FORÇA AÉREA BRASILEIRA
Asas que protegem o País

SIGE 2023

SIMPÓSIO DE APLICAÇÕES OPERACIONAIS EM ÁREAS DE DEFESA

Introdução à Criptografia Quântica

Prof. Dr. André Jorge C. Chaves (ITA)

REALIZAÇÃO APOIO PARCEIROS PATROCÍNIO

Sumário

Criptografia Clássica

- Existe há mais de 2000 anos
- **Criptografia “segurança perfeita”:** teorema de Shannon: o texto criptografado não possui nenhuma informação sobre o texto. **Exemplo:** chave totalmente aleatória gerada com k bits é suficiente para a segurança perfeita de uma mensagem de até k bits (Cifra de Vernam)
- Criptografia por chaves simétricas: tanto remetente quanto destinatário possuem as mesmas chaves (privadas)
- Criptografia por chaves assimétricas: destinatário possui uma chave pública (para criptografar a mensagem) e uma chave privada (para descriptografar). A proteção se baseia em complexidade, i.e., por exemplo, no RSA, não há algoritmo conhecido para se fatorar números primos em tempo polinomial

Criptografia Quântica

- Proteção por leis da física
- Primeiro protocolo (distribuição de chave quântica) proposto em 1984 por Charles Bennett e Gilles Brassard (BB84). Se a implementação for perfeita, ele é 100% seguro.
- Protocolos que usam emaranhamento (Ekert 91)
- Protocolos cuja segurança independem do dispositivo
- + protocolos além de distribuição de chave quântica já propostos

Noções de Mecânica Quântica

Conceito 1: Vetor de estado

O vetor de estado, de forma inequívoca, possui todas as informações acessíveis ao sistema. $|\alpha\rangle$

Conceito 2: Observáveis e autoestados

Tudo que pode ser medido na natureza chamamos de observáveis. Os estados possíveis de serem encontrados em uma medição serão chamados de autoestados $|n\rangle$

Conceito 3: Superposição

Chamamos de estado superposto aquele que é uma combinação linear de diferentes autoestados

$$|\alpha\rangle = c_1|1\rangle + c_2|2\rangle$$

Exemplo: polarização de fóton

A componente elétrica do campo eletromagnético de uma onda plana pode possuir diferentes polarizações (linear, circular,elíptica). No caso linear, podemos decompor sempre em dois eixos perpendiculares à direção de propagação, que iremos chamar de x e y.

Um fóton em um estado de onda plana pode ser descrito como:

$$|\text{foton}\rangle = c_x|x\rangle + c_y|y\rangle$$

onde os coeficientes c's são números complexos

Regra de Born e Colapso de Função de Onda

$$|\text{foton}\rangle = c_x|x\rangle + c_y|y\rangle$$

Probabilidade de medir o fóton tendo polarização em x:

$$|c_x|^2$$

Probabilidade de medir o fóton tendo polarização em y:

$$|c_y|^2$$

Após a medição, o estado do fóton se torna o estado medido!

Probabilidade em outros eixos

Na escolha de eixos x',y', um fóton inicialmente polarizado x, pode ser decomposto na base x',y':

$$|x\rangle = \frac{1}{\sqrt{2}}|x'\rangle - \frac{1}{\sqrt{2}}|y'\rangle$$

Caso desejemos fazer uma medição nesses outros eixos, um fóton polarizado em x, terá 50% de chance de ser medido com polarização em x' e 50% em y'.

Protocolo BB84

Protocolo para a transmissão de chaves criptográficas

Definiremos como “base” a escolha do eixo que os fótons estão polarizados (xy ou x’y’). Alice enviará fótons polarizados em uma das duas bases de forma aleatória, e Bob decidirá de forma aleatória em qual base realizar as medições

Protocolo BB84: tabela de probabilidades

Alice	Bob	
x	xy	100% de chance de medir x
	x'y'	50% de chance de medir x' e 50% y'
x'	xy	50% de chance de medir x e 50% y
	x'y'	100% de chance de medir x'

Protocolo BB84

Alice gera duas listas de bits aleatórios:

Lista de “base”-> decide se Alice irá enviar os bits na base xy (0) ou x’y’ (1)

Lista de bits da chave -> A chave propriamente dita, 0 para x ou x’, e 1 para y ou y’.

Exemplo:

Base	Chave	Pol. do Fóton
0	0	x
0	1	y
1	0	x’
1	1	y’

Protocolo BB84

Bob também gera uma lista aleatória, que usará para fazer as medições:

0-> faz a medição em xy

1-> faz a medição em x’y’

Se Alice e Bob escolheram a mesma base, Bob irá medir o mesmo bit que Alice enviou

Caso contrário, Bob tem apenas 50% de chance de medir o bit correto.

Protocolo BB84

Após enviar N bits, Alice revela a sua lista de bits de base.

Bob usa a lista de bits de base para saber quais os bits que ele mediu na mesma base (estatisticamente, 50%) e descarta os outros bits

Com os bits restantes, Alice revela k bits. Considerando um canal perfeito, se algum bit não coincidir, o canal está comprometido e Alice e Bob precisam recomeçar a estratégia

Caso todos os k bits sejam iguais

Teorema da não-clonagem

É impossível criar uma cópia idêntica de um estado quântico desconhecido.

E se o canal for ruidoso?

A presença de alguém escutando a comunicação entre Alice e Bob pode ser detectada por mudanças na estatística de bits recebidos corretamente

Outros protocolos de QKD

- Protocolo de EPR/Ekert (inclui emaranhamento)
- Bases maiores que 2 (qudits ao invés de qubits)
- Variações de BB84(exemplo: geração de bits de base do BB84 não for 50% / 50%)
- Device Independent QKD (DIQKD)

Emaranhamento

Se temos dois estados quânticos (e.g., dois fótons), um exemplo de estado emaranhado pode ser escrito como:

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|x_1, x_2\rangle + |y_1, y_2\rangle \right)$$

se o observador 1 medir polarização em x, ele tem absoluta certeza que o observador 2 também vai medir polarização em x

Desigualdades de Bell

O emaranhamento gerou uma série de questionamentos, o mais famoso feitos por Einstein, Podolsky e Rosen (aparente inconsistência entre Mecânica Quântica e relatividade).

J. Bell mostrou que, caso seja suposto que exista alguma “variável oculta”, correspondente à uma noção de localidade (i.e., sem “ação a distância”), implica em uma série de desigualdades estatísticas. Experimentos rotineiramente obtêm resultados que violam a desigualdade de Bell

Protocolo EPR/Ekert 91

Utilizando as desigualdades de Bell, Ekert propôs outro protocolo de QKD:

Um par de fótons emaranhados é gerado e enviado simultaneamente para Alice e Bob. A partir daí é similar à BB84:

- Alice e Bob sorteiam cada uma base (porém, agora são 3 distintas) e fazem medições desses fótons
- Trocam as informações de base
- Comparando as informações das medições em bases incompatíveis (que no BB84 eram descartadas), eles conseguem descobrir se alguém está interferindo na medição utilizando as desigualdades de Bell

TABLE I. List of quantum hacking strategies.

Attack	Source or detection	Target component	Manner	Year
Photon number splitting (Brassard *et al.*, 2000; Lütkenhaus, 2000)	Source	WCP (multiphotons)	Theory	2000
Detector fluorescence (Kurtsiefer *et al.*, 2001)	Detection	Detector	Theory	2001
Faked state (Makarov and Hjelme, 2005; Makarov, Anisimov, and Skaar, 2006)	Detection	Detector	Theory	2005
Trojan horse (Vakhitov, Makarov, and Hjelme, 2001; Gisin *et al.*, 2006)	Source and detection	Backreflection light	Theory	2006
Time shift (Qi, Fung *et al.*, 2007; Zhao *et al.*, 2008)	Detection	Detector	Experiment[a]	2007
Time side channel (Lamas-Linares and Kurtsiefer, 2007)	Detection	Timing information	Experiment	2007
Phase remapping (Fung *et al.*, 2007; Xu, Qi, and Lo, 2010)	Source	Phase modulator	Experiment[a]	2010
Detector blinding (Makarov, 2009; Lydersen *et al.*, 2010)	Detection	Detector	Experiment[a]	2010
Detector blinding (Gerhardt *et al.*, 2011a; Gerhardt *et al.*, 2011b)	Detection	Detector	Experiment	2011
Detector control (Lydersen, Akhlaghi *et al.*, 2011; Wiechers *et al.*, 2011)	Detection	Detector	Experiment	2011
Faraday mirror (Sun, Jiang, and Liang, 2011)	Source	Faraday mirror	Theory	2011
Wavelength (Li *et al.*, 2011; Huang *et al.*, 2013)	Detection	Beam splitter	Experiment	2011
Dead time (Henning *et al.*, 2011)	Detection	Detector	Experiment	2011
Channel calibration (Jain *et al.*, 2011)	Detection	Detector	Experiment[a]	2011
Intensity (Jiang *et al.*, 2012; Sajeed, Radchenko *et al.*, 2015)	Source	Intensity modulator	Experiment	2012
Phase information (Sun *et al.*, 2012, 2015; Tang *et al.*, 2013)	Source	Phase randomization	Experiment	2012

Memory attacks (Barrett, Colbeck, and Kent, 2013)	Detection	Classical memory	Theory	201
Local oscillator (Jouguet, Kunz-Jacques, and Diamanti, 2013; Ma *et al.*, 2013a)[b]	Detection	Local oscillator	Experiment	201
Trojan horse (Jain *et al.*, 2014, 2015)	Source and detection	Backreflection light	Experiment	201
Laser damage (Bugge *et al.*, 2014; Makarov *et al.*, 2016)	Detection	Detector	Experiment	201
Laser seeding (Sun *et al.*, 2015)	Source	Laser phase or intensity	Experiment	201
Spatial mismatch (Sajeed, Chaiwongkhot *et al.*, 2015; Chaiwongkhot *et al.*, 2019)	Detection	Detector	Experiment	201
Detector saturation (Qin, Kumar, and Alléaume, 2016)[b]	Detection	Homodyne detector	Experiment	201
Covert channels (Curty and Lo, 2019)	Detection	Classical memory	Theory	201
Pattern effect (Yoshino *et al.*, 2018)	Source	Intensity modulator	Experiment	201
Detector control (Qian *et al.*, 2018)	Detection	Detector	Experiment	201
Laser seeding (Sun *et al.*, 2015; Huang *et al.*, 2019; Pang *et al.*, 2019)	Source	Laser	Experiment	201
Polarization shift (Wei, Zhang *et al.*, 2019)	Detection	SNSPD	Experiment	201

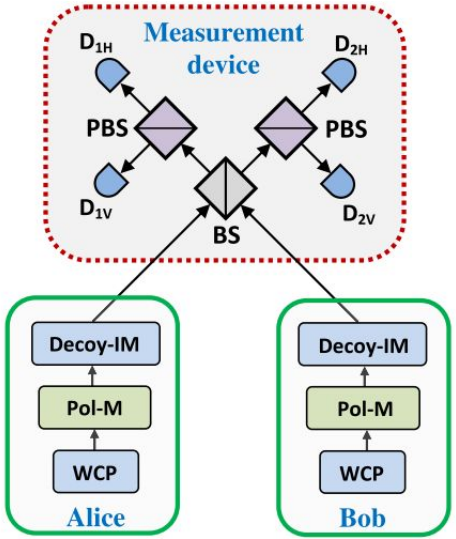
RMP 92 (2020)

Device Independent QKD (DI QKD)

- Não confiamos no dispositivo de QKD
- O dispositivo de QKD pode até ter sido construído por um agente malicioso
- É possível obter protocolos que garantem a troca segura de informação mesmo nessa condição? Sim!
- Requisito: dispositivo não se comunica com o meio externo
- Problemas: baixa taxa de transmissão de chaves, curtas distâncias e depende de alta eficiência de detecção

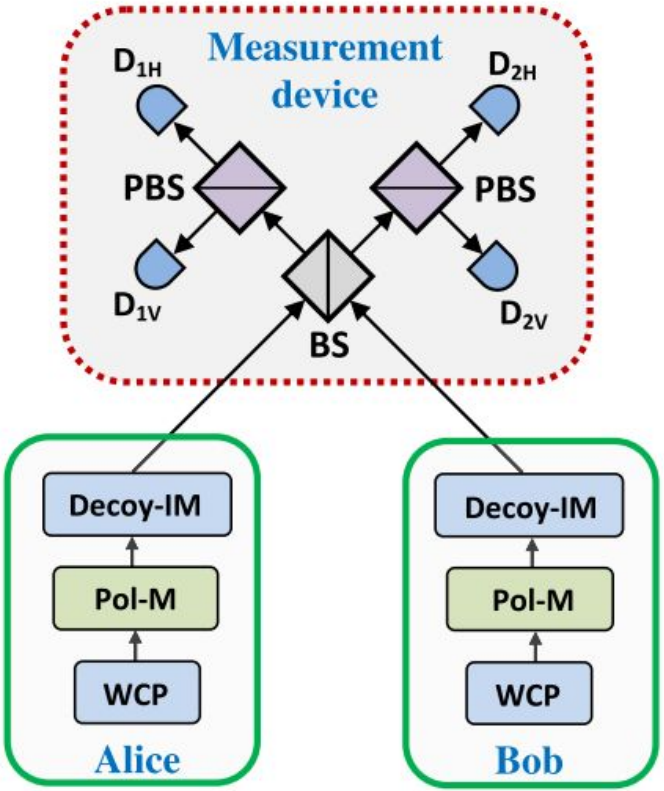
Measurement Device Independent QKD (MDI QKD)

- Objetivo: Impedir a maioria dos “ataques de canal lateral” no detector
- Uso de estado “isca”
- Estados são misturados e medidos por um terceiro



PRL 108 (2012)

MDI-QKD



PRL 108 (2012)

Teletransporte quântico

- Um par de fótons emaranhados é gerado e Alice e Bob cada um guarda esse par.
- Alice que enviar a informação de um fóton para Bob. Primeiro Alice emaranha esse fóton com o fóton que já possui.Alice faz uma medição do estado emaranhado que tem em posse, e envia essa informação para Bob. Com essa informação, dependendo da informação obtida por Alice, Bob sabe o que fazer para
- Usado para transmitir informação quântica

Teletransporte quântico

Motivação: transmitir informação quântica

Uso de estados emaranhados

Alice e Bob recebem um par de fótons emaranhados:

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|x_A, x_B\rangle + |y_A, y_B\rangle \right)$$

Alice tem um estado descrito por $c_x|x\rangle + c_y|y\rangle$

e quer enviar para Bob

Teletransporte quântico

O estado total do sistema pode ser escrito como:

$$(c_x|x\rangle + c_y|y\rangle) \otimes |\frac{1}{\sqrt{2}}(|x_A, x_B\rangle + |y_A, y_B\rangle) =$$

$$\frac{1}{\sqrt{2}}(c_x|x, x_A, x_B\rangle + c_x|x, y_A, y_B\rangle + c_y|y, x_A, x_B\rangle + c_y|y, y_A, y_B\rangle)$$

Bases de Bell

$$|\psi_+\rangle = \frac{1}{\sqrt{2}}|x_1, x_2\rangle + \frac{1}{\sqrt{2}}|y_1, y_2\rangle,$$

$$|\phi_+\rangle = \frac{1}{\sqrt{2}}|x_1, y_2\rangle + \frac{1}{\sqrt{2}}|y_1, x_2\rangle,$$

$$|\psi_-\rangle = \frac{1}{\sqrt{2}}|x_1, x_2\rangle - \frac{1}{\sqrt{2}}|y_1, y_2\rangle,$$

$$|\phi_-\rangle = \frac{1}{\sqrt{2}}|x_1, y_2\rangle - \frac{1}{\sqrt{2}}|y_1, x_2\rangle,$$

$$|x_1, x_2\rangle = \frac{1}{\sqrt{2}} \left(|\psi_+\rangle + |\psi_-\rangle \right),$$

$$|y_1, y_2\rangle = \frac{1}{\sqrt{2}} \left(|\psi_+\rangle - |\psi_-\rangle \right),$$

$$|x_1, y_2\rangle = \frac{1}{\sqrt{2}} \left(|\phi_+\rangle + |\phi_-\rangle \right),$$

$$|y_1, x_2\rangle = \frac{1}{\sqrt{2}} \left(|\phi_+\rangle - |\phi_-\rangle \right),$$

Teletransporte quântico

$$\frac{1}{\sqrt{2}}\left(c_x|x, x_A, x_B\rangle + c_x|x, y_A, y_B\rangle + c_y|y, x_A, x_B\rangle + c_y|y, y_A, y_B\rangle\right)$$

usaremos que:

$$|x, x_A, x_B\rangle = \frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}\left(|x, x_A\rangle + |y, y_A\rangle\right) + \frac{1}{\sqrt{2}}\left(|x, x_A\rangle - |y, y_A\rangle\right)\right] \otimes |x_B\rangle$$

Teletransporte quântico

$$(c_x|x\rangle + c_y|y\rangle) \otimes |\frac{1}{2}\left(|x_A, x_B\rangle + |y_A, y_B\rangle\right) = \frac{1}{2}c_x\left(|\psi_+\rangle + |\psi_-\rangle\right) \otimes |x_B\rangle +$$
$$+\frac{1}{2}c_x\left(|\phi_+\rangle + |\phi_-\rangle\right) \otimes |y_B\rangle +$$
$$+\frac{1}{2}c_y\left(|\phi_+\rangle - |\phi_-\rangle\right) \otimes |x_B\rangle +$$
$$+\frac{1}{2}c_y\left(|\psi_+\rangle - |\psi_-\rangle\right) \otimes |y_B\rangle$$

Teletransporte quântico

O estado total pode ser reescrito como:

$$(c_x|x\rangle + c_y|y\rangle) \otimes |\frac{1}{2}\left(|x_A, x_B\rangle + |y_A, y_B\rangle\right) = \frac{1}{2}|\psi_+\rangle \otimes (c_x|x_B\rangle + c_y|y_B\rangle) +$$
$$+\frac{1}{2}|\psi_-\rangle \otimes (c_x|x_B\rangle - c_y|y_B\rangle) +$$
$$+\frac{1}{2}|\phi_+\rangle \otimes (c_x|y_B\rangle + c_y|x_B\rangle) +$$
$$+\frac{1}{2}|\phi_+\rangle \otimes (c_x|y_B\rangle - c_y|x_B\rangle)$$

Se Alice fizer uma medição na base de estados de Bell, tem 25% de chance de medir cada uma delas. O vetor de estado irá colapsar para uma das 4 bases.

Ela avisa Bob em um canal clássico o resultado de sua medição. Se for $|\psi_+\rangle$ ob já possui a informação quântica:

$$c_x|x_B\rangle + c_y|y_B\rangle$$

caso contrário, ele saberá qual transformação precisa fazer em seu fóton para obter a informação quântica

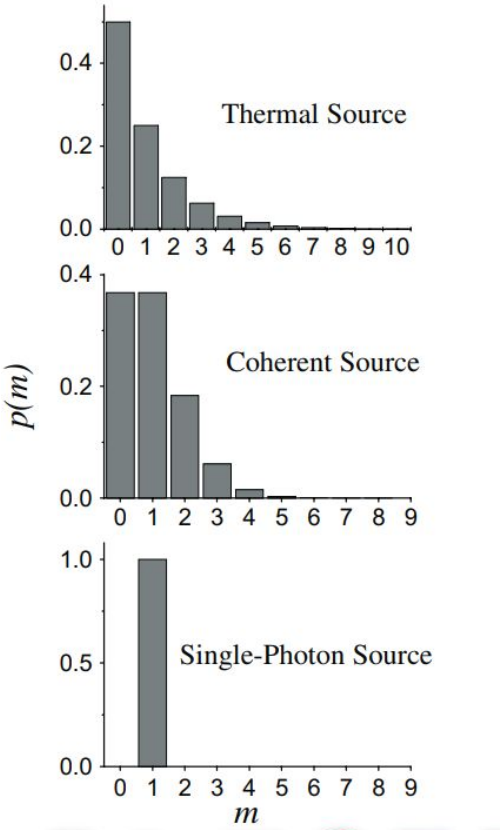
Hardware

Fontes de fótons únicos

- Átomos
- Moléculas orgânicas
- Centros de Cor
- Pontos Quânticos Semicondutores
- Materiais 2D

Formas de excitar fótons únicos

- Bombeamento incoerente
- Preparação coerente



Rep. Prog. Phys. 68 1129 (2005)

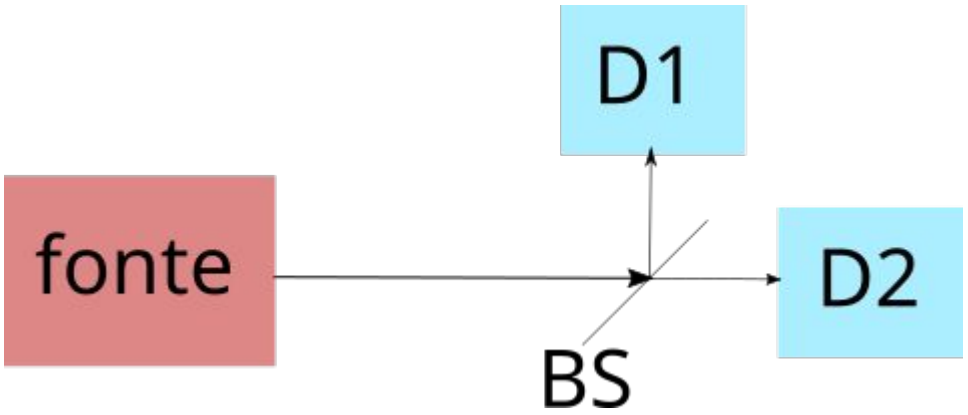
Table 2. Comparison of characteristic features of different single quantum emitters as potential sources of single photons. T = temperature; Col. cent. RT = colour centre room temperature; Q-dot = quantum dot; nanocryst. = nanocrystal; Max. rate of emiss. = maximum rate of emission; Multi-excit. = multi-excitation; reproduc. = reproducible; Operat. temper. = operation temperature; liq. = liquid.

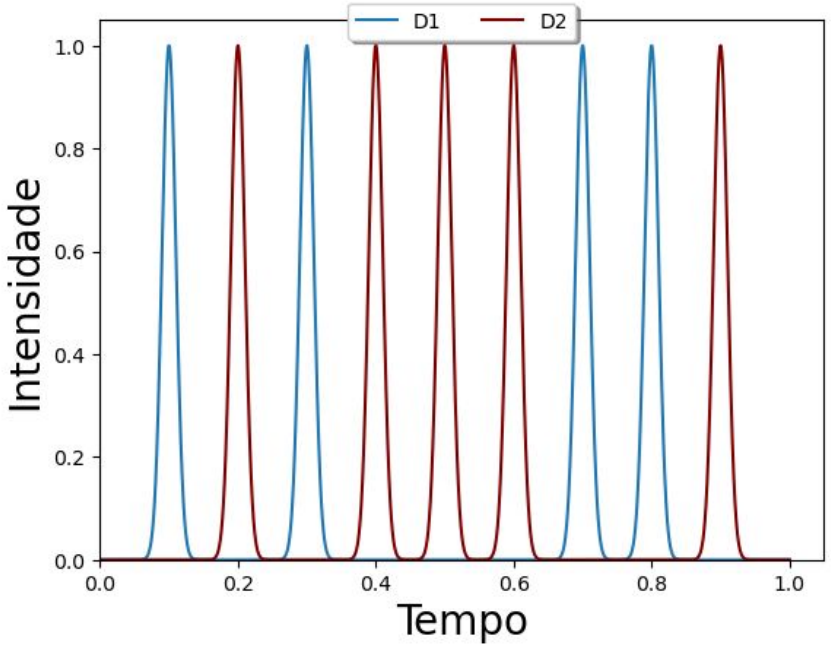
	Cold atom	Ion in trap	Molecule low T	Molecule RT	Col. cent. RT	III–V Q-dot	II–VI nanocryst.
Emission spectrum	Sharp line	Sharp line	ZPL + broad lines	Broad band	Broad line, band	Sharp line	Broad line
Typical linewidth	10 MHz	10 MHz	30 MHz, 30 GHz	10 THz	1–30 THz	1 GHz	30 GHz
Emission lifetime	15 ns	15 ns	4 ns	4 ns	10 ns	300 ps	30 ns
Fourier-limited	Yes	Yes	Yes, no	No	No	Yes	No
Max. rate of emiss.	100 kHz	100 kHz	100 MHz	100 MHz	10 MHz	1 GHz	10 MHz
Dark states	No	No	Yes	Yes	Yes	No	Yes
Multi-excit.	No	No	No	No	No	Yes	No
Long-term stability	No, but reproduc.	Yes	Yes	No, in general	Yes	Yes	No, blink
Operat. temper.	μK	mK	1–10 K	300 K	300 K	1–30 K	300 K
Requirements	UHV, lasers	UHV, trap	Liq. He	Easy	Easy	MBE, liq. He	Easy

Laser “fraco” ou atenuado

- Em um estado coerente, fótons seguem uma distribuição de Poisson
- Com intensidades suficientemente pequenas, poucos fótons são emitidos por um laser.

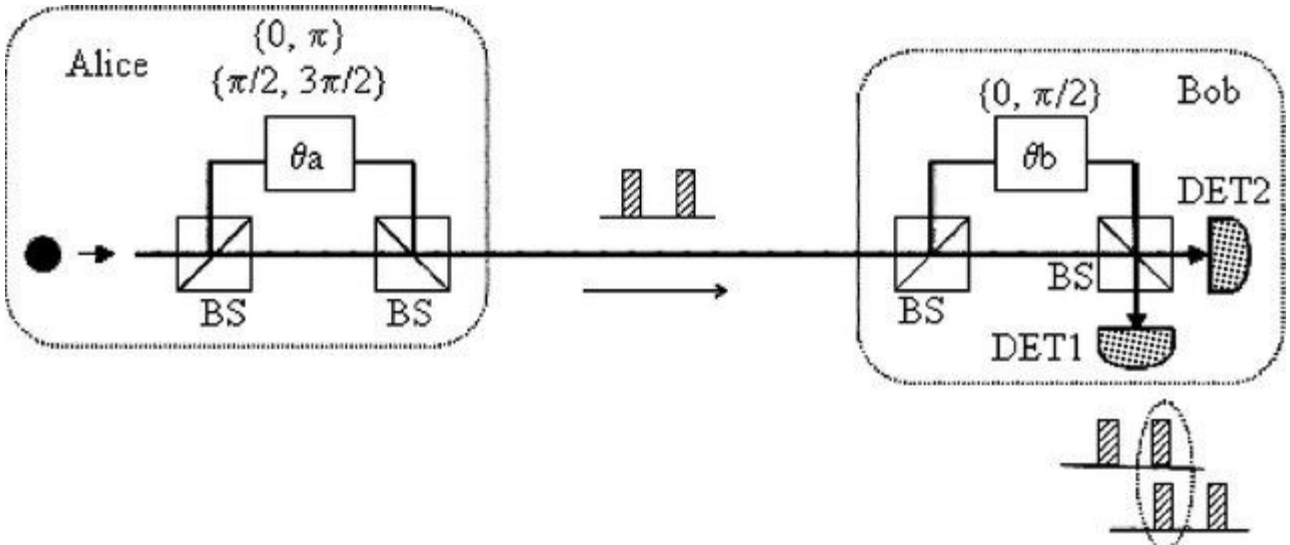
Caracterizando fontes de fótons únicos: *“antibunching”*

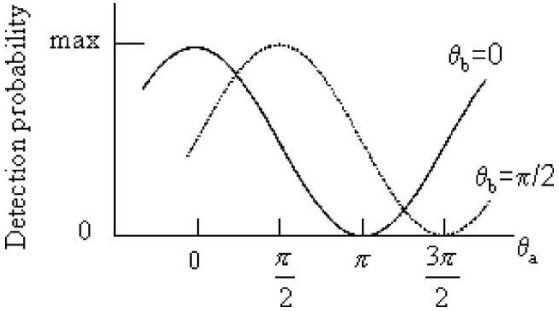




Codificando a informação

- Por controle de polarização (usando células de Pockel ou rotacionando polaróides)
- Por fase usando interferômetro de Mach-Zehnder





Construindo emaranhamento

- Conversão paramétrica descendente
- Geração de fótons emaranhados
- Beam-Splitter

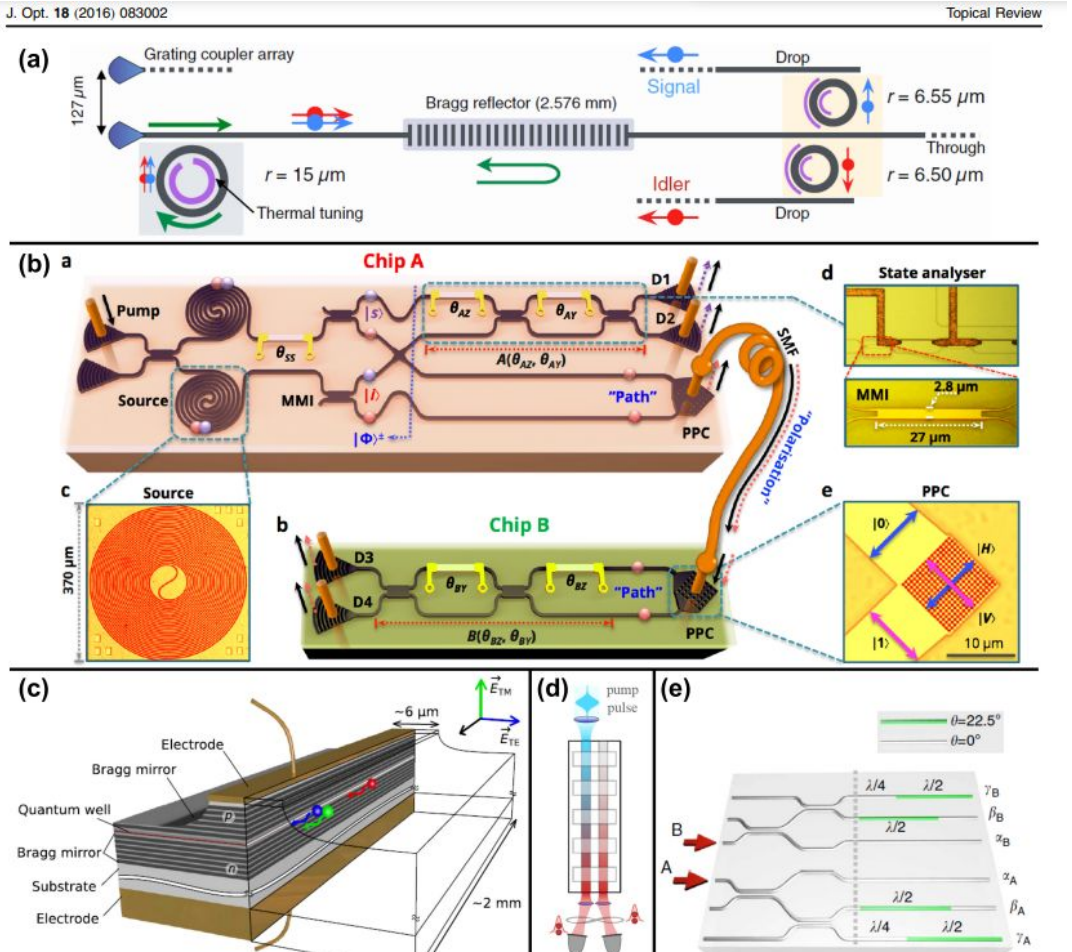
QKD: Detectores de fótons únicos

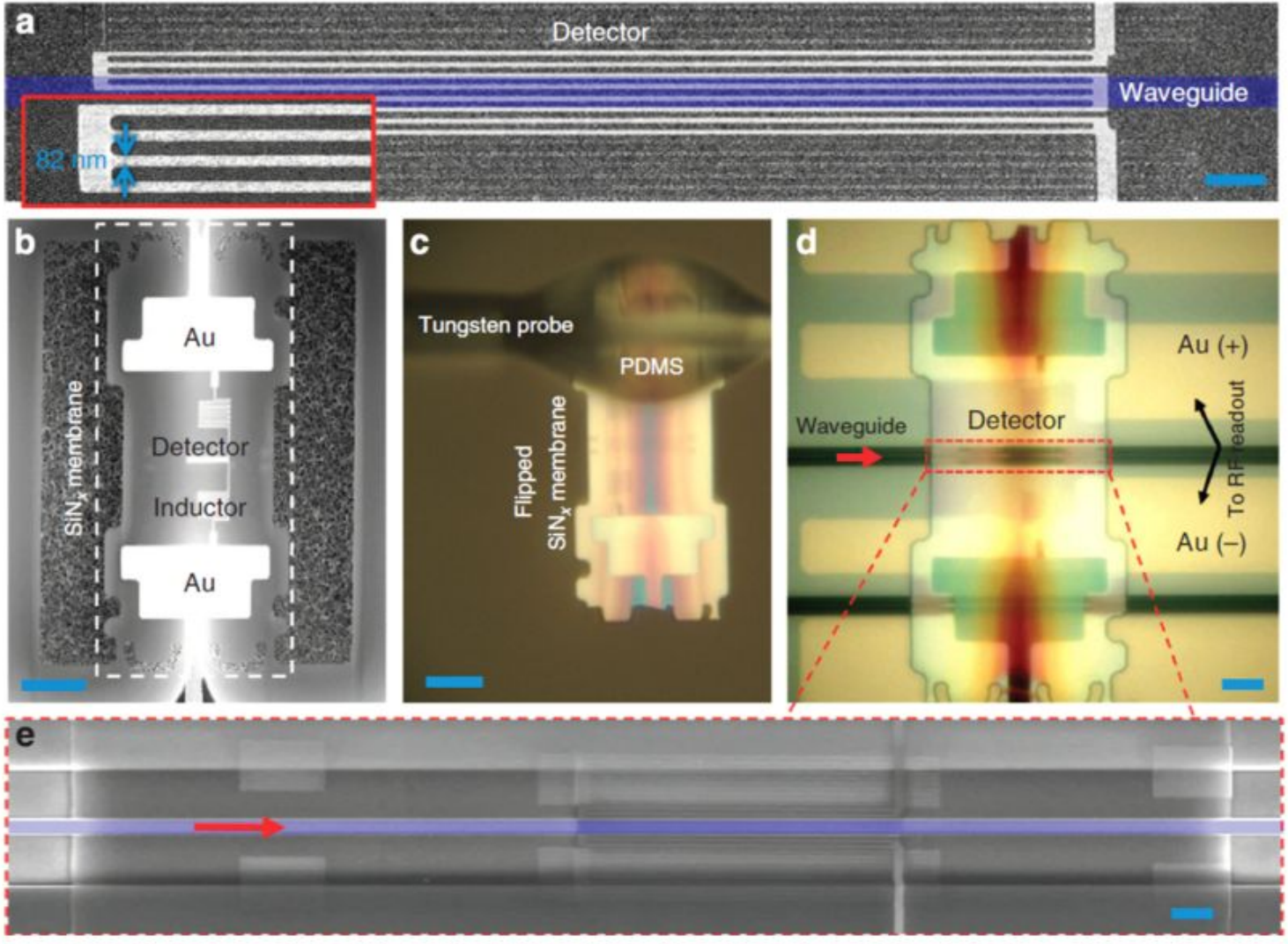
- Desejável que seja capaz de identificar o número de fótons
- Primeiro detector (tubo fotomultiplicador) de 1949
- Características de funcionamento
  - Temperatura de funcionamento
  - Eficiência de detecção
  - Tempo de instabilidade (*jitter time*): tempo entre absorver um fóton e gerar o sinal elétrico
  - Taxa de contagem escura

Table 1 | Comparison of single-photon detectors.

Detector type	Operation temperature (K)	Detection efficiency, η	Jitter time, Δt (FWHM)	Dark count rate, D (ungated)	Figure of merit	Max. count rate	Resolves photon number?
PMT (visible–near-infrared)[31]	300	40% @500 nm	300 ps	100 Hz	1.33×10^7	10 MHz	Yes
PMT (infrared)[32]	200	2% @1,550 nm	300 ps	200 kHz	3.33×10^2	10 MHz	Yes
Si SPAD (thick junction)[38]	250	65% @650 nm	400 ps	25 Hz	6.5×10^7	10 MHz	No
Si SPAD (shallow junction)[41]	250	49% @550 nm	35 ps	25 Hz	5.6×10^8	10 MHz	No
InGaAs SPAD (gated)[55]	200	10% @1,550 nm	370 ps	91 Hz	2.97×10^5	10 kHz	No
InGaAs SPAD (self-differencing)[57]	240	10% @1,550 nm	55 ps	16 kHz	1.14×10^5	100 MHz	Yes
Frequency up-conversion[65]	300	9% @1,550 nm	400 ps	13 kHz	1.7×10^4	10 MHz	No
Frequency up-conversion[65]	300	2% @1,550 nm	40 ps	20 kHz	2.5×10^4	10 MHz	No
VLPC[69]	6	88% @694 nm	—	20 kHz	—	—	Yes
VLPC*	6	34% @633 nm	270 ps	7 kHz	1.83×10^5	—	Yes
TES[76]	0.1	50% @1,550 nm	100 ns	3 Hz	1.67×10^6	100 kHz	Yes
TES[20]	0.1	95% @1,550 nm	100 ns	—	—	100 kHz	Yes
SNSPD (meander)[90]	3	0.7% @1,550 nm	60 ps	10 Hz	1.16×10^7	100 MHz	No
SNSPD (new)[87]	1.5	57% @1,550 nm	30 ps	—	—	1 GHz	No
QD (resonant tunnel diode)[96]	4	12% @550 nm	150 ns	2×10^{-3} Hz	4×10^9	250 kHz	No
QD (field-effect transistor)[93]	4	68% @805 nm	—	—	—	1 Hz	Yes

Fotônica quântica integrada




a
Detector
Waveguide
82 nm
b
Au
SiNx membrane
Detector
Inductor
Au
c
Tungsten probe
PDMS
Flipped
SiNx membrane
d
Au (+)
Waveguide
Detector
To RF readout
Au (–)
e

Redes de distribuição de Chave Quântica atuais

DARPA (2002-2007)

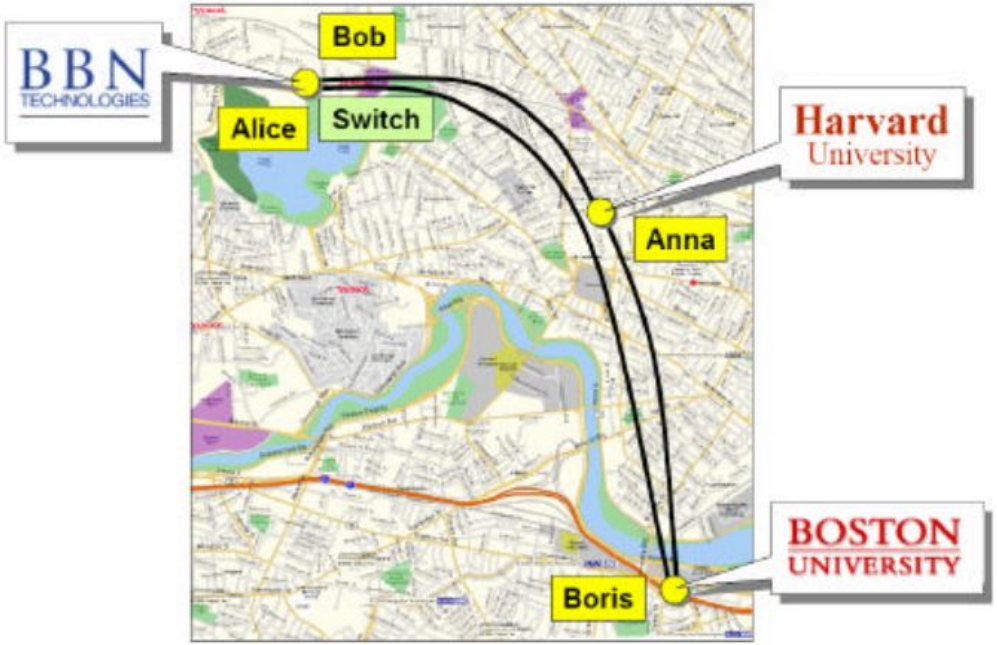


Figure 1. The Metro-Fiber Portions of the DARPA Quantum Network.

Elliott, Chip. "The DARPA quantum network." *Quantum Communications and cryptography*. CRC Press, 2018. 91-110.

Geneva (2007-)

10 years ago the State of Geneva in Switzerland installed quantum cryptography to protect its elections. It was the first ever deployment of a commercial quantum cryptography system. A decade later Geneva is still using the system to protect the integrity of its elections.

SwissQuantum

Figure 1. Map of the SwissQuantum network. Two nodes are in the Geneva city centre and the third one is on the site of CERN in France (the border is in red). The white lines are drawn for illustration: they do not represent the fibres.

Espanha


Telefónica PoP
Norte
3.9 Km
6 dB
5.0 Km
6.0dB+7.0dB
6.4 Km
7.0+4.0 dB
Telefónica PoP
Concepción
Telefónica Global
Innovation Lab.
CDAD. LINEAL
SAN PASCUAL
QUINTANA
SALAMANCA
Google Maps

Inglaterra - Londres

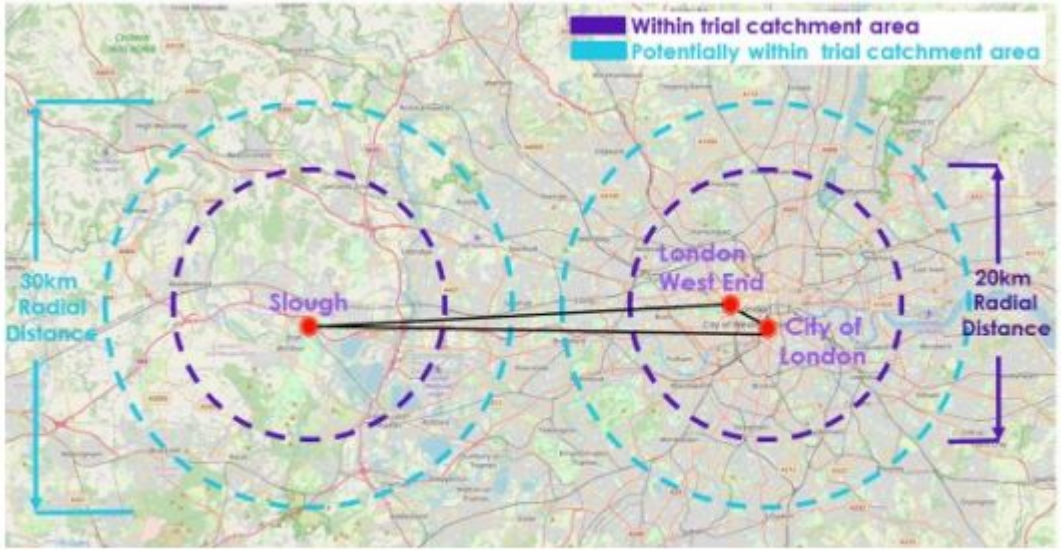
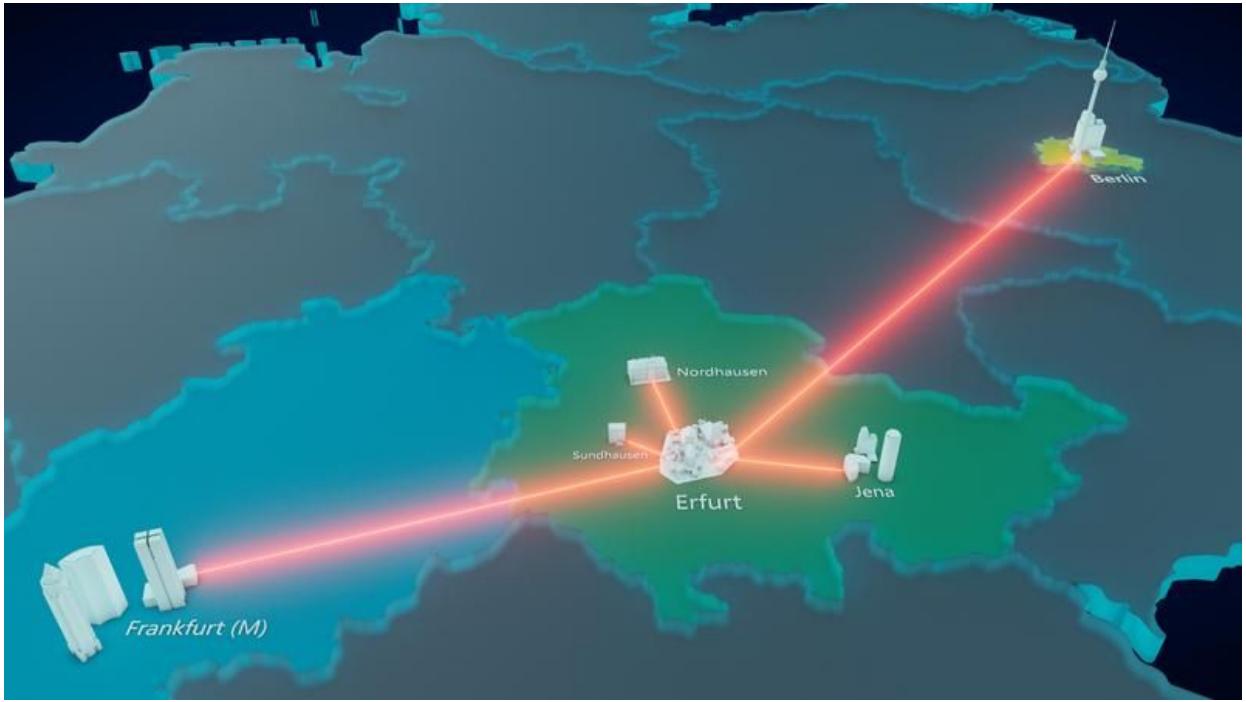


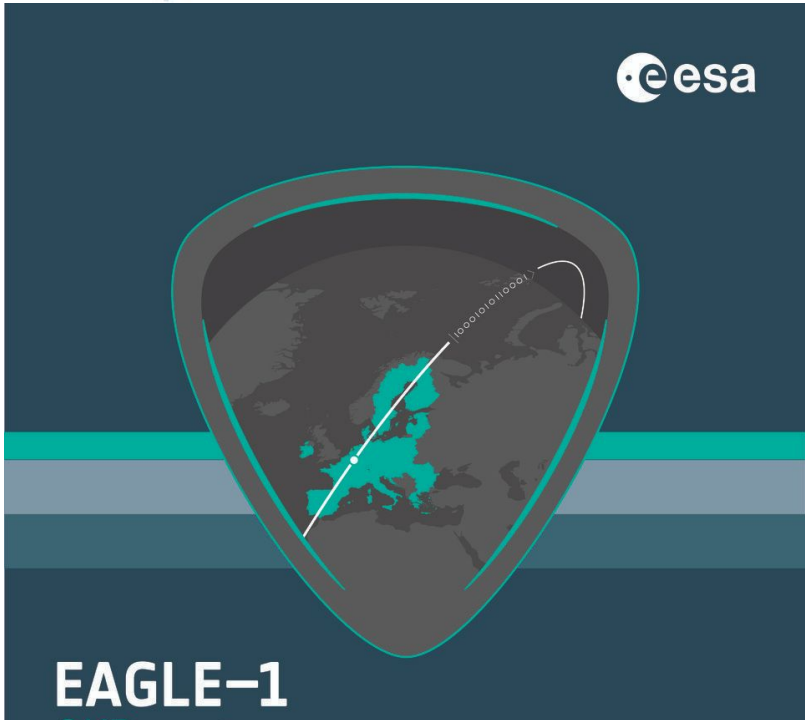
Fig.1 Map of London Quantum Metro Network

Alemanha

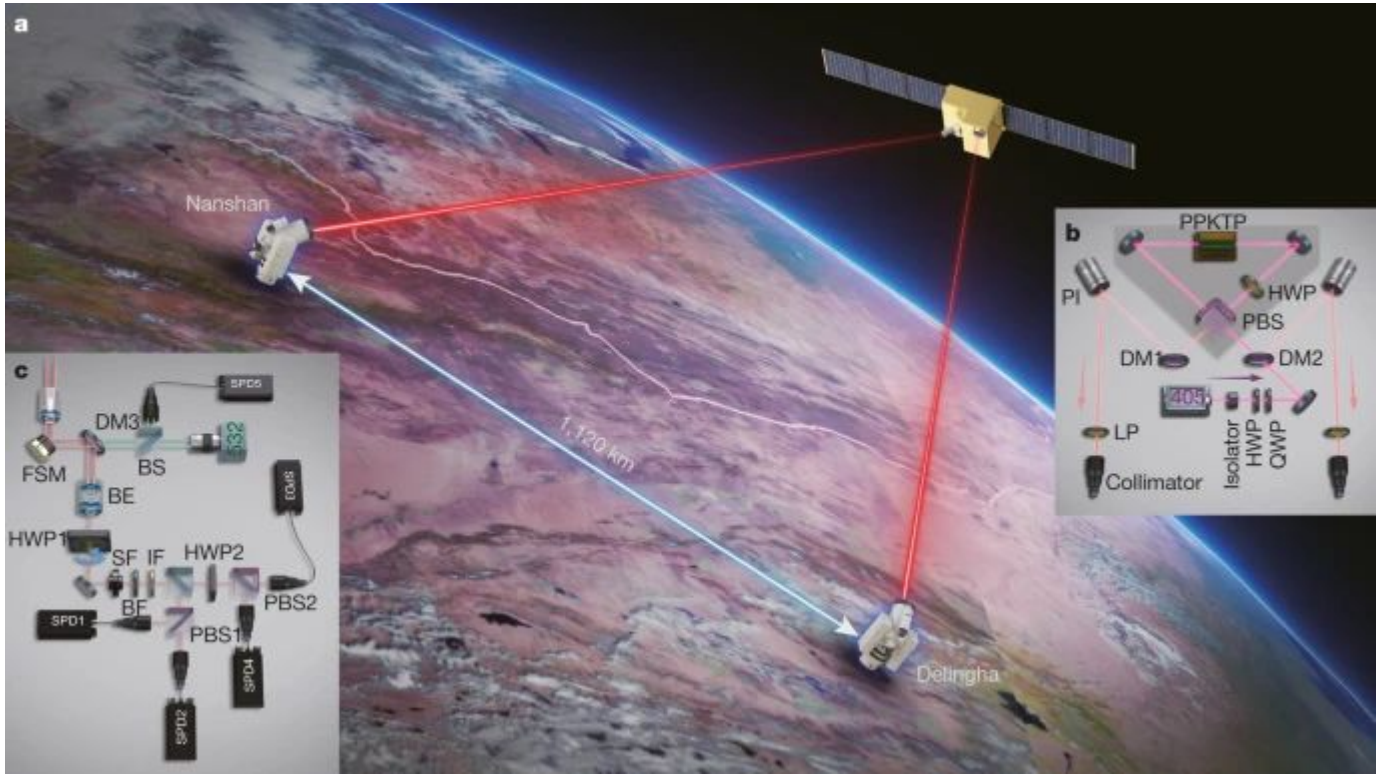


Eagle-1

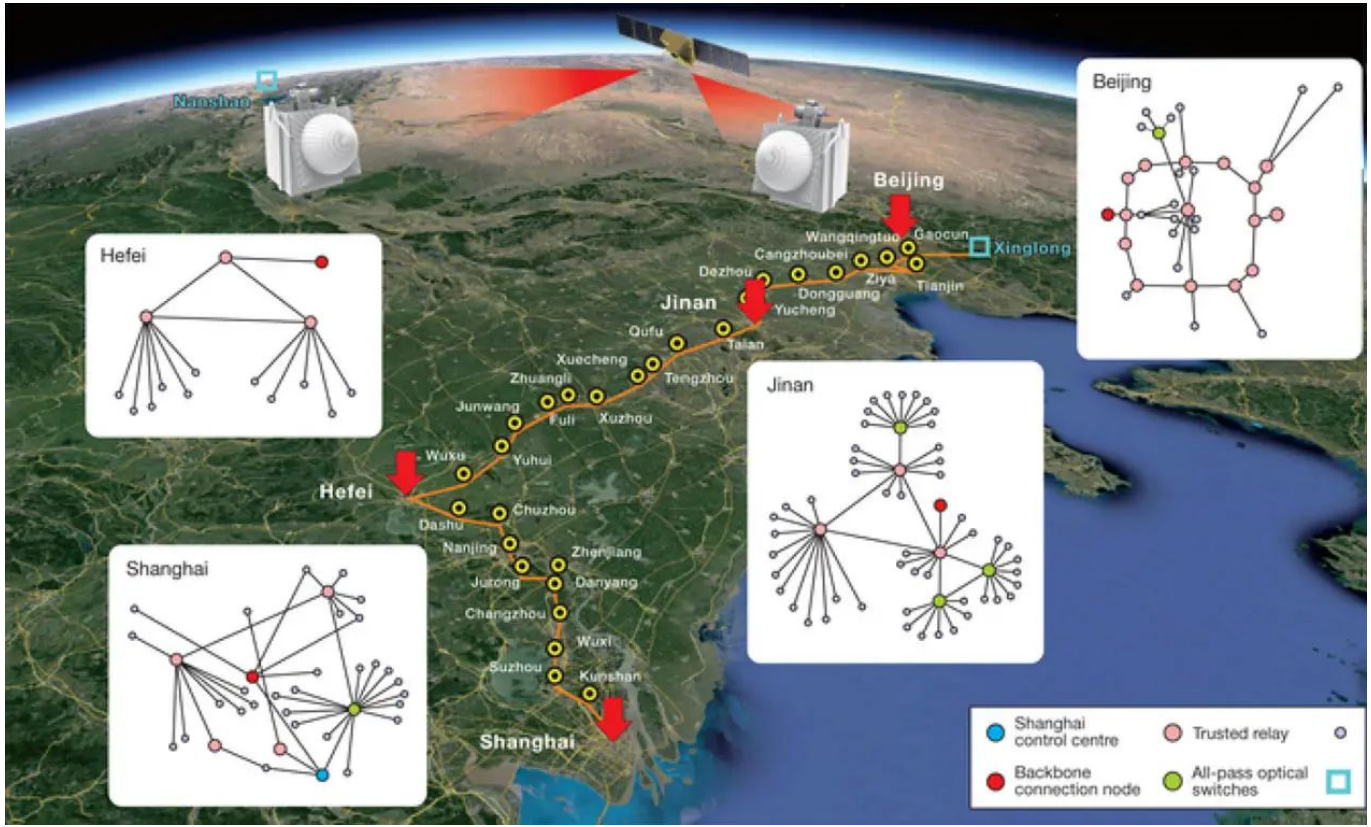
The Eagle-1 satellite will be the first space-based quantum key distribution system to be developed under a partnership between ESA, the European Commission and space companies in Europe.



Satélite Micius



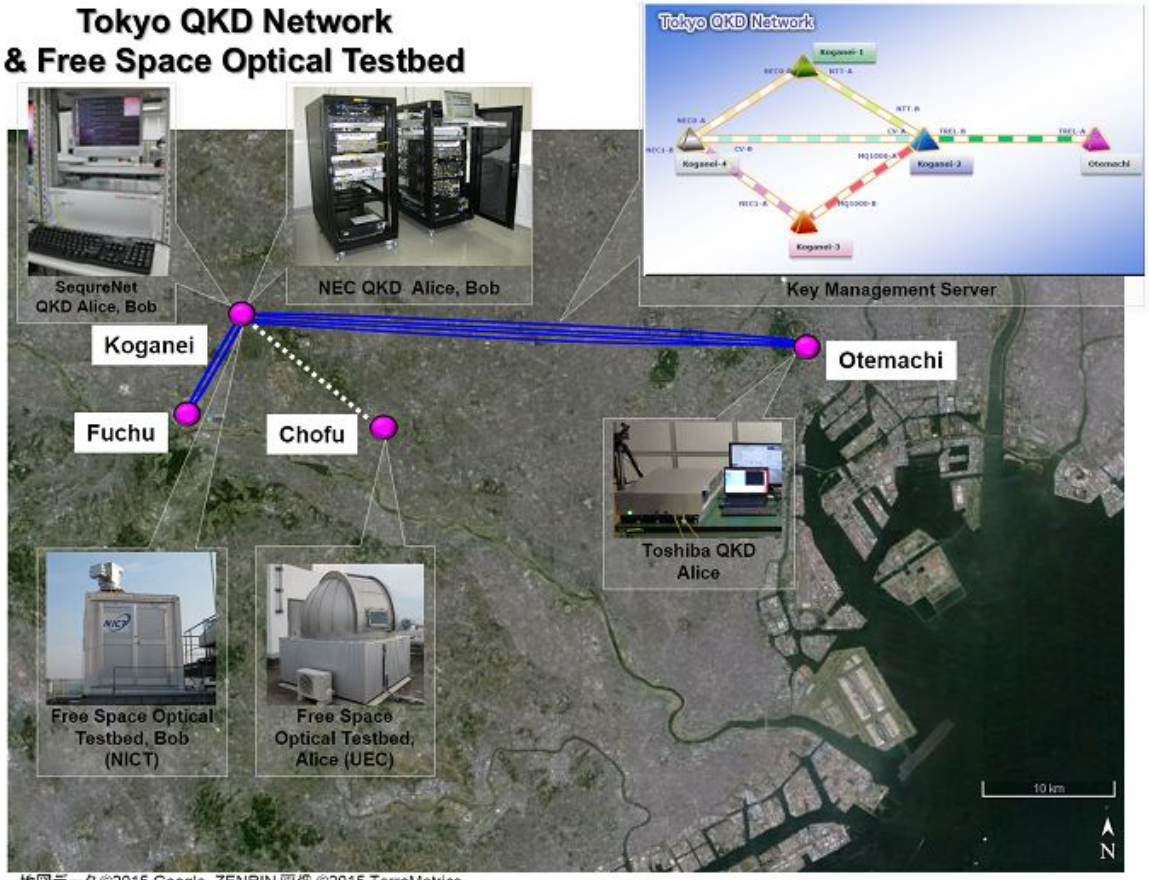
China


Nanshan
Beijing
Gaocun
Xinglong
Wangqingtuo
Cangzhoubei
Dezhou
Ziya
Tianjin
Dongguang
Jinan
Yucheng
Qufu
Talan
Xuecheng
Zhuangli
Tengzhou
Junwang
Fuli
Xuzhou
Wuxu
Yuhui
Hefei
Chuzhou
Dashu
Nanjing
Zhenjiang
Jurong
Danyang
Changzhou
Wuxi
Suzhou
Kunshan
Shanghai
Hefei
Shanghai
Beijing
Jinan
Shanghai control centre
Trusted relay
Backbone connection node
All-pass optical switches

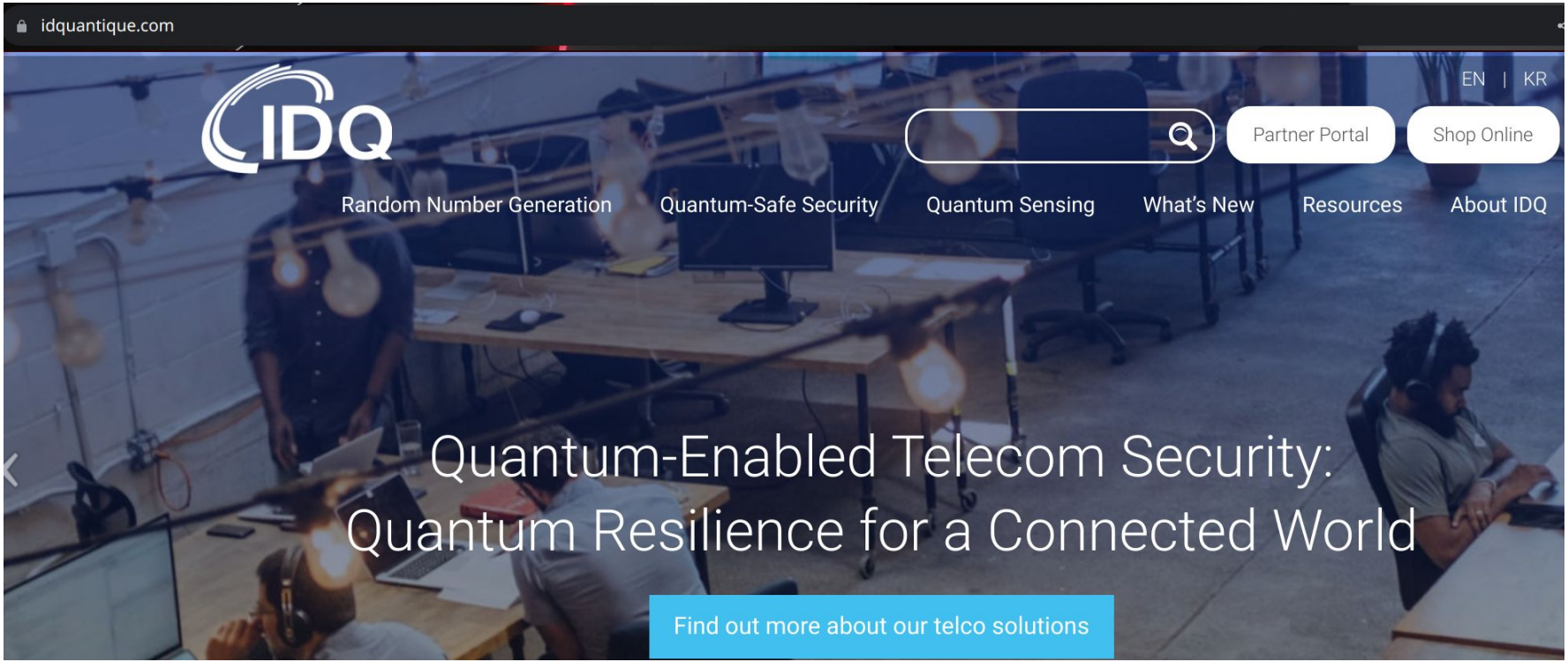
Coréia


South Korean QKD Network
Phase 1 (~2015): Bundang-Suwon-Seoul
Phase 2 (~2017): Seoul-Sejong-Daejeon
Phase 3 (~2020): National Network
충청북도
경상북도
전라북도
경상남도
전라남도
대구
울산
광주

Japão (Tokyo QKD)



ID Quantique - Suíça



Outras empresas

- Quantum CTEK - China
- Anhui Qasky Quantum Technology Co - China
- Toshiba Europe

RedeRio


UFRJ
UFF
CBPF
PUC
≈ 13 Km
≈ 7 Km
≈ 7 Km
Rio de Janeiro
GAMBOA
SÃO CRISTÓVÃO
CENTRO
Niterói
BOTAFOGO
HUMAITÁ
LAGOA
COPACABANA
LEBLON
IPANEMA

Crítica à QKD (NSA)

- Ausência de autenticação da fonte -Solução via Criptografia Pós-Quântica
- Hardware específico para QKD -Ano após ano a P&D encontra soluções melhores
- A distribuição de chaves quânticas aumenta os custos de infraestrutura e os riscos de ameaças internas. -Device Independent
- Segurança e validação de chaves
- Suscetível a DoS

Para levar para casa

- Criptografia quântica tem proteção por leis da física, ao contrário da criptografia clássica
- QKD já está disponível comercialmente e implementada em diferentes países
- QKD e teletransporte quântico já foram testados tanto em fibra quanto em ar, incluindo satélite
- Implementação em diversos países
- Grande vantagem: proteção a nível físico, imune a qualquer avanço em poder computacional
- Ainda muitos desafios tanto em *hardware* quanto em protocolos

Obrigado!