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

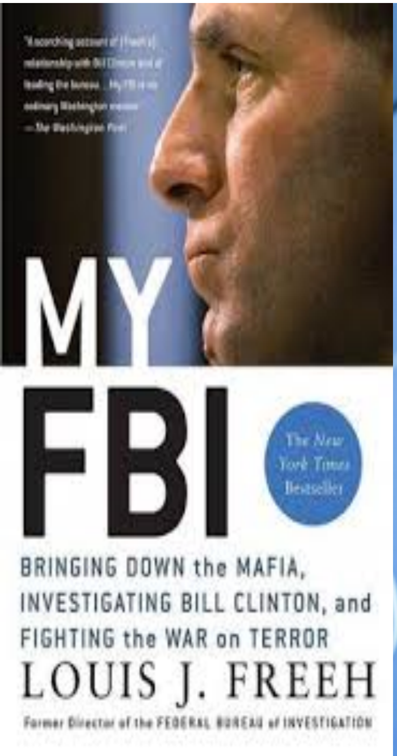
NSA Programs : Black Budget for Quantum research

- ‘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

DATA ON UK CITIZENS STORED FOR 1 YR
IN 'BIG BROTHER' STYLE SURVEILLANCE
NEWS
IVESTORS WHICH COULD FINALLY PREVENT IT DEFA

To Ban or Cripple Strong Encryption?

- The original crypto wars
- What do Freeh / Comey / Cameron-Teresa May / FR-Cazeneuve & DE - de Maizière ministers of interior want?
- On backdoors, front doors, and golden key management
- Magical Thinking

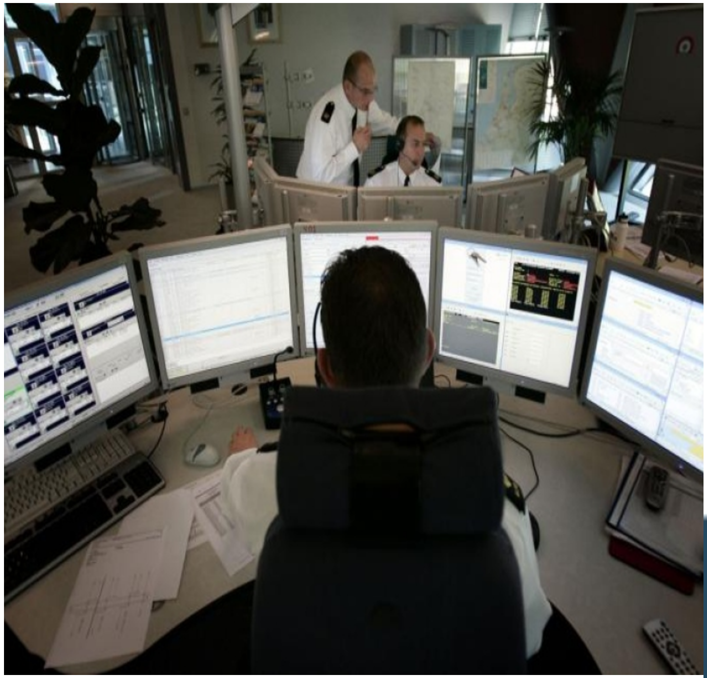

"A scorching account of [Freeh's] relationship with Bill Clinton and of leading the bureau... My FBI is no ordinary Washington memoir."
—The Washington Post
MY FBI
The New York Times Bestseller
BRINGING DOWN the MAFIA, INVESTIGATING BILL CLINTON, and FIGHTING the WAR on TERROR
LOUIS J. FREEH
Former Director of the FEDERAL BUREAU of INVESTIGATION

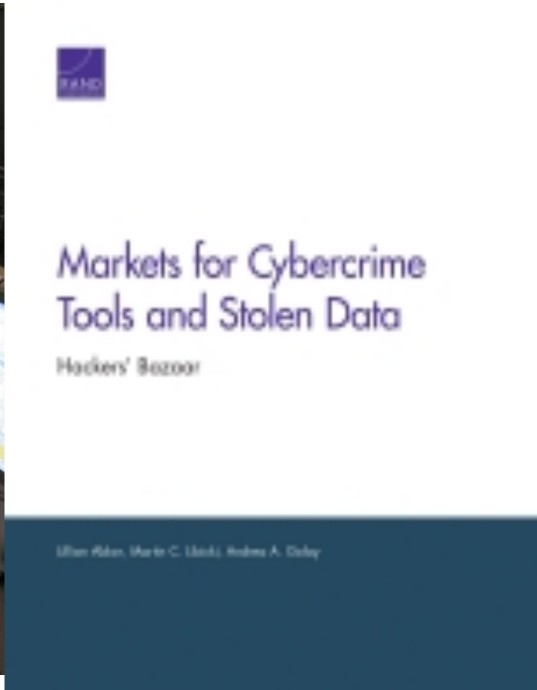
The Overhaul of Intelligence Regulations

- Investigatory Powers Tribunal (GCHQ - NSA) – 7 years of illegality - Draft Communications bill – Teresa May
- E.G. - Al Qaeda's Drafts folder – requires more than connection intercepts
- US Freedom Act -June 2, 2015
- **WIV (NL)- draft**

The Service Provider Pretzel

- Global phenomena of nationalism- Splinternet +++
- Hack Back vs. Guaranteeing continuity
- 3Musketeers– all for 1 target / 1 zero day for us all
- Trickle down effect of vulnerabilities





Markets for Cybercrime Tools and Stolen Data

Hackers' Bazaar

Lillian Ablon, Martin C. Libicki, Andrea A. Golay

So what's this quantum stuff about?

Classical physics

Before 1900

– Describes the **macro**scopic world –

– Deterministic –

– Intuitive –

Quantum physics

After 1900

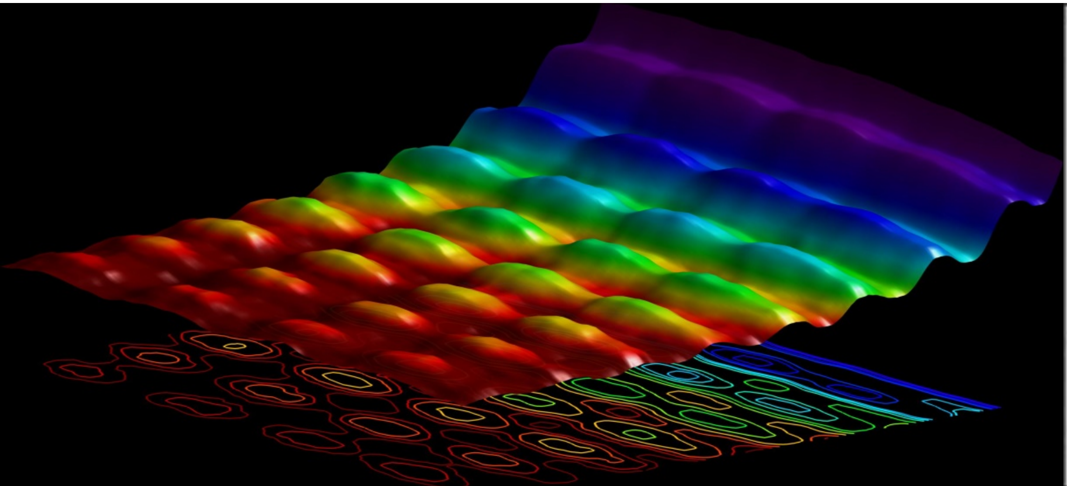
– Describes of the **micro**scopic world –

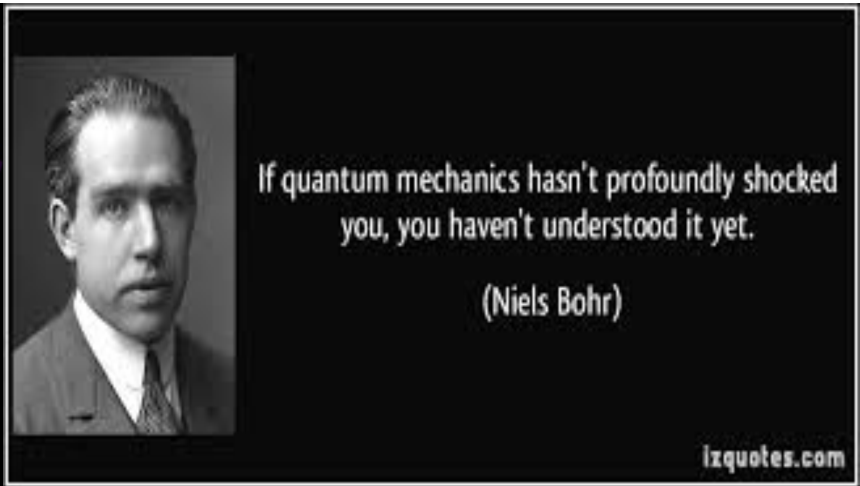
– Probabilistic –

– Central role of the observer –

– Not very intuitive –

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





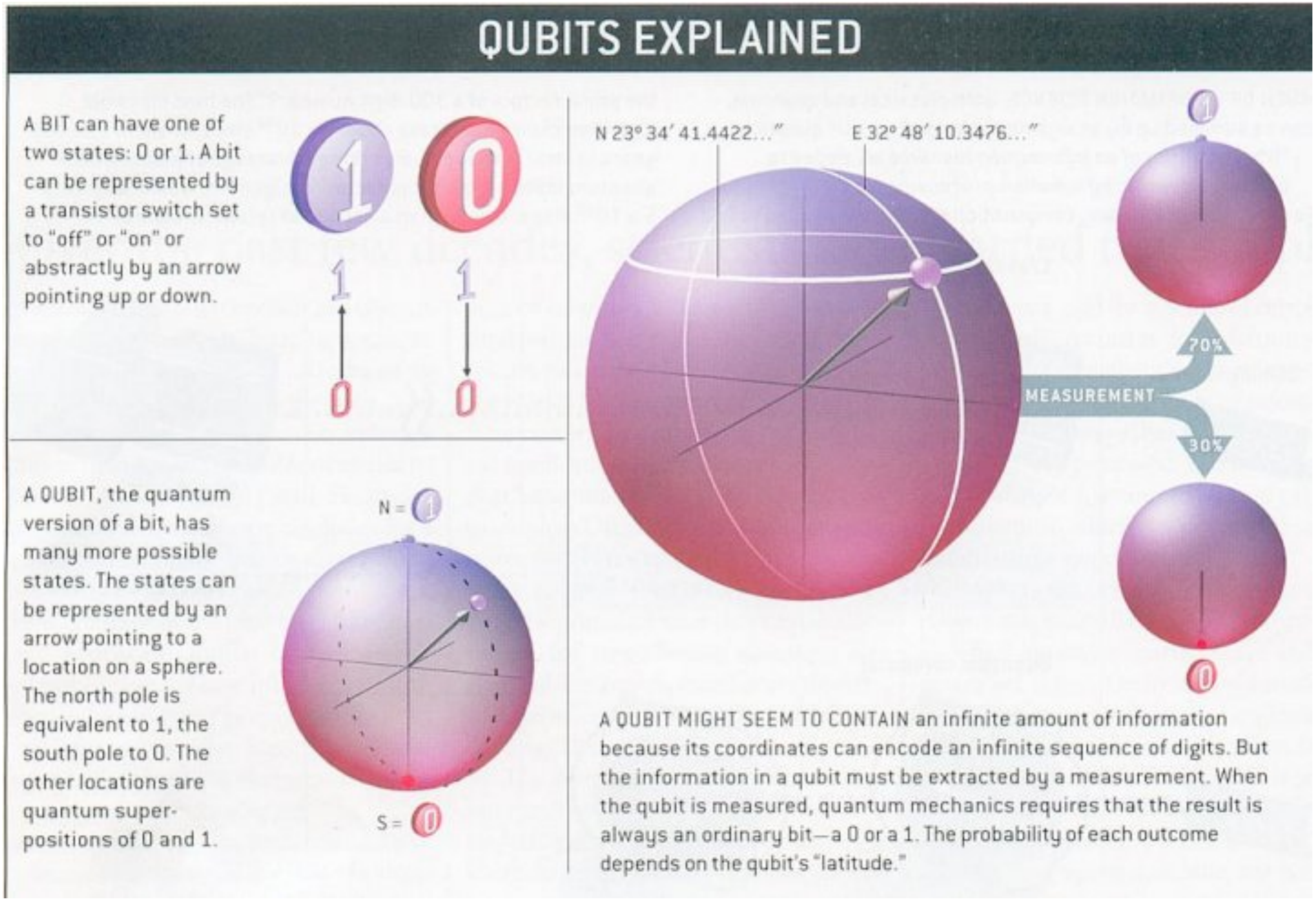
If quantum mechanics hasn't profoundly shocked you, you haven't understood it yet.

(Niels Bohr)

izquotes.com

What are the properties of a quantum computer?

Current computers use bits but quantum computers use qubits.



QUBITS EXPLAINED

A BIT can have one of two states: 0 or 1. A bit can be represented by a transistor switch set to "off" or "on" or abstractly by an arrow pointing up or down.

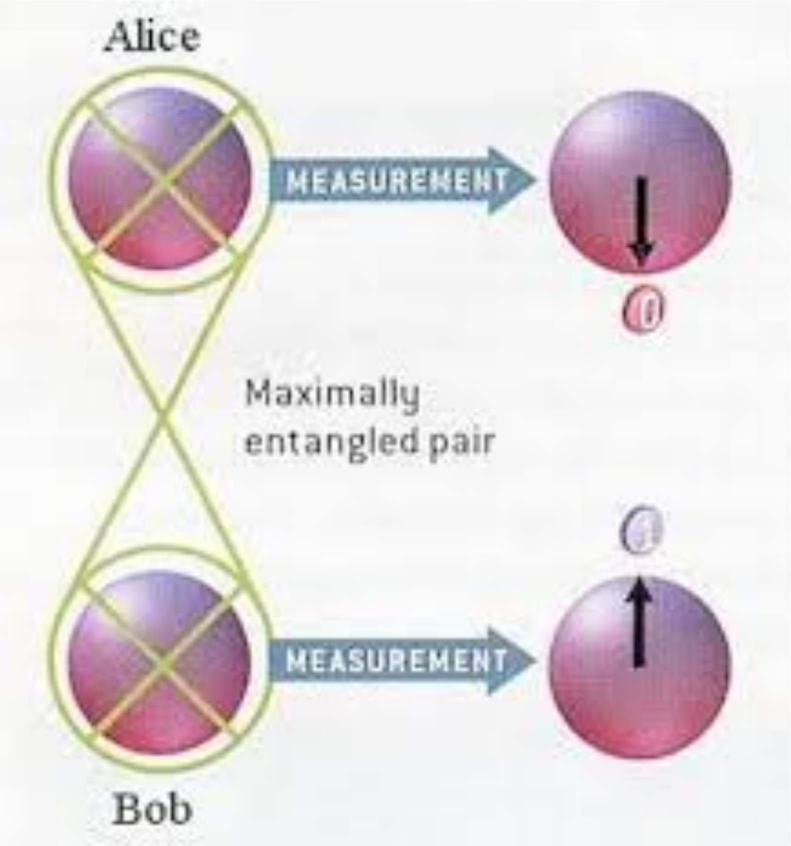
A QUBIT, the quantum version of a bit, has many more possible states. The states can be represented by an arrow pointing to a location on a sphere. The north pole is equivalent to 1, the south pole to 0. The other locations are quantum superpositions of 0 and 1.

A QUBIT MIGHT SEEM TO CONTAIN an infinite amount of information because its coordinates can encode an infinite sequence of digits. But the information in a qubit must be extracted by a measurement. When the qubit is measured, quantum mechanics requires that the result is always an ordinary bit—a 0 or a 1. The probability of each outcome depends on the qubit's "latitude."

Entanglement

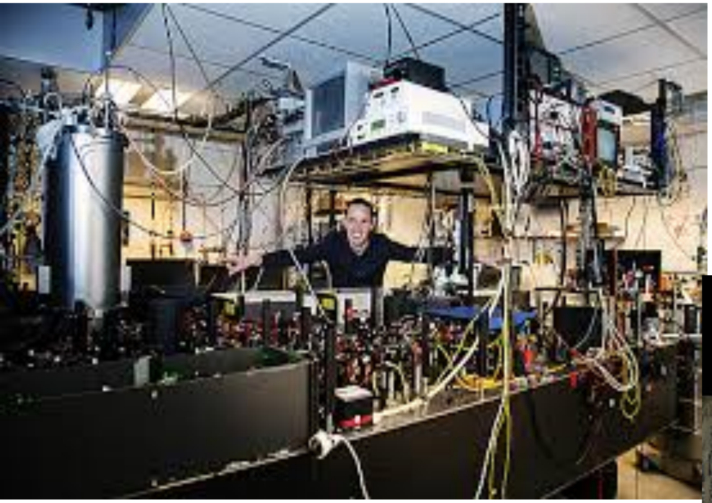
- ***It thus appears that one particle of an entangled pair "knows" what measurement has been performed on the other, and with what outcome, even though there is no known means for such information to be communicated between the particles, which at the time of measurement may be separated by arbitrarily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

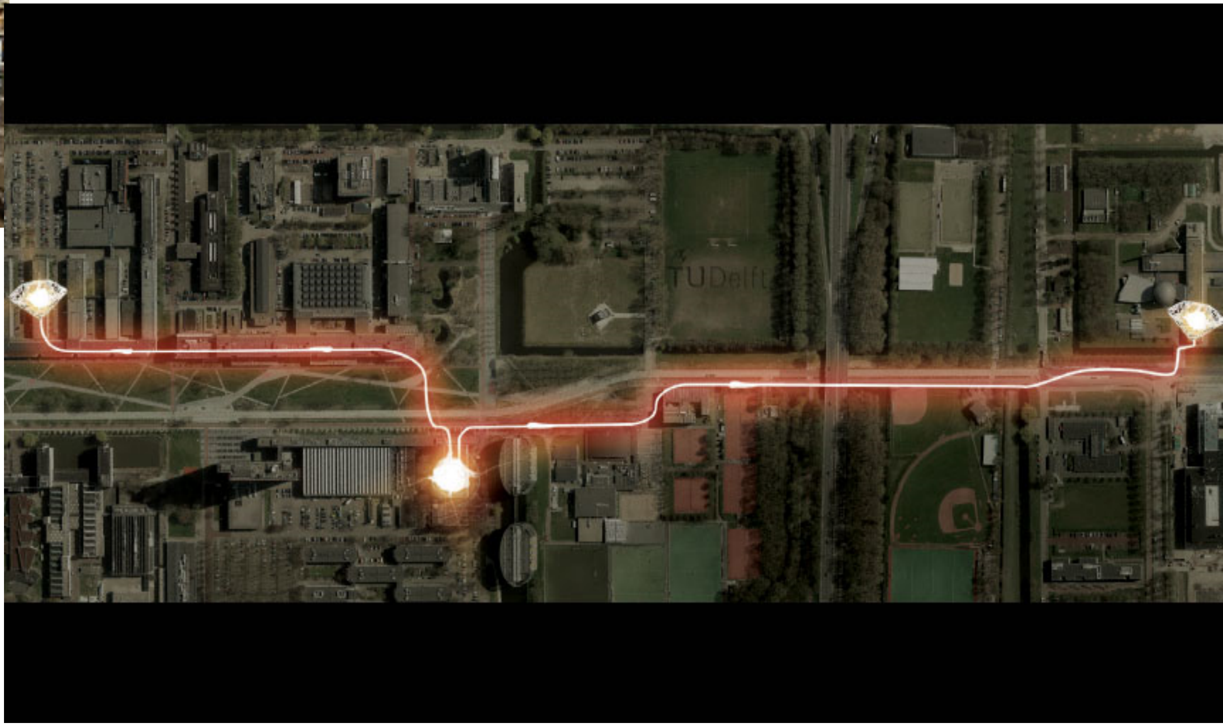


Entanglement
Loophole Free Bell Test

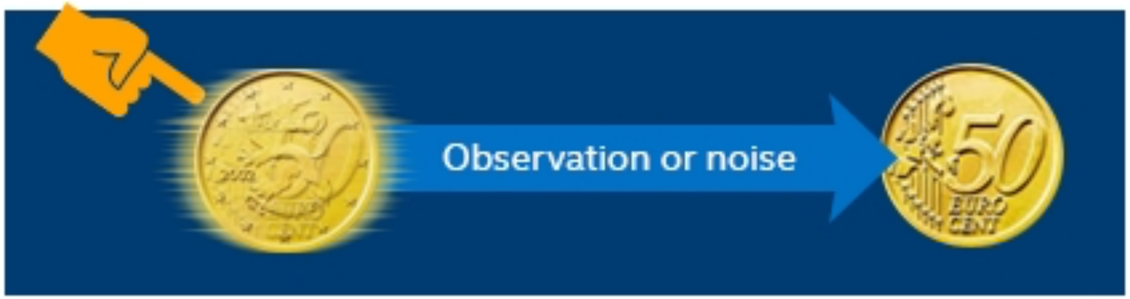
Ronald Hanson –TU Delft



Spooky Action at a distance



Fragility & No-Cloning



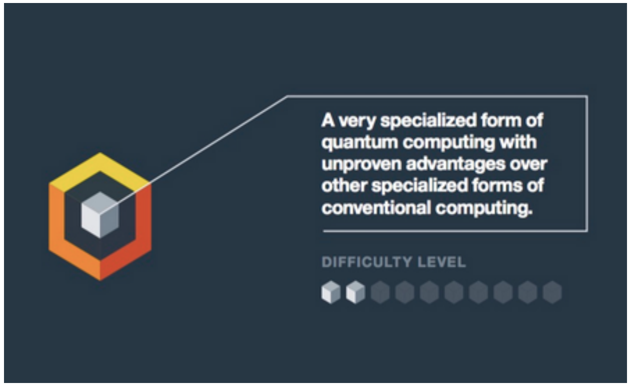
A **quantum state** collapses to a classical state if disturbed by noise or measurement.

DIGITAL COMPUTING
Copy or eavesdrop
QUANTUM COMPUTING
Copy or eavesdrop

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

There's more than 1 type of Quantum Computer?

- Quantum Annealer

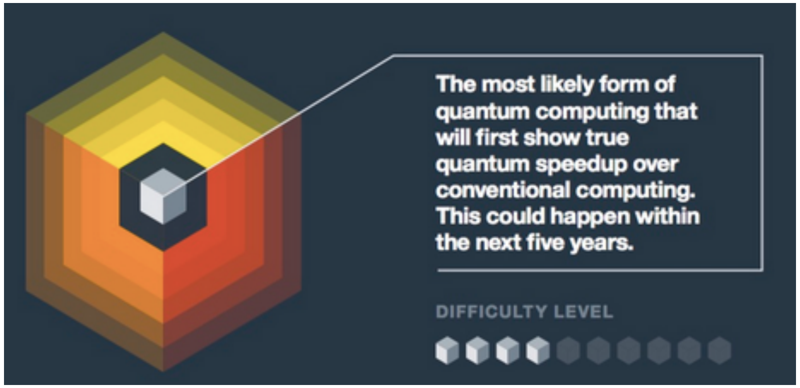


A very specialized form of quantum computing with unproven advantages over other specialized forms of conventional computing.

DIFFICULTY LEVEL

●●○○○○○○○○

- Analog Quantum



The most likely form of quantum computing that will first show true quantum speedup over conventional computing. This could happen within the next five years.

DIFFICULTY LEVEL

●●●●○○○○○○

- Universal Quantum Computer

The true grand challenge in quantum computing. It offers the potential to be exponentially faster than traditional computers for a number of important applications for science and businesses.

DIFFICULTY LEVEL

●●●●●●●●●●

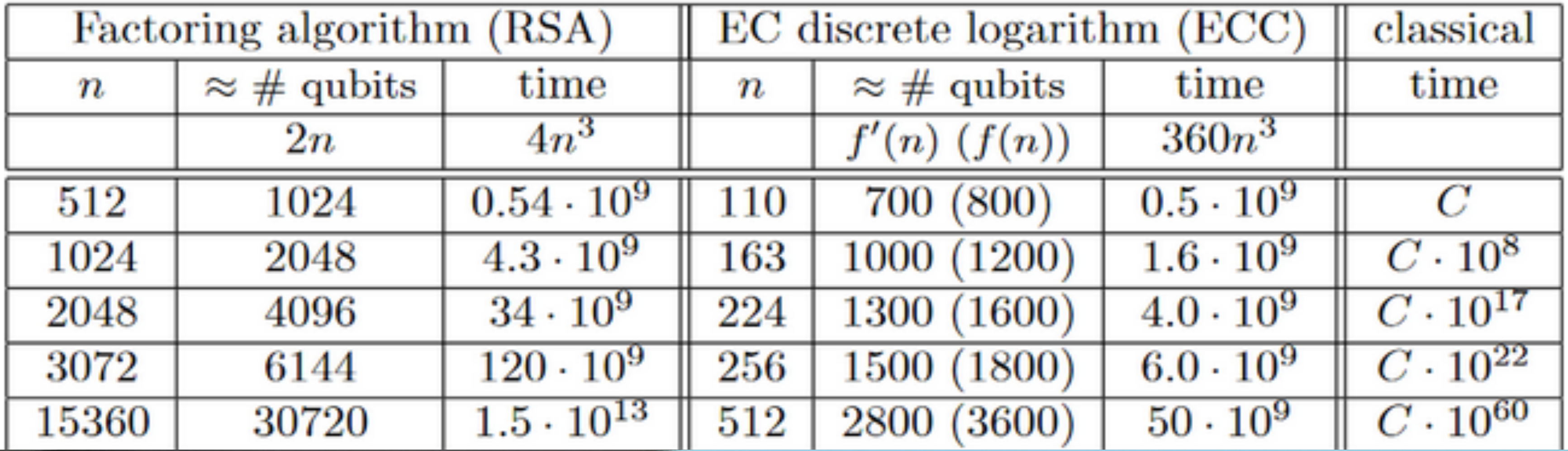
What's it all mean?

- 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

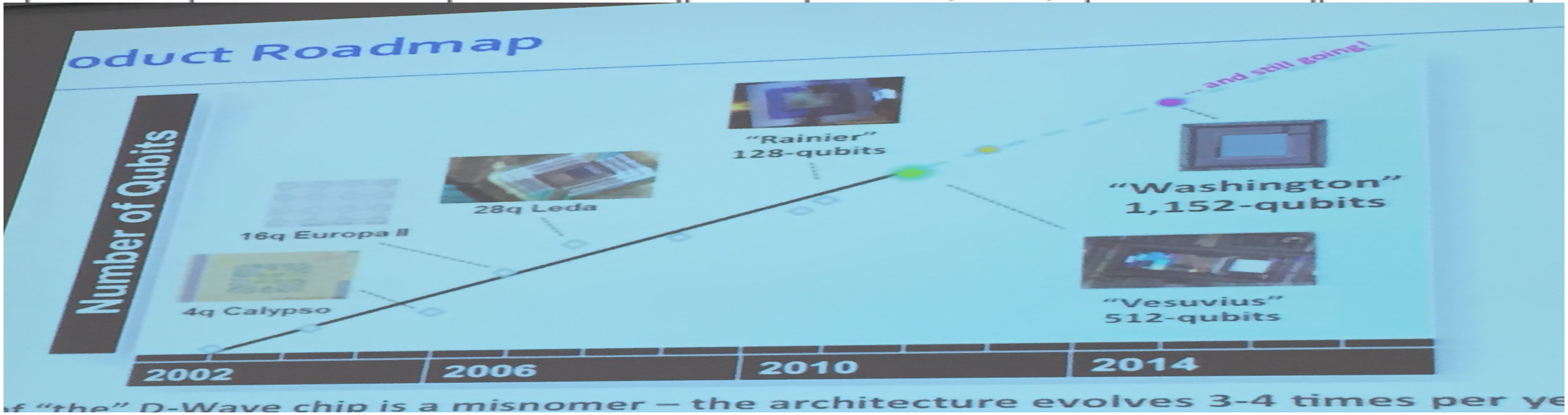
© 2012 D-Wave Systems Inc

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)	$50 \cdot 10^9$	$C \cdot 10^{60}$

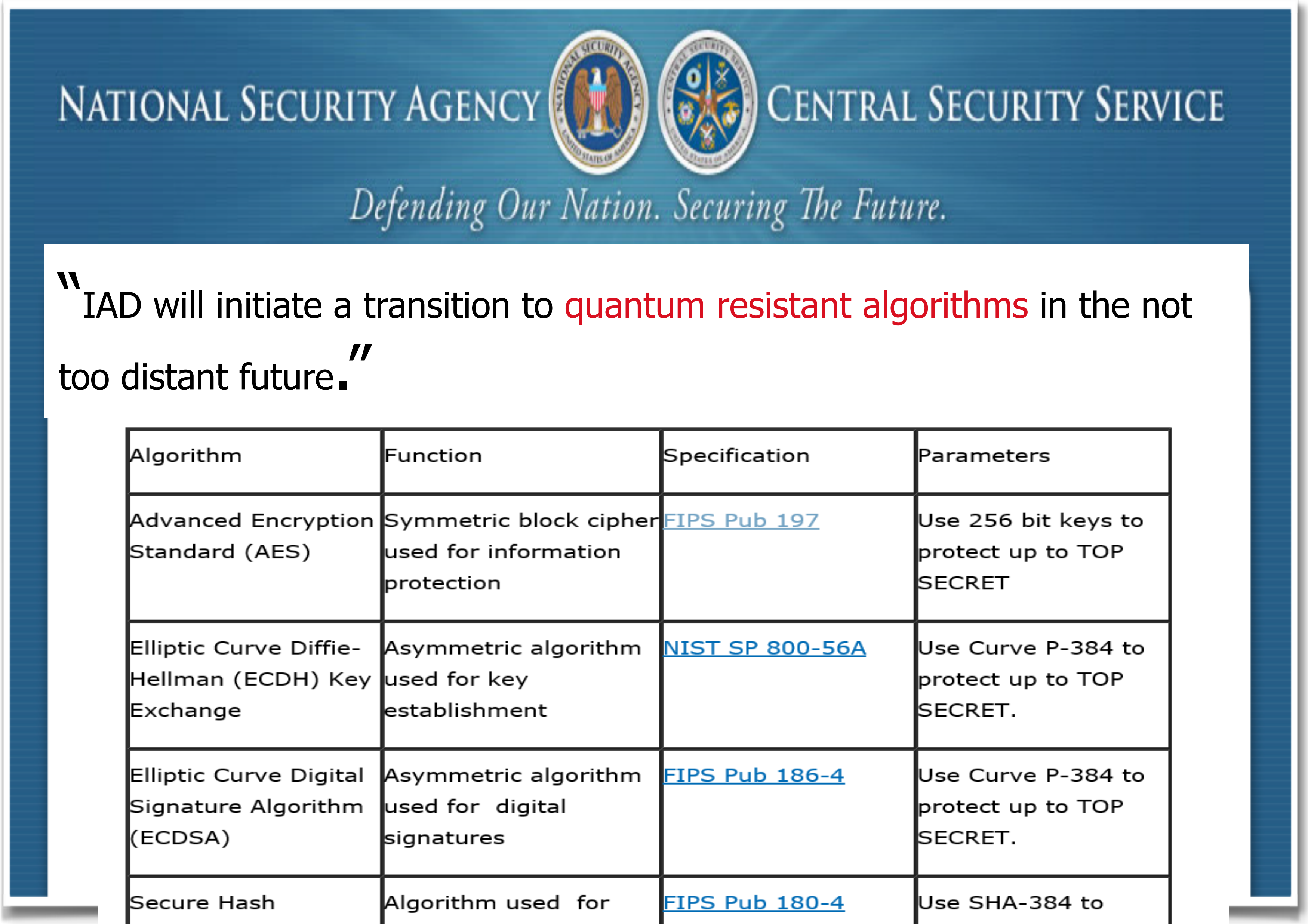


f "the" D-Wave chip is a misnomer – the architecture evolves 3-4 times per ye

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



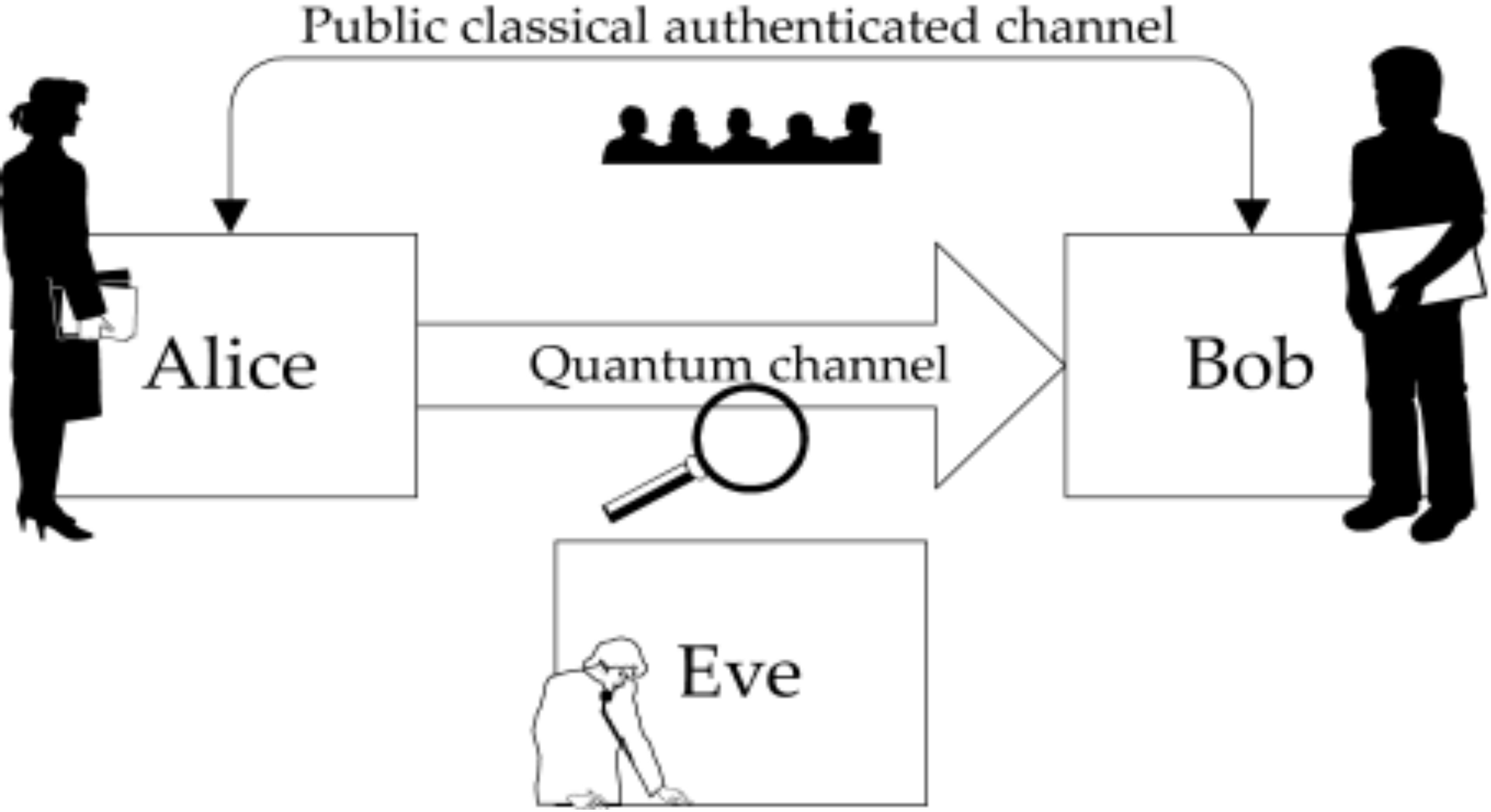
NATIONAL SECURITY AGENCY CENTRAL SECURITY SERVICE

Defending Our Nation. Securing The Future.

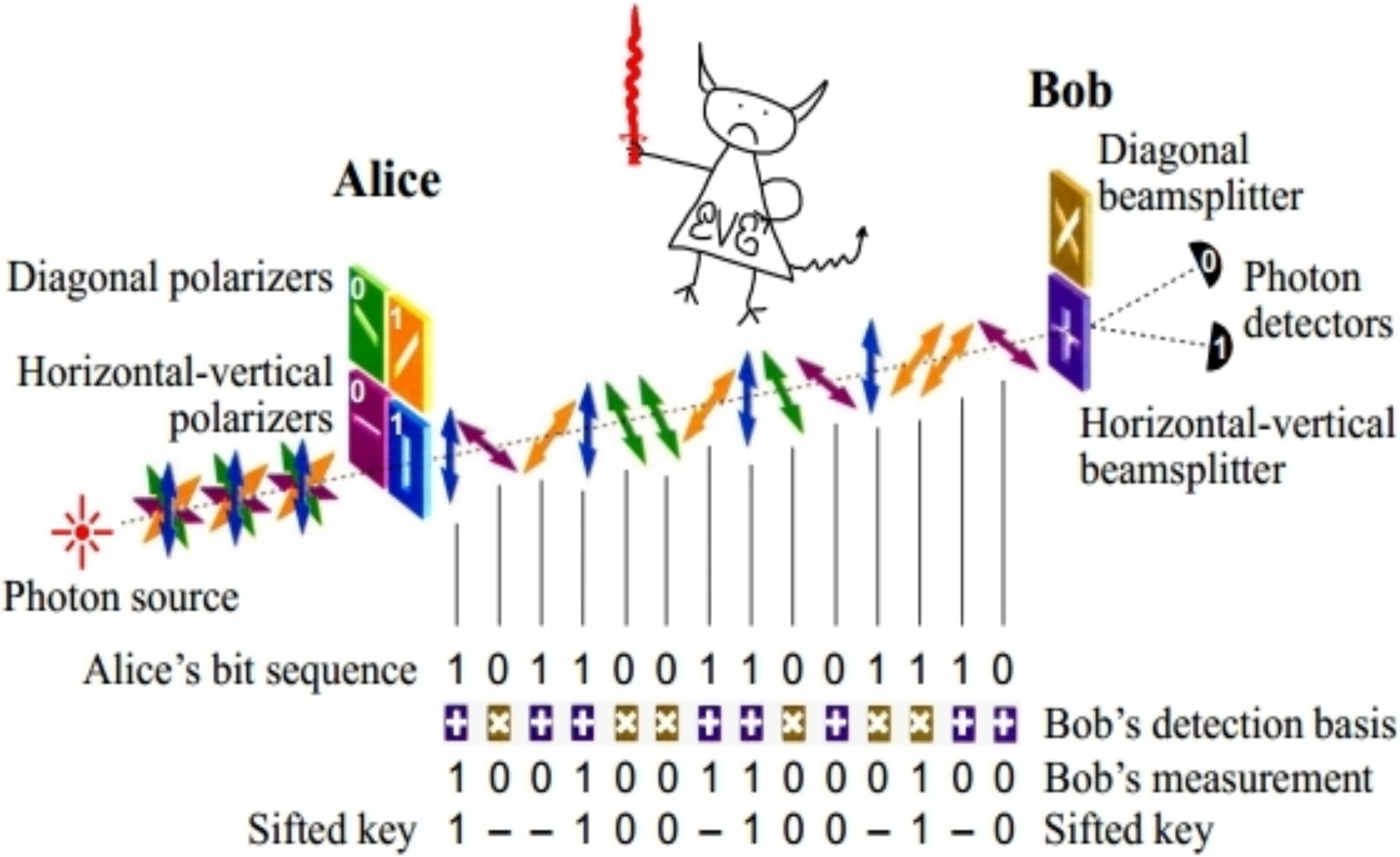
"IAD will initiate a transition to quantum resistant algorithms in the not too distant future."

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

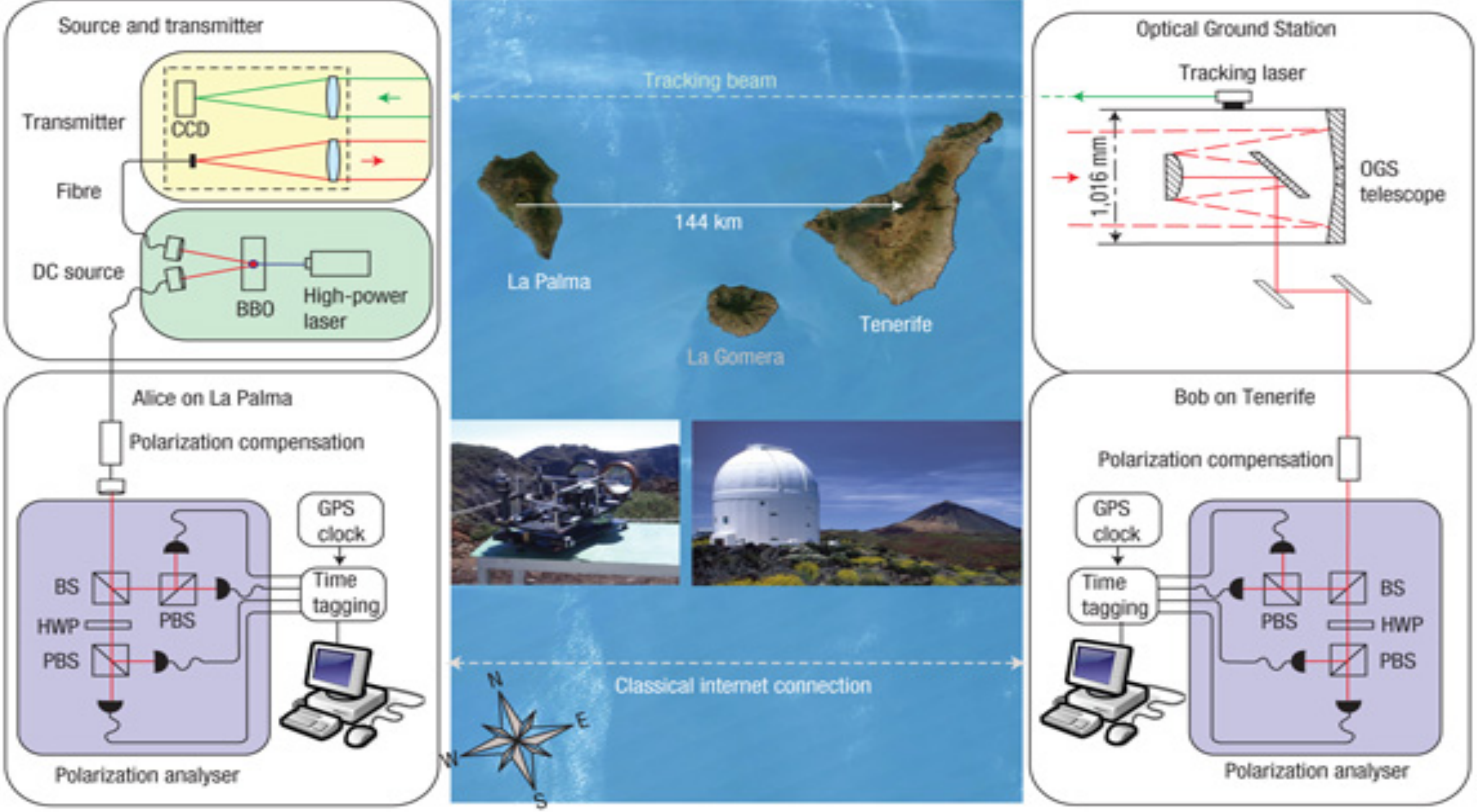


QKD



Alice’s bit sequence	1	0	1	1	0	0	1	1	0	0	1	1	1	0	
	+	×	+	+	×	×	+	+	×	+	×	×	+	+	Bob’s detection basis
	1	0	0	1	0	0	1	1	0	0	0	1	0	0	Bob’s measurement
Sifted key	1	–	–	1	0	0	–	1	0	0	–	1	–	0	Sifted key

Free Space QKD



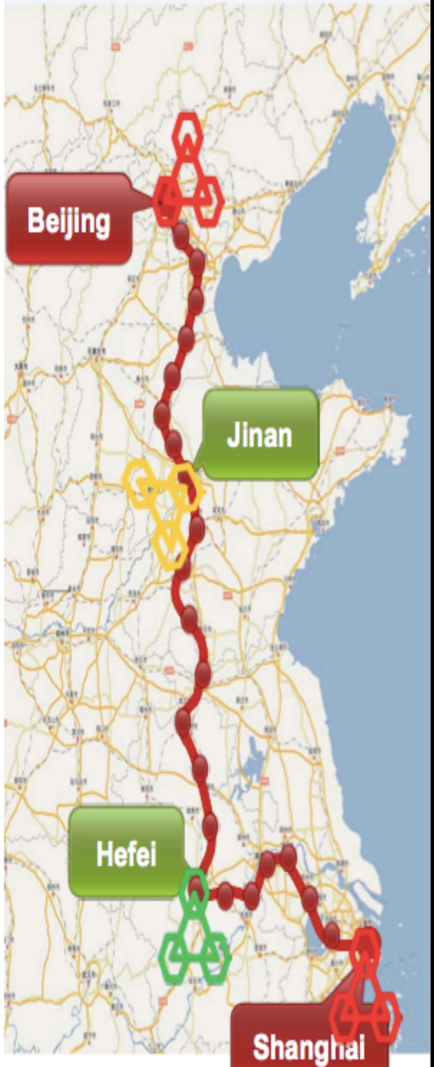
Global Developments –
Qiang Zhang – Uni. of Science & Technology of China

Quantum Backbone

- Total Length 2000 km
- Metropolitan networks

  Existing: Hefei, Jinan

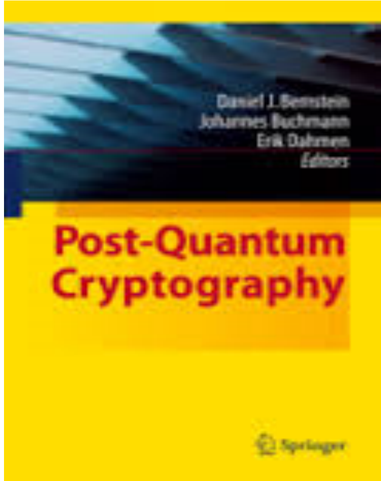
  New: Beijing, Shanghai
- Customer: China Industrial & Commercial Bank; Xinhua News Agency; CBRC



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



Daniel J. Bernstein
Johannes Buchmann
Erik Dahmen
Editors

Post-Quantum Cryptography

Springer

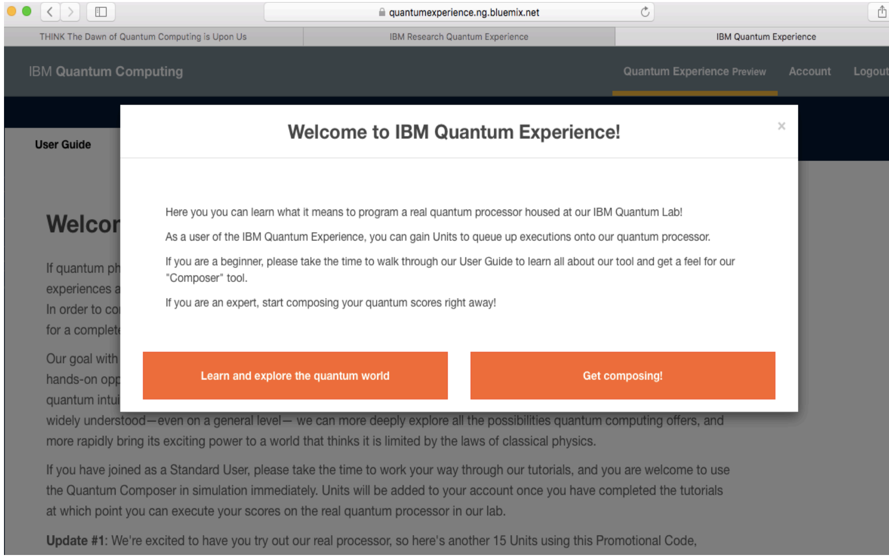
KPN's Quantum leap with IDQuantique

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/COxMJTh06zl
- Providing **thought leadership and action** in the field of future security controls
- Combining options for defense in depth – like we're used to


quantumexperience.ng.bluemix.net
THINK The Dawn of Quantum Computing is Upon Us
IBM Research Quantum Experience
IBM Quantum Experience
IBM Quantum Computing
Quantum Experience Preview
Account
Logout
User Guide
Learn and explore the quantum world
Get composing!

Welcome to IBM Quantum Experience!

Here you you can learn what it means to program a real quantum processor housed at our IBM Quantum Lab!

As a user of the IBM Quantum Experience, you can gain Units to queue up executions onto our quantum processor.

If you are a beginner, please take the time to walk through our User Guide to learn all about our tool and get a feel for our "Composer" tool.

If you are an expert, start composing your quantum scores right away!

Welcor

If quantum ph
experiences a
In order to co
for a complete

Our goal with
hands-on opp
quantum intui
widely understood—even on a general level— we can more deeply explore all the possibilities quantum computing offers, and more rapidly bring its exciting power to a world that thinks it is limited by the laws of classical physics.

If you have joined as a Standard User, please take the time to work your way through our tutorials, and you are welcome to use the Quantum Composer in simulation immediately. Units will be added to your account once you have completed the tutorials at which point you can execute your scores on the real quantum processor in our lab.

Update #1: We're excited to have you try out our real processor, so here's another 15 Units using this Promotional Code,

THANK YOU!
Questions? Comments? Stuff?

- Jaya Baloo
- @jayabaloo (twitter)

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