

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





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?
 <u>What are we going to do about it?</u>
- 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 microscopic 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.



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

The qua will qua com This the

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

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.

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





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)	$6.0\cdot10^9$	$C \cdot 10^{22}$
15360	30720	$1.5\cdot10^{13}$	512	2800(3600)	$50 \cdot 10^9$	$C \cdot 10^{60}$



of "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		Use 256 bit keys to protect up to TOP SECRET
Elliptic Curve Diffie- Hellman (ECDH) Key Exchange			Use Curve P-384 to protect up to TOP SECRET.
	Asymmetric algorithm used for digital signatures		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







Free Space QKD

Tracking beam

144 km

Classical internet connection

Tenerife









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 Rochmann Erik Dahmen Editors

Post-Quantum Cryptography



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	a.ng.bluemix.net	<u> </u>			Ê
THINK The Dawn of Quan	tum Computing is Upon Us	IBM Research Quantum Experience			IBM Quantum Experience		
User Guide	,	Welcome to IBM Qua	ntum Experie	nce!	:	×	
Welcor		at it means to program a real quantum					
If quantum ph experiences a In order to co for a complete	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!						
Our goal with hands-on opp quantum intui	Learn and explore	the quantum world		Get composing!			
	°	we can more deeply explore all t d that thinks it is limited by the la		, ,	ers, and		
the Quantum Con	nposer in simulation immedi	take the time to work your way th ately. Units will be added to your n the real quantum processor in c	account once you ha				
Update #1: We're	excited to have you try out	our real processor, so here's ano	her 15 Units using th	is Promotional Cod	de.		

THANK YOU! Questions? Comments? Stuff?

- Jaya Baloo
 - Jaya.baloo@kpn.com

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

