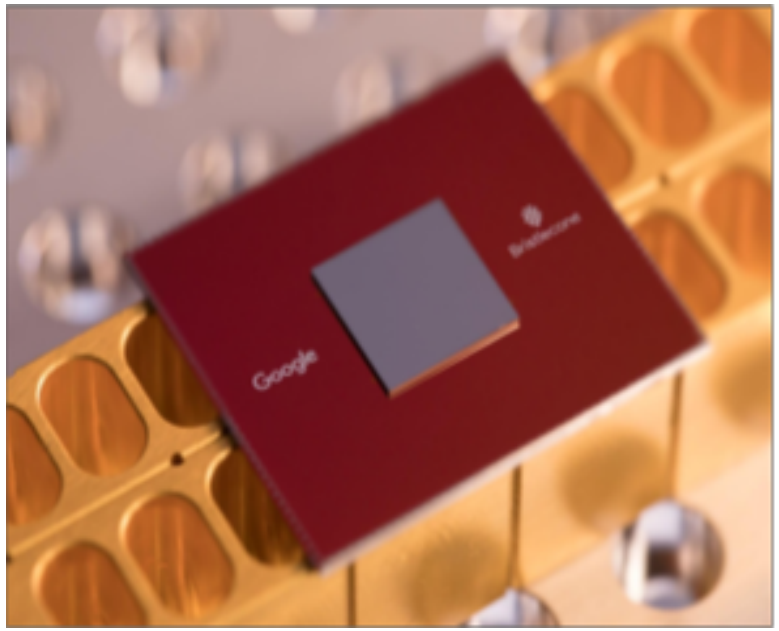
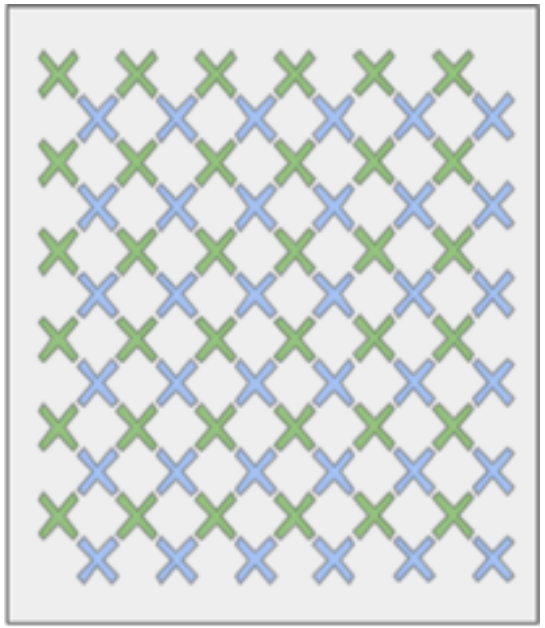
Our Quantum Future

Jaya Baloo

11/1/2018

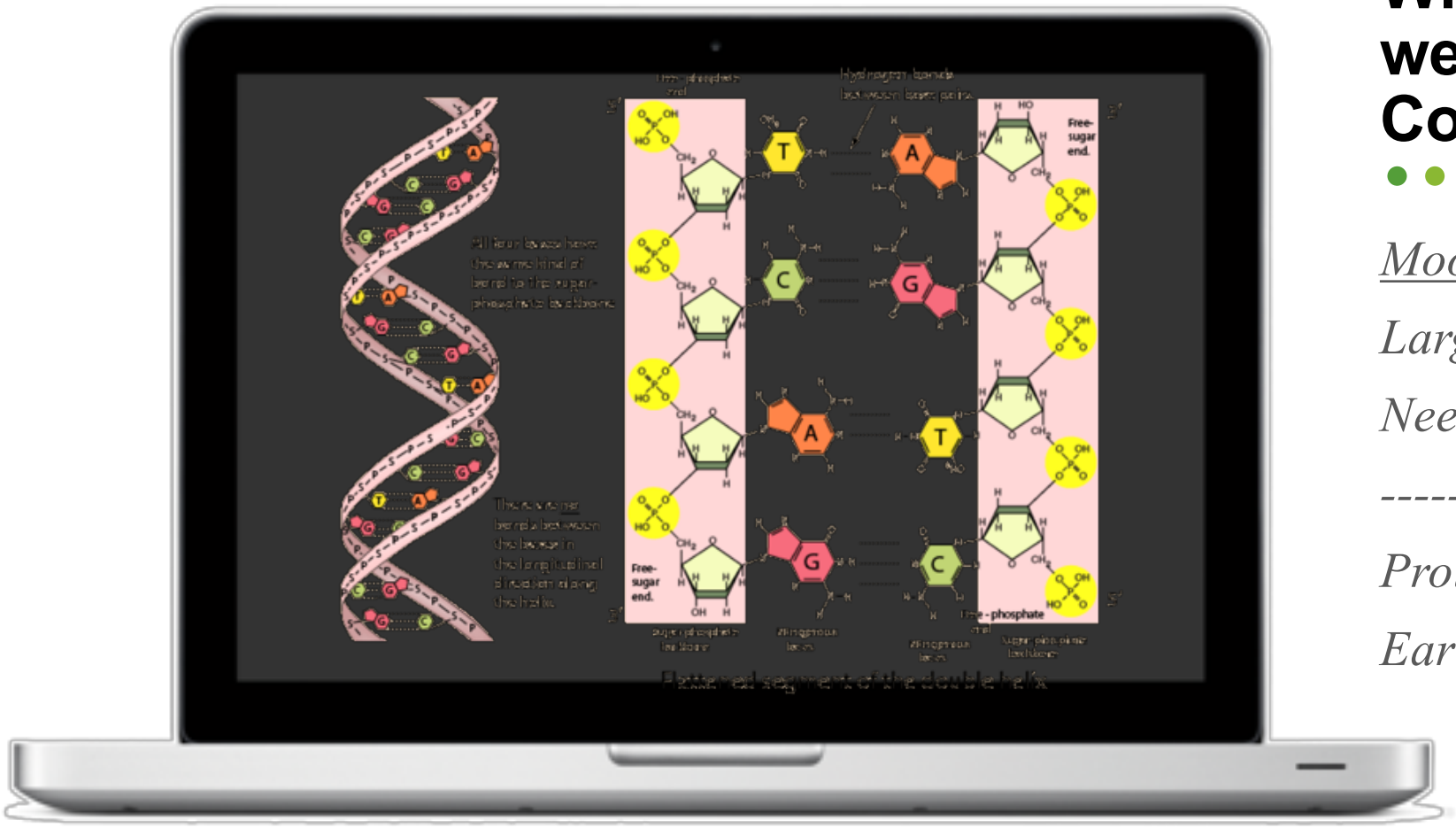
Bristlecone is here – and on the job for Quantum Supremacy





..”quantum supremacy can be comfortably demonstrated with 49 qubits, a circuit depth exceeding 40, and a two-qubit error below 0.5%”

The Race is on …Microsoft, Google, Intel, IBM, ….



What type of problems can we solve with a Quantum Computer

Moore Vs. Amdahl

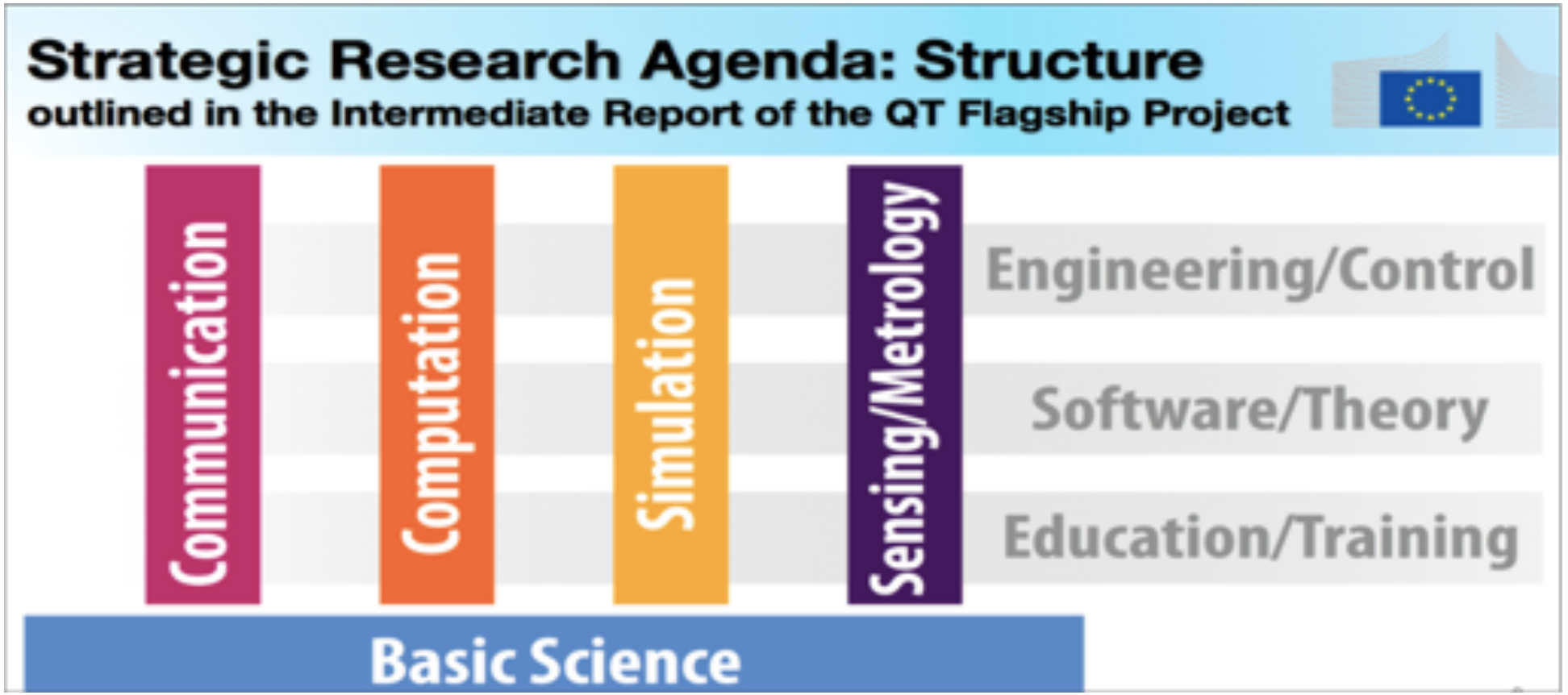
Large data set problems

Needle in haystack problems

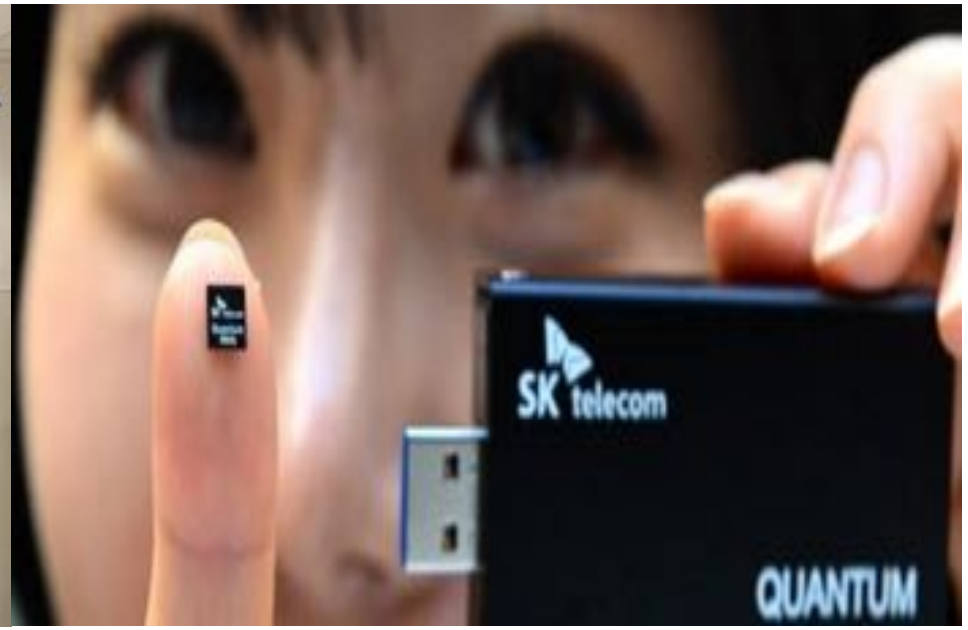
Protein mapping and drug interaction

Earlier detection of cancer

Four Pillars and supporting areas

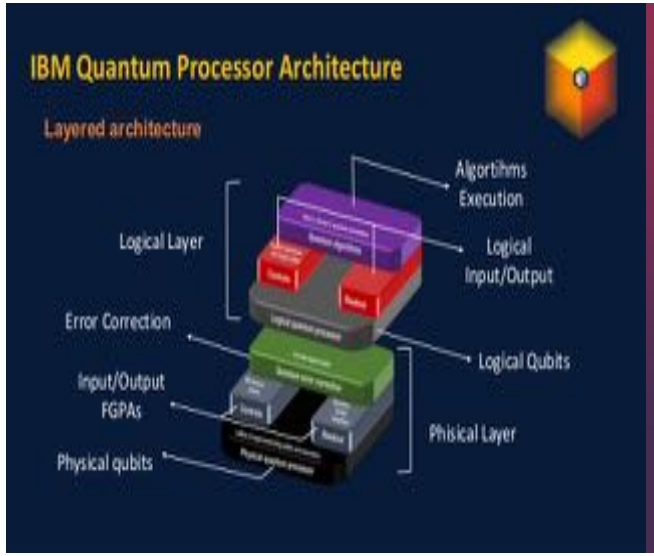


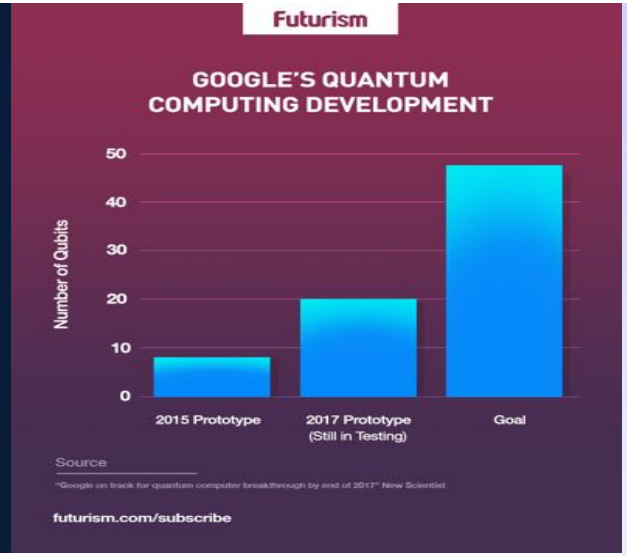
Quantum Communication

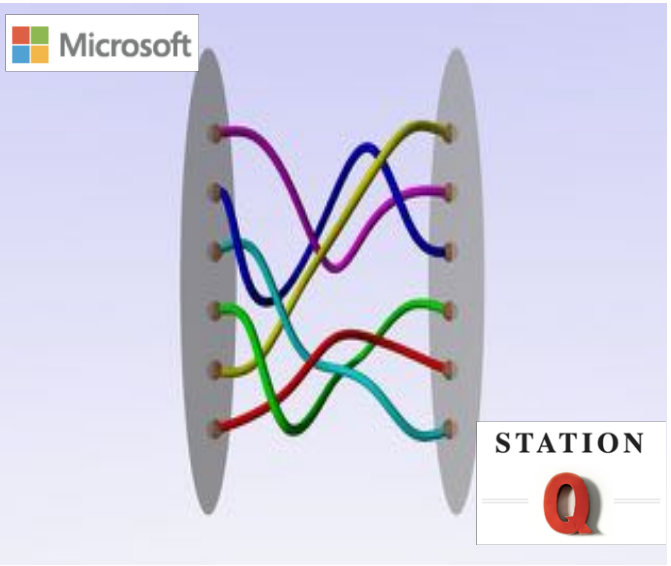


- Quantum Key Distribution
- Quantum Random Number Generator
- Fully Quantum repeater
- Trusted Node Networks

Quantum Computing

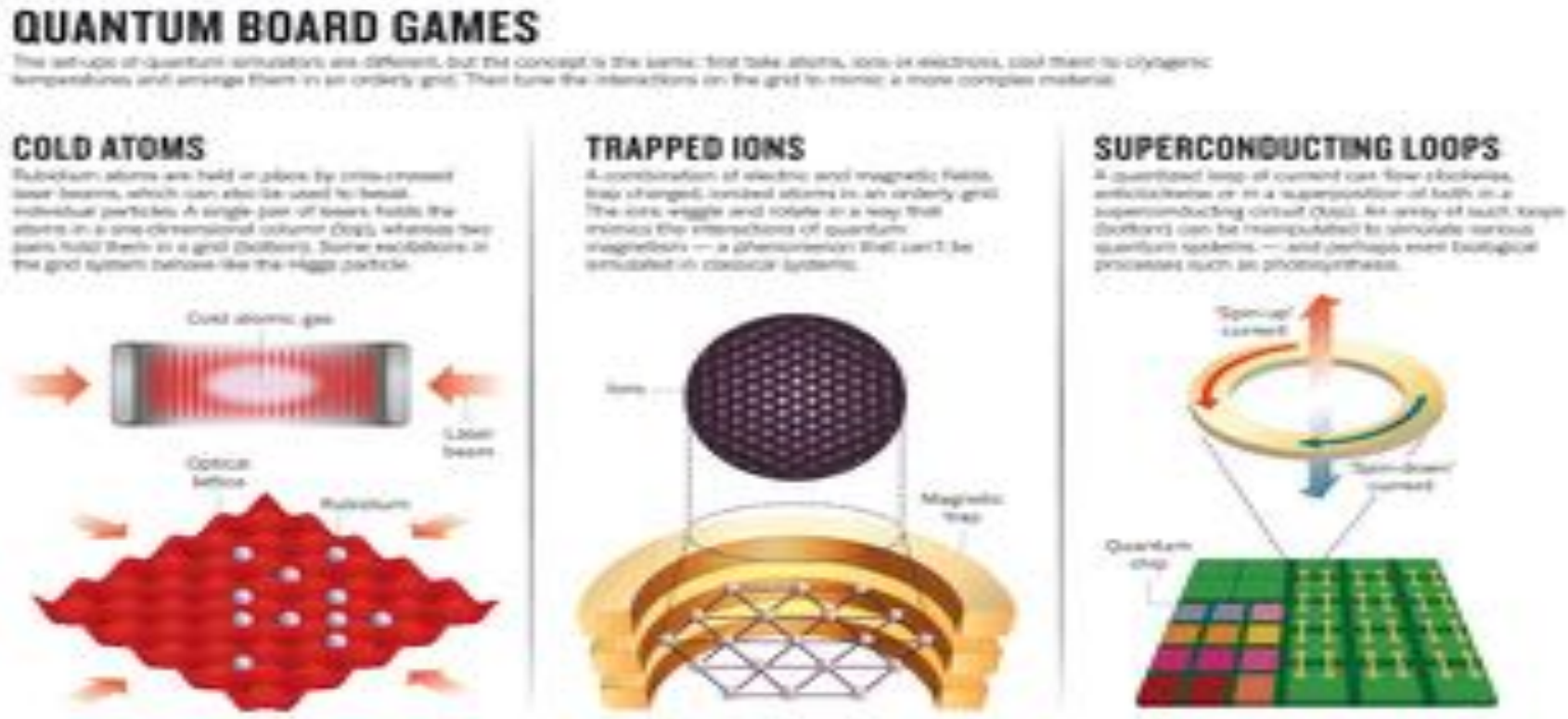






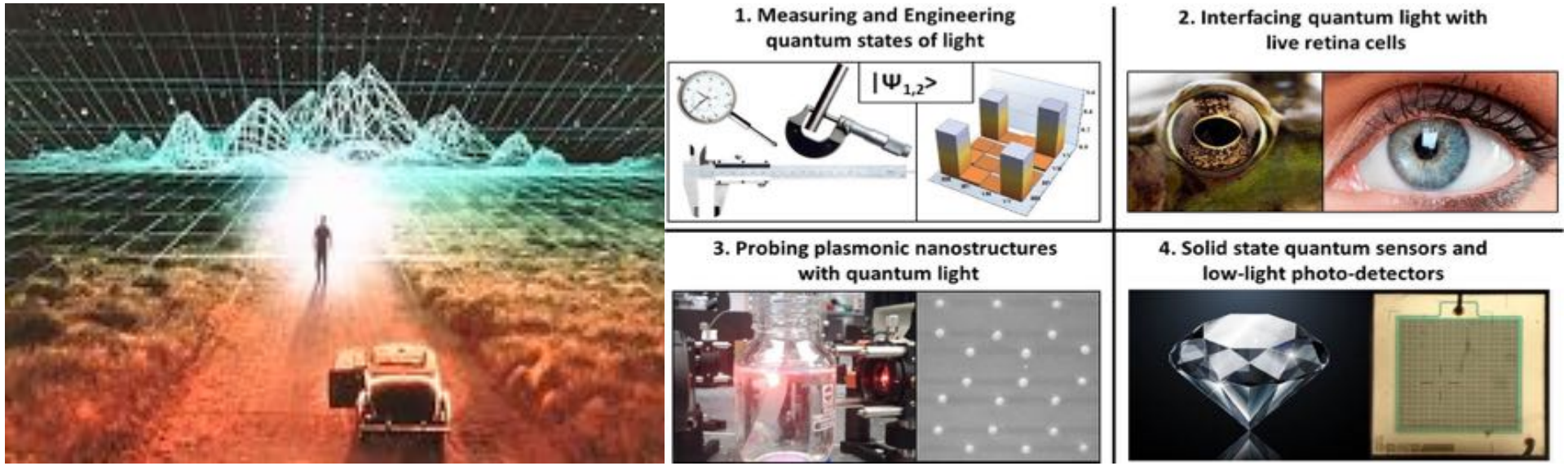
- Quantum computing - stable, scalable architecture
- Error Correcting, Robust Qubits
- Quantum memory
- Demonstrating Quantum Speedup

Quantum simulation



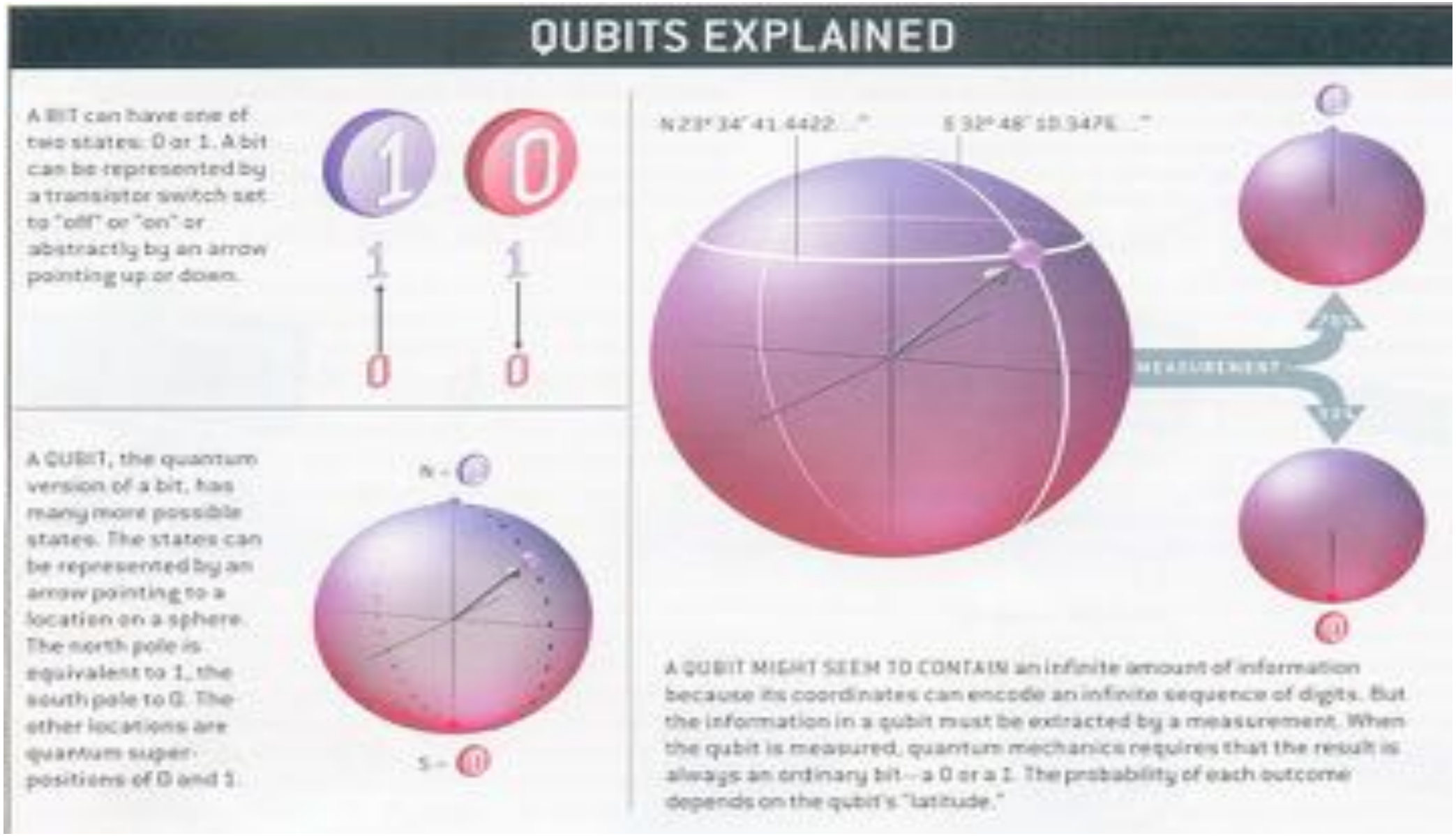
- Quantum Simulator platform
- High temperature superconductivity
- Energy storage, distribution, transportation

Quantum Sensing and Metrology



- Solid State Quantum Sensors – ie. MRIs
- Quantum Imaging devices – ie. Better image resolution
- Atomic and molecular interferometer devices- ie. navigation
- Quantum Metrology – ie. time measurements

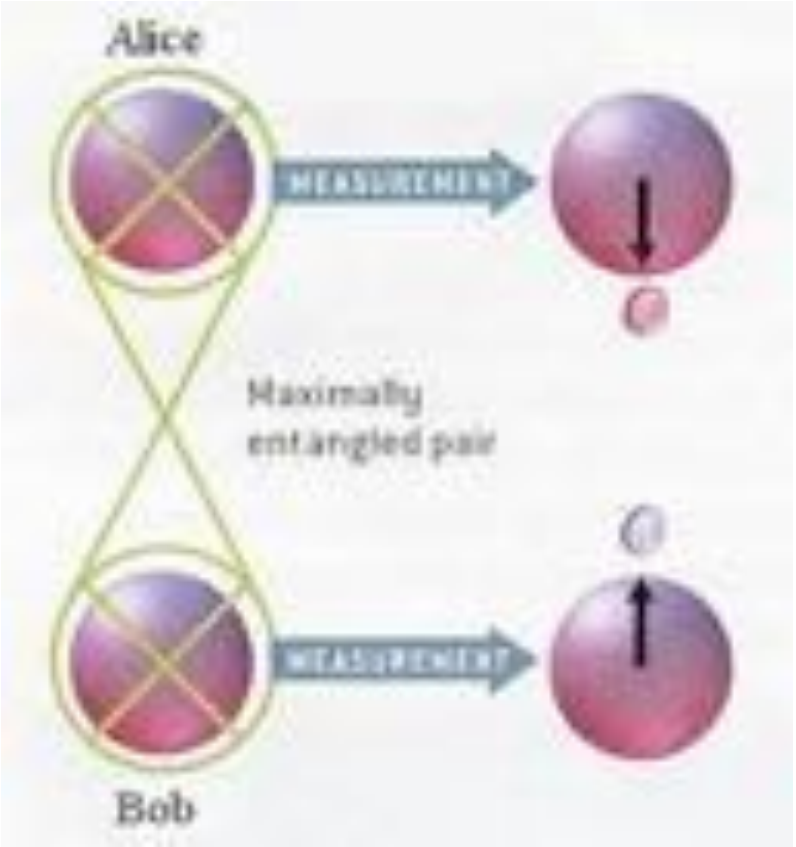
How does it work?



Entanglement

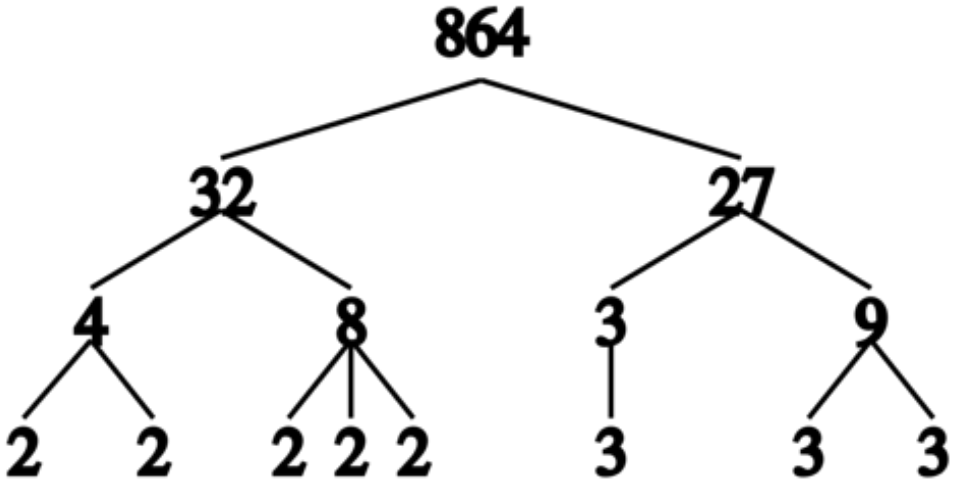
- ***It thus appears that one particle of an entangled pair "knows" what measurement has been performed on the other, and with what outcome, even though there is no known means for such information to be communicated between the particles, which at the time of measurement may be separated by arbitrarily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

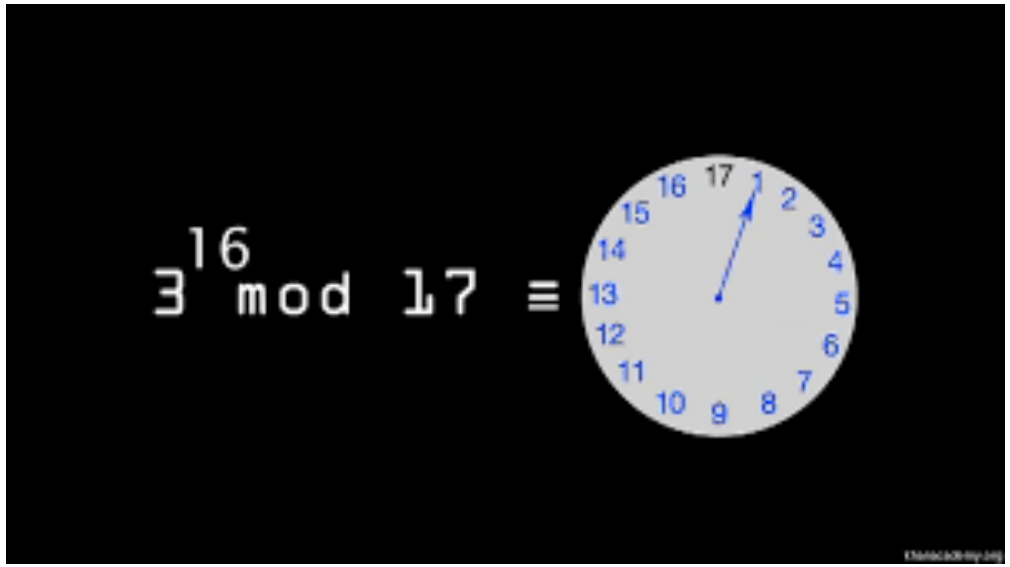
- Its entanglement that gives quantum computing the ability to scale exponentially, as entangled qubits can represent 4 states. The more linked qubits, exponential increase in states and thus computing power.



	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

Prime numbers



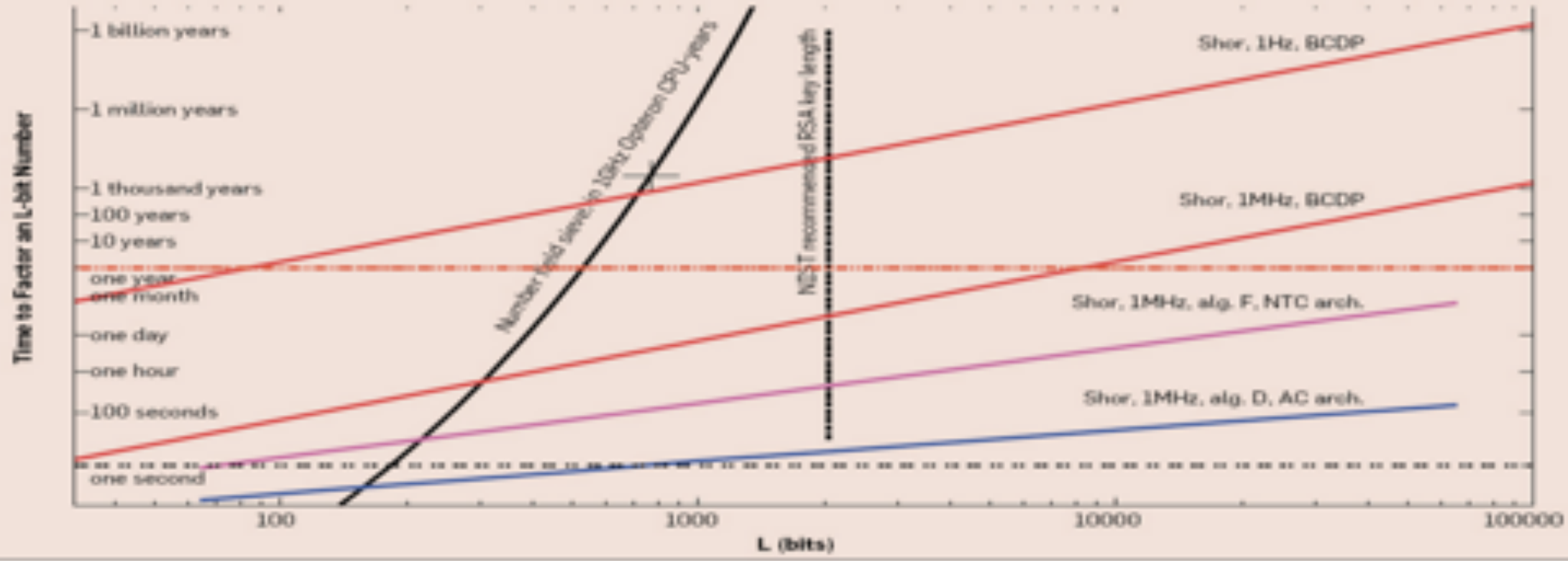


Quantum computing threat to cryptography

- Cryptography is based on 2 difficult math problems:
  - Integer Factorization
  - Discrete Log
- The strength of a one way function depends on the time needed to reverse it
- Meet Shor & Grover!

When?

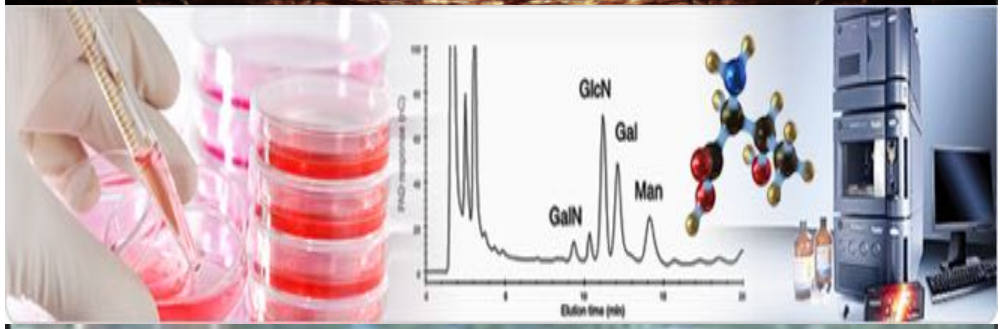
The horizontal axis is the length of the number to be factored. The steep curve is NFS, with the marked point at $L = 768$ requiring 3,300 CPU-years. The vertical line at $L = 2048$ is NIST's 2007 recommendation for RSA key length for data intended to remain secure until 2030. The other lines are various combinations of quantum computer logical clock speed for a three-qubit operation known as a Toffoli gate (1Hz and 1MHz), method of implementing the arithmetic portion of Shor's algorithm (BCDP, D, and F), and quantum computer architecture (NTC and AC, with the primary difference being whether or not long-distance operations are supported). The assumed capacity of a machine in this graph is $2L^2$ logical qubits. This figure illustrates the difficulty of making pronouncements about the speed of quantum computers.



Impact

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES-256	Symmetric key	Encryption	Larger key sizes needed
SHA-256, SHA-3		Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Table 1 - Impact of Quantum Computing on Common Cryptographic Algorithms



Power, Potential & Threat of a quantum computer

- How long do we need to keep our encryption secure?
- How long before there is a viable quantum computer that breaks our secrets?
- How long will we need to transition our network and systems to one that is quantum safe?

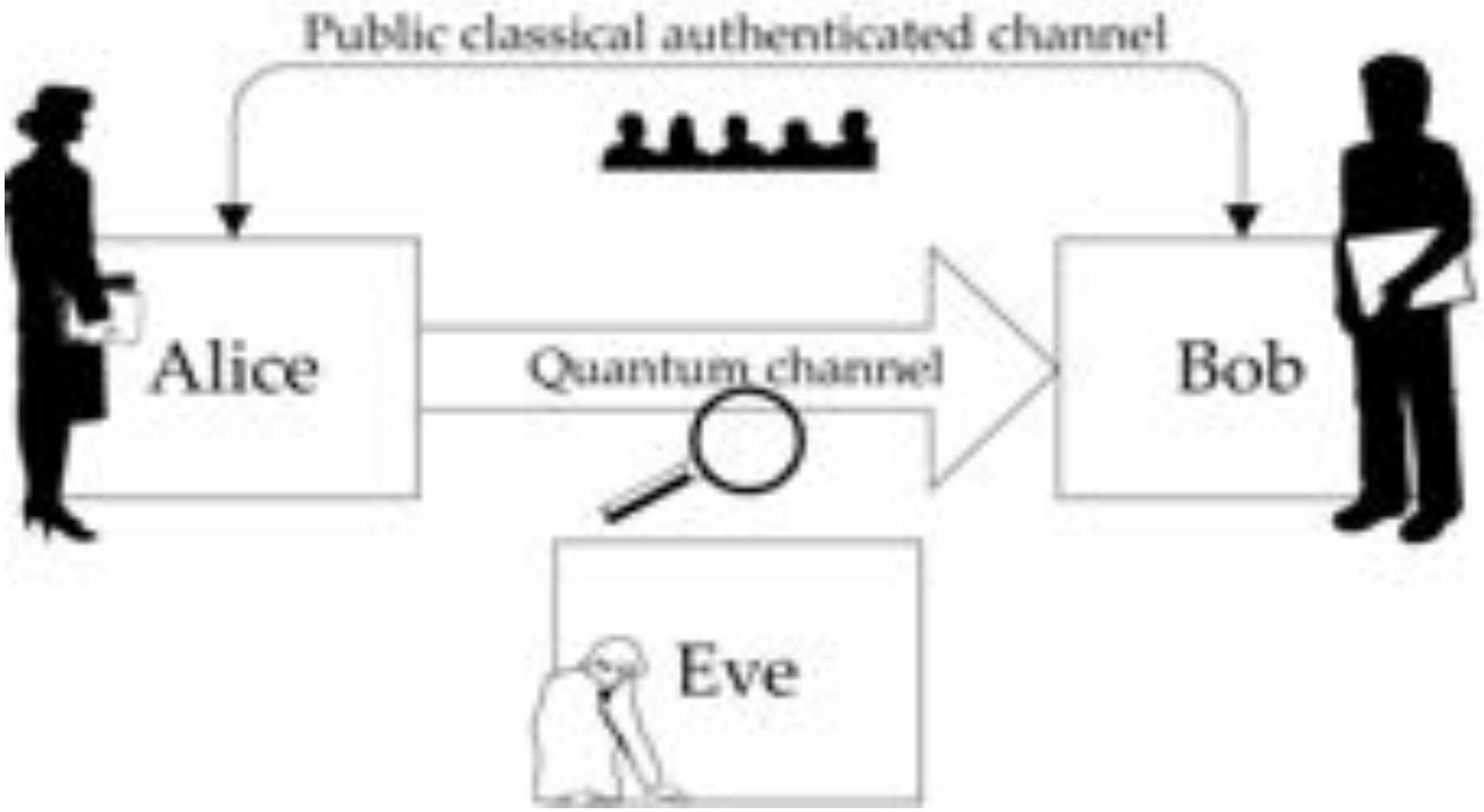
Capture Now Decrypt Later

The predictive force of old secrets means that you can not only see what you have done, but what you're planning on doing

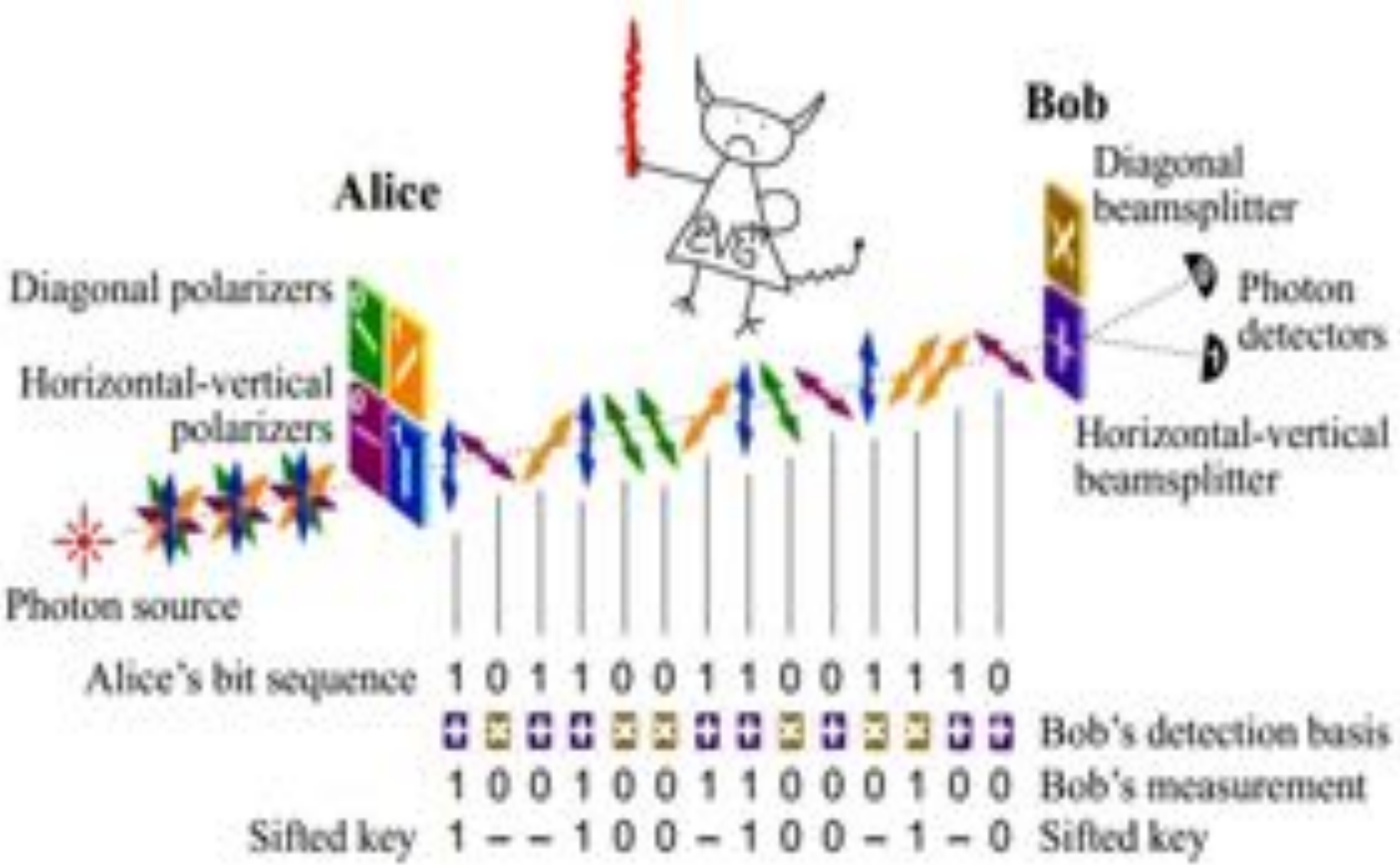
Phased plan of defense

- Increase Key Length of Current Crypto used
- *Investigate options for Quantum Key Distribution*
- *Investigate Post Quantum Algorithms*

Quantum Key Distribution – QKD



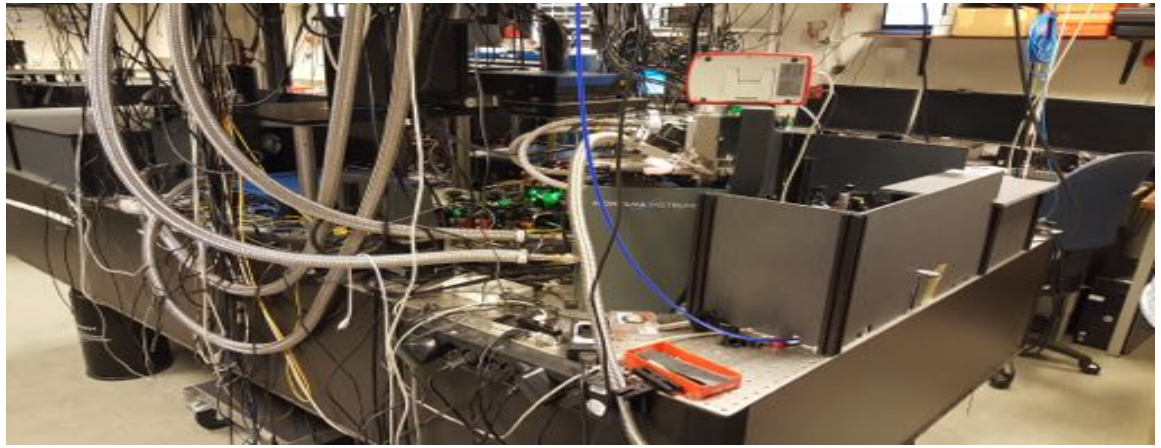
QKD


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
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

KPN’s Quantum leap with IDQuantique

NL Quantum Internet Backbone

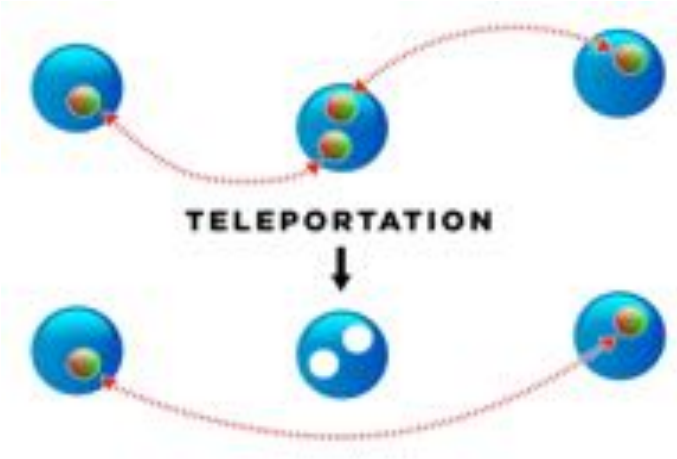
NL Quantum Internet Backbone – Step 1 – Delft & DH



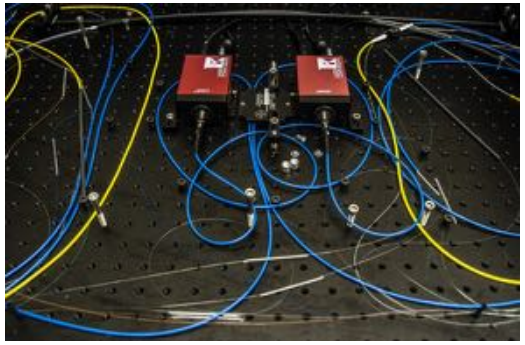
Quantum networks

- New applications with connected quantum computers

- This will be made possible using a **quantum repeater**

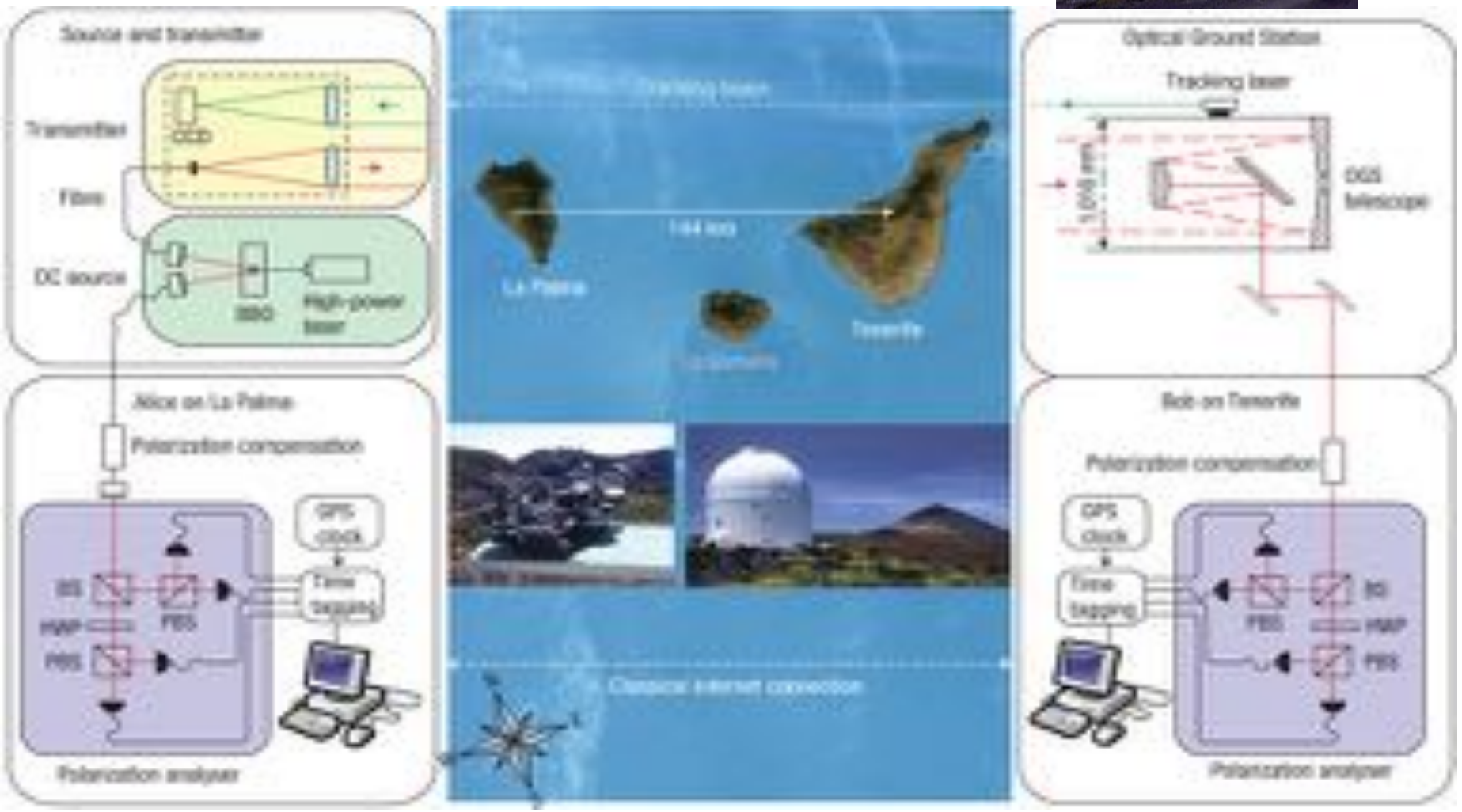


Delft Rijswijk Den Haag



Entanglement generation in Rijswijk

Free Space QKD



China launched the world's 1st Quantum Communications Satellite

"China is completely capable of making full use of quantum communications in a regional war. The direction of development in the future calls for using relay satellites to realize quantum communications and control that covers the entire army."

Professor Pan Jianwei

University of Science and Technology of China

+10bn QIS +AliBaba

Timelines for PQ Standards

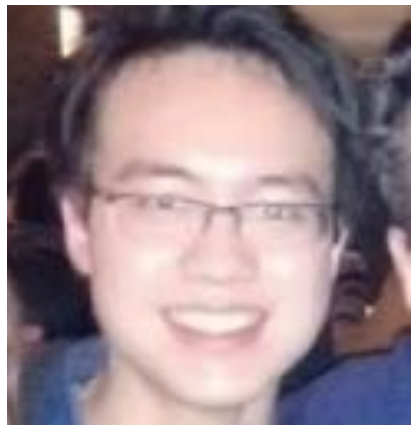
Timeline

*This is a tentative timeline, provided for information, and subject to change.

Date	
Feb 24-26, 2016	NIST Presentation at PQCrypto 2016: *Announcement and outline of NIST's Call for Submissions (Fall 2016)*, *Dustin Moody*
April 28, 2016	NIST releases NISTIR 8105, Report on Post-Quantum Cryptography
Dec 20, 2016	Formal Call for Proposals
Nov 30, 2017	Deadline for submissions
Dec 4, 2017	NIST Presentation at AsiaCrypt 2017: *The Ship Has Sailed: The NIST Post-Quantum Crypto "Competition"*, *Dustin Moody*
Dec 21, 2017	Round 1 algorithms announced (69 submissions accepted as "complete and proper")
Apr 11, 2018	NIST Presentation at PQCrypto 2018: *Let's Get Ready to Rumble - The NIST PQC "Competition"*, *Dustin Moody*
April 11-13, 2018	First PQC Standardization Conference - Submitter's Presentations
2018/2019	Round 2 begins
August 2019 *(tentative)*	Second PQC Standardization Conference
2020/2021	Round 3 begins or select algorithms
2022/2024	Draft Standards Available

Our Quantum Labs Team within CISO

- Dedicated resources
- Commitment with universities
- Specialization
- Choices in applied research

Post Quantum Cryptography – Roadmap

PQ-VPN: wrapping up
- 1.1 WireGuard is chosen
  - 1.1.1 faster and more secure than other VPNs
  - 1.1.2 being merged into mainline Linux kernel
- 1.2 Protocol design done, minor review ongoing
- 1.3 Linux implementation done
- 1.5 Planned to publish an academia paper on this. For Jan 2019
  - 1.5.1 Partnered with Peter Schwabe from Radboud University
  - 1.6 Can be deployed once a Windows client is implemented
- 1.7 Classic McEliece and Kyber were chosen in combination to replace the Curve25519

2. PQ-SSH: early stage
- 1.1 OpenSSH is chosen
  - 1.3 Work with original designer of SSH

3. PQ-PGP: planned
- 1.1 OpenPGP standard is chosen
- 1.2 Code base to start with: TBD, can be GnuPG, OpenPGP.js, etc

Post Quantum Cryptography

- Inventory of crypto assets
- Think it through for implementation readiness
- Look for crypto agility and opportunities
- Create Policies for innovation areas
- Engage with HW & SW vendors
- Supplier Security Annex
- Start Failing early !

THANK YOU!
Questions? Comments? Stuff?

@jayabaloo