



Share experience. Build resilience

Welcome to SECCON NL 2022

digital trust
center.



HSD
securitydelta.nl

CYBERVEILIG
NEDERLAND



Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

telindus
a Proximus company

avit

CISCO
SECURE



Impact of Quantum

A General Outlook

Sam Samuel
Cisco Systems
September 2022



Agenda

- 1 Background
 - General QC stuff
- 2 Timeframe of interest
- 3 Options
 - PQC
 - QKD
- 4 A Quantum Vision
- 5 Summary



What is Quantum Computing?

Superposition (of qubits)

classical
0100110101

quantum
 p_0 0000000000
 $+p_1$ 0000000001
 $+p_2$ 0000000010
 \vdots
 $+p_{2^N}$ 1111111111

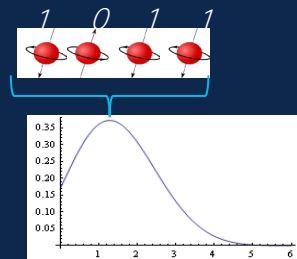
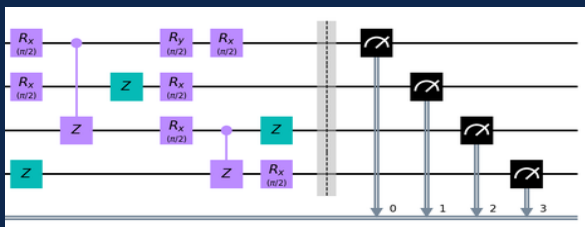
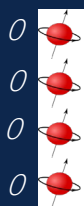
N bits describe the state 2^N Qubits describe the state

Entanglement (strange correlations)

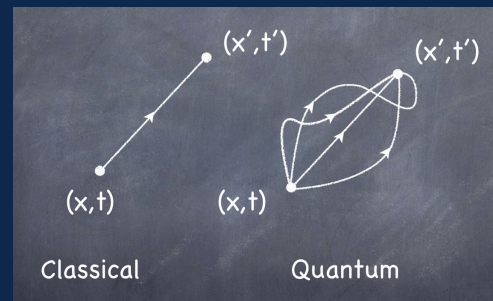


We know the state of the system as a whole, not the individual pieces

Quantum circuits are probabilistic in nature



A quantum computer explores all possible configurations. Simultaneously!



At the moment Quantum Computing is impacted by noise which makes reliable computing problematic

Share experience. Build resilience.



Potential Problem ... or Opportunity

Quantum Computer potency follows a double exponential law on the number of Qubits

Generation (G)	0	1	2	3	4	5	...	N
Exponential E.g. Moore's Law (2^G)	1	2	4	8	16	32	...	2^N
Double Exponential E.g. Nevin's Law (2^{2^G})	2	4	16	256	65546	$\sim 4.3 \cdot 10^9$...	2^{2^N}

Hartmut Neven: Observed that quantum computers are gaining computational power at a doubly-exponential rate

Shor's algorithm does comply with Neven's law

If Quantum Computing delivers on its promise then there could be a threat to the security of a network



In Practical Terms

... It is a matter of time before Quantum Impacts us

AES key-length k	RSA Bits	Elliptic Curve (bits length)	Notes
48	480	96	DO NOT USE (trivial)
50	512		
56	640	112	Advised against
62	768		
64	816	128	
73	1024		Caution - well funded criminal gangs
80	1248	160	
89	1536		
103	2048		Nation state ?
112	2432	224	
128	3248 (or 3072)	256	2030's
Probably OK 160	5312 (or 4096)	320	Beyond 2030's
192	7936 (or 7680)	384	
OK 256	15424 (or 15360)	512	

Neven's Law

Quantum acceleration?



Not OK - Impacts any key exchange

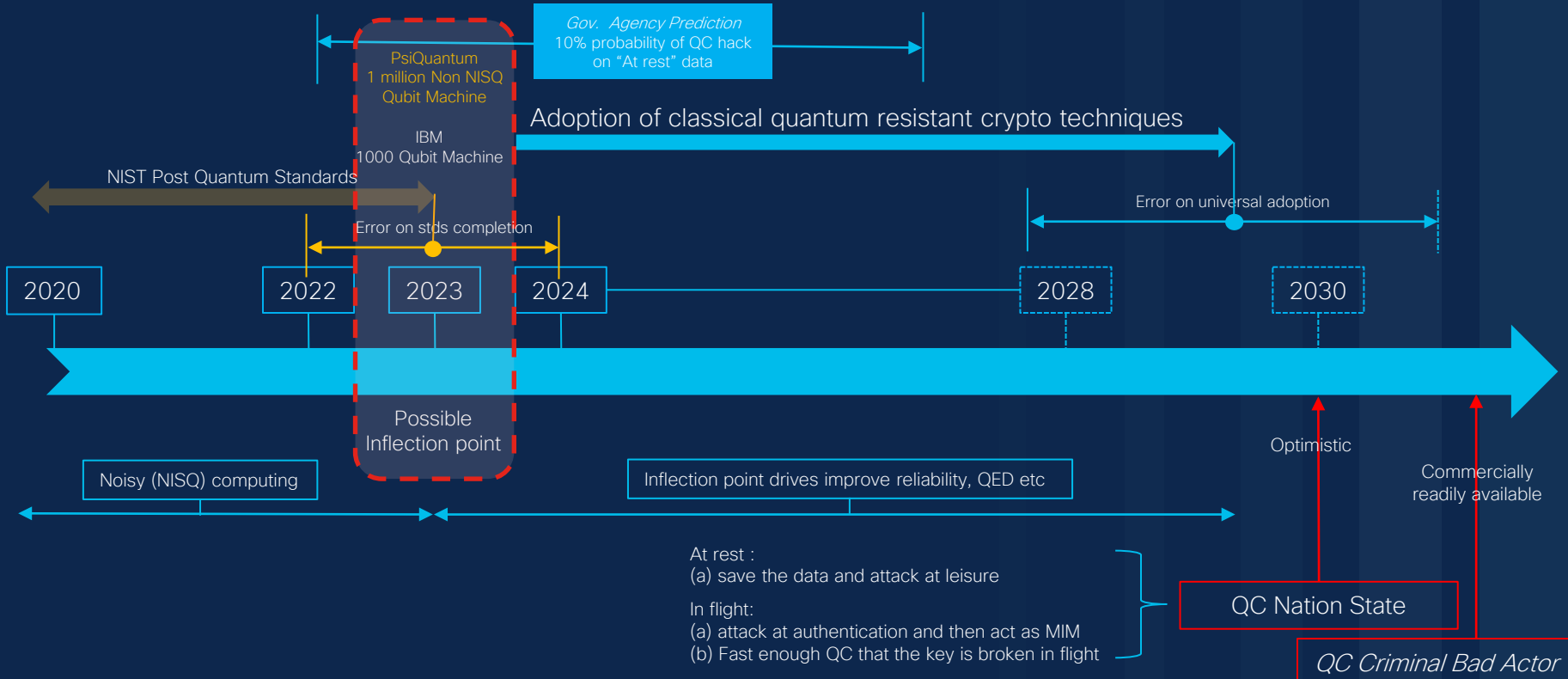


Agenda

- 1 Background
 - General QC stuff
- 2 Timeframe of interest
- 3 Options
 - QKD
 - PQC
- 4 A Quantum Vision
- 5 Summary



Post Quantum Security Time Line



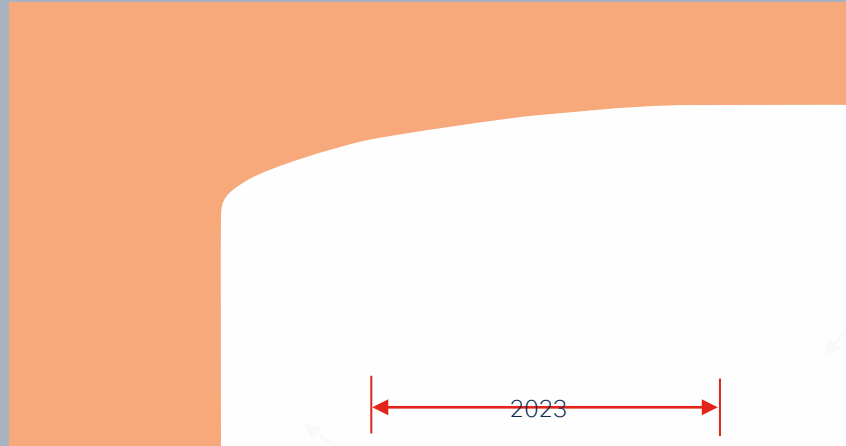
Think of this as a 10-year generational shift



Between NISQ and Nirvana

NISQ: Noisy Intermediate Scale Quantum
FTQC: Fault Tolerant Quantum Computing

Source: William John Munro et al, Designing Quantum Computers, NTT Technical Review, Vol19 No 5 May 2021



Universal quantum computers (Nirvana)

Tasks potentially performed with quantum advantage (Noise limited)



Agenda

- 1 Background
 - General QC stuff
- 2 Timeframe of interest
- 3 Options
 - PQC
 - QKD
- 4 A Quantum Vision
- 5 Summary

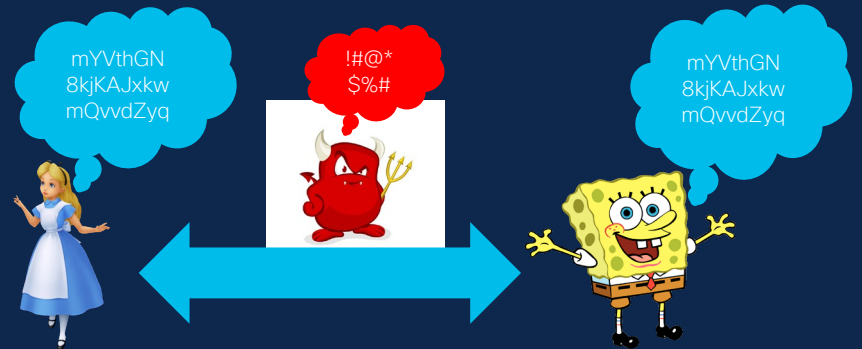


Initial method for postquantum security – symmetric

The insight: Quantum Computers aren't very good at breaking long symmetric keys.
Hence, if we can configure both sides with the same long key, we can be Quantum Safe

Here is how it works:

1. We give Alice a long key
2. We give Bob the same long key
3. Alice and Bob create a secure tunnel that depends on the key
4. Someone trying to listen in can't, even if they have a Quantum Computer



The best attack our devil would have would be Grover's algorithm, which doesn't scale with a long key
Against a key with 256 bit entropy, Grover's will take at least 2^{128} operations, which is infeasible

We have this enhancement with IPsec (RFC 8784), which we have implemented on Cisco equipment

One issue: how do we get that key to both sides?



Post Quantum Approaches



Postquantum cryptography


NIST Finalists – 5th July 2022

CRYSTALS Dilithium (Sig)	Falcon (Sig)
CRYSTALS Kyber (KEM)	SPHINCS+ (Sig)

NSA – 7th Sept 2022 Commercial National Security Algorithm Suite 2.0

Public Key	Symmetric Key	S/W & F/W Signatures
CRYSTALS Dilithium	AES	XMSS
CRYSTALS Kyber	SHA	LMS

Begin deprecating RSA/Diffie–Hellman and Elliptical curve Cryptography (ECDH ECDSA)
Transition to be completed by 2035



Postquantum cryptography

The Practical Implications

- Need to update protocols to use these new primitives.
- Need to be able to negotiate the new protocols (so we don't have to update everything at once)
- New protocols use more bandwidth (so sometimes fragmentation becomes an issue)
- Pair with conventional cryptography
 - This is to make sure we don't make anything worse
- The IETF is looking to update the TLS, IPsec and Certificate standards



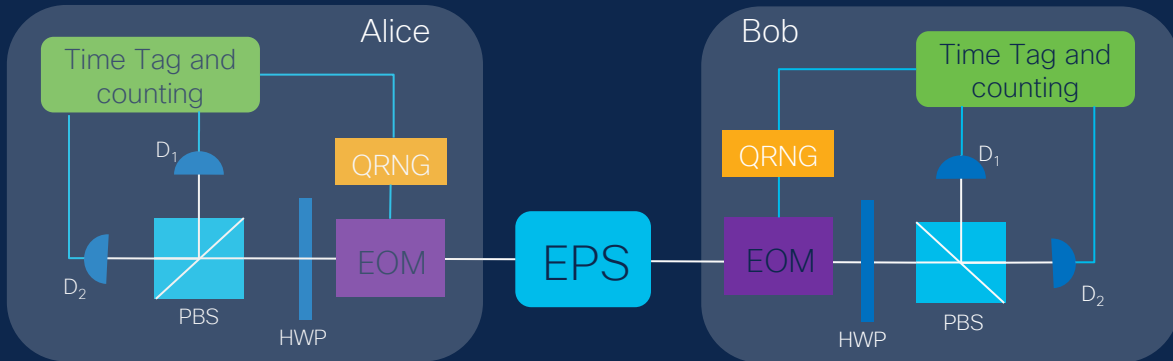
Keys, the final frontier



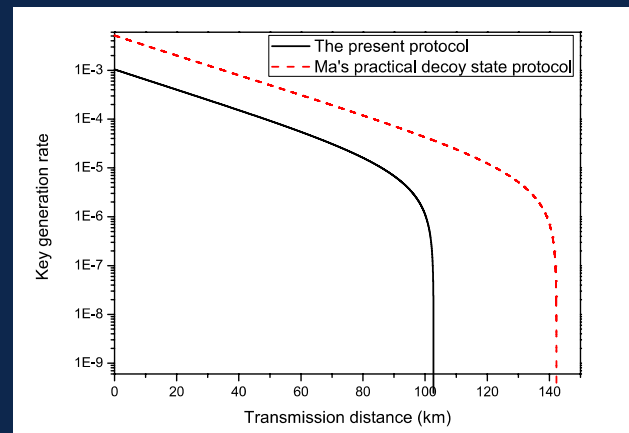
QKD (Quantum Key Distribution)

The idea: secure communication method utilizing laws of quantum physics for exchanging encryption keys only known between shared parties.

QKD works by transmitting many light particles, or photons, over fiber optic cables between parties. Each photon has a random quantum state, and collectively, the photons sent make up a stream of ones and zeros.



- EPS Entangled Photon Source
- EOM Electro optical modulator
- QRNG Quantum Random Number Generator
- PBS Polarising Beam Splitter
- HWP Half-wave Plate
- D Detector



Quantum key distribution with prepare-and-measure Bell test, Yong-gang Tan, 2016, www.nature.com/scientificreports

Share experience. Build resilience.



QKD - still has challenges

Challenges:

- Integration of QKD systems into current infrastructure
- Distance limitations for coherence
- Adoption of QKD as a protocol
- Incorporation of wireless

Various types of QKD are around:

- Prepare-and-measure protocols
- Entanglement-based protocols
- Discrete variable QKD (DV-QKD)
- Continuous variable QKD (CV-QKD)
- Eckert 91 (E91)

Same problem as other security approaches - i.e. time to universal adoption



NSA guidance on QKD

But ... (there is always a but ...)

NSA supplied specific guidance

- QKD only forms a part of the cryptographic system
- Not recommended for National Security Systems (NSS)
- Yes, it is scientifically interesting – but only addresses some of the security threats
- Requires a significant re-engineering modifications to some systems
- Does not consider QKD a practically secure solution for NSS



Agenda

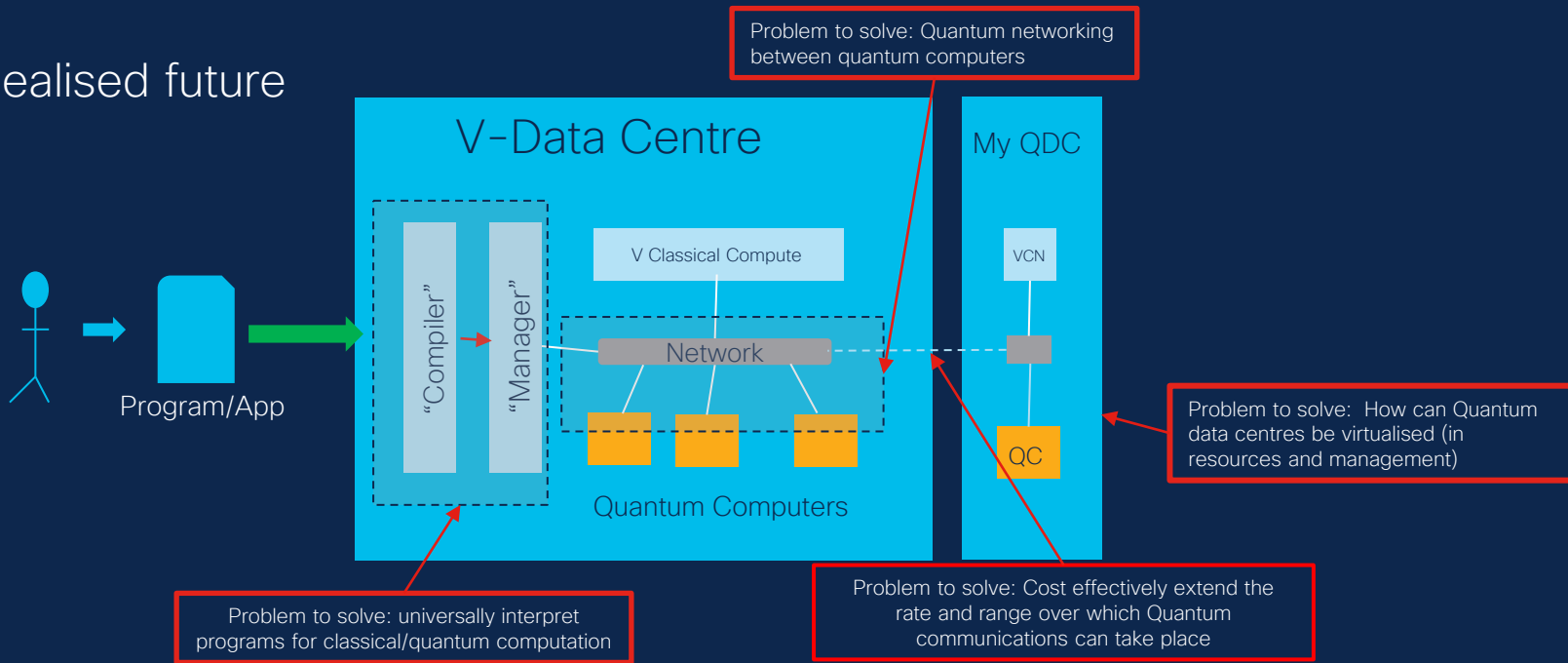
- 1 Background
 - General QC stuff
- 2 Timeframe of interest
- 3 Options
 - PQC
 - QKD
- 4 A Quantum Vision
- 5 Summary



Where could we go?

The quantum data centre

Idealised future



Possible end state and problems to solve



Current Reality ...

There is brilliant progress being made ..

Item	Current	Requirement 2025	Gap	Notes
Entanglements/sec	2.8	2 Mebit/sec	10^6	If fidelity of 0.9 or above were requested the entanglement rate could drop below <0.25 e/sec
Distance	2m	(10km<d<20km)	10^3	Experiment is repeaterless
Fidelity	0.8	0.99999	10^4	But can set requested fidelity

... but long-distance quantum communications is still a long way to go





Agenda

- 1 Background
 - General QC stuff
- 2 Timeframe of interest
- 3 Options
 - QKD
 - PQC
- 4 A Quantum Vision
- 5 Summary



An Approach to Future Network Security

- First Aim: Ensure the network remains secure in light of progress in Quantum technologies
- If Quantum Technologies deliver on their computational potency promise more effort will have to be placed on accelerating PQC adoption
 - Have to take a pragmatic approach on adoption. Likely to be SSH replacement or IPv6 adoption timescales
- A leading indicator (likely inflection point) will occur around 2023
 - Appearance of large number of Qubit devices
 - Combined with advances in QEC could accelerate the inflection point
- In parallel with the cryptographic threat that quantum presents
 - Actively exploring quantum tech for communication scenarios (i.e. continue to explore the upside)
 - This technology is still in mainly in academia or in a start-up lab
 - We expect to see quantum entangled distribution rates in the MQubits/sec in the 2025 time frame
 - Commercial maturity likely to occur towards the end of this decade (2030 timeframe)



Summary of the cryptographic approaches

Category	Symmetric	QKD	Postquantum
Security	Good	Good	Good
Media Flexibility	Good	Limited	Good
Range	Good	Limited	Good
Ease of Use	Difficult to Config	Good	Good
PFS	No	Good	Good
Current Hardware	Yes	QKD Required	Yes
Available Now	Yes	Yes	In a few years



Ask me anything

Share experience. Build resilience.