Quantum Research at BT

Neil J. McRae
Chief Architect
BT

Who we are

- In 180 countries around the world
- £24bn revenue, £5bn free cashflow
- c.100,000 people
- Recruiting 1700 grads and apprentices for 2018

‘Purposeful innovation’ in telecoms has transformed the world since 1837

1846 Electric Telegraph Company

1926 Two-way transatlantic telephone conversation by radio

1943 Electronic Programmable computer: Colossus

1962 Telephone call via satellite

1968 Digital telephone exchange

1980 Purpose-designed optical fibre submarine cable

1984 140Mbps commercial single-mode optical fibre link

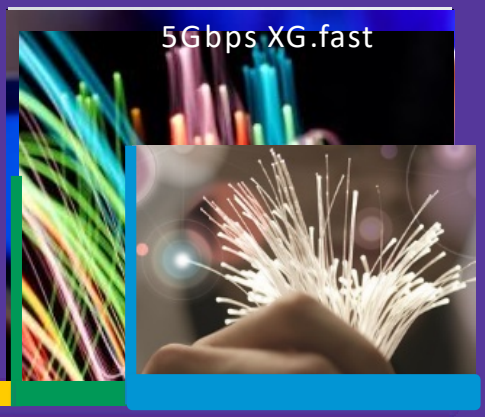
1989 Satellite telephone system: Skyphone

1999 GPRS live data call over a mobile network

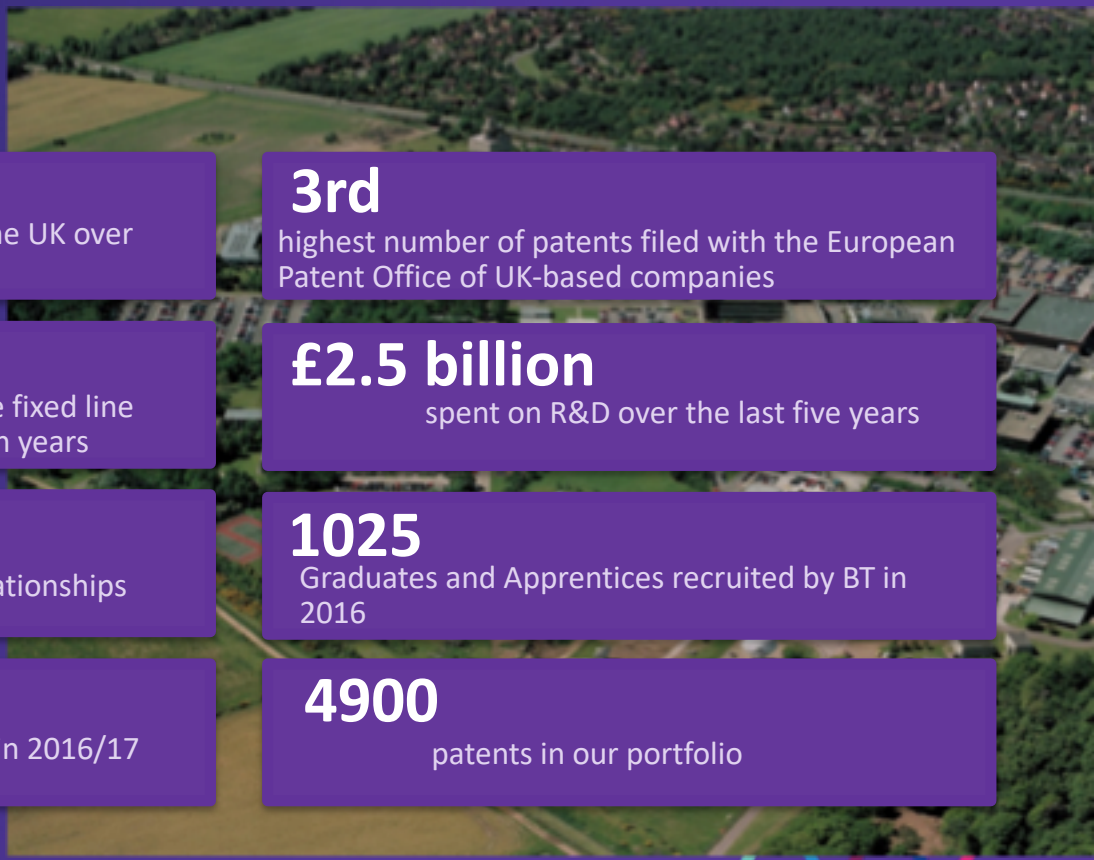
2013 World’s first G.fast trial

2014 2015

cryptography



Investing in Research & Development



3rd
largest investor in R&D in the UK over past ten years*

3rd
highest number of patents filed with the European Patent Office of UK-based companies

2nd
largest investor in R&D in the fixed line telecoms sector over past ten years

£2.5 billion
spent on R&D over the last five years

30+
Direct university research relationships

1025
Graduates and Apprentices recruited by BT in 2016

102
Number of inventions filed in 2016/17

4900
patents in our portfolio

Network bottle-necks / challenges

SDN-based Control / Orchestration

Millions of nodes | *Thousands of nodes* | *Dozens of nodes*

- Gb/s access
- Wireless femtocells
- Deep fibre
- 5G KPIs
- Convergence
- Infrastructure cost

- Multiple CPs
- Tb/s switching
- Remote storage / compute
- NfV
- Dynamic config
- Whitebox

- 10-25G transport
- Many wavelengths
- Limited flexibility
- Cheap 10G over 50km

- Multi Tb/s switching
- Data centre functions
- Multi layer 1-3
- ROADM optical switching
- Sliceable spectrum

- > 1Tb/s per fibre
- Increased flexibility
- Cost less critical
- Elastic Optical Networks

BT

Major current work threads

- **SDN**
  - Datacenter optical interconnect with SDN control
  - Ciena Blue Planet SDN evaluation
  - Multiple PoCs for Media and Broadcast
  - Working with Zeetta Networks on demos
  - Whitebox
- **Converged Digital Infrastructure**
  - Building optical infrastructure / orchestration
- **5G Metro**
  - E2E 5G PoC with Adva (+ other vendors)
  - Leading large EU project (Metro-Haul)
- **Core Transport**
  - Multicore fibres. Hollow core fibres
  - Cambridge-Huawei research centre focused on multi-band / multi-core
  - IIT Delhi Centre focused on Elastic Optical Networks with quantum security
- **Optical Access**
  - Future PON standardisation
  - Future PON PoCs / research
  - Free Space Optical project with Glasgow University
  - FINDIT – detecting infrastructure underground using GPR / acoustic waves etc
  - Fibre Monitoring using Fibre Bragg Gratings etc
- **Quantum**
  - Cambridge-Adastral QKD link
  - Direct engagement with ID-Quantique, Toshiba, Huawei, KETS (TEAC) leading to customer trials
  - Innovate UK projects EQUIP, Q-CAPS, FQ-NET
  - ESA Satellite QKD project starting imminently
  - Understanding quantum market potential
  - ETSI standards

Underpinned by an optical infrastructure: Cambridge-Adastral, LEANet resurrected (Ipswich, UEA, Essex), Adastral labs connectivity, NDFIS links around the country (inc. Bristol), NPL, Harwell…

Security agenda on the front page

NHS

NHS computer hack: North Korea and Russia are implicated as phishing attack is ruled out

The NHS computer hack using Wanna Decryptor ransomware shut down IT systems with 75,000 attacks in 99 countries

ion in 15 Days

ing with stock traders made hundreds of transa
uthorities say—including trades in just 15 days
that netted millions.

Date	Stock	Profit, approximately
Oct. 2013 (2 days)	Align Technology	$1.45 million
Jan. 2012 (2 days)	Caterpillar	$1 million
Oct. 2013 (2 days)	Panera Bread	$1 million
April 2013 (2 days)	Edwards Lifesciences	$844,000
July 2012 (3 days)	Acme Packet	$685,000
Oct. 2011 (4 days)	Caterpillar	$648,000

Source: U.S. Justice Department

THE WALL STREET JOURNAL.

NSA

AT&T's 'extraordinary, decades-long' relationship with NSA – report

- New York Times and ProPublica cite newly released NSA documents
- Telecoms giant assisted with 'wiretapping United Nations headquarters'

How U.S. government is tapping internet and phone calls from international undersea cables

- Another top-secret National Security Agency slide, published by The Washington Post, exposes the even wider reach of the government's intelligence programs
- Slide shows the surveillance of an extensive network of underwater fiber cables that go from North America to the rest of the world
- This method is used in parallel to the government's monitoring of PRISM

NSA retract their promotion of elliptic curves for public-private keys – August 2015

And so a major concern for telcos

BT

Cryptography today

Public Key Cryptography

2 keys – related via a mathematical algorithm (e.g. RSA)

Encrypt using public key

Decrypt using private key

Finding private key from public key computationally hard

Quantum computers might make this easier

*Inventors of **RSA**: Ron **R**ivest, Adi **S**hamir and Leonard **A**dleman*

Symmetric Key Cryptography

Same (private) key used to encrypt and decrypt

Encryption often uses AES (Advanced Encryption Standard)

Need secure method of distributing the key

Currently key distribution uses couriers

That's better than this

Solution

Symmetric Key Cryptography with secure key distribution

We need a method of transmitting keys securely

BT

Fibre vulnerability

Fibre tapping is straight forward

Access the cable, expose the glass, bend it to allow some of the light to escape, detect the light and store / read the data

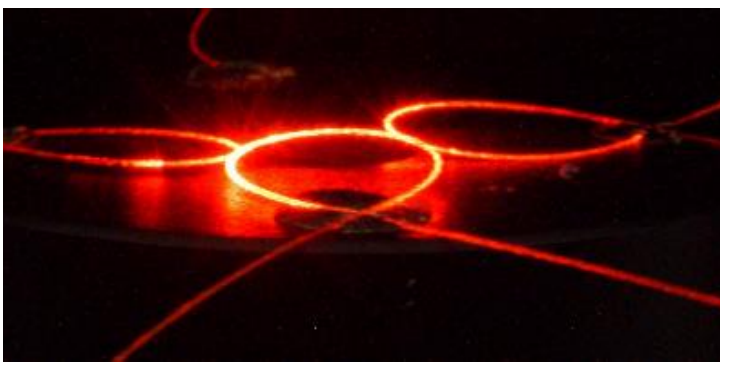
Millions km vulnerable fibre around the world

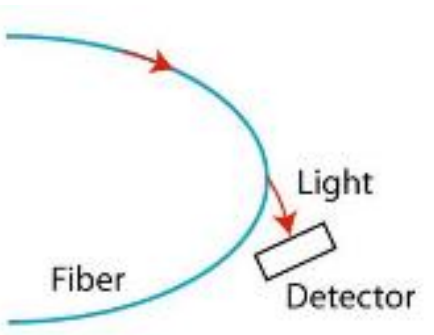
Often installed by contractors – taps could be built in

1% taps impossible to detect

Data can be stored and studied or decrypted at a later time

Data shelf life concept





BT

Quantum Computer threat to today's cryptography

Symmetric Key Cryptography
De-facto standard for securely encrypting data

E.g. AES 256 / 512

Requires symmetric key (same at both ends)

Key distribution alternatives
Public Key Cryptography (e.g. RSA)

Attaché case in white van

Quantum computer threat to PKC

Google says it will make a quant computing breakthrough by the 2017 that could lead to machine capable of answering mind-bogg scientific problems

- Google is testing a quantum processor twice as powerful as its pre
- It aims to more than double this computing power again by the enc
- If successful it will have created a chip more powerful than any cor
- This could lead to quantum supercomputers capable of solving problems far beyond the reach of current technology

By TIM COLLINS FOR MAILONLINE
PUBLISHED: 14:40, 23 June 2017 | **UPDATED:** 14:40, 23 June 2017

Share

2 View comments

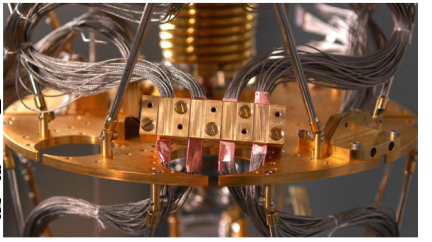
The world's most powerful quantum computer processor could be created by Google, if research underway at the firm pays off.

The company is currently testing a quantum processor more than twice as powerful as its previously announced chip, and claims it will be ready by the end of 2017.

Why Microsoft believes we're on the threshold of quantum computing

By Mary Branscombe December 20, 2016 Computing

The time is right to make quantum computing real...



PAGE 1 OF 2: INTRODUCTION AND FROM THEORY TO ENGINEERING

Microsoft has been putting money into the science of quantum computing for

Leads to two parallel approaches:

- Post Quantum Cryptography
  - Algorithms resilient to quantum computers
- Quantum Key Distribution
  - Relying on the validity of quantum physics

BT

Why quantum computers will be able to crack today's encryption

Encryption algorithms rely on being easier one way than the other

If 7 is a factor of N = 21, what's the other factor? → Simple division

What are the factors of 21? → Brute force search through all possibilities

Now imagine N is a random 2048 bit number….

Division is still straight forward, but factorisation would take billions of years using classical computers

Quantum computers could dramatically reduce the time taken to find factors

Shor's Algorithm runs quickly on a quantum computer

Uses Euler's order (period) finding discovery

2, 4, 8, 16, 32, 64, 128, 256….

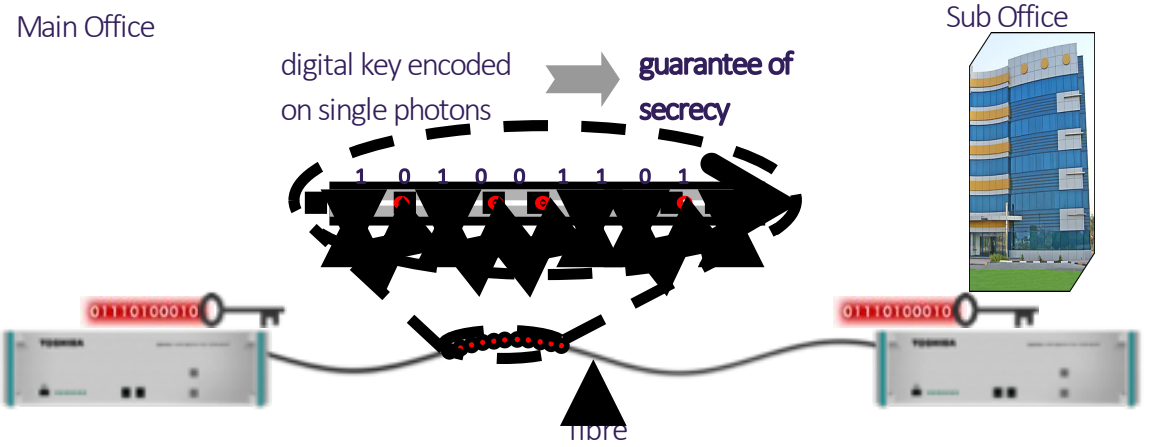
– Mod 15 = 2, 4, 8, 1, 2, 4, 8, 1… (P=4)

– Mod 21 = 2, 4, 8, 16, 11, 1, 2… (P = 6)

Shor's quantum algorithm can find P without having to compute long sequences

BT

Quantum Key distribution (QKD) in essence



- Encryption keys formed out of a stream of single photons
- Photons carry keys via phase / polarization / position modulation
- Key is refreshed constantly
- Impossible to hack into the key during transmission
- Keys are created using Random Number Generators. One method uses a quantum technique which might involve single photon sources

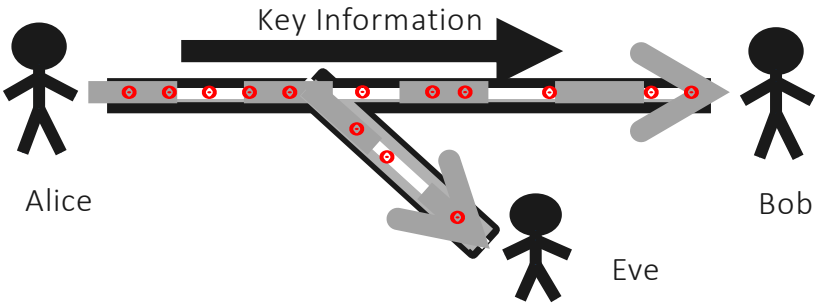
BT

Effect of inserting a tap device

Alice, Bob and Eve(sdropper)
Secure channel means that the all-important key is kept secure
Key info thrown away if intruder detected

Key established from transferred photons

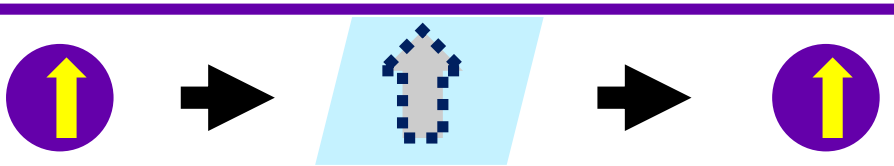
Once the key is established, data can be encrypted using AES etc



Stealing photons no good
But Eve can't clone / copy them either
Observation of photon modifies it (collapses its wavefunction)

BT

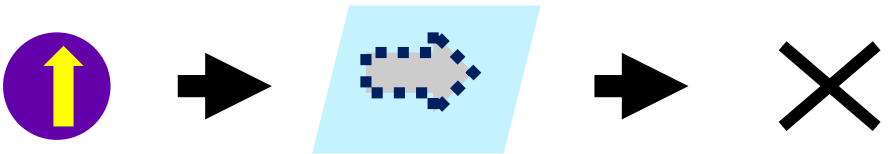
Single photon polarisation behaviour



Single photon polarised vertically

Polariser sheet aligned vertically

Photon always passes through

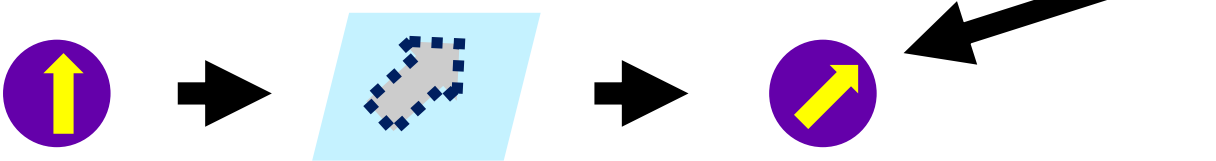


Single photon polarised vertically

Polariser sheet aligned horizontally

Photon never passes through

Strange quantum behaviour – what is happening?



Single photon polarised vertically

Polariser sheet aligned at 45 degrees

Photon passes through with 50% probability and a new polarisation

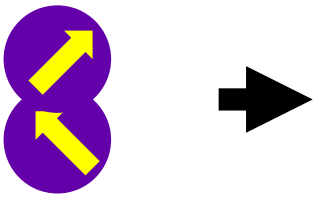
BT

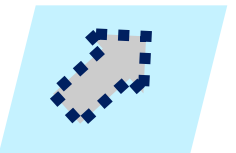
Single photon polarisation behaviour (2)

Single photon polarised vertically

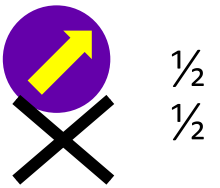
Can be viewed as

Being potentially in both of the above states until it is observed





Polariser serves as an observation

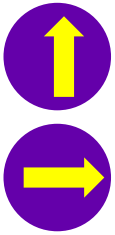


- Polarisation not often used due to difficulty of controlling it.
- Similar behaviour seen replacing polarisation with phase, or pulse position….

BT

QKD basis states

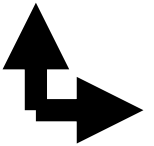
Measure in the same basis as the sender and you will accurately record what was sent.

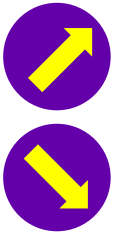


= “1”

= “0”

In Horizontal / Vertical basis states



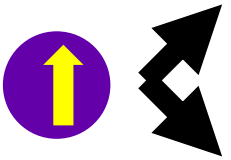


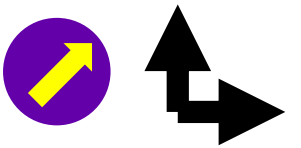
= “1”

= “0”

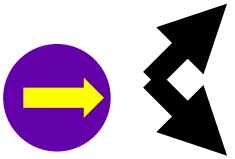
In 45 degree basis states

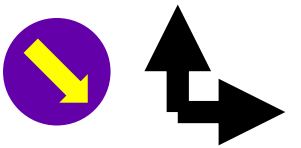
But not if you measure in the other basis state:





= “0” or “1” with probability ½





BT

More details

The receiver (Bob) compares his (random) measured basis state with the sender (Alice – also random) for EVERY photon

They do this AFTER the photons have been sent and received
They DISCARD all results where the basis sets were different

For ALL the others – they know they should get the same result
Alice and Bob reserve some photons for intruder detection

The evesdropper (Eve) doesn't know which basis state to measure in

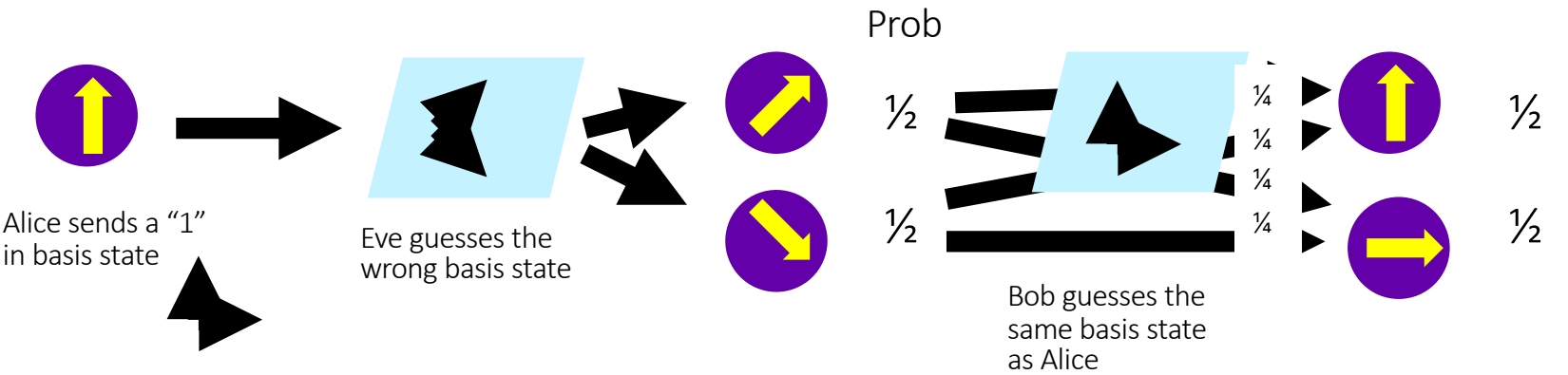
If she guesses wrong, she CHANGES the polarisation so that Alice and Bob get different results when they should agree

So they know there is an intruder

Many QKD protocols have been proposed to harness this effect (e.g. BB84)

BT

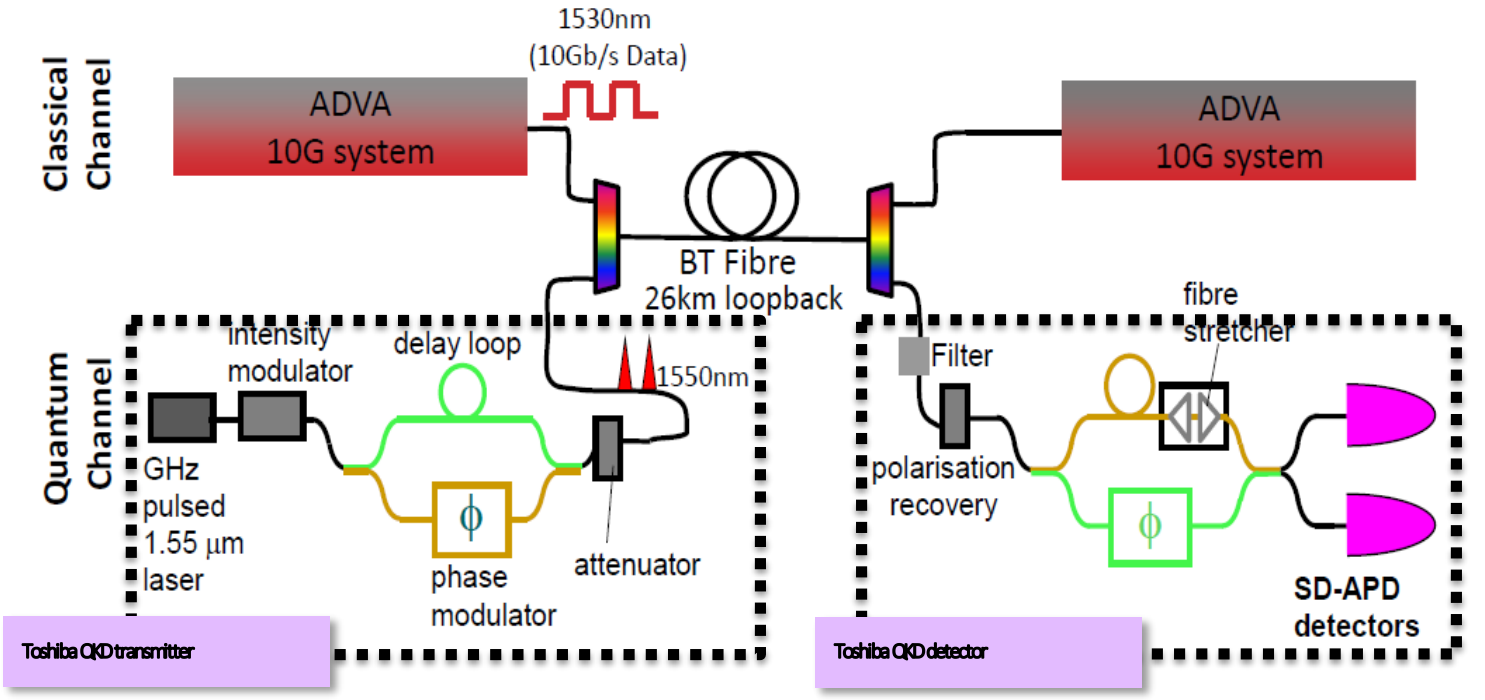
If Bob guesses the wrong basis state, they reject any results later after comparing states used



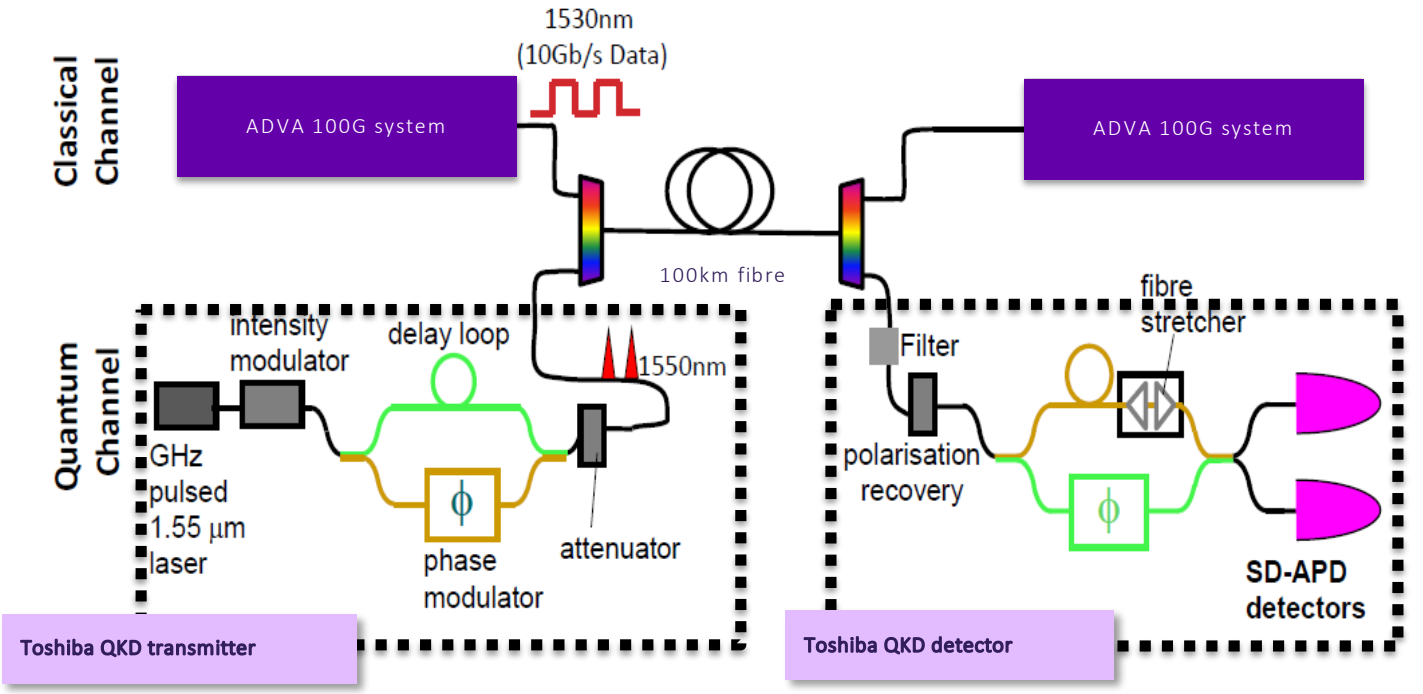
If Eve tries to observe, she will affect Bob’s results in a detectable way

BT

World first real time QKD + 10Gb/s field trial using commercial hardware (2014) - Adastral Park – Ipswich (27km)



World first real time QKD + 100Gb/s field trial using commercial hardware (August 2015)

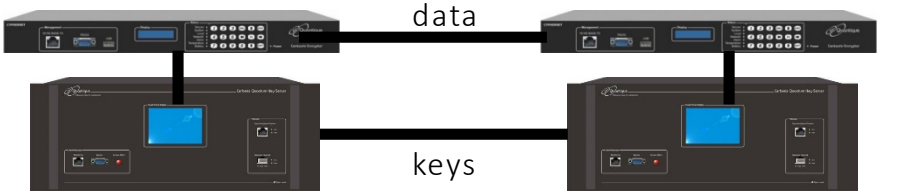


BT

Innovation Week Demo: World First Quantum Protected 100GE Encryption

Combining Quantum Key Distribution (QKD) links with the best available High Speed Encryption systems

First 100GE encryptors integrated with Quantum Key Distribution – world first
Shows huge developments in QKD capability as well as high speed Ethernet encryption
Demos involving various partners – Adva, Senetas, ID Quantique



High speed, transparent L2 AES256 encryption of a 100G Ethernet link, with latencies lower than 1 µs, using Gemalto Safenet CN9010.

Encryption keys are derived from a combination of two sources:

* Integrated FIPS certified Diffie-Hellman key exchange
* Quantum Communications Hub Cerberis Quantum Key Distribution system from IDQuantique.

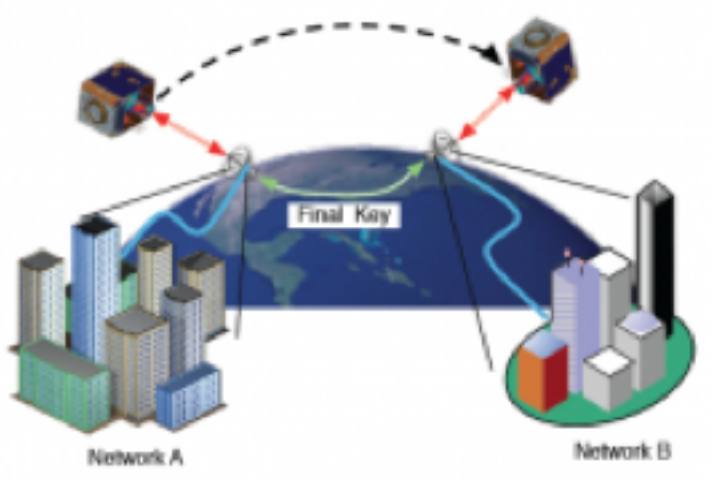
Demo of secure virtual server mobility.
We use HSE with QKD on the link, to provide extremely high protection against external eavesdropping as the VM is transferred across the link.

QUANTUM COMMUNICATIONS HUB

IDQ AVAYA gemalto security to be free BT

Satellite QKD for longer distance QKD

- Fibre Optic QKD limited to ~100km.
- Key established between a major node and the satellite
- Satellite then establishes a key with another major node
- Satellite can then use this second key to encrypt the first key and send it to the second node
- This creates keys between node pairs around the globe
- Keys can then be used to encrypt conventional transmission
- QSAT projects in early stages of preparation
- Entanglement-based QKD removes the need to trust the satellite



China launches quantum-enabled satellite Micius

16 August 2016 | China

Share

The rocket containing the satellite took off from the Gobi Desert

Some QKD Use Cases

Government and other company security requirements

E.g. finance, health etc

Cf Toshiba human genome project in Japan

Data Center interconnect

Distributed data centers communicate across a vulnerable network

Data Center back up for sensitive data

Cloud

Customer record storage and back-up

QKD encryption for credit cards

Major Infrastructure control

Power grids, telecoms networks…

Satellite QKD Use Cases

Transfer of valuable data / sensitive commercial information to/from remote locations (offshore, maritime, deserts, polar regions and more general isolated areas)

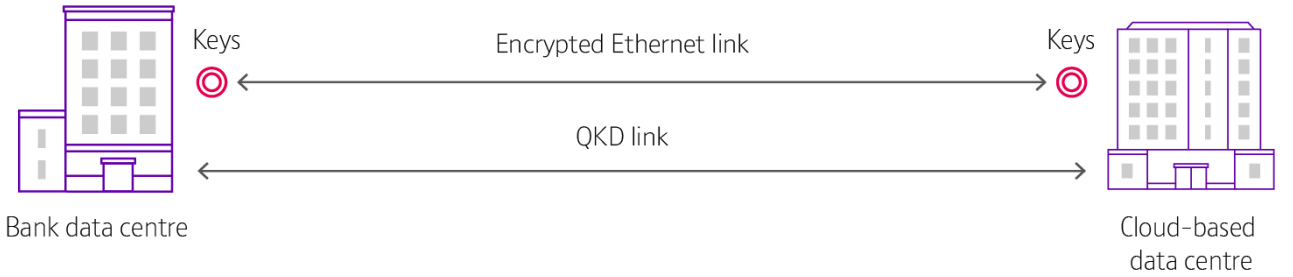
Sectors – mining, oil and gas survey data, financial data, utility management / control data

Government – Specialist emergency response teams, international communications, military comms and data

BT

Ultra-secure data back-up for financial services

Secure back-up of customer records for financial services institution between their own data centre and cloud based data centres



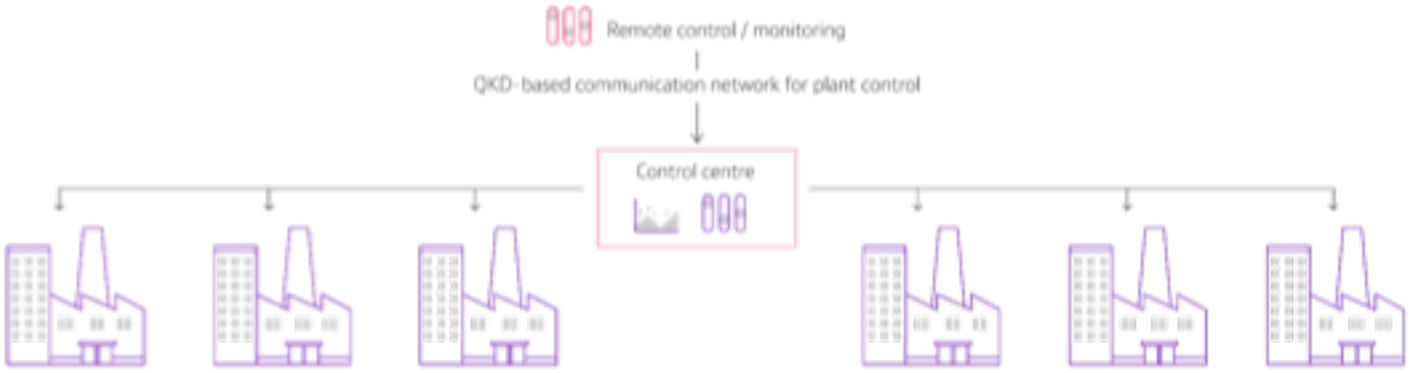
- **QKD establishes symmetric keys between the bank's data centre and the cloud data centre**
- **Keys used to encrypt an Ethernet service (e.g. GE, 10GE) between the two end points**
- **Additional keys could be used to encrypt data at rest in the cloud – 'Bring Your Own Key'**
- **Ultra secure transport and storage for transactions, customer records etc**

Equifax hack puts data of 400,000 UK customers at risk

US credit rating firm's announcement comes after UK authorities order it to alert British clients of cybersecurity breach

BT

Deployment of automation protocols in plants



- Secures control of major manufacturing plant
- Prevents hacking into control systems
- Prevents enormous potential damage to plant and possibly the environment
- Increased automation increases the need for security of control
- Combine with 5G management to give ultra secure 5G slicing control

Cyberattack on German steel factory causes 'massive damage'

By Loek Essers
Amsterdam Correspondent, IDG News Service | DECEMBER 19, 2014

A German steel factory suffered massive damage after hackers managed to access production networks, allowing them to tamper with the controls of a blast furnace, the government said in its annual IT security report.

BT

An actual NFV use case!!!!

What is it?

- NFV consolidates many network equipment types onto industry-standard high volume servers, removing the need for a separate box per piece of functionality.
- Network functions – for example routers, firewalls and WAN accelerators - are software-based, and run on commodity hardware.

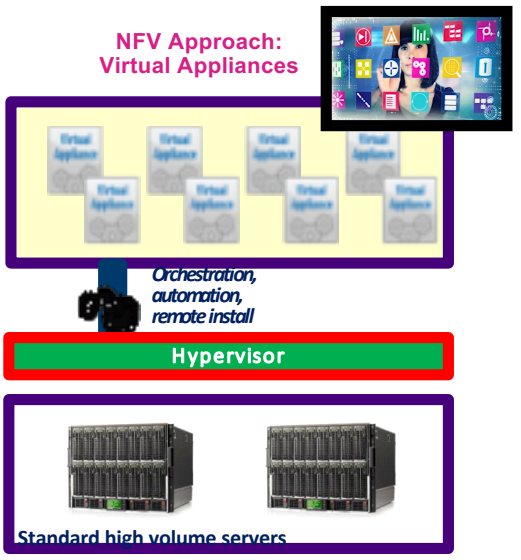
Customer Benefits

- Faster and more flexible service provision possible by remote installation & configuration (less site visits).
- Increased potential for "try-before-you-buy" network services.
- Simplified network infrastructure ("one box").

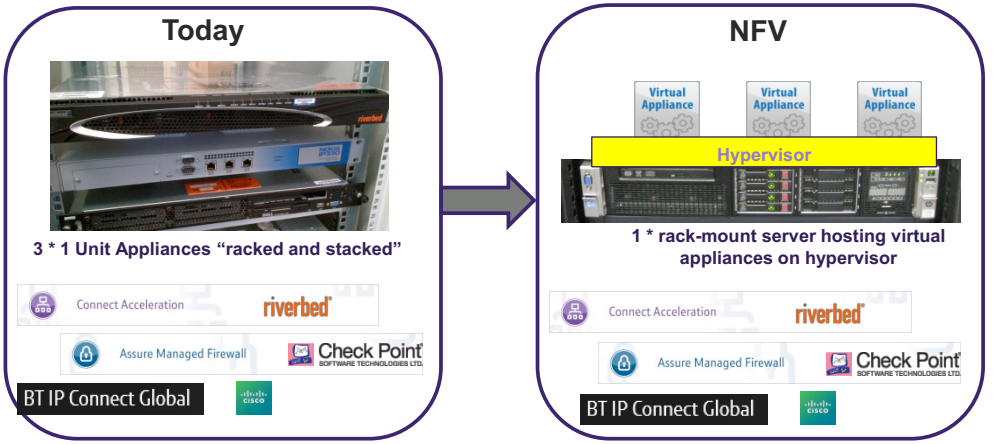
Service Provider Benefits

- Faster delivery of managed network services ("months to minutes").
- Promotes ability to up-sell and cross sell network capabilities.
- Accelerated "Concept-to-Market" i.e. new service introduction, since greater flexibility afforded by software-based appliances.

Overview



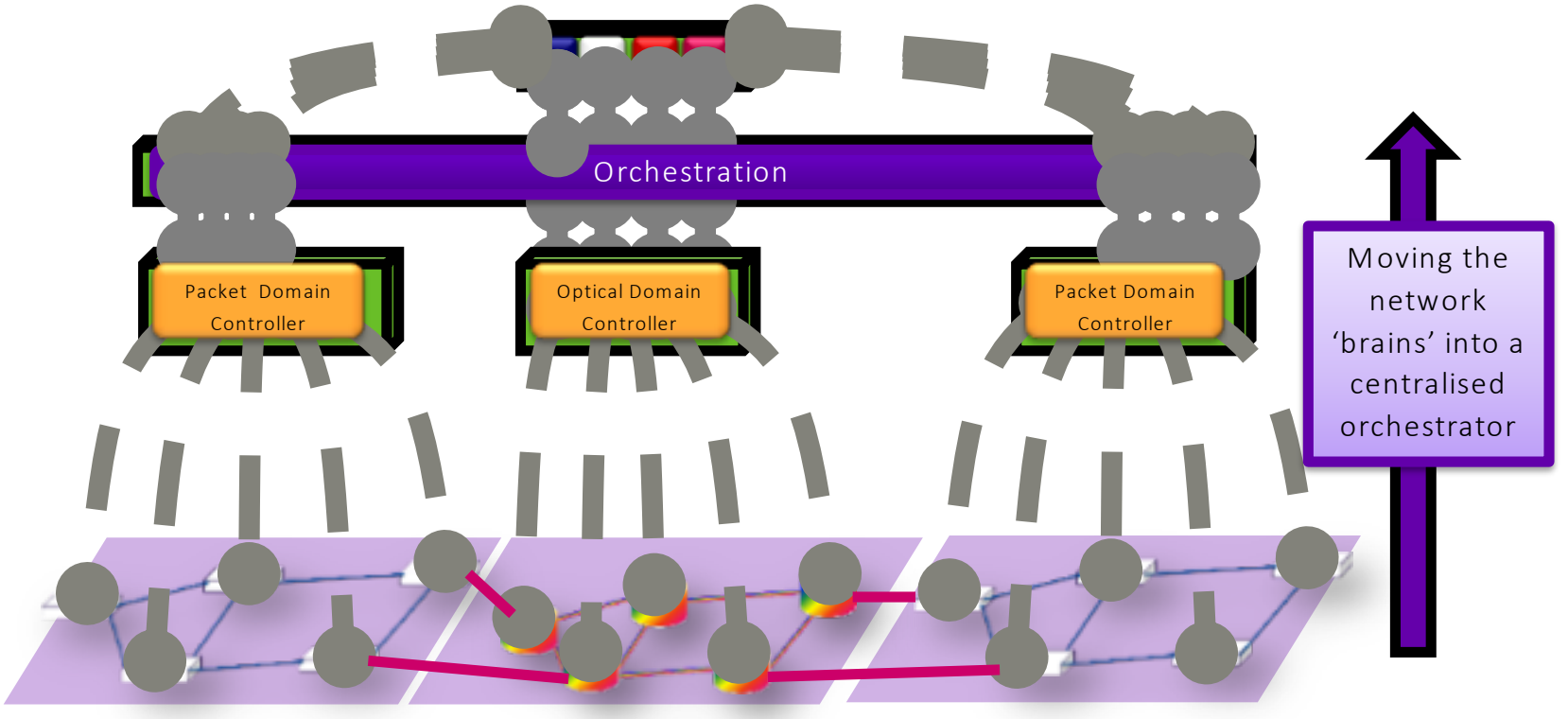
Specific Use Case- vCPE



NfV functions need high security for installation = QKD Use Case

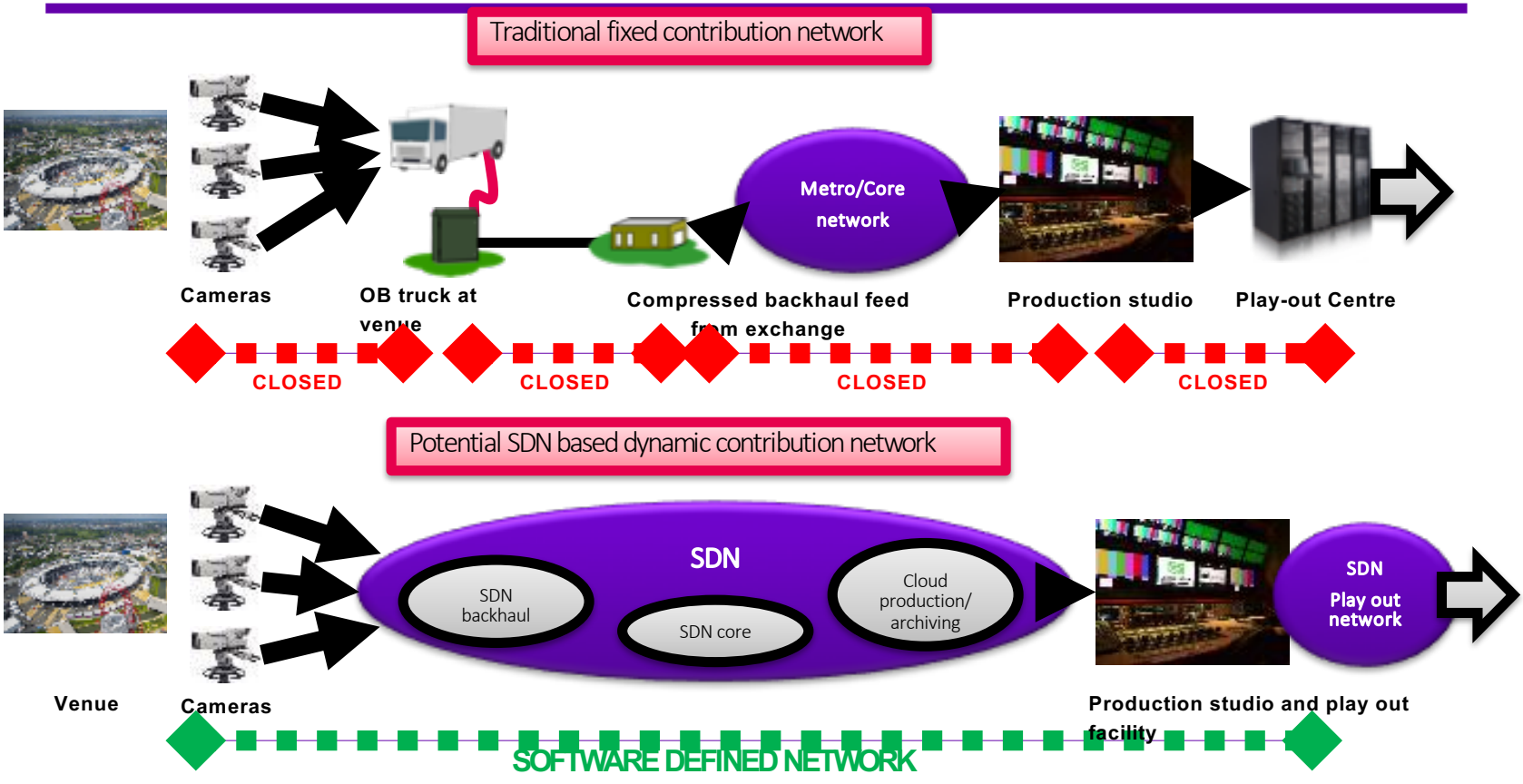
BT

SDN - Decoupling + Programmability + Centralisation + Orchestration



BT

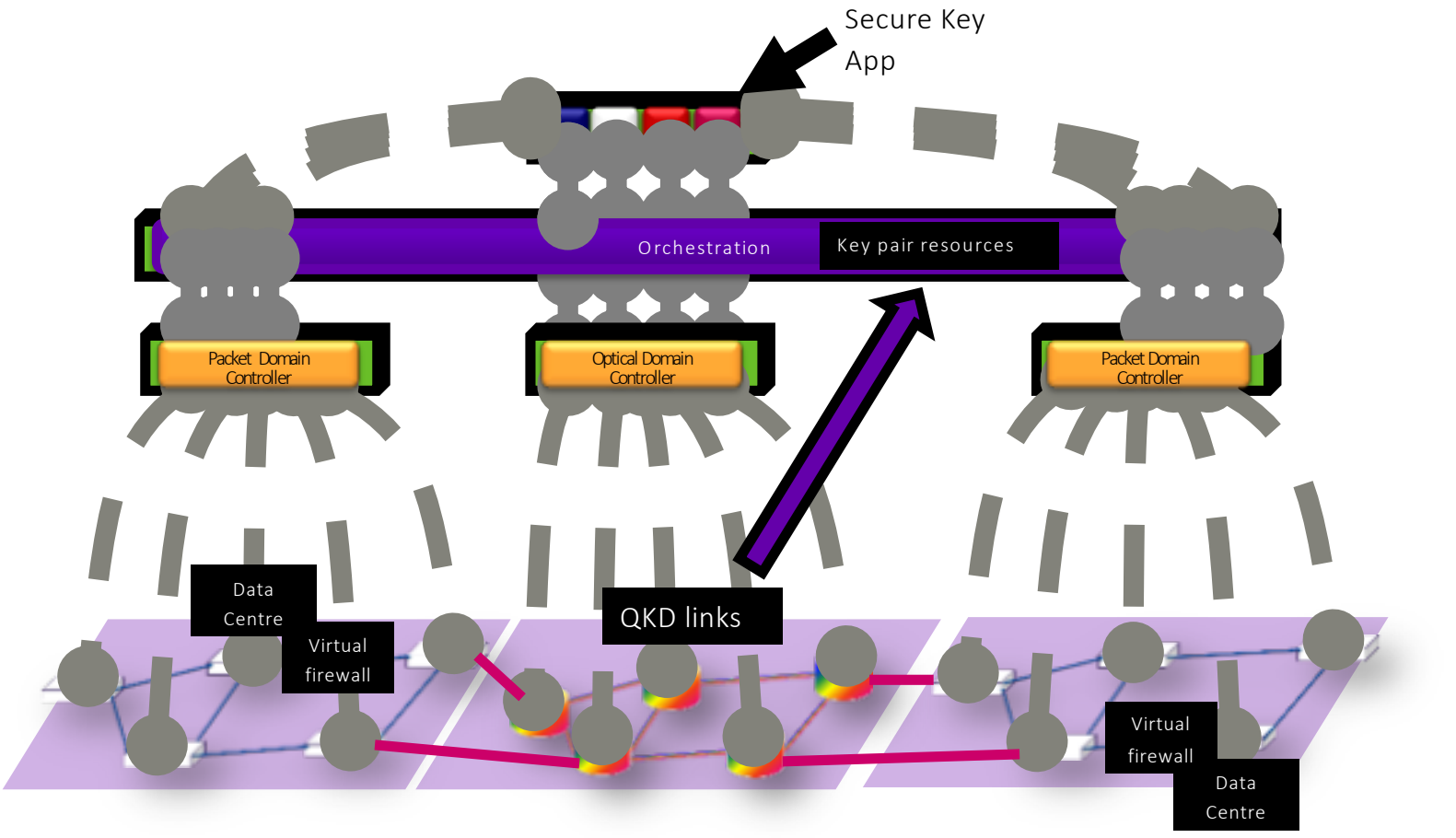
SDN Use Case – Video Contribution Networks



Moving from expensive static closed systems to a dynamic Software Defined *Video* Network

BT

Putting it together



BT

First Experimental Demonstration of Secure NFV Orchestration over an SDN-Controlled Optical Network with Time-Shared Quantum Key Distribution Resources

- ***University of Bristol High-Performance Network Group***
- ***University of Bristol Centre for Quantum Photonics***
- ***BT Research Lab***

Paper submitted to the European Conference on Optical Communications

BT

ETSI NFV architecture for distributed DCs

Distributed architecture, composed by:

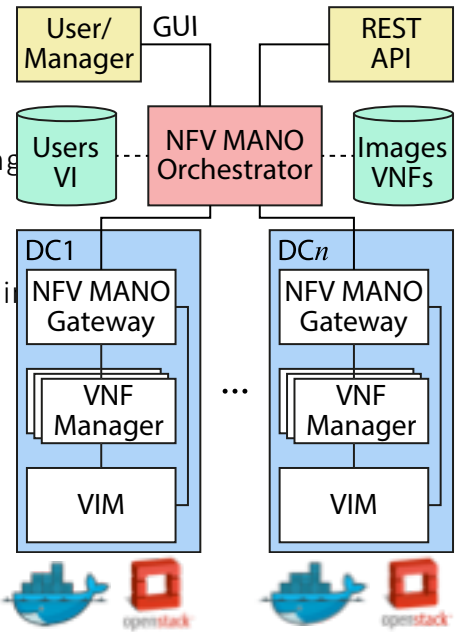
Centralized orchestrator: contains information of users, their required resources, the distributed nodes and a catalogue of functions.

ETSI NFV stack composed by:

– NFVMano Gateway: takes care of the secure communication, decrypting the images that are sent from the centralized orchestrator.

– VNF Managers: takes care of the lifecycle of the VNFs and monitors their performance. Not implemented for the initial test.

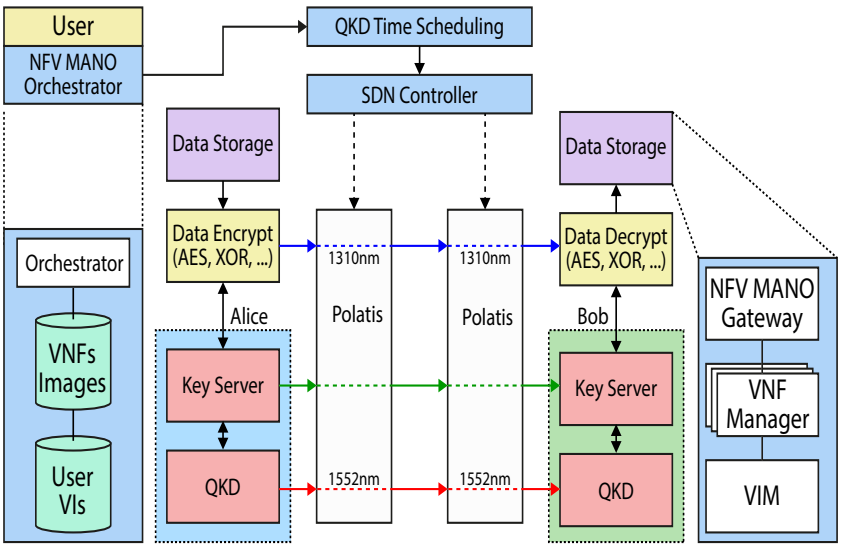
– Virtual Infrastructure Manager: Takes care of the instantiation of the required infrastructure to deploy the VNF.



BT

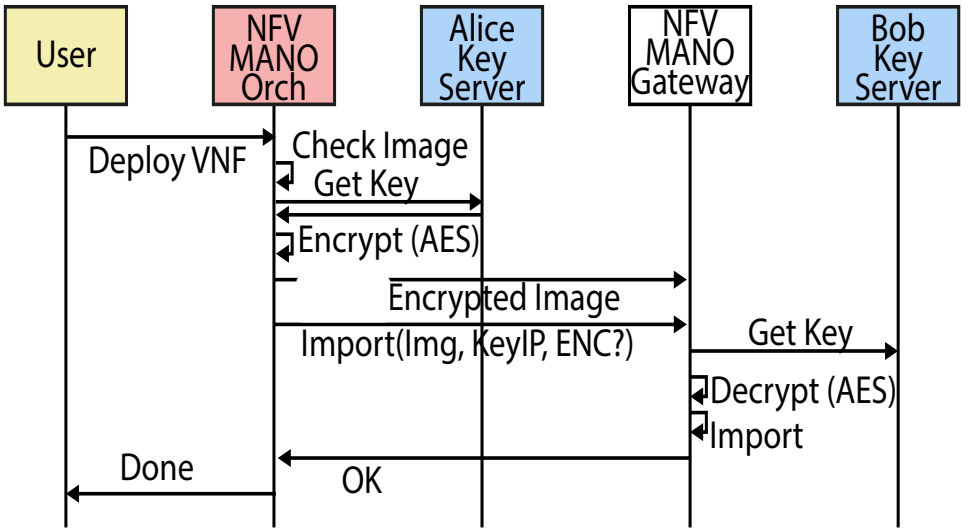
Integration with QKD Boxes: End-to-end test

- Our orchestrator contains a network scheduler for the QKD time-shared approach, which utilizes ODL Hydrogen with optical extensions to reconfigure the optical network.
- The software encryption/decryption is performed in the end points (Dell servers), using AES-256.
- The end-to-end test was executed between two Dell PowerEdge servers, hosting an orchestrator and the ETSI NFV stack.
- The orchestrator is logically co-located with Alice QKD box and Alice Key server.
- The ETSI NFV stack is logically co-located with Bob QKD box and Bob Key server.



BT

Integration with QKD Boxes: End-to-end workflow

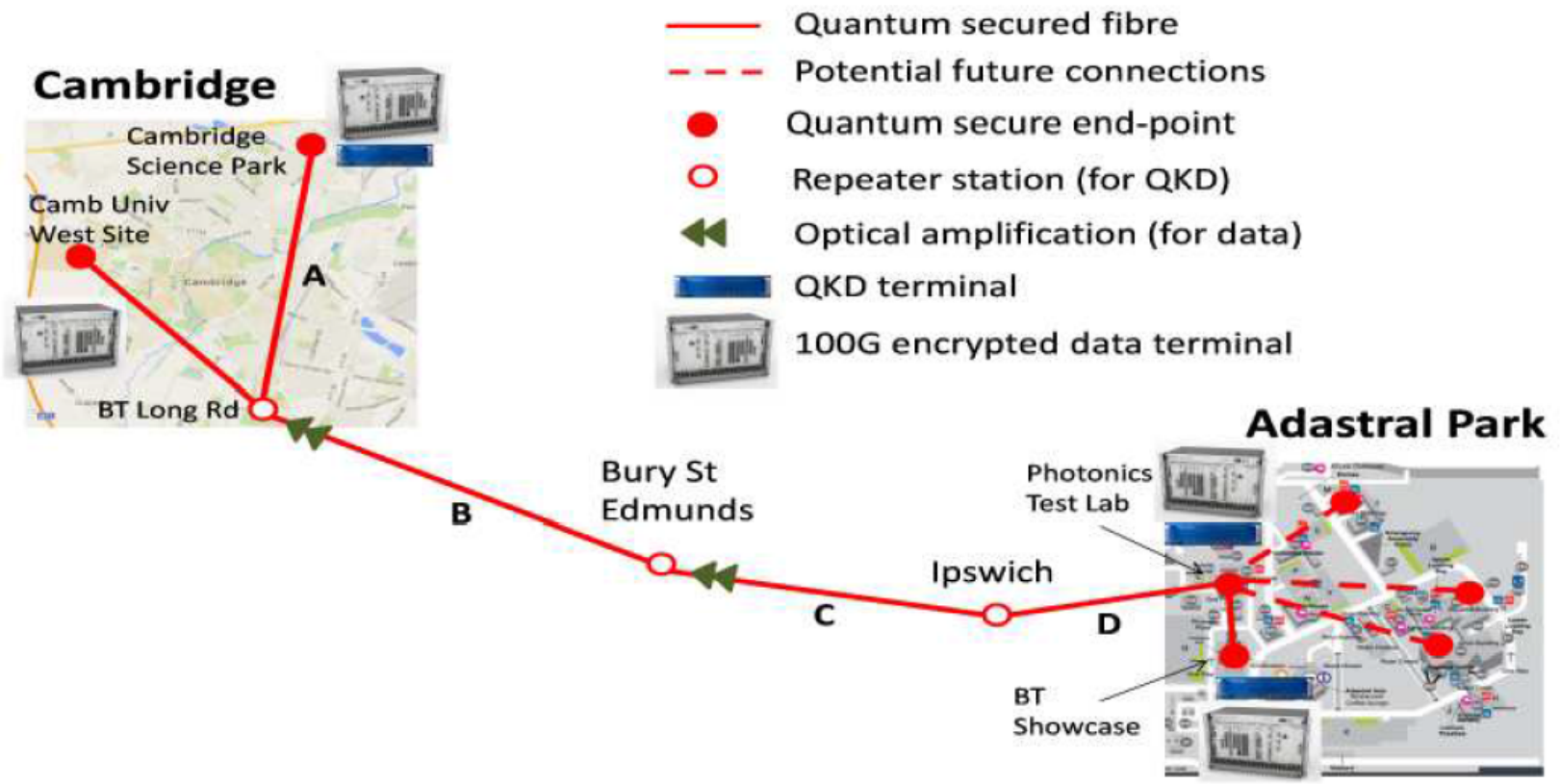


Explanation of the capture and the workflow

172.51.217	137.204.221	HTTP	POST /rest/nfvo/image HTTP/1.1 (application/x-www-form-urlencoded)
137.204.221	137.204.213	HTTP	PUT /controller/nb/v2/flowprogr ...:00:00:05:1e/staticCFlow/backplane...
137.204.213	137.204.213	OpenFlow	Type: Unknown message type
137.204.213	137.204.221	HTTP	HTTP/1.1 201 Created (text/plain)
137.204.221	137.204.213	HTTP	PUT /controller/nb/v2/flowprogr ...:00:00:05:1e/staticCFlow/backplane...
137.204.213	137.204.213	OpenFlow	Type: Unknown message type
137.204.213	137.204.221	HTTP	HTTP/1.1 201 Created (text/plain)
137.204.221	137.204.197	UDP	Source port: 56447 Destination port: 5323
172..3	172..2	TCP	34599→60000 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1915738 TSecr=133
172..3	172..2	TCP	34599→60000 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=2048 TSval=1915738 T
			...
172..3	172..2	TCP	34599→60000 [ACK] Seq=12185 Ack=1 Win=29312 Len=1448 TSval=1915738 TS
172..2	172..3	TCP	60000→34599 [ACK] Seq=1 Ack=2049 Win=33152 Len=0 TSval=133413767 TSec
172..3	172..2	HTTP	POST /nfvgw/rest/images/centos-ovs/ HTTP/1.1 (application/json)
137.204.222	137.204.73	UDP	Source port: 53203 Destination port: 5323
172..2	172..3	HTTP	HTTP/1.1 200 OK

Cambridge Adastral Quantum Link

World First high data rate QKD with commercial kit



BT

Inter-city 500Gb/s + Quantum communication link

We are building a permanent QKD link between Ipswich (Adastral Park) and Cambridge

Goes live in 2 months

Fully encrypted 5 x 100Gb/s optical tx + QKD key distribution using single photons

All sent along the same optical fibre

We have a lab demo of the world's first encrypted 100GE using QKD

Use Cases

Government and other company security requirements E.g. finance, health etc

Data Center interconnect, customer record storage and back-up

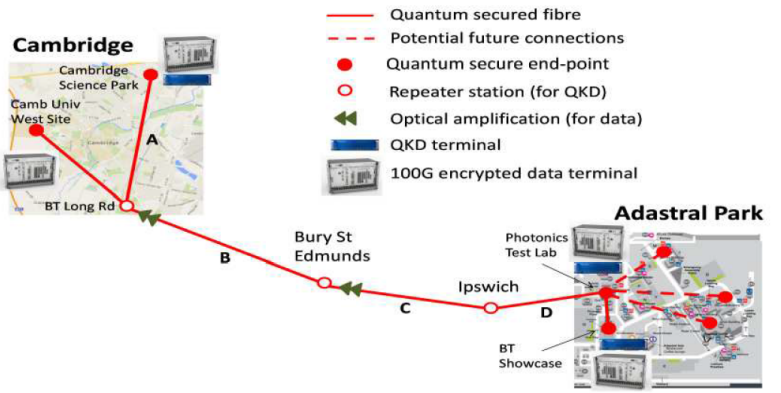
QKD encryption for credit cards

Major Infrastructure control: power grids, telecoms networks…

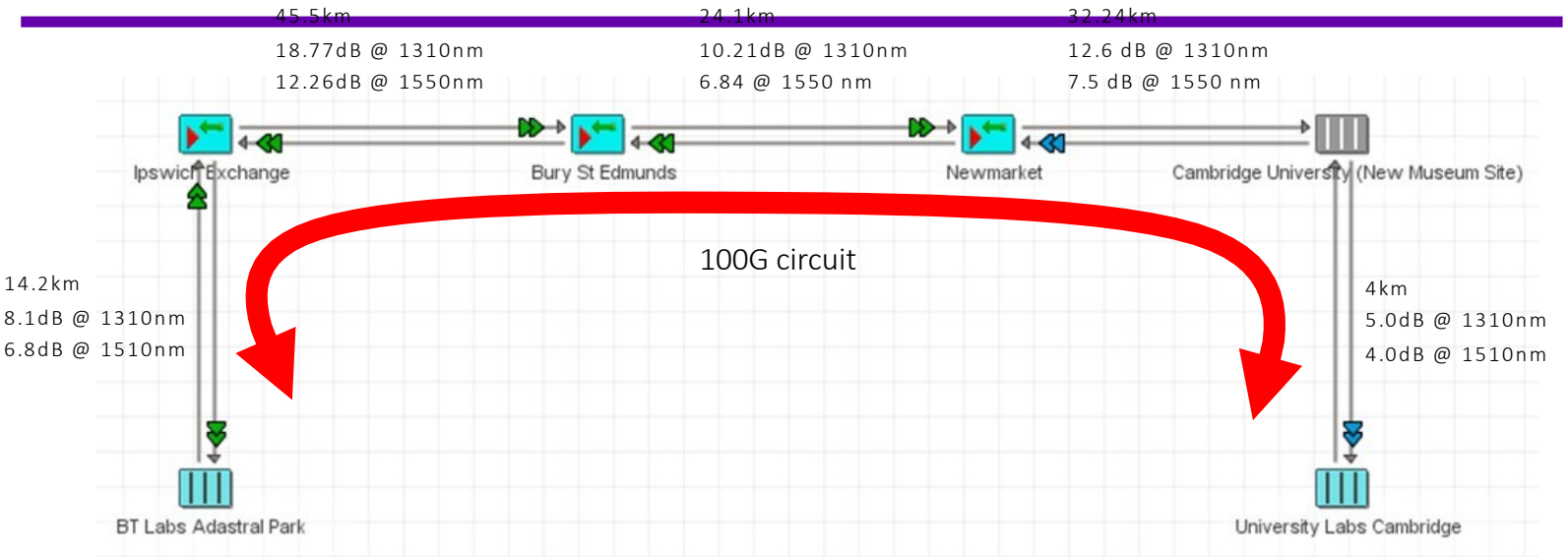
BT trialling other quantum tech:

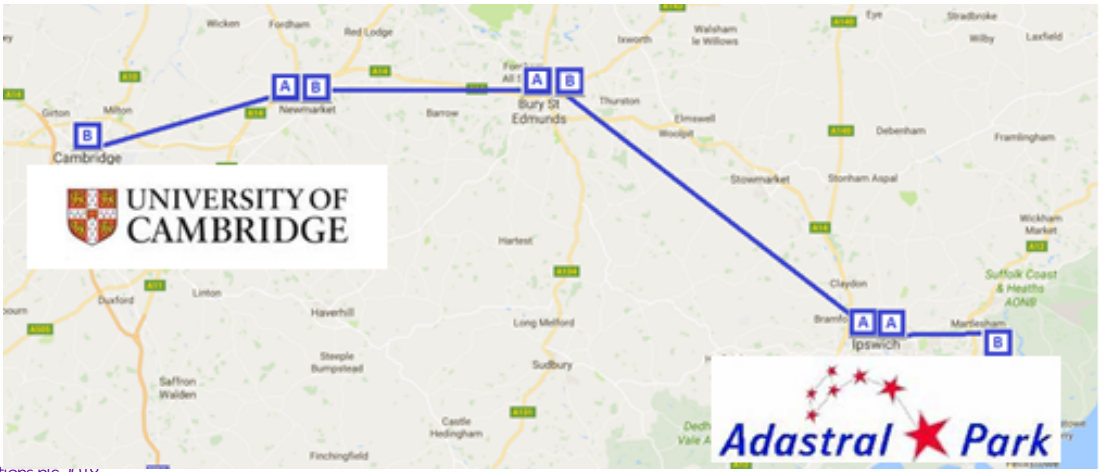
Quantum gravity sensors for underground infrastructure detection

Ultra precise quantum clocks better than GPS



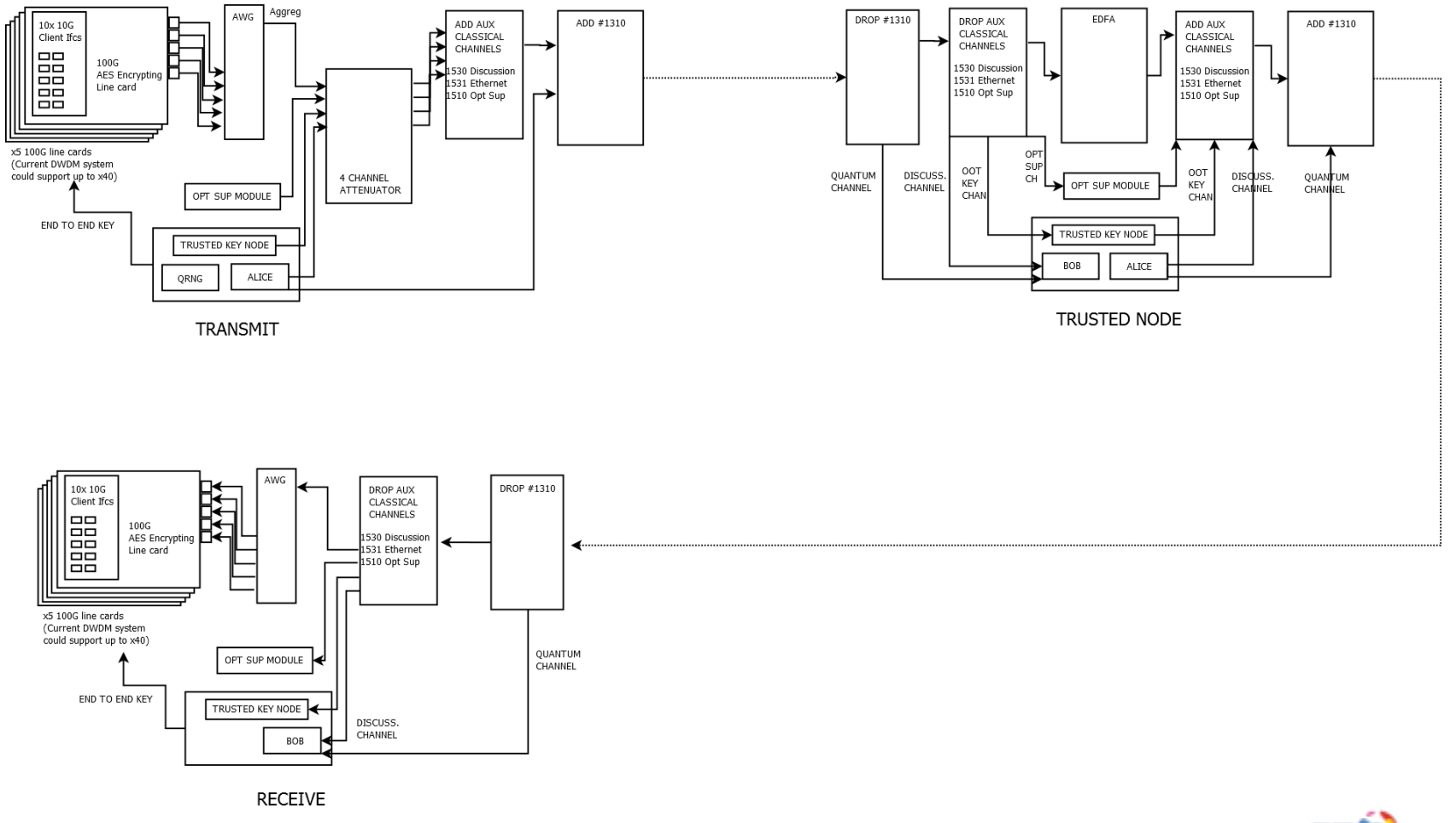
Cambridge – Adastral topology



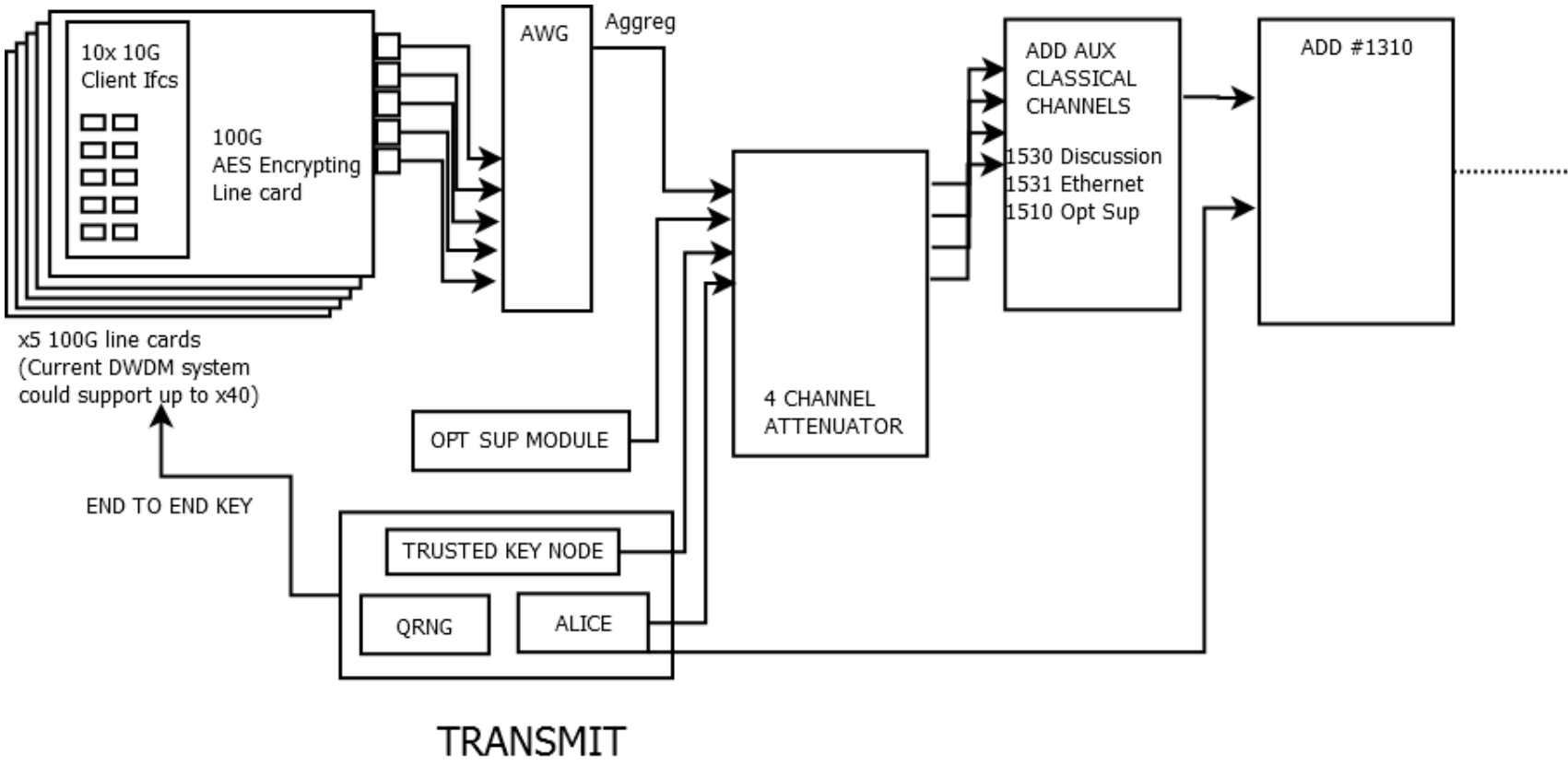


System With One Trusted Node

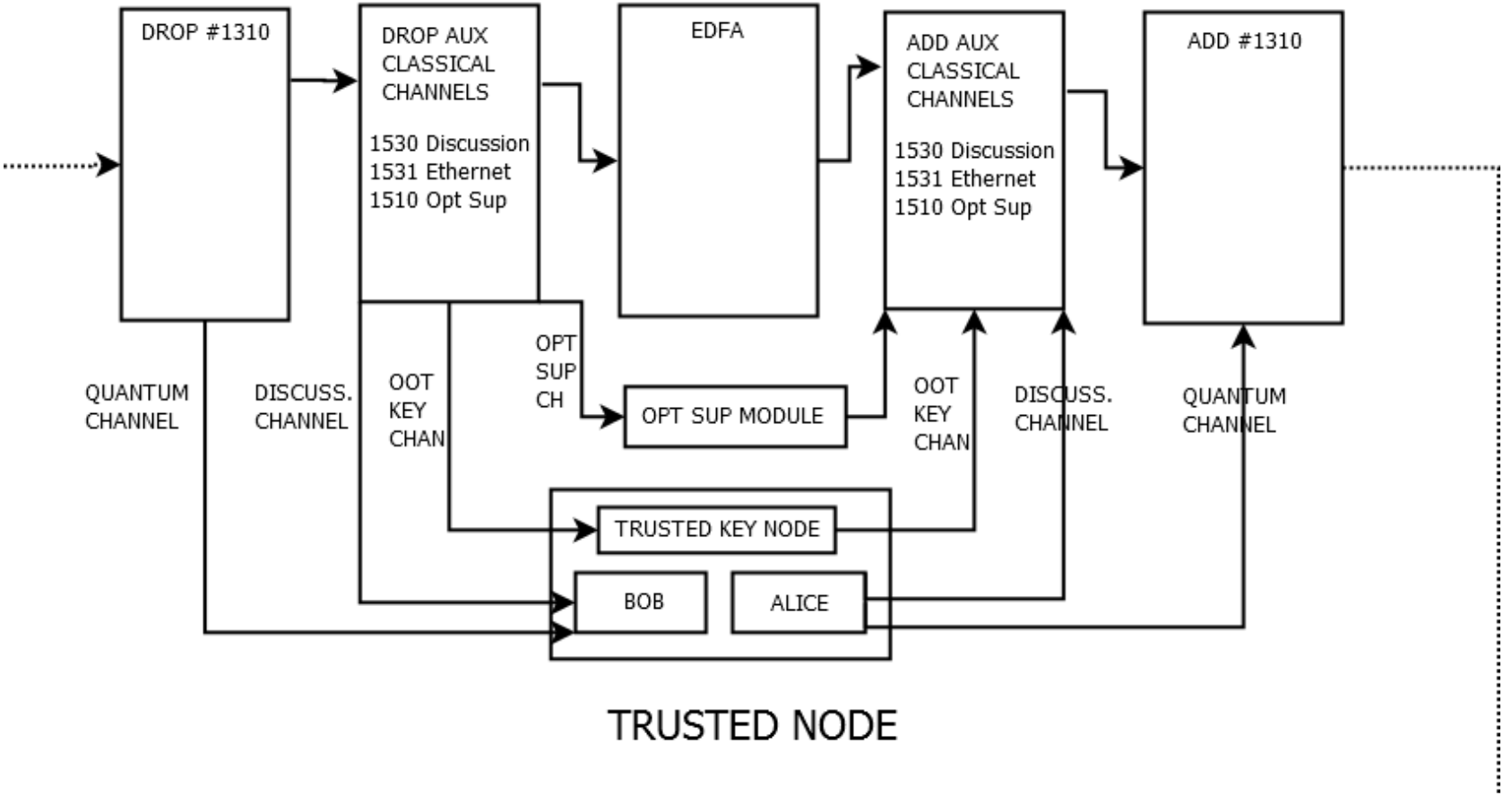
Diagram shows one direction



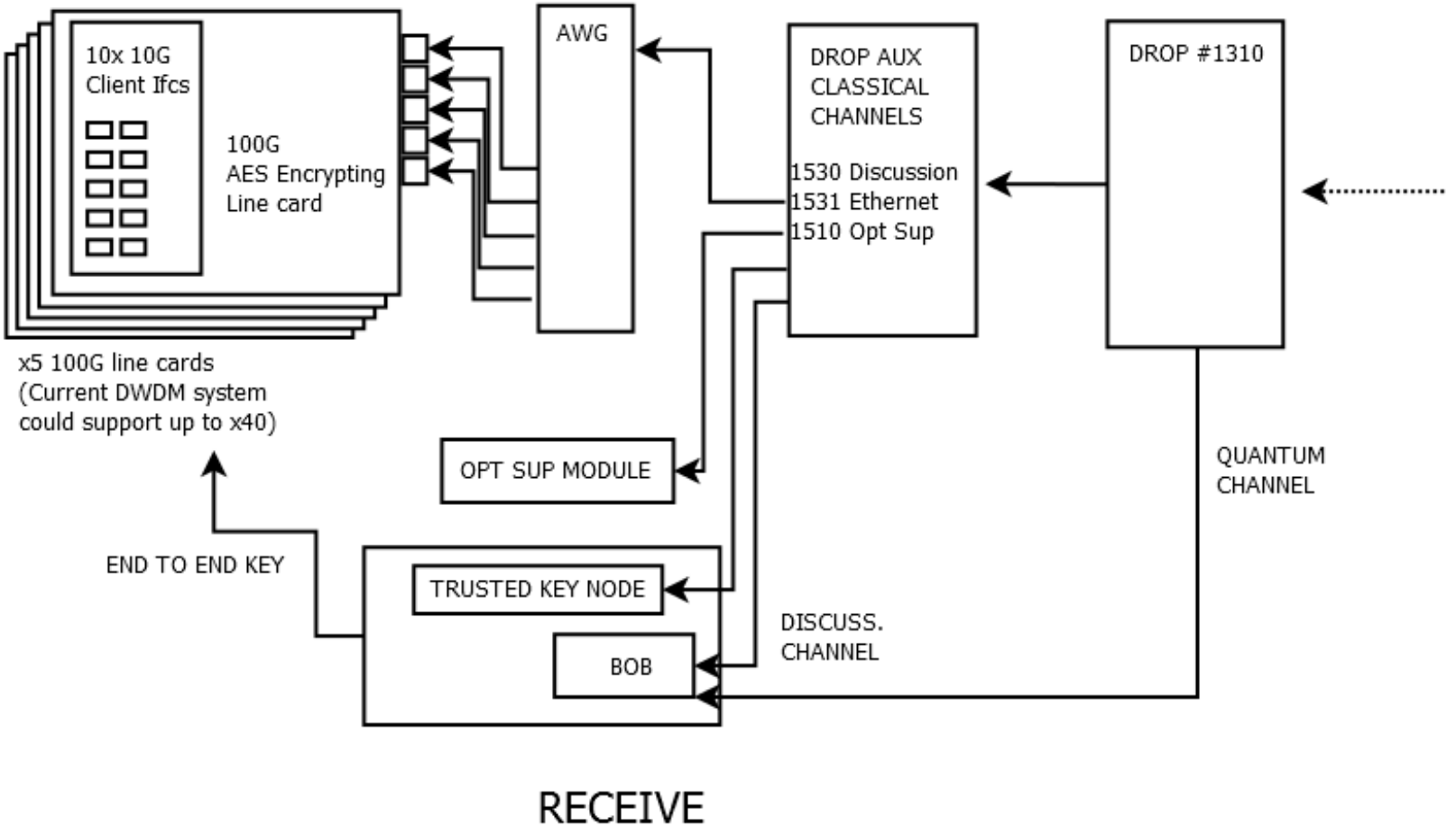
Details



Trusted Node



Receiver



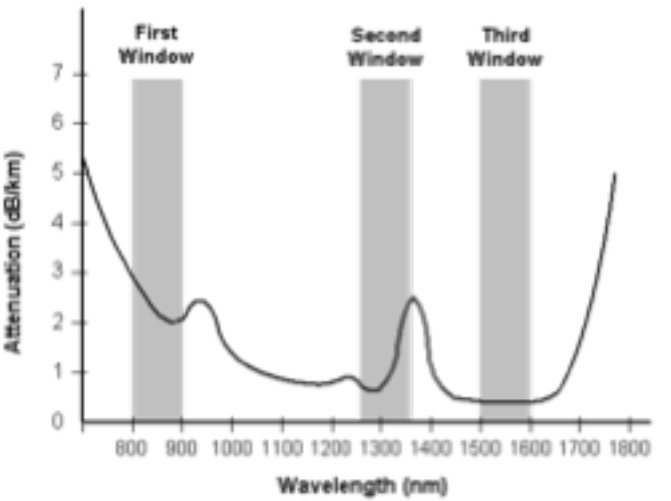
Design considerations – lessons learnt

If QKD has its own fibre – this is MUCH easier and works FAR better! Try to do this!
Should QKD be combined with data?
Customers might want everything associated with their secure data transport to be on the same physical connection

Fibre cost

Entire solution integrated into a single piece of hardware

- Optical transport uses 1.5um window
- If we insert QKD keys at 1.5um, Raman noise severely restricts performance
- QKD at 1.3um has ~50% higher fibre loss which equates to 50% less distance – but significantly reduced Raman noise



BT

Current Status

Permanent QKD link between Adastral Park and Cambridge being built

Dedicated £2M government funding

Expansion to Bristol via London

Toshiba-based QKD demonstration part of Future Agile Bank Showcase

PoCs with major customers scheduled for later this year

Live demo at DSEI 2017 in September at the London Excel (World leading Defence and Security event)

Satellite QKD project with ESA about to start

Government Blackett report written (BT co-authored the quantum comms chapter) with direct recommendations to trial QKD

Close collaboration with UK Quantum Communications Hub

Future roadmap

Now - bespoke QKD security systems here for early adopters

2 years – accreditation / system security testing will result in hardened solutions for secure data transfer

Links > 100km will require trusted node interfaces

5 years – QKD solutions for wide range of use cases

Security for NfV implementations – but cloud native question?

5 years – first commercial QKD satellites distributing global keys

BT involved in early project with European Space Agency

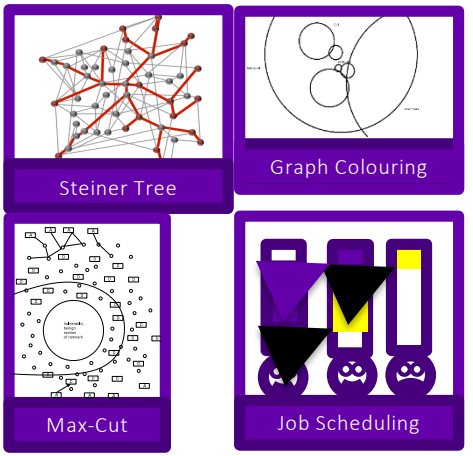
7 years – quantum entanglement allows long distance QKD networks

Potentially linking quantum computer resources

QCAPS Quantum Computation Pilot 2017/18

- Innovate UK project (50% funding) (Academic partners funded by EPSRC.)
- Lead (Dr Roberto Desimone) – experienced BAE Systems CyberIntelligence / AI expert
- Partners: D-Wave, University of Bristol (lead Ashley Montaro), University College London (lead Dr Paul Warburton)

Hard Computational Problems from Telecommunications



DWave Approach (experiment)

- Led by UCL (with DWave support)
- Using 2000Q DWave Processor
- Quantum Annealing
- Initial review of similar previous work by NASA
- Selection of promising problems
- Suitability constraints: Problems must be formulated as a sparse Binary quadratic optimisation. And problems with a flat energy landscape are not suitable. Tall, narrow energy barriers 'tunnelling' processes to be computationally useful.

Universal Quantum Computation (theory)

- Led by Bristol (Maths Department)
- Dr Ashley Montanaro
- Theory and simulation

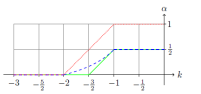


Figure 1: Query complexity of Search with Advice in different models, for power law distributions $p_x \propto x^{-k}$. For each k, the query complexity of the algorithms given in this paper is $\Theta(n^\alpha)$ for some α (ignoring log factors); the graph plots the exponent α against k. Dotted red line: best classical algorithm; solid green line: quantum, known probability distribution; dashed blue line: quantum, unknown probability distribution.

Algorithm 3: Quantum search with unknown probability distribution

Input: Function $f : [n] \to \{0, 1\}$ such that f takes the value 1 on precisely one input x;
oracle operator $O_\mu : |0\rangle \mapsto |\mu\rangle$; inverse O_μ^{-1}; real $k > 1$
Output: The marked element x
for $j = 0$ *to* $\lfloor \log_k \sqrt{n} \rfloor$ **do**
  sample from distribution μ;
  if *marked element found* **then**
    return *marked element*;
  end
  pick i uniformly at random from integers $\{0, \ldots, \lfloor k^j \rfloor - 1\}$;
  perform i iterations of amplitude amplification;
  if *marked element found* **then**
    return *marked element*;
  end
end
perform exact Grover search for one marked element on $[n]$;
return *marked element*;


BT