Everything is Quantum

Our mission is to keep KPN reliable & secure and trusted by customers, partners and society – part of the vital infra of NL

CISO

kpn

Contents

Whats the problem?

- Surveillance Problem / Weak Crypto /& Threat
- Explain Quantum Computing – superpositioning, entanglement, fragility, nocloning - types of computers/annealing/ universal
- What's everyone up to? DWAVE/DELFT/IBM/NSA Are we there yet?

What are we going to do about it?

- Explain the Plan (3 steps)
- Back up from NSA / AIVD -> key length (maybe use time slide)
- QKD explanation & QKD attacks
- Free Space
- Post Quantum explanation Lattice ,Post Q attacks Soliliqy , SIDH
- Whats everyone doing – Europe plan / UK / Chinese slides
- Crypto currencies
- Google – quantum supremacy experiment w/in 1 year
- IBM – cloud
- KPN

The Threat

- Intelligence agencies possess total information awareness - 2011
  - Location ; contacts & confederates; digital life dossier;
- Intelligence agencies fear of crypto – Going Dark problem
- Despite Snowden revelations - lack of informed public opinion
- Renewed Global Crypto Wars

NSA Programs : Black Budget for Quantum research

- 'Penetrating Hard Targets' - project that aims to break strong encryption – development of a Quantum Computer
- 'Owning the Net' - facilitate offensive operations to compromise target networks – where quantum is part of a larger program

So what's this quantum stuff about?

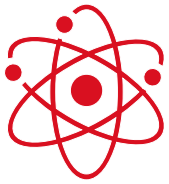
Classical physics

Before 1900

– Describes the **macro**scopic world –

– Deterministic –

– Intuitive –



Quantum physics

After 1900

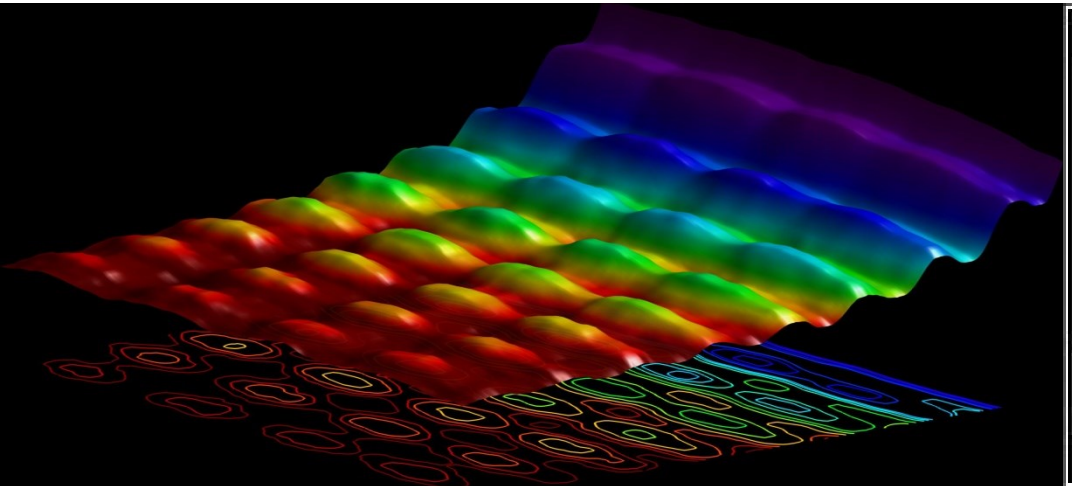
– Describes of the **micro**scopic world –

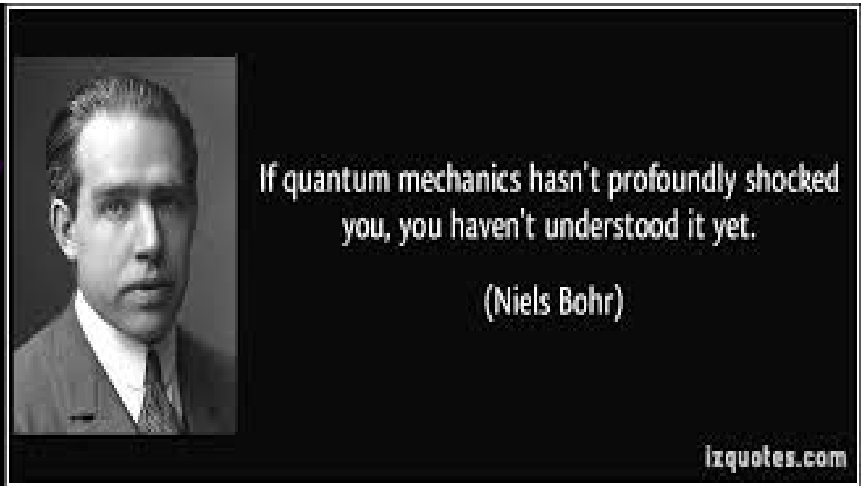
– Probabilistic –

– Central role of the observer –

– Not very intuitive –

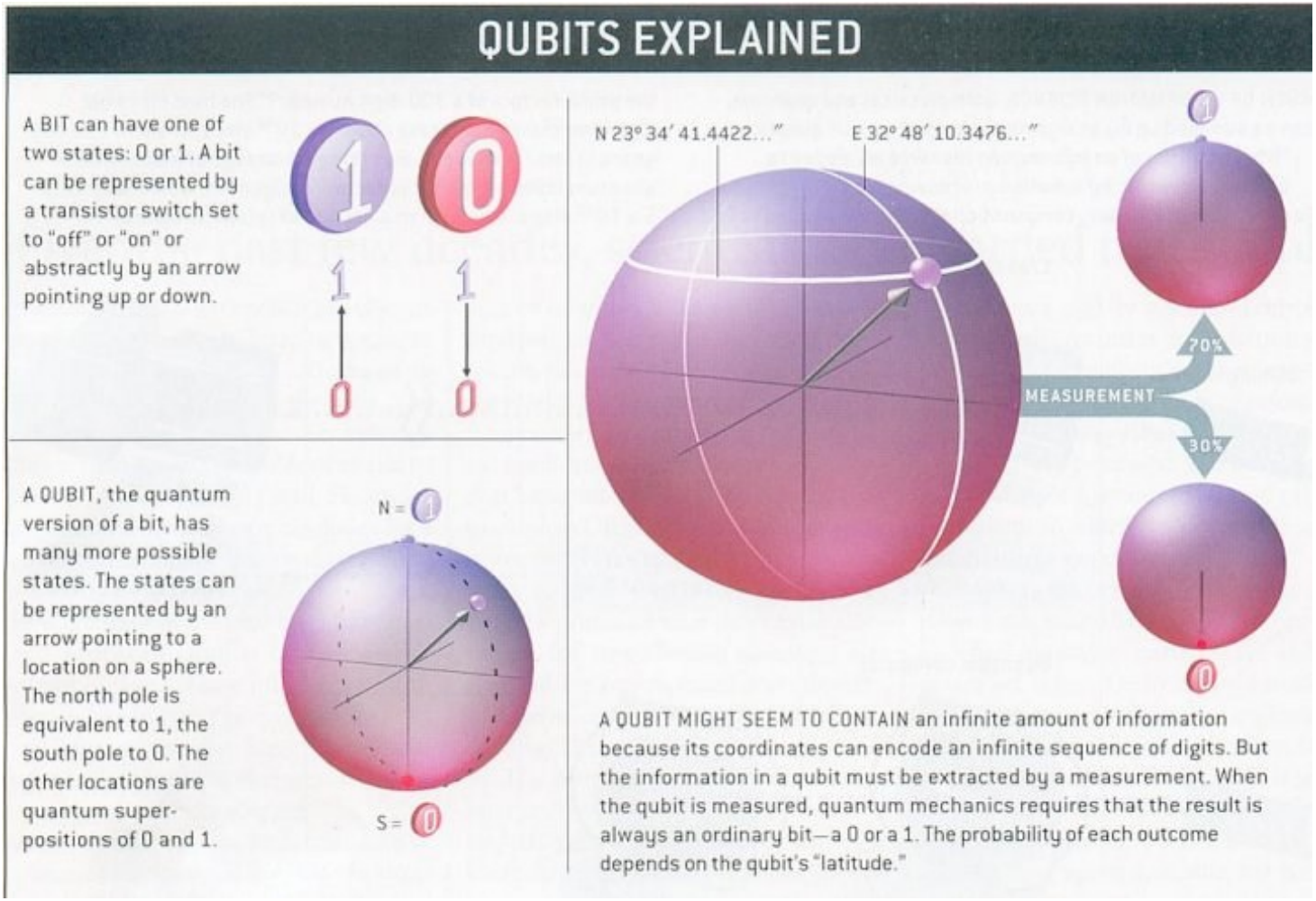
When will the Post Quantum Era arrive?
–A World with quantum computers





What are the properties of a quantum computer?

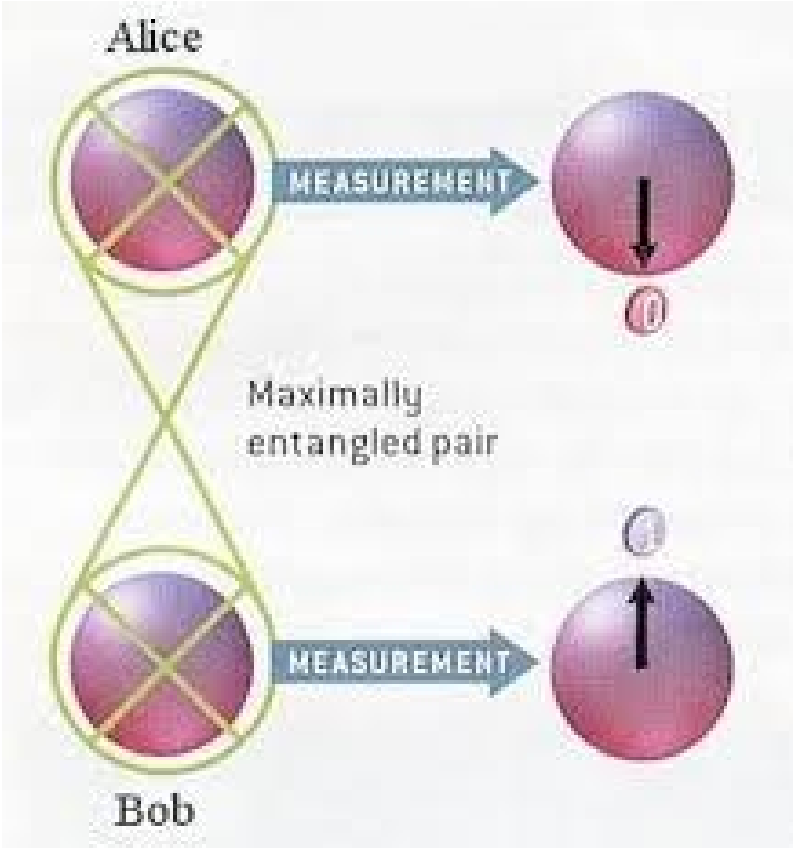
Current computers use bits but quantum computers use qubits.



Entanglement

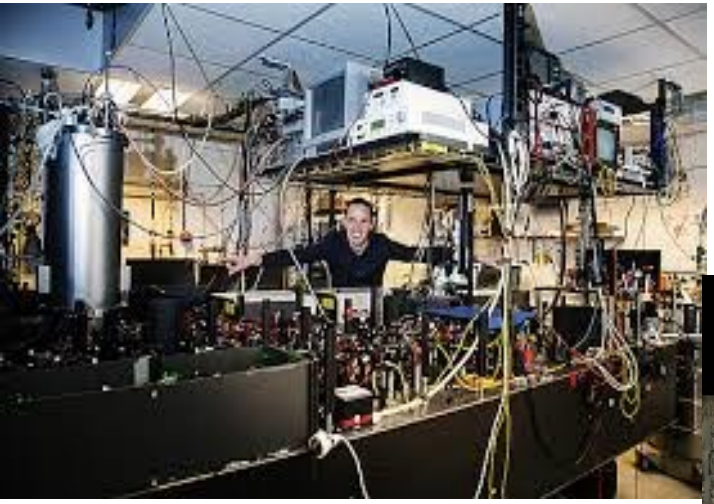
- ***It thus appears that one particle of an entangled pair "knows" what measurement has been performed on the other, and with what outcome, even though there is no known means for such information to be communicated between the particles, which at the time of measurement may be separated by arbitrarily large distances***

- Its entanglement that gives quantum computing the ability to scale exponentially, as entangled qubits can represent 4 states. The more linked qubits, exponential increase in states and thus computing power.

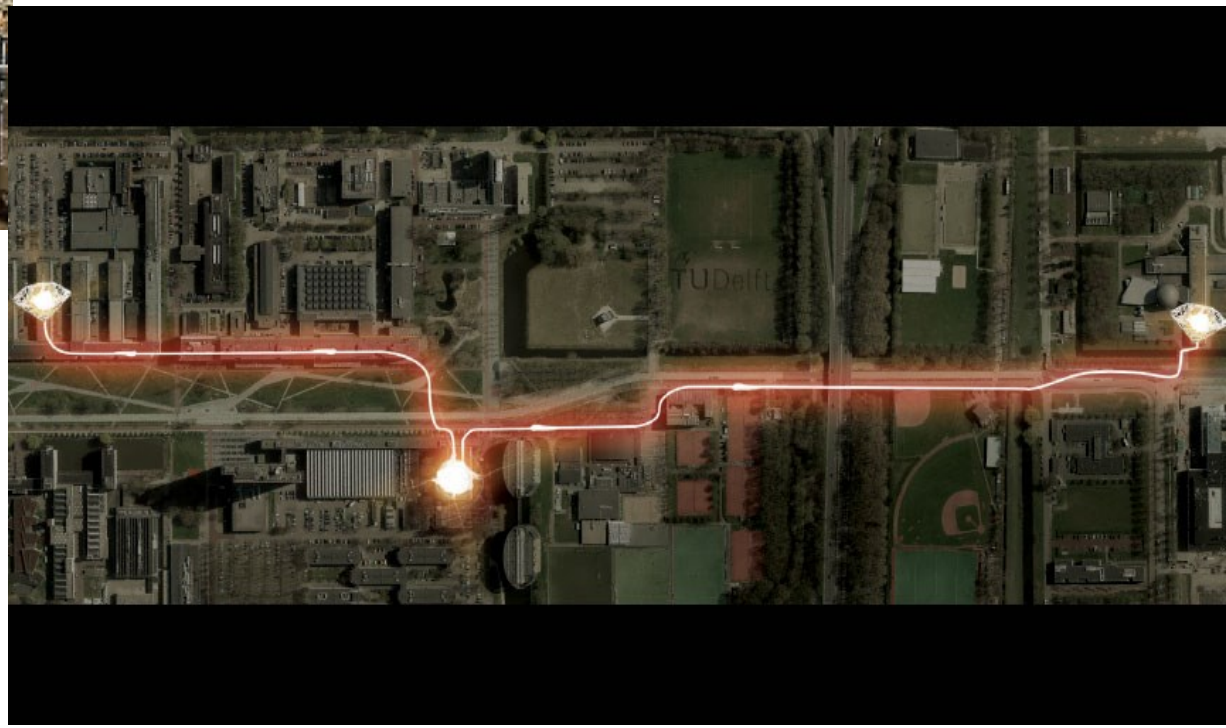


Entanglement
Loophole Free Bell Test

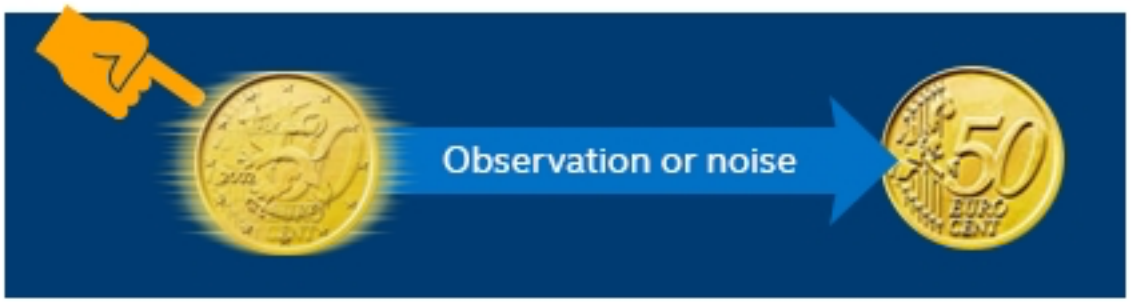
Ronald Hanson –TU Delft



Spooky Action at a distance



Fragility & No-Cloning

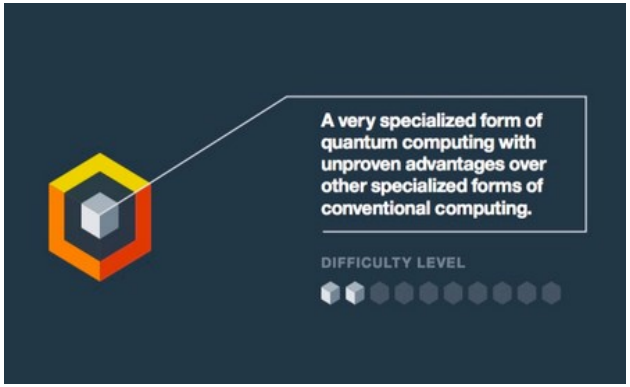


A **quantum state** collapses to a classical state if disturbed by noise or measurement.

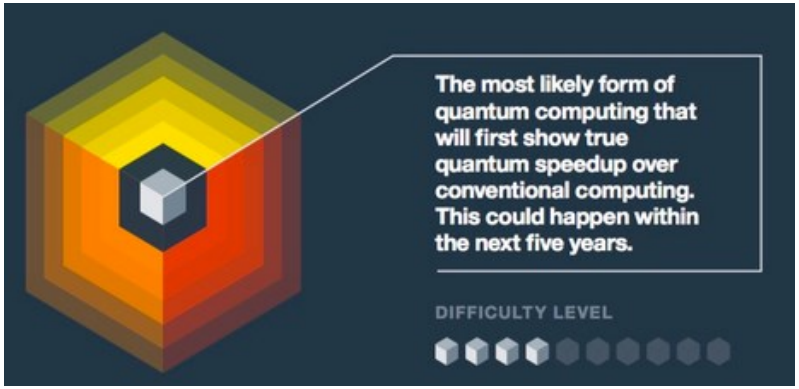
One **cannot** copy, intercept or steal without ruining a quantum state.

There's more than 1 type of Quantum Computer?

- Quantum Annealer



- Analog Quantum



- Universal Quantum Computer

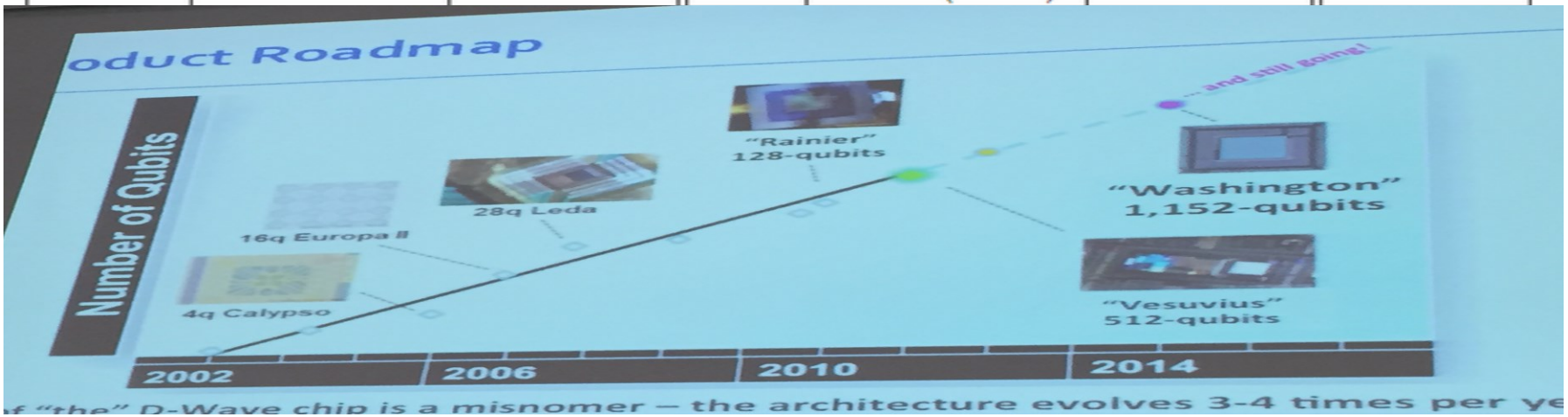
What's it all mean?

- Amdahl's Law & processing power
- Shor – integer factorization
- Grover – unsorted database
- Other really cool stuff
- Everyone is trying to do this – globally –
- European Commission 1bn Euros

Are we there yet?

Viable Quantum Computer:: currently – no

Factoring algorithm (RSA)			EC discrete logarithm (ECC)			classical
n	$\approx$ # qubits	time	n	$\approx$ # qubits	time	time
	$2n$	$4n^3$		$f'(n)$ $(f(n))$	$360n^3$	
512	1024	$0.54 \cdot 10^9$	110	700 (800)	$0.5 \cdot 10^9$	C
1024	2048	$4.3 \cdot 10^9$	163	1000 (1200)	$1.6 \cdot 10^9$	$C \cdot 10^8$
2048	4096	$34 \cdot 10^9$	224	1300 (1600)	$4.0 \cdot 10^9$	$C \cdot 10^{17}$
3072	6144	$120 \cdot 10^9$	256	1500 (1800)	$6.0 \cdot 10^9$	$C \cdot 10^{22}$
15360	30720	$1.5 \cdot 10^{13}$	512	2800 (3600)	$50 \cdot 10^9$	$C \cdot 10^{60}$



What are we going to do about it?

1. Increase Key Length of Current Crypto used

2. Investigate options for Quantum Key Distribution for high critical links with demands for long term secrecy

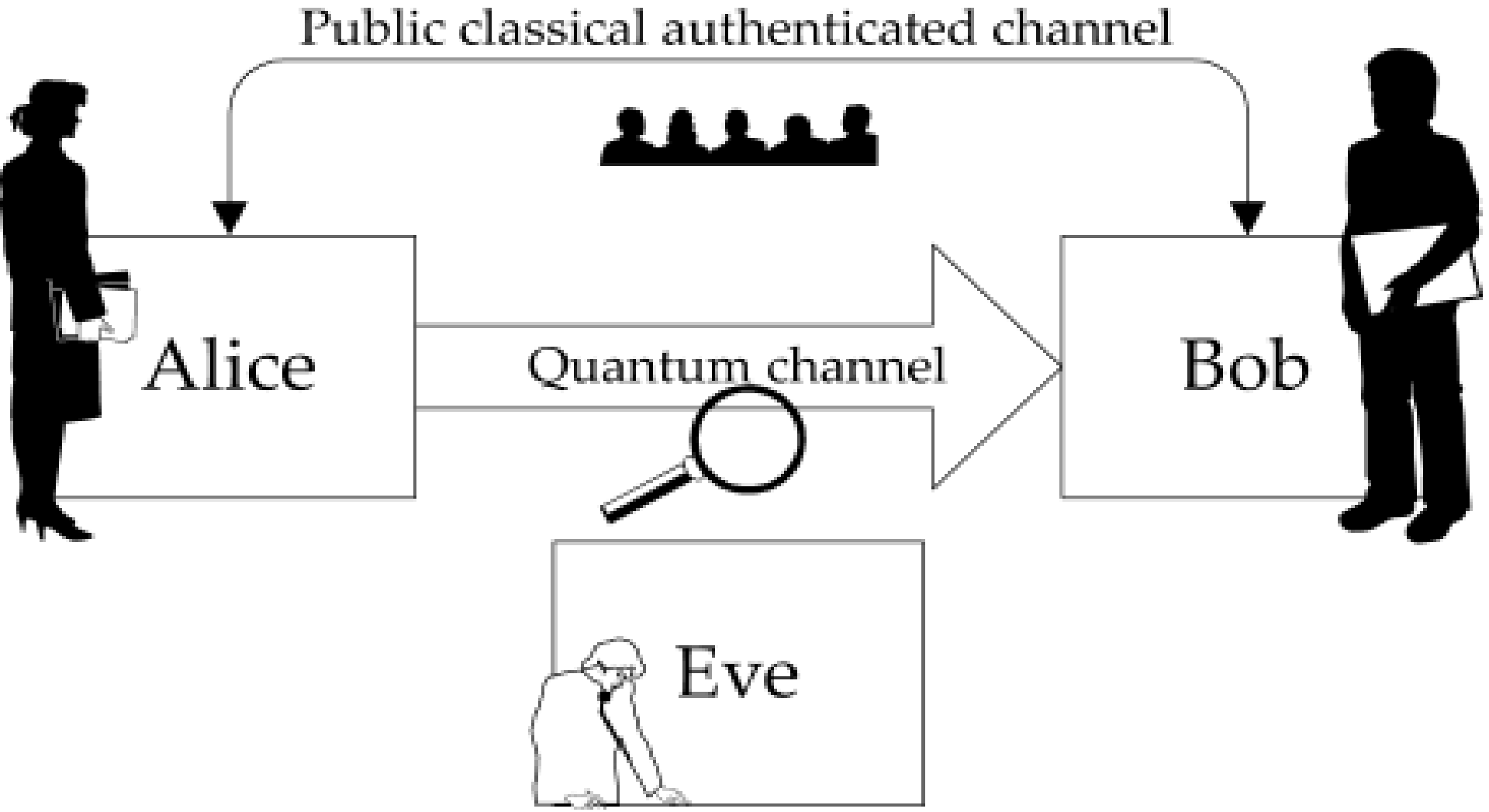
3. Investigate Post Quantum Cryptographic Algorithms and determine deployment strategy

Key length -> NSA Advice

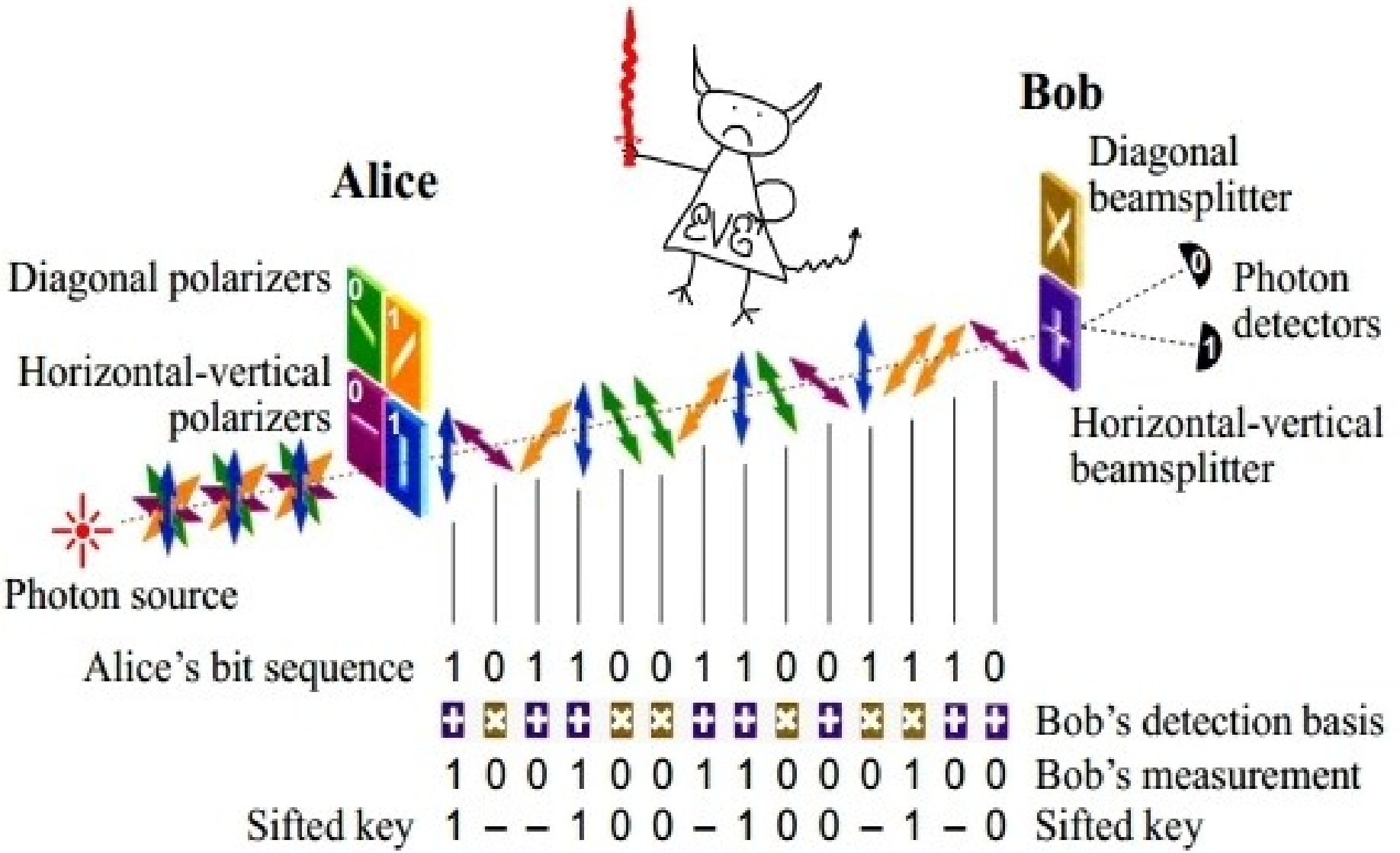
"IAD will initiate a transition to quantum resistant algorithms in the not too distant future."

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher used for information protection	FIPS Pub 197	Use 256 bit keys to protect up to TOP SECRET
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	Asymmetric algorithm used for key establishment	NIST SP 800-56A	Use Curve P-384 to protect up to TOP SECRET.
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithm used for digital signatures	FIPS Pub 186-4	Use Curve P-384 to protect up to TOP SECRET.
Secure Hash	Algorithm used for	FIPS Pub 180-4	Use SHA-384 to

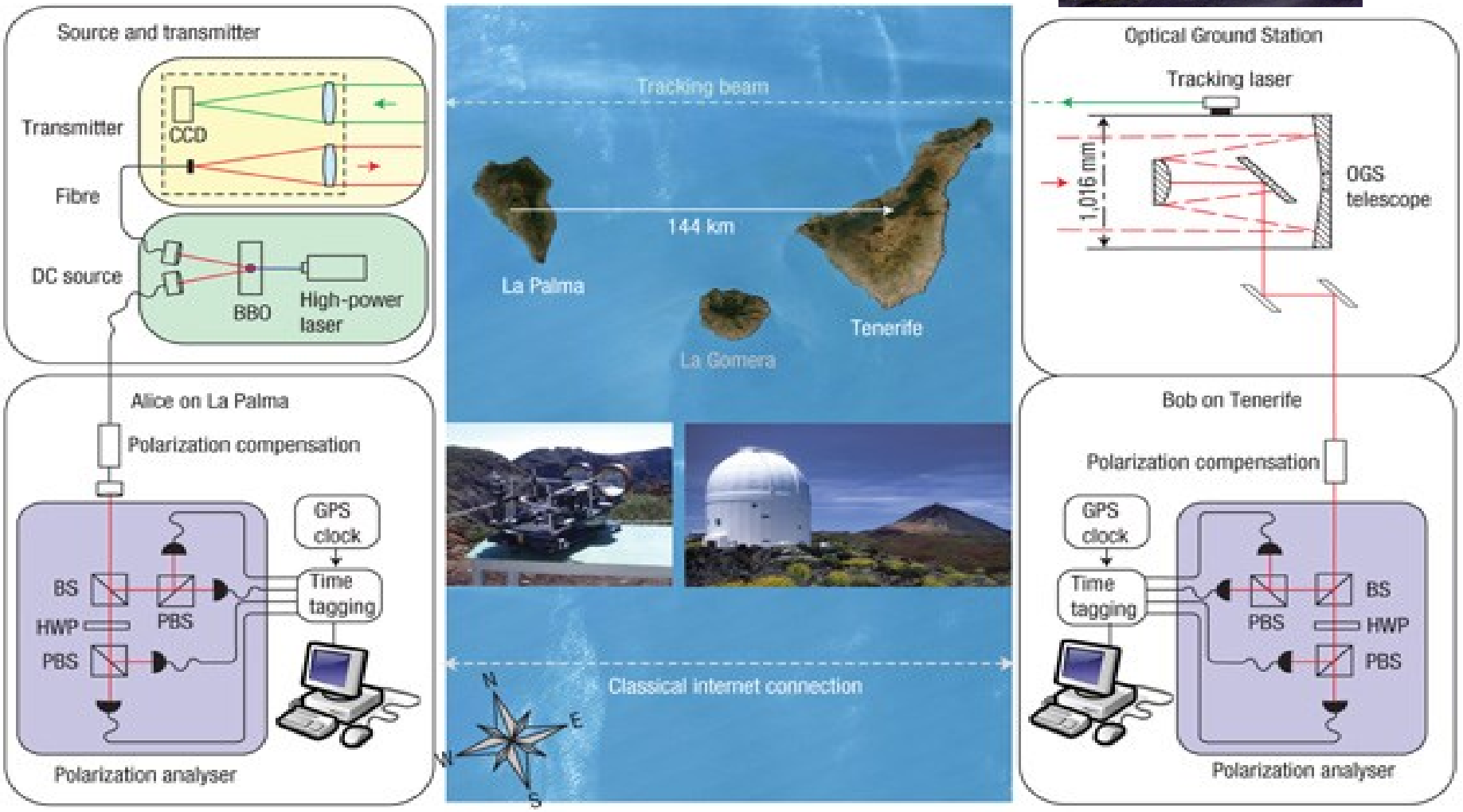
Quantum Key Distribution – QKD



QKD


Alice
Bob
Diagonal polarizers
Horizontal-vertical polarizers
Photon source
Diagonal beamsplitter
Photon detectors
Horizontal-vertical beamsplitter
Alice's bit sequence 1 0 1 1 0 0 1 1 0 0 1 1 1 0
Bob's detection basis
Bob's measurement 1 0 0 1 0 0 1 1 0 0 0 1 0 0
Sifted key 1 – – 1 0 0 – 1 0 0 – 1 – 0
Sifted key

Free Space QKD



Global Developments –
Qiang Zhang – Uni. of Science & Technology of China

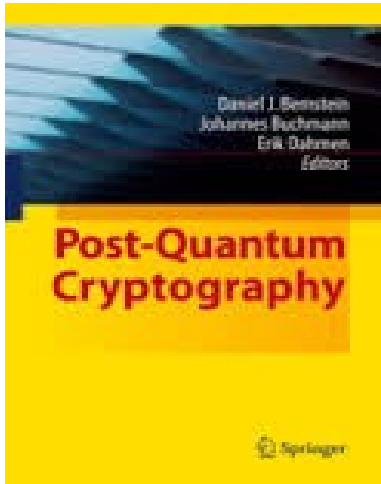
Quantum Backbone

- Total Length 2000 km
- Metropolitan networks
  - Existing: Hefei, Jinan
  - New: Beijing, Shanghai
- Customer: China Industrial & Commercial Bank; Xinhua News Agency; CBRC

Post Quantum Cryptography – PQCRYPTO
A new hope

- PQCRYPTO.org -> Tanja Lange & Dan Bernstein
- Lattice Based - McElise since 1978
- CESG & Soliliqy
- Supersingular Isogeny Diffie Hellman – (SIDH) – aka- 'the hottest thing we have'' – Phil Zimmermann - Post Quantum Crypto at internet scale

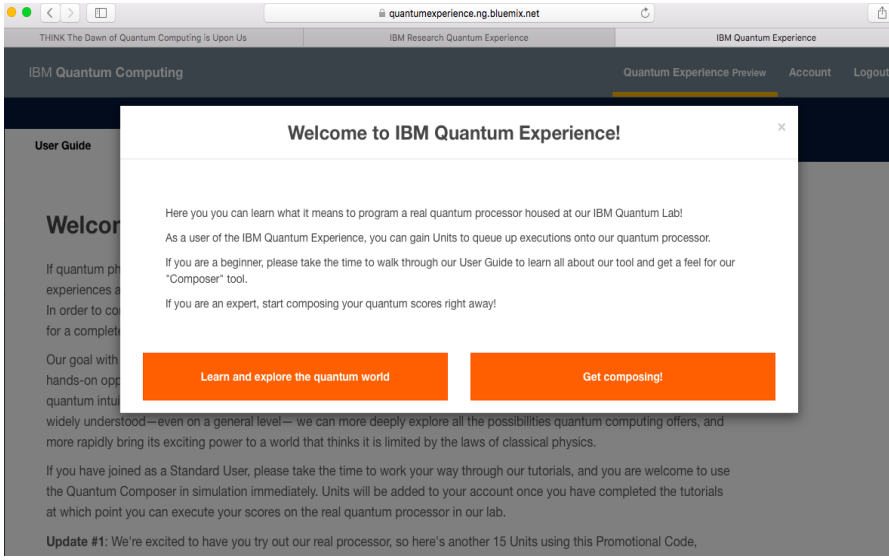
- *Without quantum-safe encryption, everything that has been transmitted, or will ever be transmitted, over a network is vulnerable to eavesdropping and public disclosure.* ETSI



KPN's Quantum leap with IDQuantique

In Conclusion…. We're just getting started

- IBM – Public Access to Quantum Computing Platform – 5 qubits
- Google – Quantum Supremacy Experiment – 50 qubits -within 1 year



What we will need in coming days, months, years:

- Common way forward – http://youtu.be/COxMJTh06zI
- Providing **thought leadership and action** in the field of future security controls
- Combining options for defense in depth – like we're used to

THANK YOU!
Questions? Comments? Stuff?

- Jaya Baloo
  - Jaya.baloo@kpn.com

Thanks – to all web content folks for images that were borrowed!