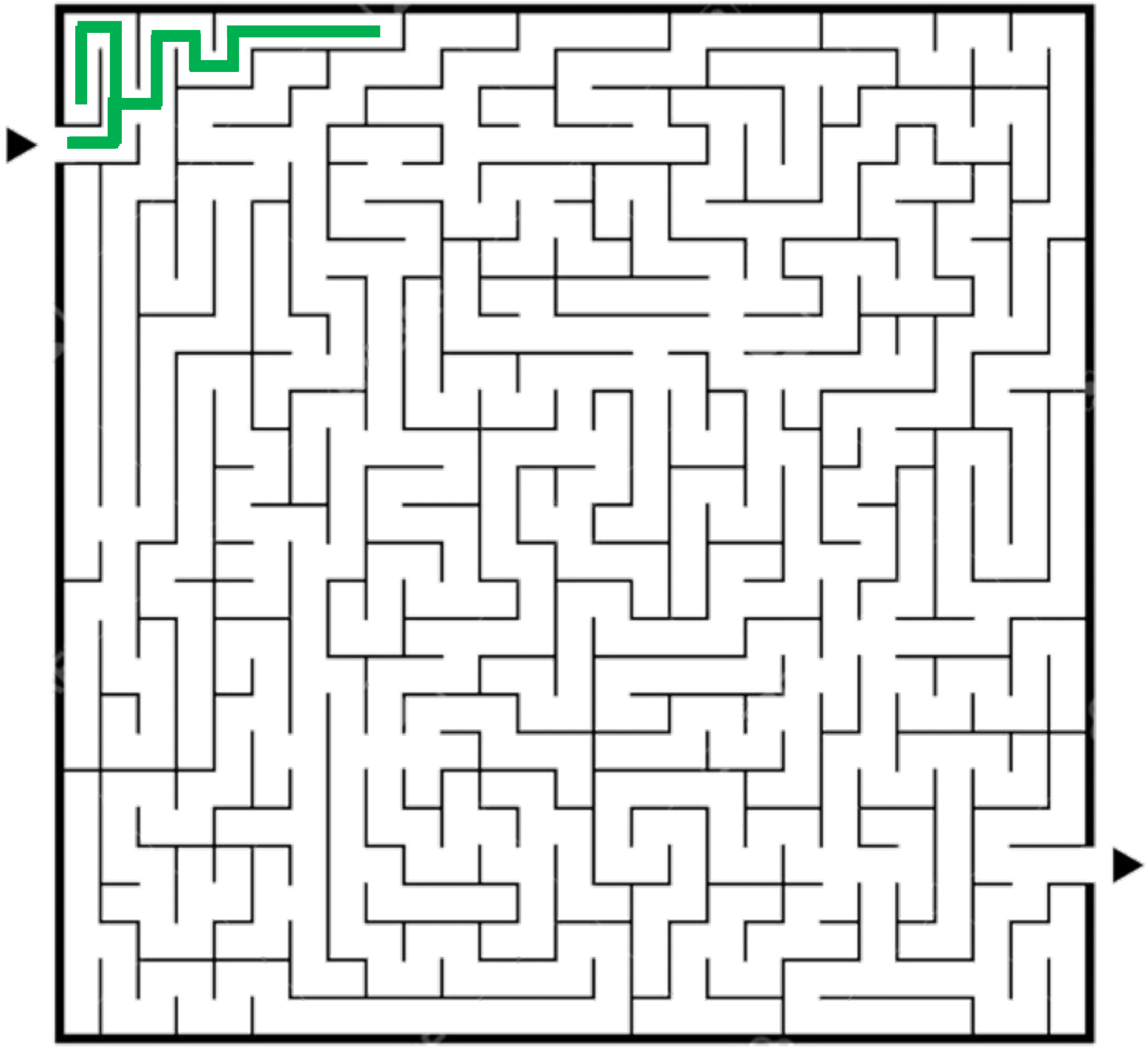
Classical vs Quantum Computing

A Classical Serial Approach to
Identifying the Correct Path or Key

How long does it take to **factor** 2048-bit integer?

Classical cost of factoring [1]:
~4.7 billion CPU years

[1] Kleinjung, T., Aoki, K., Franke, J., Lenstra, A. K., Thomé, E., Bos, J. W., ... & Zimmermann, P. (2010, August). Factorization of a 768-bit RSA modulus.



Quantum Focuses on the Lock – Not the Contents

Quantum computers do not break the encrypted data

- The focus is on breaking the key exchange algorithms.
- Once the key exchange algorithm is compromised, they can access the key and can use it to decrypt all the data.

Focus on the key exchange protocol options

- Quantum-safe classical algorithms
- Quantum bits for key exchange -> quantum key distribution (QKD).

General Business

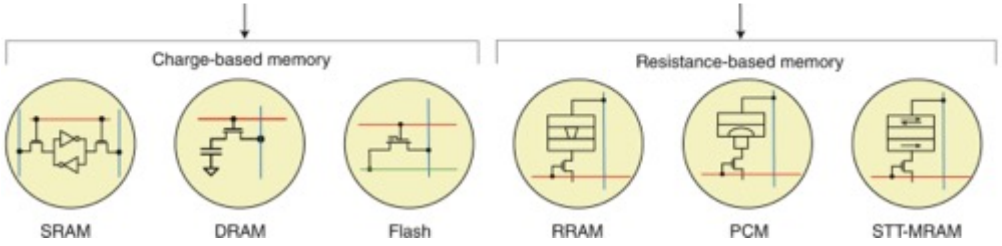
Classical vs Quantum Computing

Classical bit

0

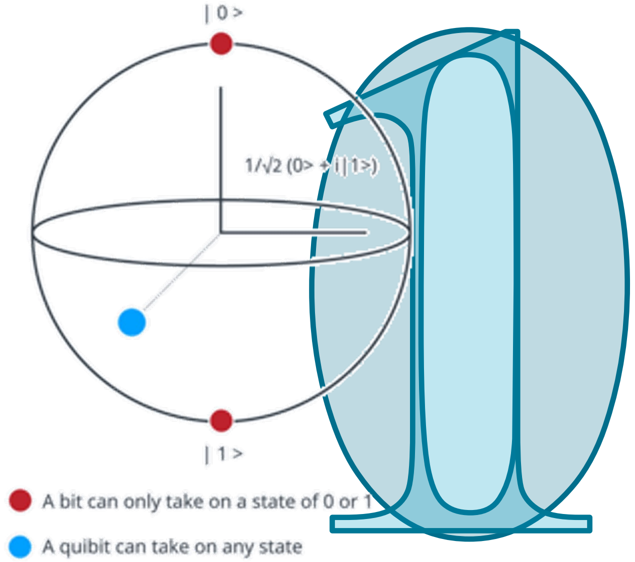
or

1



Nat. Nanotechnol. **15**, 529–544 (2020).

Quantum bit (qubit)



2 qubits

$$|00\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix} \quad |01\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix} \quad |10\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix} \quad |11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

2 Bits can provide 2 Unique Values – 2 Qubits can provide 4 Unique Values

Classical vs Quantum Computing

Classical computer

- A **bit** can have a defined state 0 or 1
- A combination of 3 bits can represent exactly **one** of $2^3=8$ distinct values

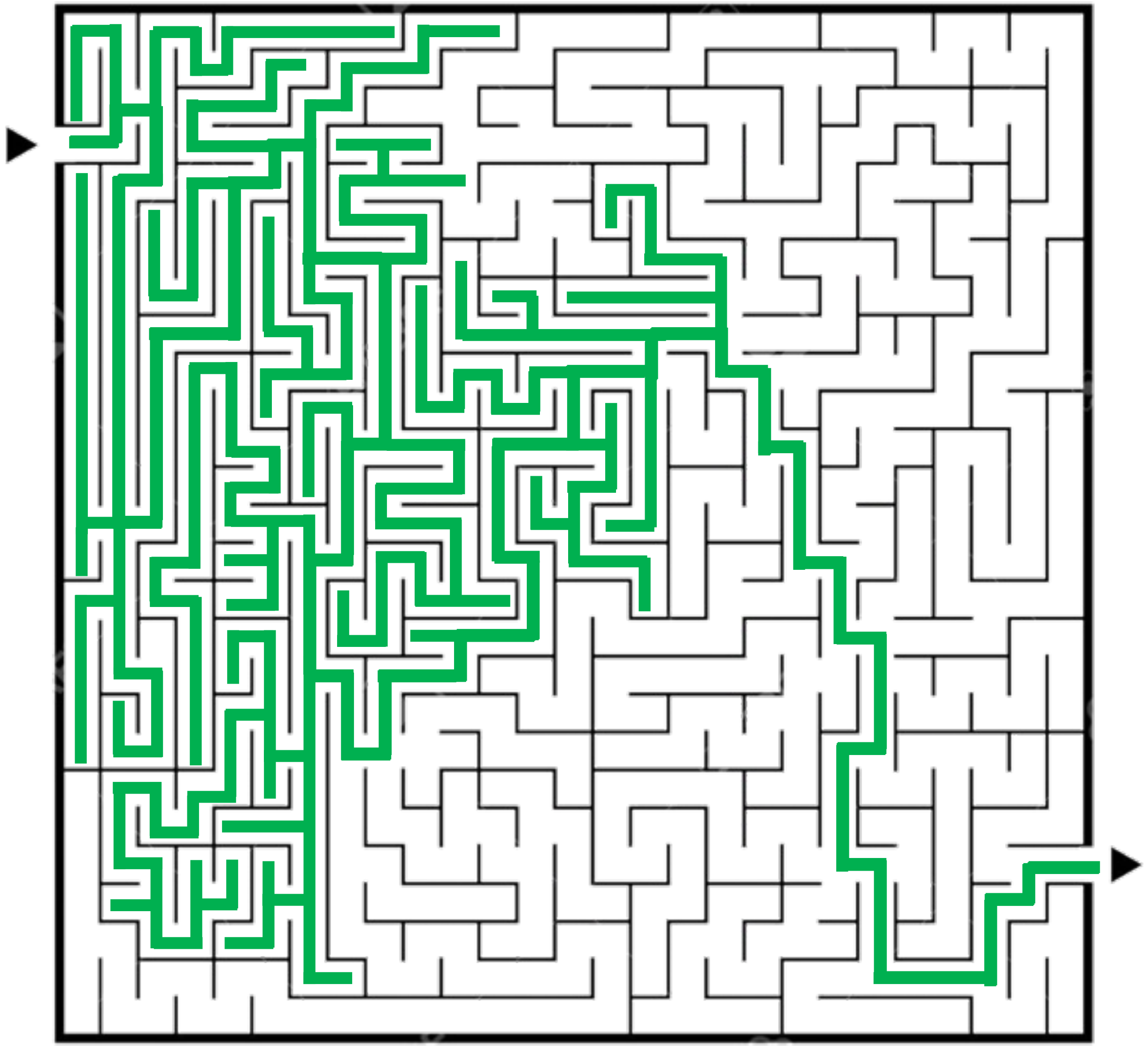
000, 001, **010**, 011, 100, 101, 110, 111

Adtran

General Business

Classical vs Quantum Computing

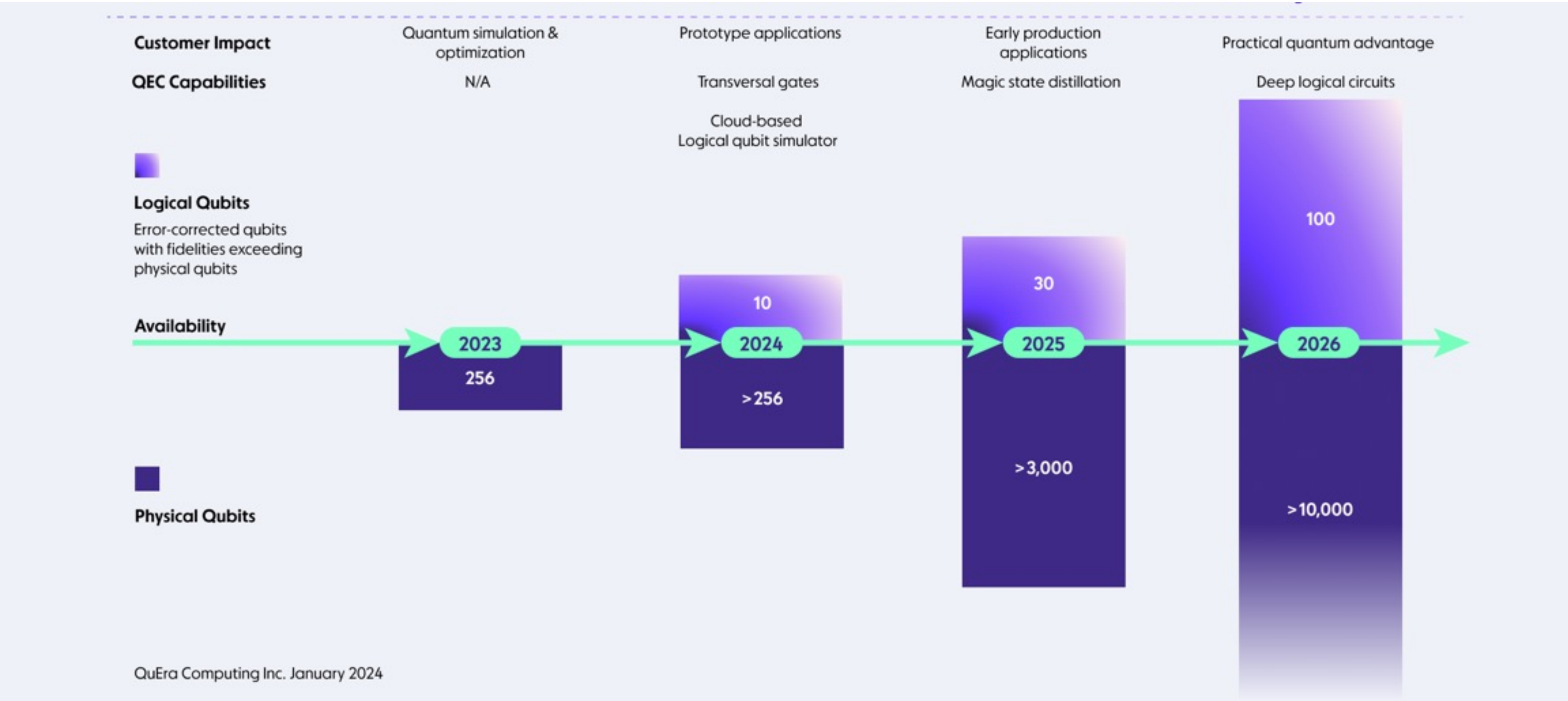
A Quantum Parallel Approach to Identifying the Correct Path or Key



Adtran

General Business

Logical vs Physical Qubits

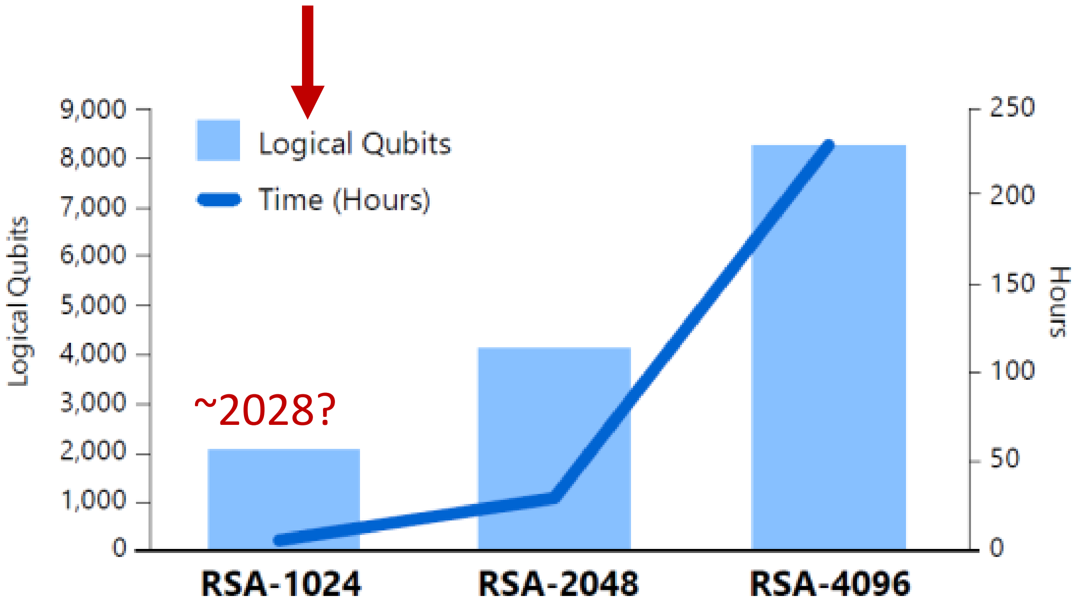


Adtran

General Business

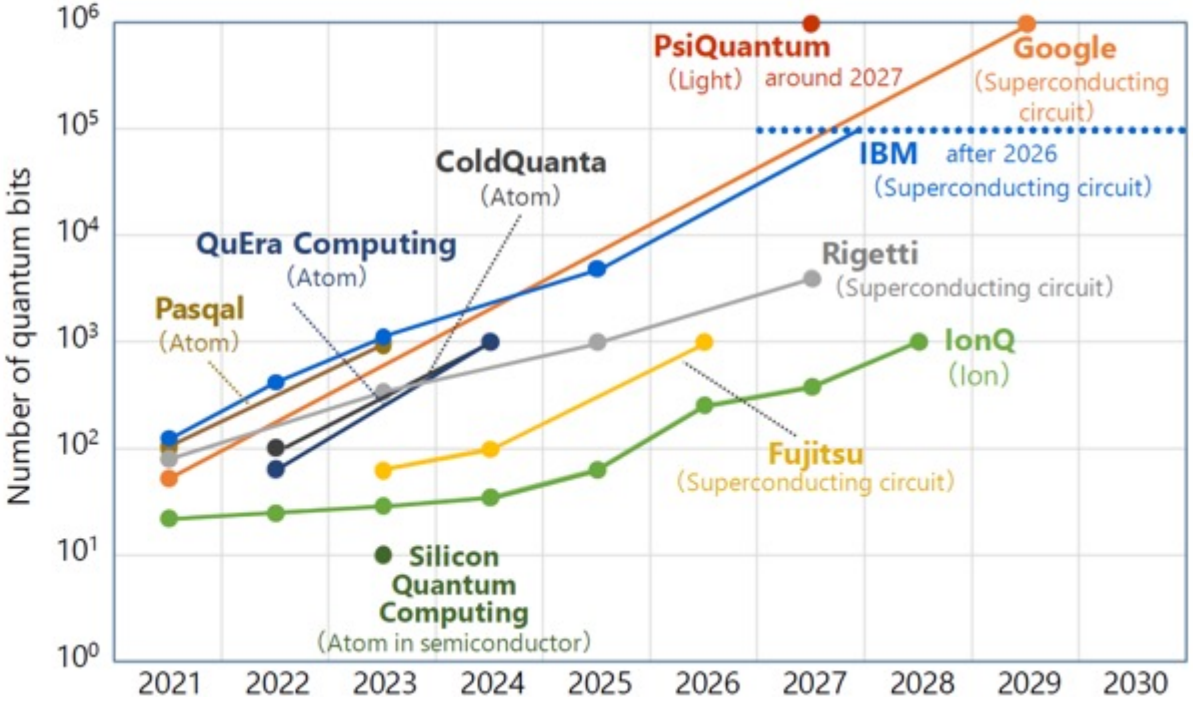
So, how many qubits are needed to break RSA?

- Estimation of RSA quantum resilience by key length



Source: QED-C, data from National Academy of Sciences, Engineering and Medicine, 2019. "Quantum computing: progress and prospects. Washington DC: The national Academies Press. https://doi.org/10.17226/25196

- Roadmap for physical Qubit count



Adtran

Post Quantum Cryptography

NIST **Post-Quantum Encryption Standards Project**

Lattice Based Post-Quantum Encryption

The "Cryptographic Suite for Algebraic Lattices" (CRYSTALS) encompasses two cryptographic primitives: Kyber, an IND-CCA2-**secure key-encapsulation mechanism** (KEM); and Dilithium, a strongly EUF-CMA-**secure digital signature algorithm**.

Hash Based Post-Quantum Encryption

SPHINCS+ is a **stateless hash-based signature scheme** developed in collaboration with industry and academic institutions

Other Post-Quantum Encryption Approaches

Code Based McEliece Cryptosystem, is the most well-known, based on decoding random linear codes, as does the Niederreiter Cryptosystem & Quasi-Cyclic Moderate Density Parity-Check QC-MDCP

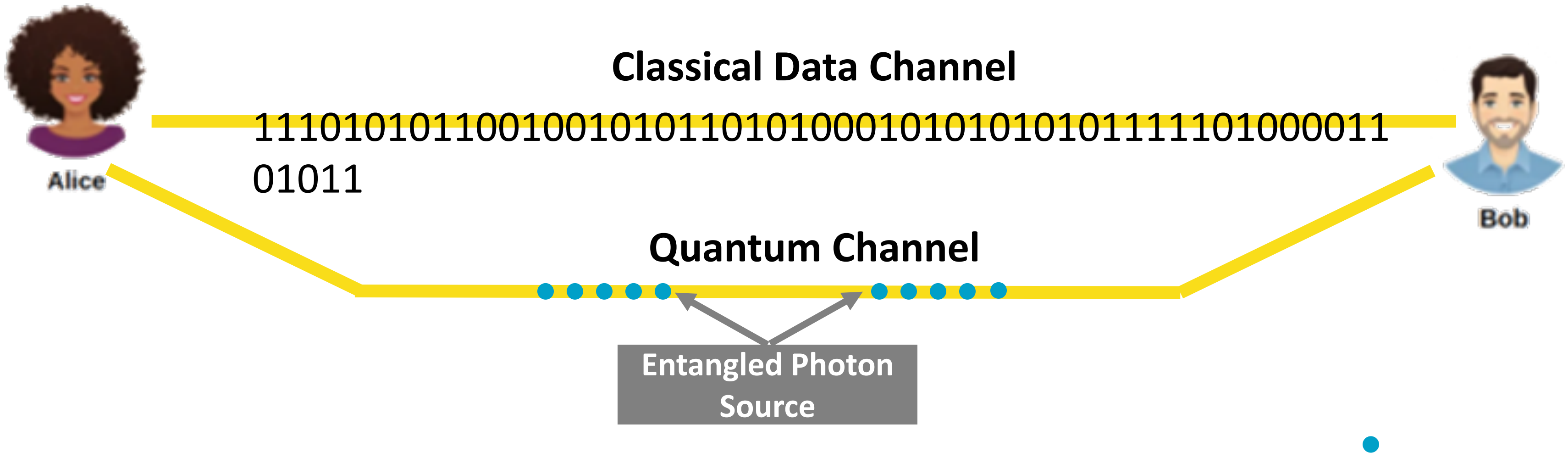
Multivariate, and Supersingular Isogeny

General Business

QKD
Quantum key distribution

QKD

Quantum Key Distribution



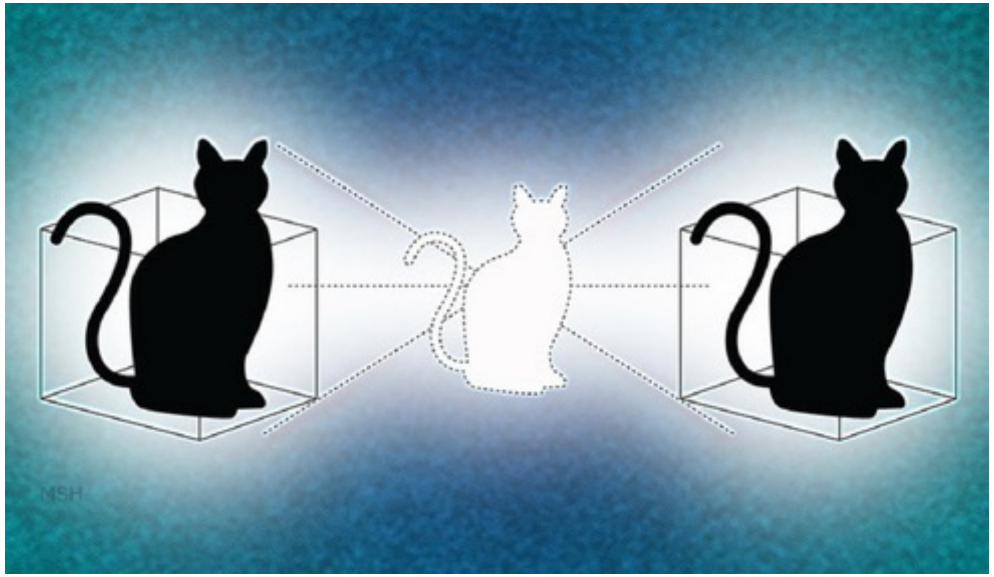
Adtran

No-Cloning Theorem

- Can you copy a Qubit (or photon) in superposition?
  - No!

- Measurement or observation “destroys” a superposition state
  - Known as no-cloning theorem

The engaged party are alerted to the interception

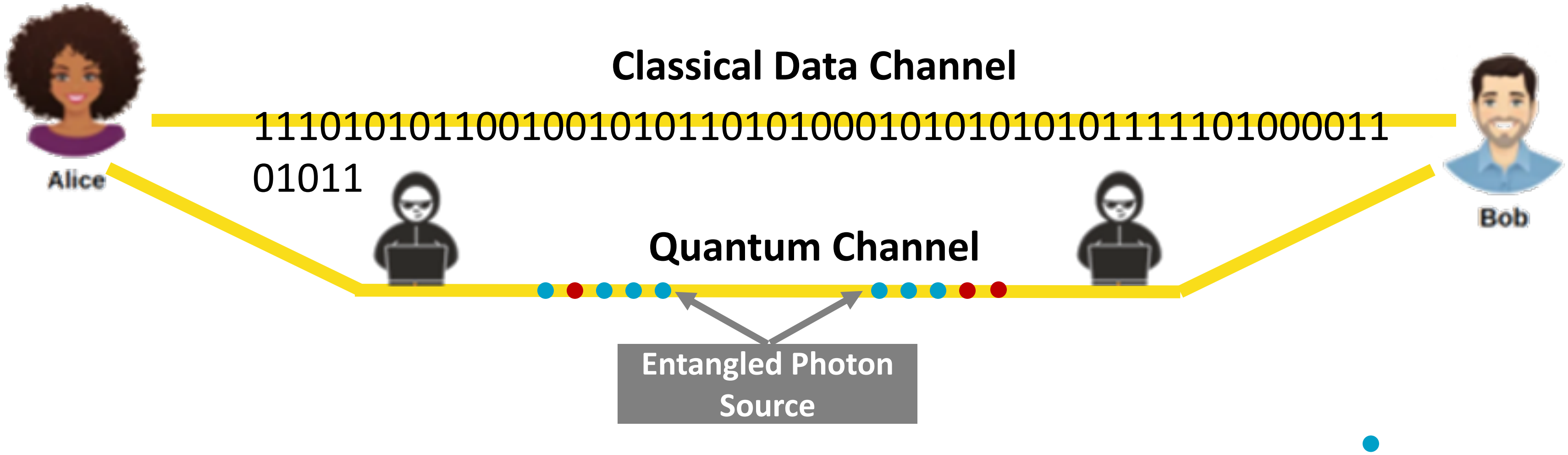


(Illustration by Michael S. Helfenbein)

General Business

QKD

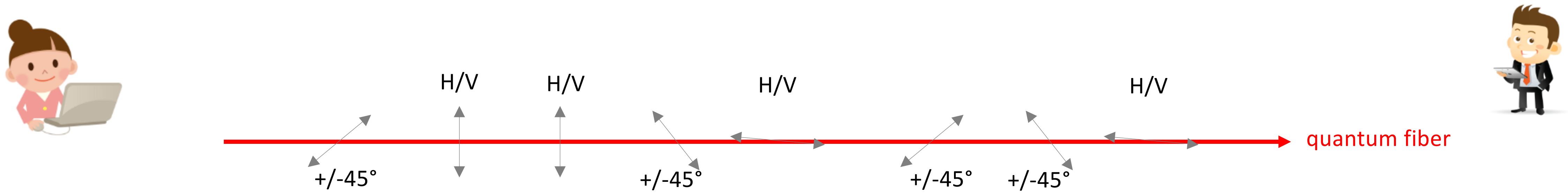
Quantum Key Distribution



Adtran

General Business

Quantum key distribution



Alice's bit sequence	**1**	**1**	**1**	**0**	**0**	**1**	**0**	**0**
Bob's measuring basis	H/V	H/V	+/-45°	+/-45°	H/V	+/-45°	H/V	+/-45°
Bob's results	0	1	0	1	0	1	1	1
Key	-	1	-	-	0	1	-	-

What's your measurement basis?

classical fiber

My basis was (+ or x)

Here, the shared secret key is 1-0-1

General Business

QKD alone is NOT “fundamentally secure”

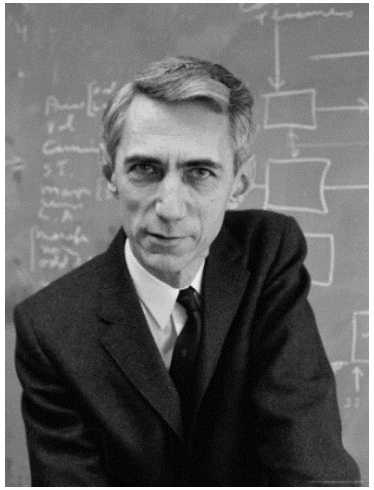
- Today’s digital communication
- **Security** = **Secure Key** + **Secure Encryption + Authentication + Protection**

- Practical QKD provides the keys, but lacks security quantification and measurable metrics
- OTP is the only known fundamentally secure algorithm
- Digital security can’t substitute physical protection

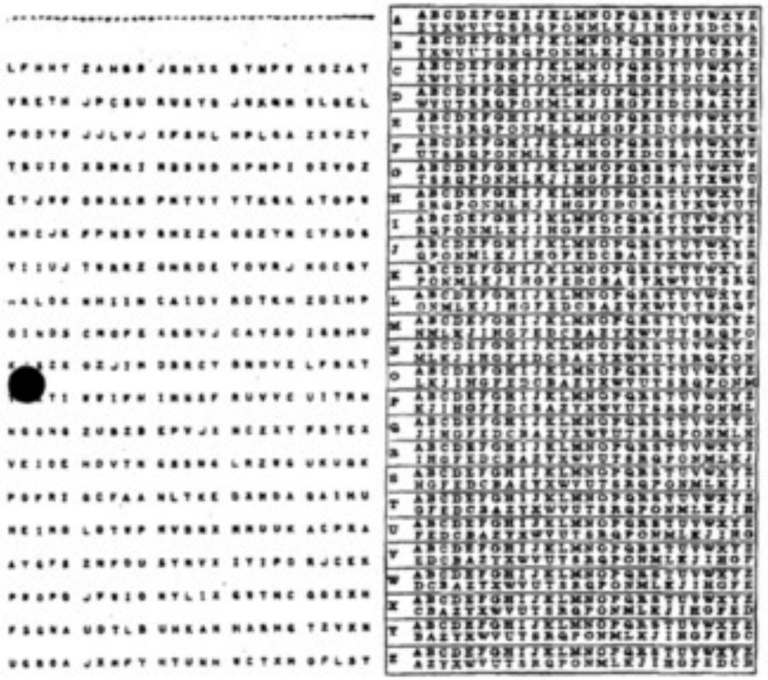
No silver bullet, but best practice

True quantum-safe: One-Time Pad (OTP)

- Key has same length as message and is used only once
- Key is fully random → highest entropy
- Theoretically unbreakable by Shannon



OTP used by the NSA:



Source: Wikipedia

OTP transforms the encryption problem into a key exchange problem

Fibre Ubiquity Must be Matched by Ubiquitous DDOS Mitigation

AES / RSA Secure in the Mid Term

Quantum Has Many Hurdles to Cross

Ronan Kelly
Adtran CTO EMEA

Adtran