



Segurança de Redes na Era Quântica

Prof. Valéria Loureiro da Silva
Valeria.dasilva@fieb.org.br

WTR-BA, Setembro 2026



MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÃO



MERCADO POTENCIAL PARA TECNOLOGIAS QUÂNTICAS ATÉ 2040



 **\$198B**
USD

(\$0.9-2.0T Economic Value)

Computação Quântica

\$45B – 131B*

Comunicação Quântica

\$24B – 36B*

Sensores Quânticos

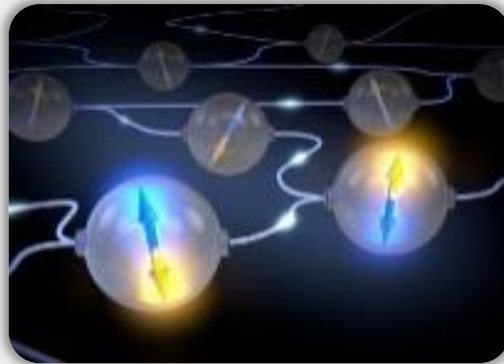
\$18B – 31B*

*Mercado estimado até 2040

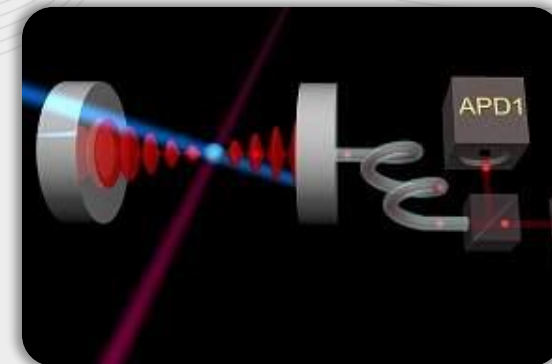
Tecnologias Quânticas 2.0



**Computação
Quântica**



**Criptografia e
Comunicação Quântica**



**Sensores
Quânticos**



Teoria de Informação Quântica & Princípios da Mecânica Quântica

Computação Quântica Sonho ou Pesadelo?



Otimização

Problemas de Logística
Portfolios e Risco



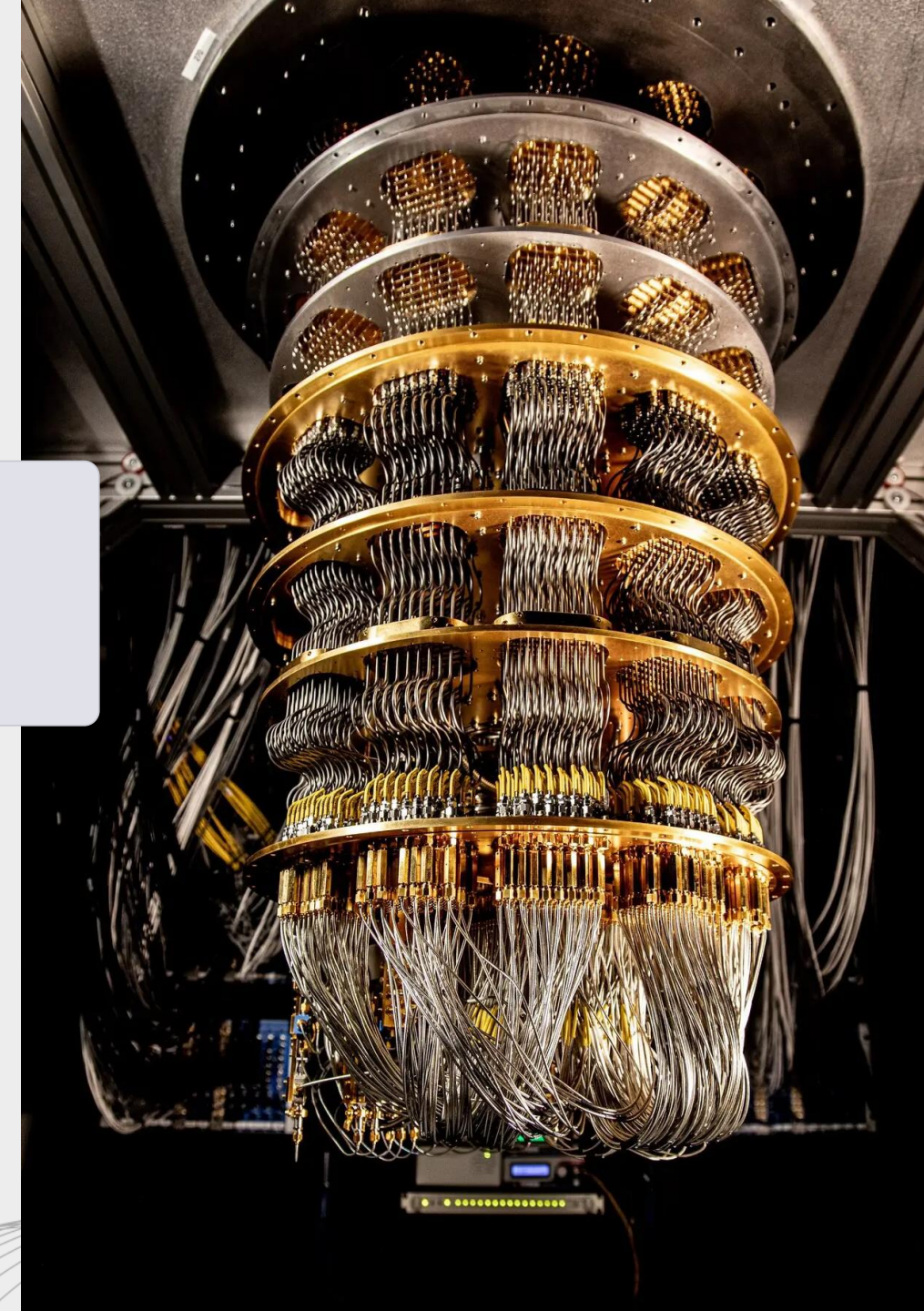
Inteligência Artificial

Modelos mais compactos
Eficiência Energética



Simulações

Modelos moleculares precisos
Novos materiais



Computação Quântica Sonho ou Pesadelo?



Otimização

Problemas de Logística
Portfolios e Risco



Inteligência Artificial

Modelos mais compactos
Eficiência Energética



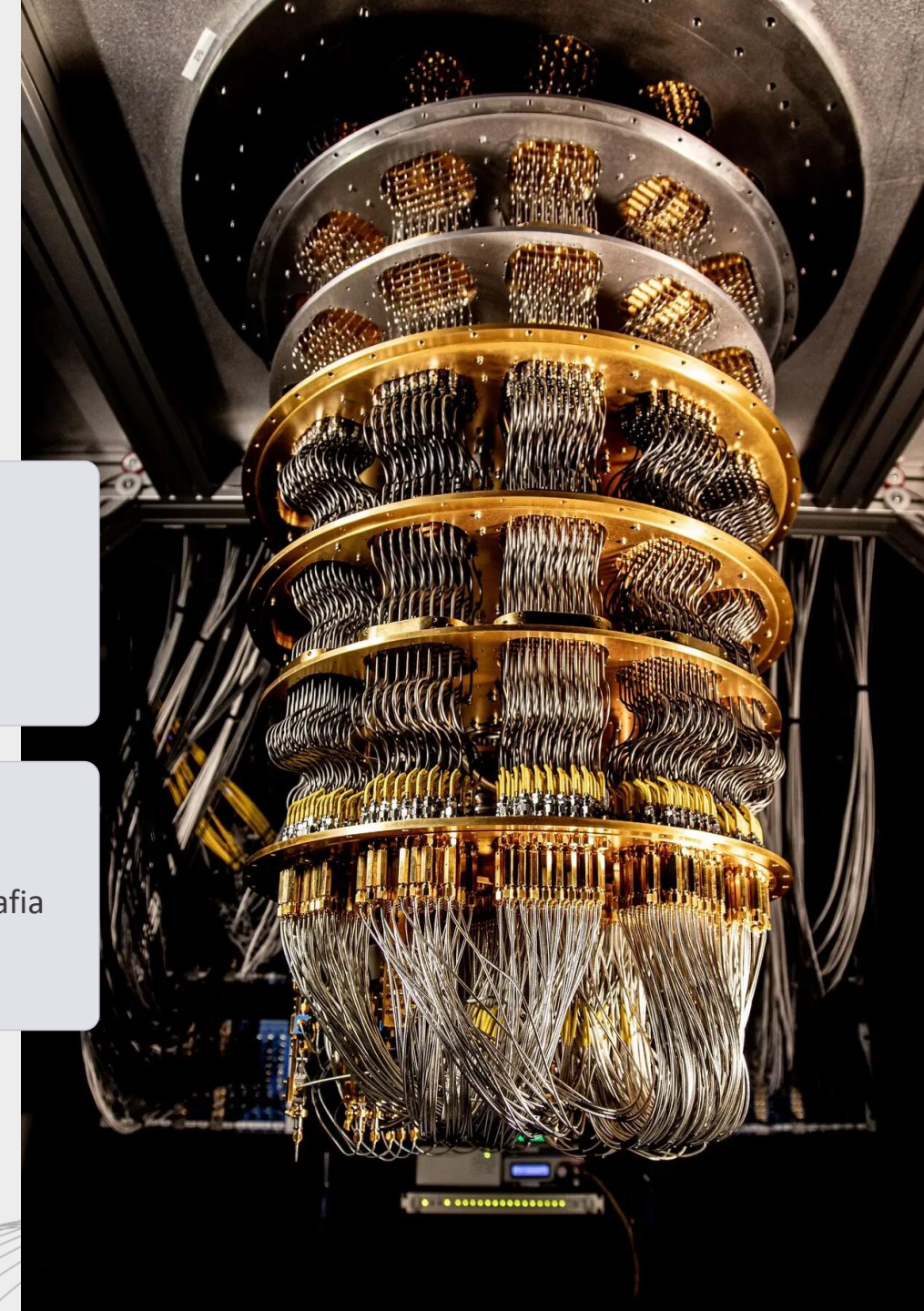
Simulações

Modelos moleculares precisos
Novos materiais

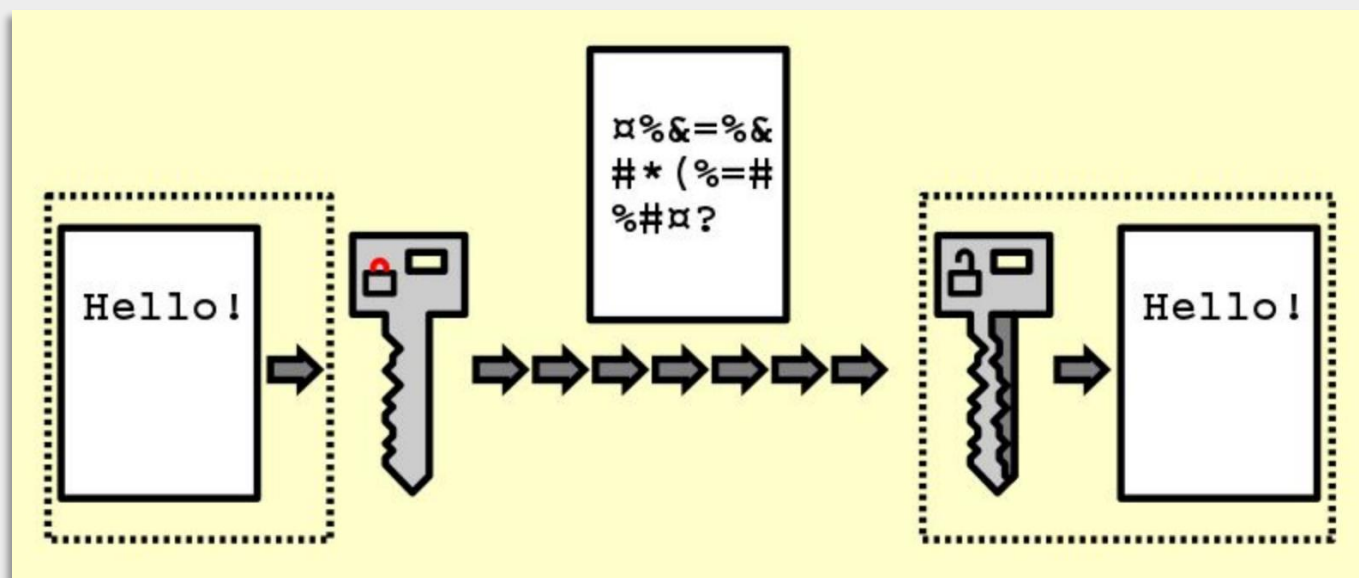


Criptanálise

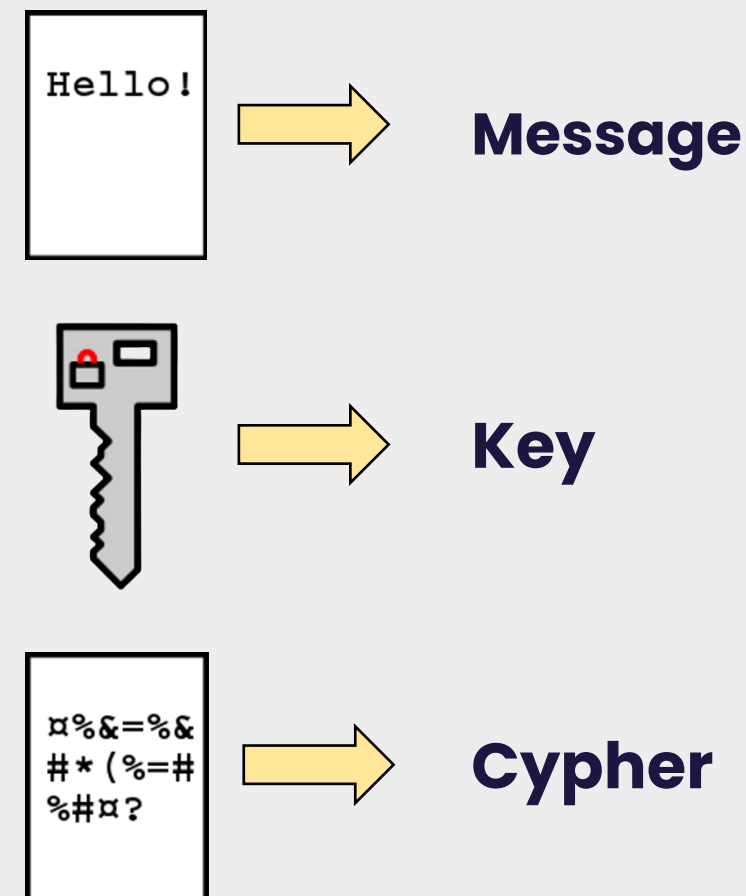
Quebra de chaves de criptografia



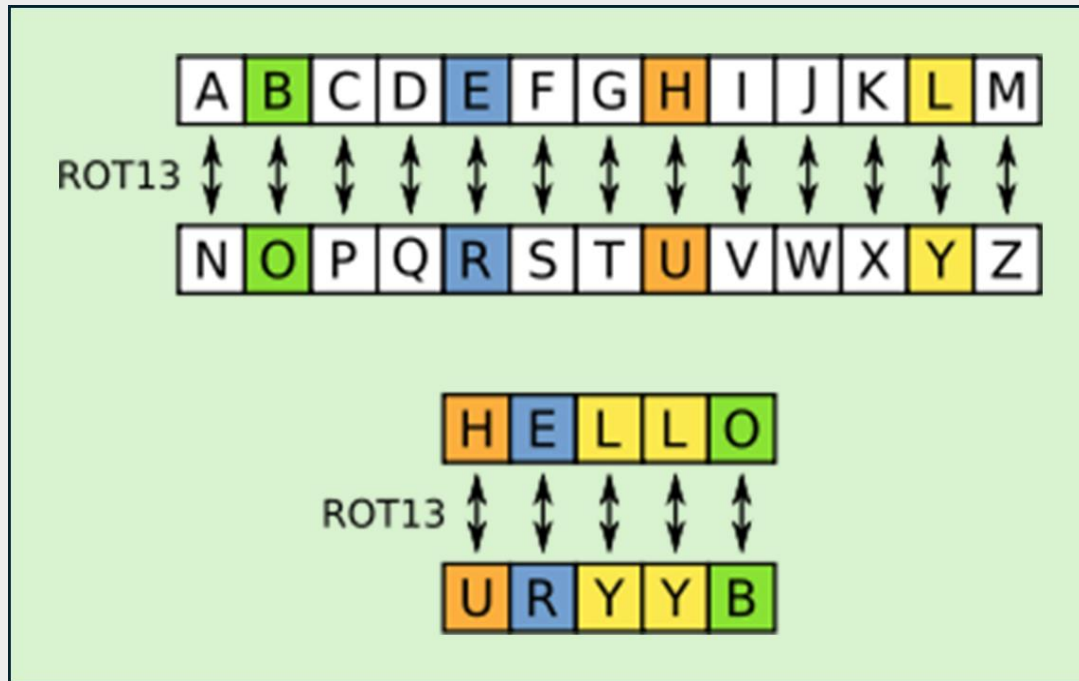
Criptografia



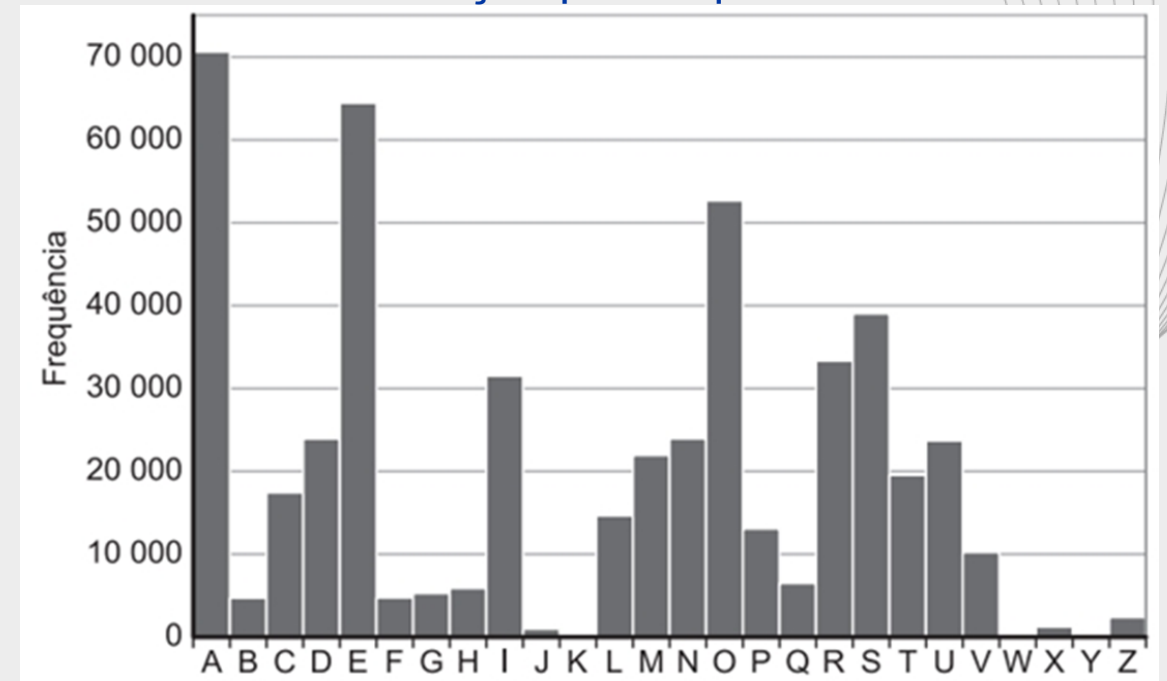
Source: Wikimedia Commons, Public_key_encryption_keys.png.



Criptografia



Decodificação por frequência

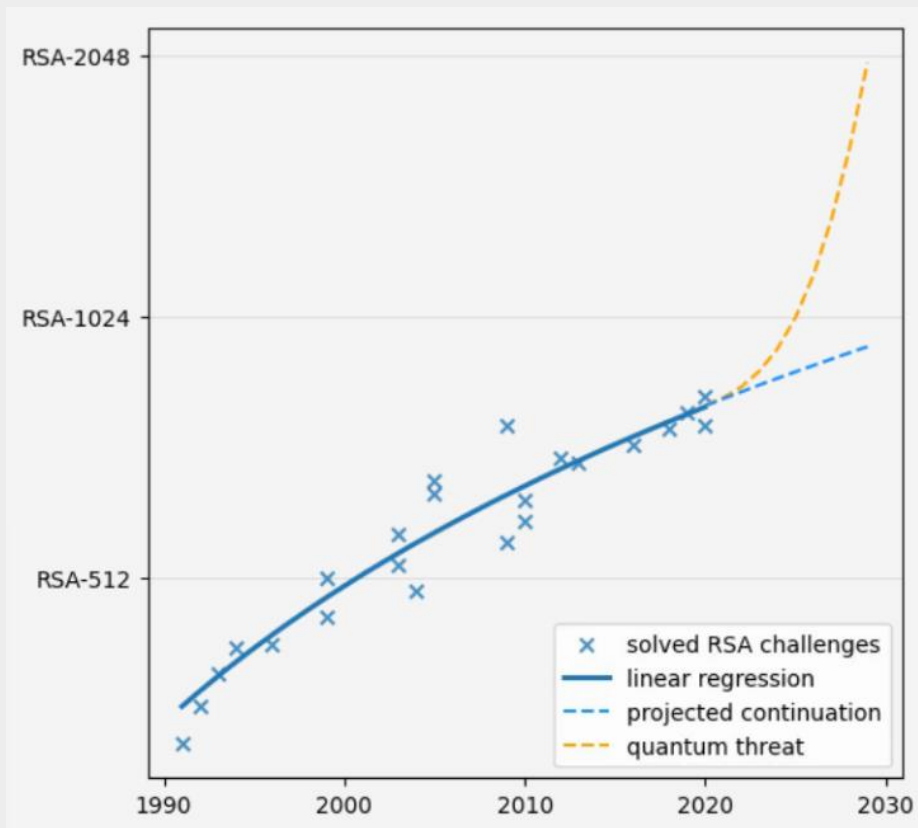


Criptografia segura requer técnicas mais elaboradas que eliminem padrão aleatórios



Geradores de números

Ameaça Quântica



<https://nexenio.com/blog/werden-quantencomputer-das-internet-unsicher-machen>

Algoritmo de Shor quebra chaves assimétricas (ex: RSA)

Algoritmo de Grover enfraquece chaves simétricas (ExS: AES)

Tipos de criptografia

Simétrica

- Alice e Bob usam a mesma chave
- A chave é privada (e secreta)
- Ex: One-time pad e AES



Assimétrica

- Alice e Bob publicam sua chave pública
- Chaves públicas encriptam a mensagem
- Chaves privadas decriptam
- Ex: RSA

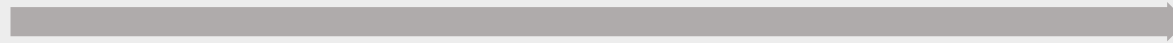


One-time Pad

Alice



Cifra



Bob



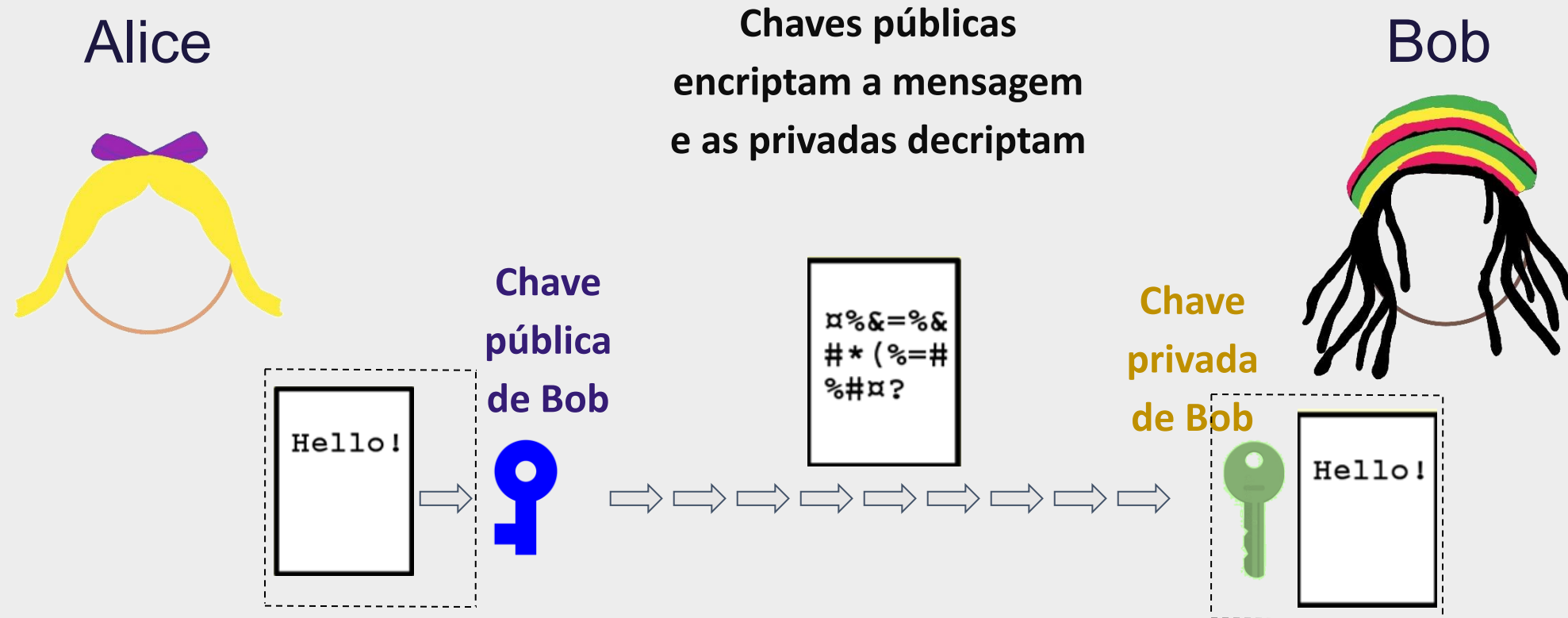
Cifrar:

$$\begin{array}{r} \oplus \\ 0100101110110110 - \text{Mensagem} \\ 1101010110101011 - \text{Chave} \\ \hline 1001111000011101 - \text{Cifra} \end{array}$$

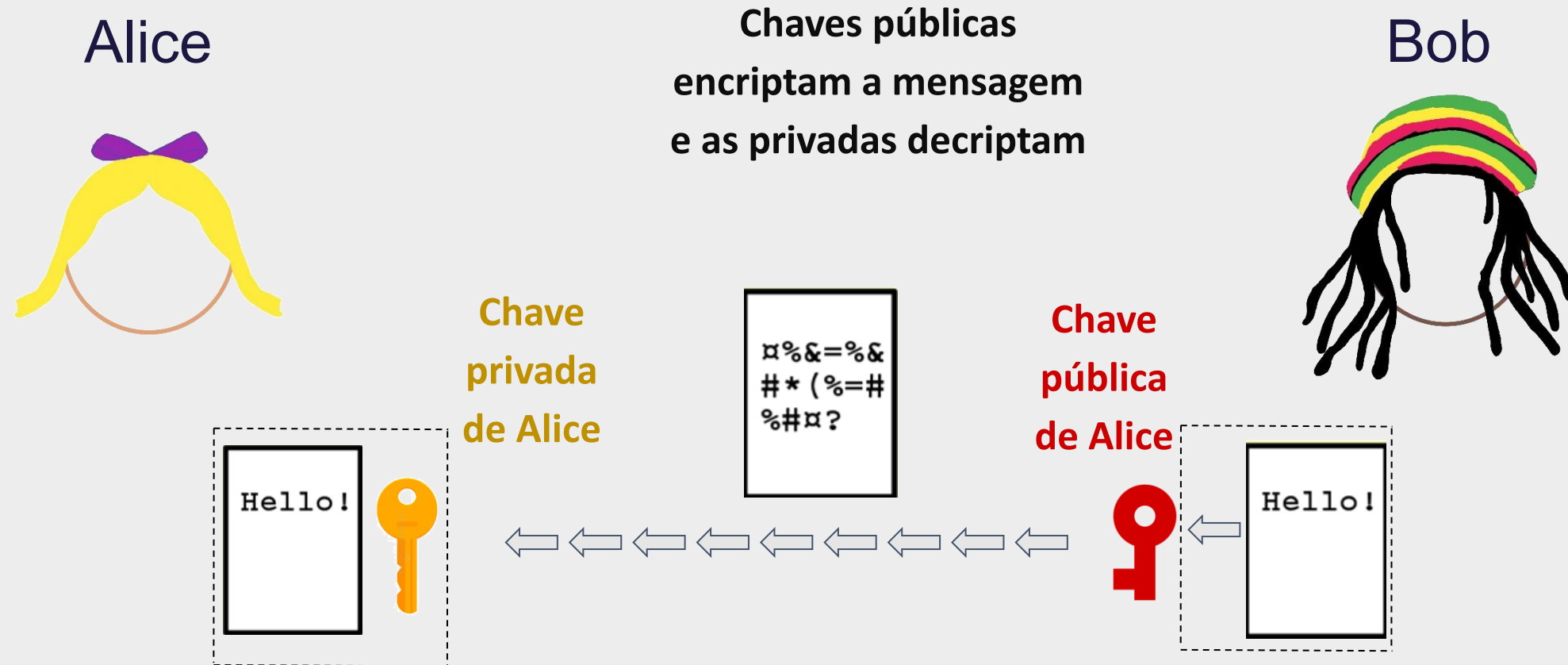
Decifrar:

$$\begin{array}{r} \oplus \\ 1001111000011101 - \text{Cifra} \\ 1101010110101011 - \text{Chave} \\ \hline 0100101110110110 - \text{Mensagem} \end{array}$$

Criptografia assimétrica



Criptografia assimétrica



Ameaça Quântica

Soluções

Geração de números aleatórios (QRNG)

- Números verdadeiramente aleatórios
- Baseada na natureza estatística da mecânica quântica
- Geração local

Criptografia Pós Quântica (PQC)

- Segurança baseada na complexidade matemática
- Pode não resistir ao tempo
 - Aparecimento de algoritmos mais eficientes
 - Evolução do poder computacional.

Criptografia Quântica (QKD)

- Segurança baseada nas leis da física
- Detecção de invasão
- Soluções comerciais disponíveis
- Requer hardware dedicado

Solução ótima utiliza combinação dessas tecnologias



Ameaça Quântica

Soluções

Geração de números aleatórios (QRNG)

- Números verdadeiramente aleatórios
- Baseada na natureza estatística da mecânica quântica
- Geração local

Criptografia Pós Quântica (PQC)

- Segurança baseada na complexidade matemática
- Pode não resistir ao tempo
 - Aparecimento de algoritmos mais eficientes
 - Evolução do poder computacional.

Criptografia Quântica (QKD)

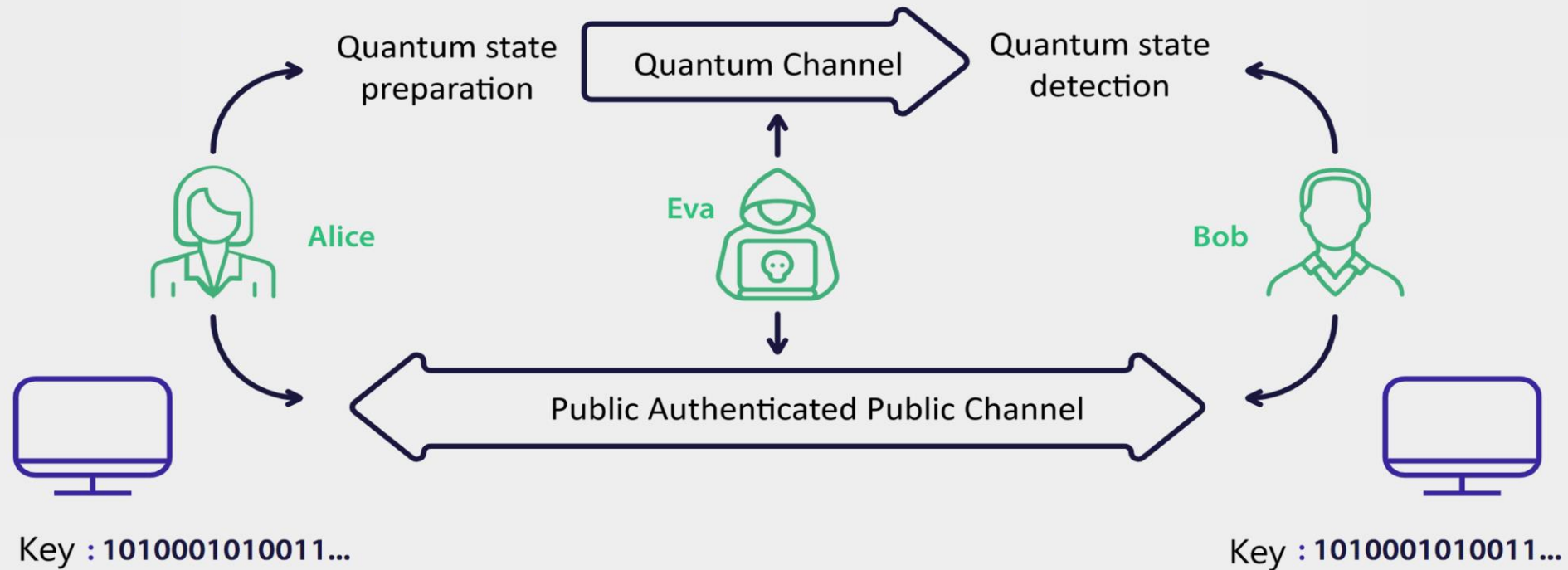
- Segurança baseada nas leis da física
- Detecção de invasão
- Soluções comerciais disponíveis
- Requer hardware dedicado

Solução ótima utiliza combinação dessas tecnologias



Quantum Key Distribution (QKD)

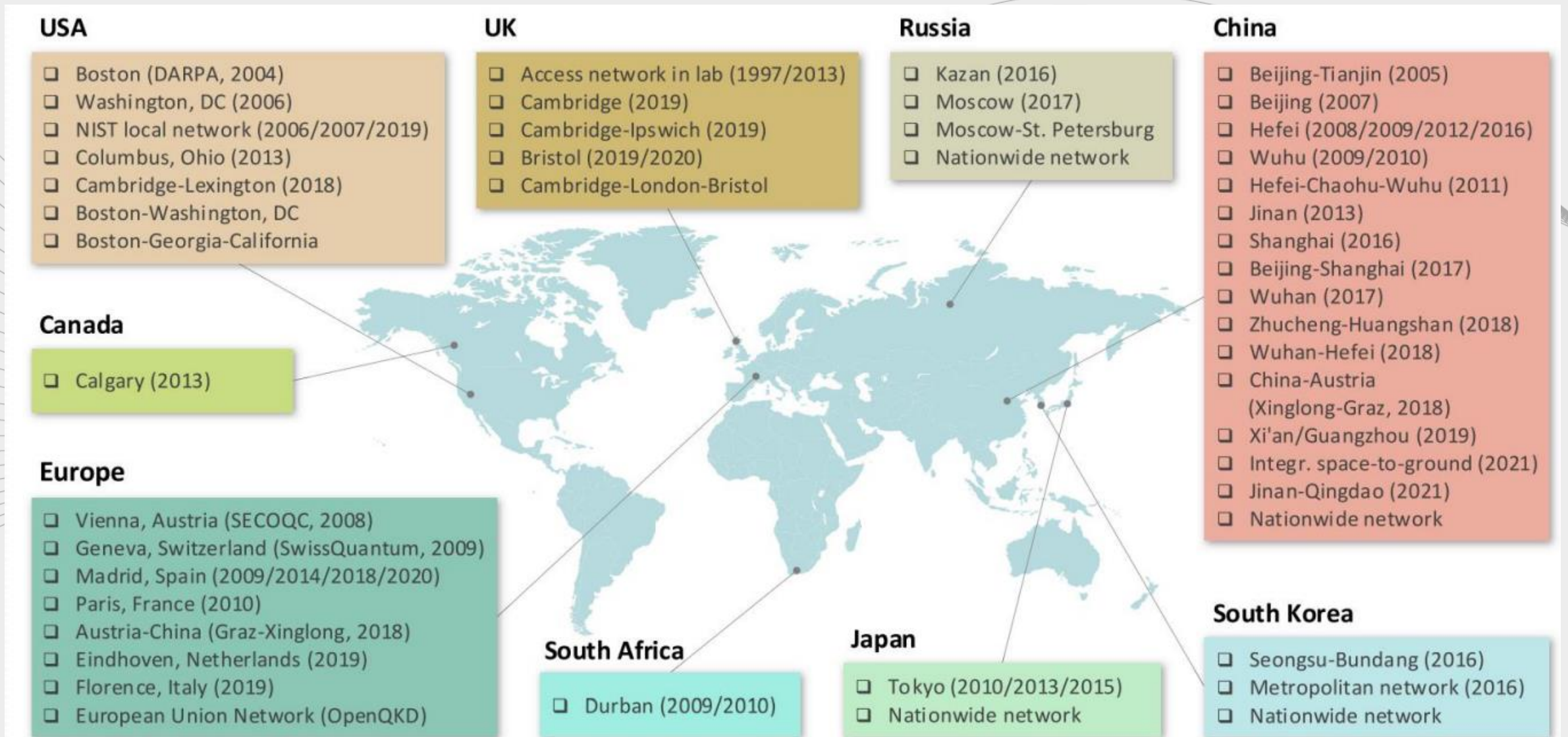
Cenário Prepara & Mede



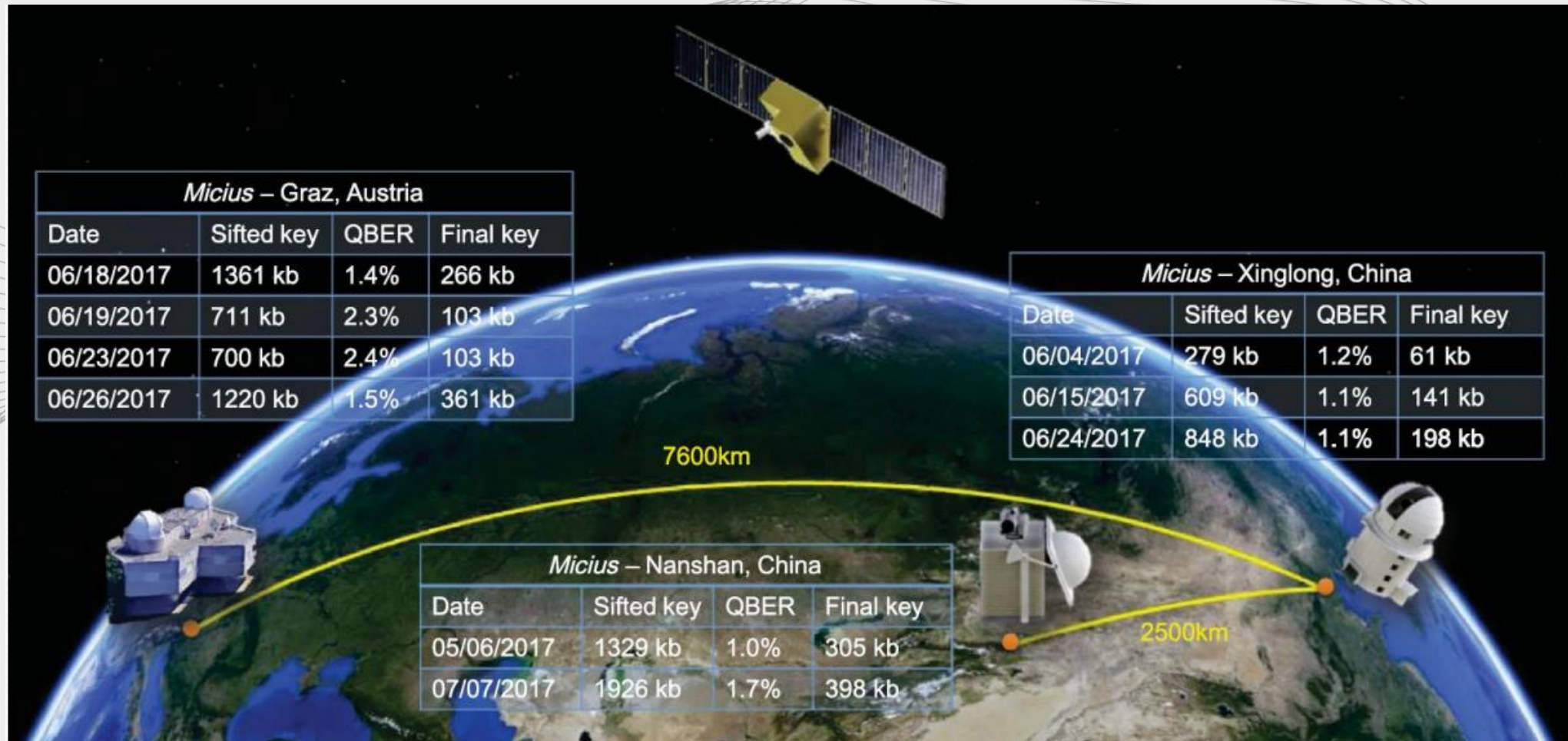
$\oplus$ 0100101110110110 - Message
1101010110101011 - Key
1001111000011101 - Cypher

$\oplus$ 1001111000011101 - Cypher
1101010110101011 - Key
0100101110110110 - Message

Redes Quânticas no mundo



Link intercontinental – Austria-China



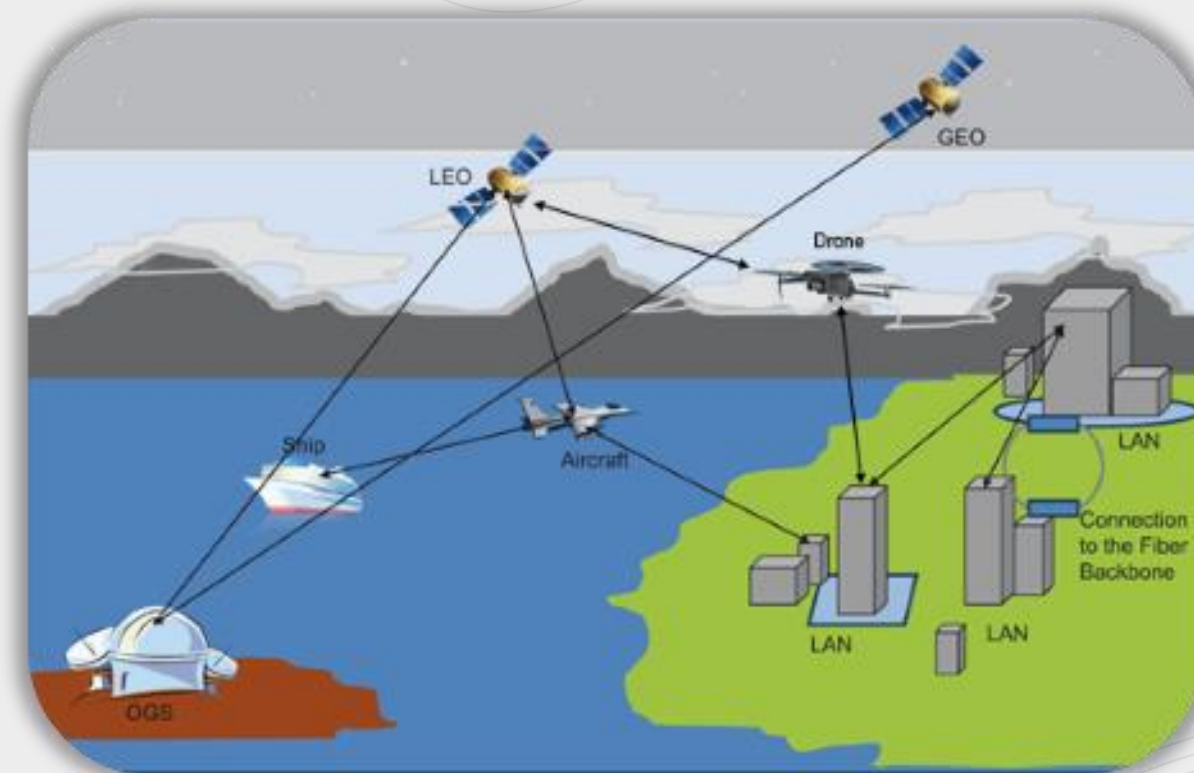
Liao et al., PRL 120(3): 030501 (2018)

QKD

Aplicações

Segurança incondicional de informações sensíveis e sigilosas

Integridade de infraestrutura crítica e dados sensíveis



QKD

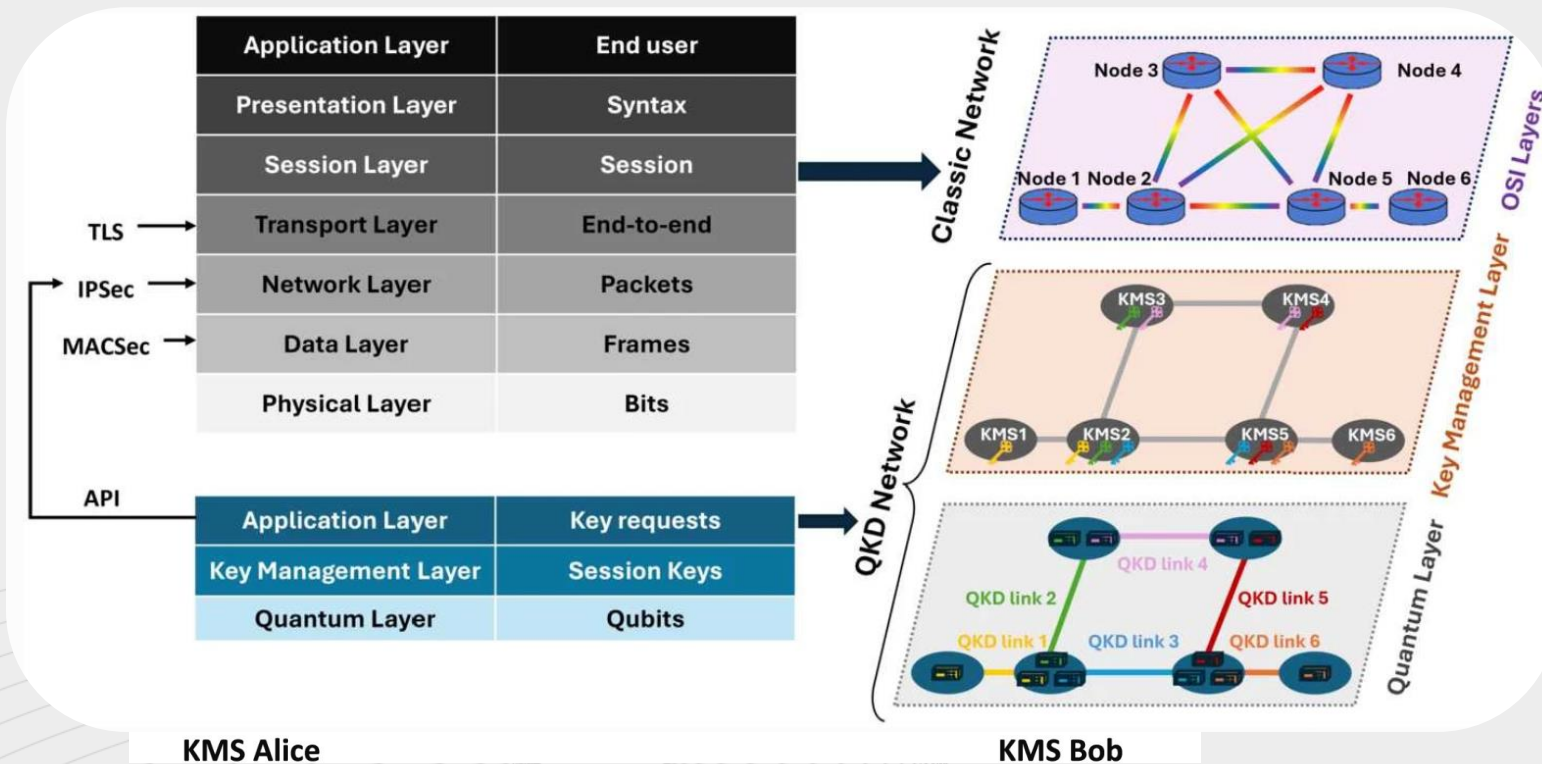
Aplicações – Infra segura

Defesa, Saúde, Energia

- Perda de controle de ativos de alto risco/custo
- Risco de Interceptação de comunicação
- Jamming



QKD Aplicações



Comunicação segura com a nuvem (API e serviços de nuvem) - proteção de serviços críticos online

Comunicação cliente-servidor pela internet (TLS – Transport Layer Security)

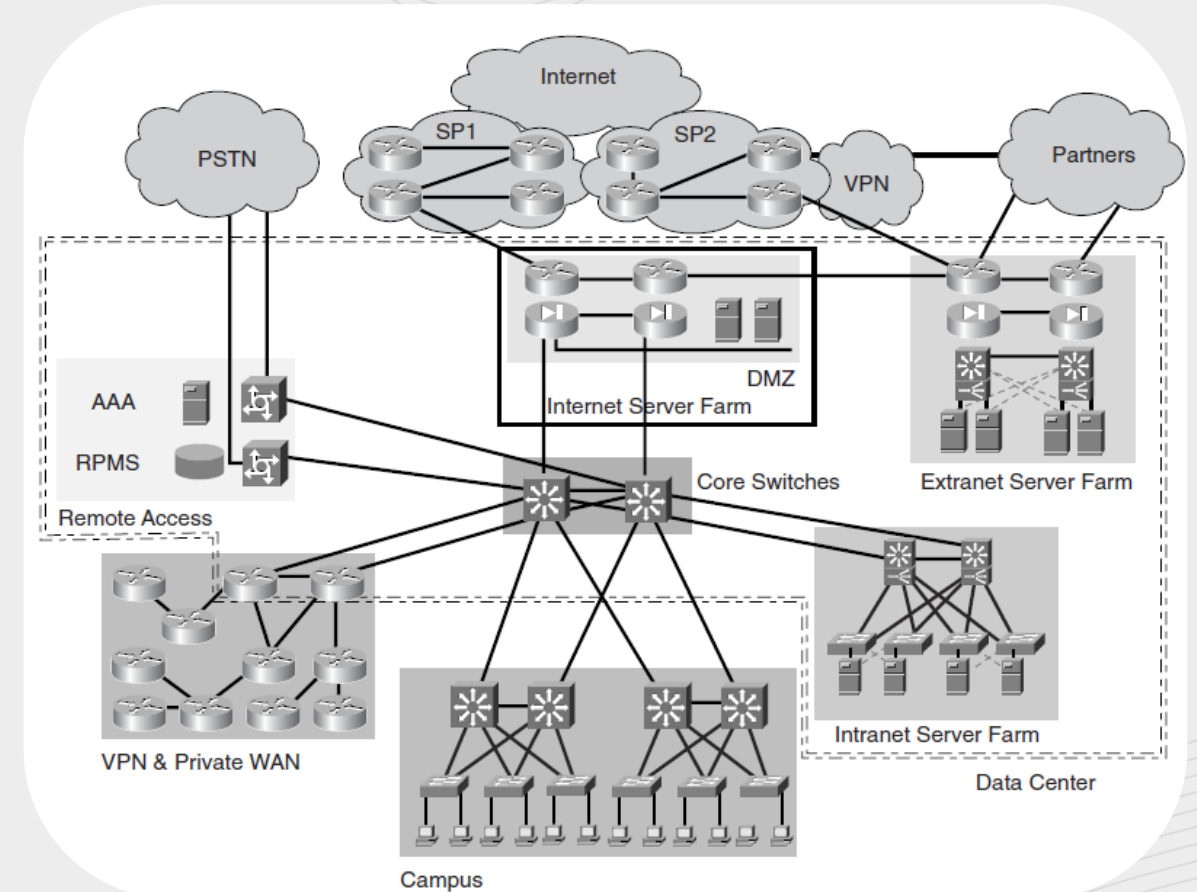
Comunicação entre data centers remotos – integridade e segurança dos dados

Conexões remotas seguras (VPN)

Comunicação Quantum Safe

Problemas

- Risco de acesso indevido a informações armazenadas em data centers remotos e nuvem
- Proteção de informações estratégicas com Soberania Digital



O primeiro Centro de Competência em Tecnologias Quânticas do Brasil

OBJETIVOS

Integrar pesquisas de ponta em aplicações industriais

- Dedicado ao desenvolvimento e à inovação em tecnologias quânticas, com foco especial em comunicação quântica;
- Desenvolvimento do ecossistema completo: PD&I, formação de RH, atração e criação de startups, interação com empresas (adoção e fornecimento de tecnologia)
- Estabelecer parcerias com outras instituições de pesquisa e empresas.

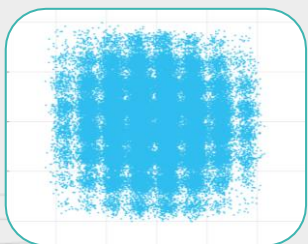
FINANCIAMENTO

PPI IoT/Manufatura 4.0 do MCTI, através do Termo de Cooperação 053/2023, firmado com a EMBRAPII

R&D no QuIIN

**Pesquisar e Desenvolver* e Integrar† Systemas Quânticos ao
Ecossistema de Cybersegurança**

QUANTUMSAFE



QKD*



QRNG *†



PQC †



**Quantum
Cybersecurity**

13

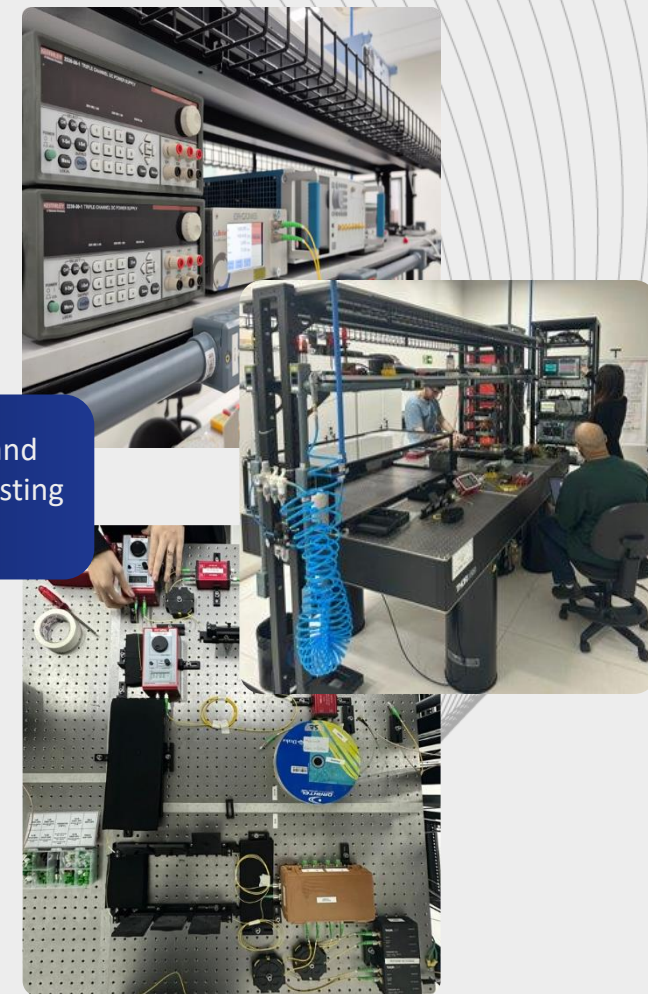
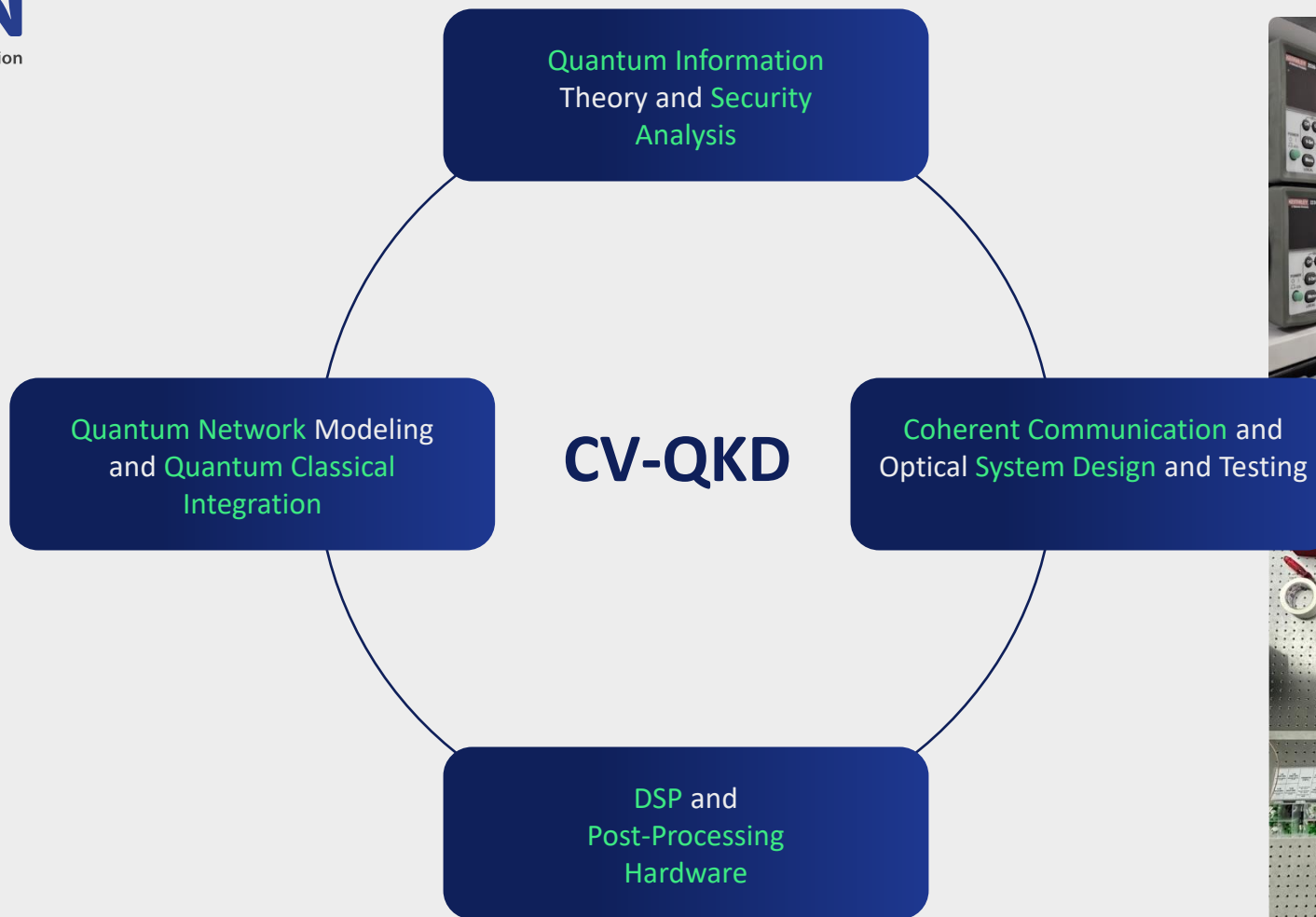
Projetos

100+

Pesquisadores,
bolsistas e
estudantes

8

Startups em
tecnologias
quânticas



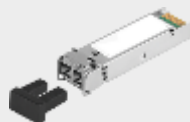
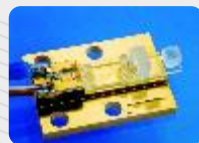
LINHAS DE PESQUISA (PD&I)

Como gerar chaves criptográficas?

Protocolo CV-QKD



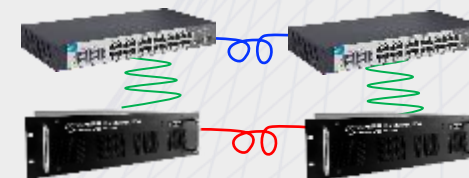
Desenvolver módulos e equipamentos próprios



Como utilizar chaves?

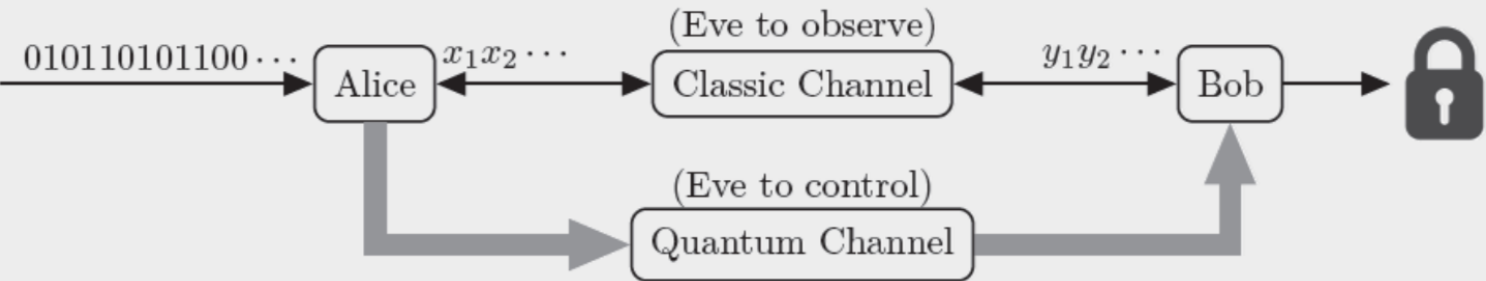


Introdução de equipamentos quânticos (comerciais) existentes em redes clássicas.

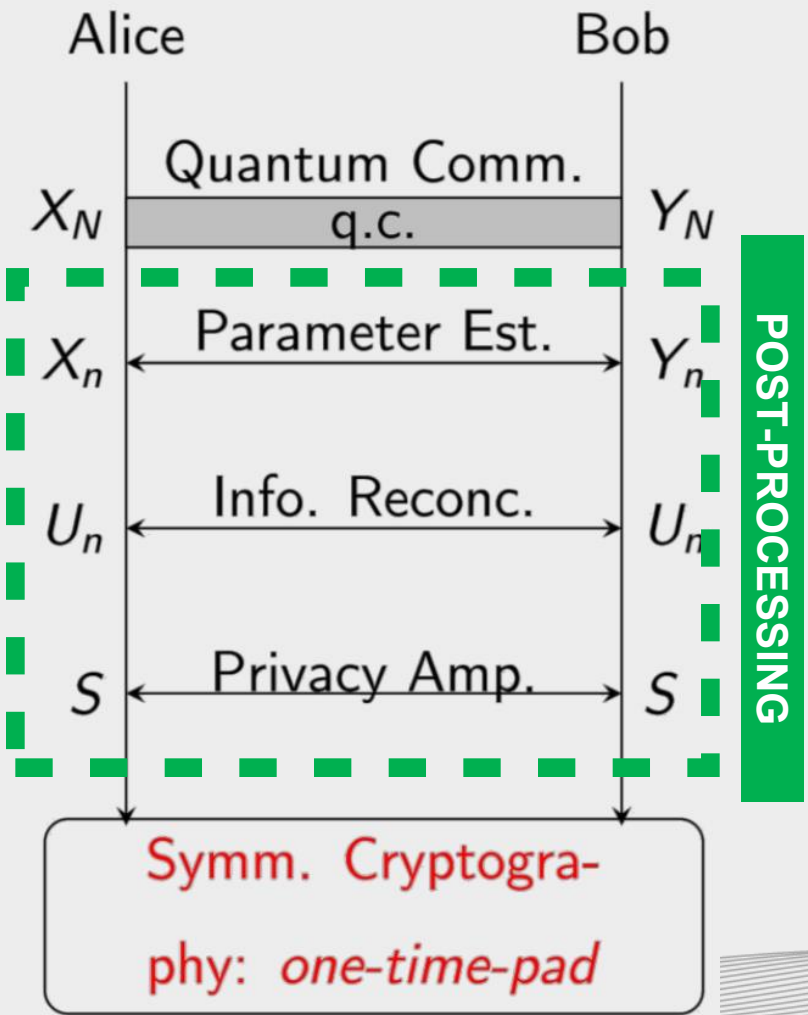


Quantum Key Distribution (QKD)

Cenário Prepara & Mede

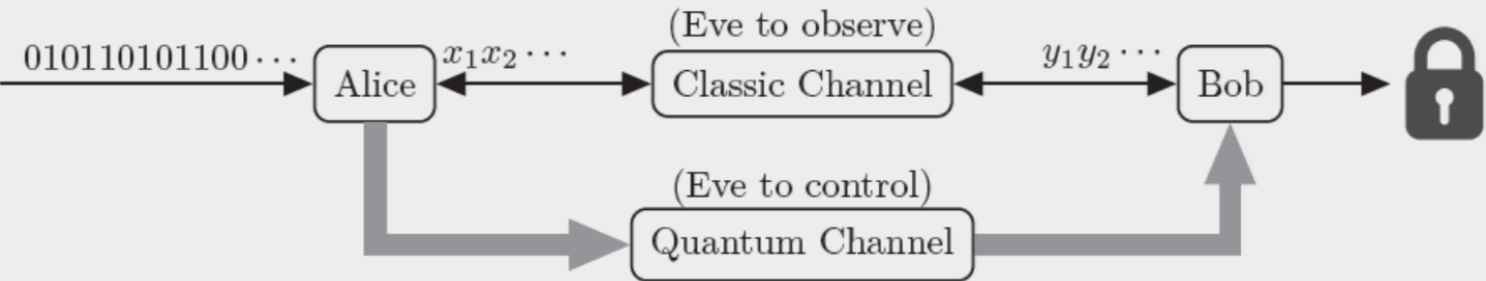


	Discrete Variables	Continuous Variables
Key encoding	Single photon polarization	Field quadrature modulation
Detection	<i>Single photon detecion</i>	Coherent (homodyne/heterodyne)
Post processing	Low complexity	High complexity: Low SNR, DSP Stack, LDPC w/ unusual lengths

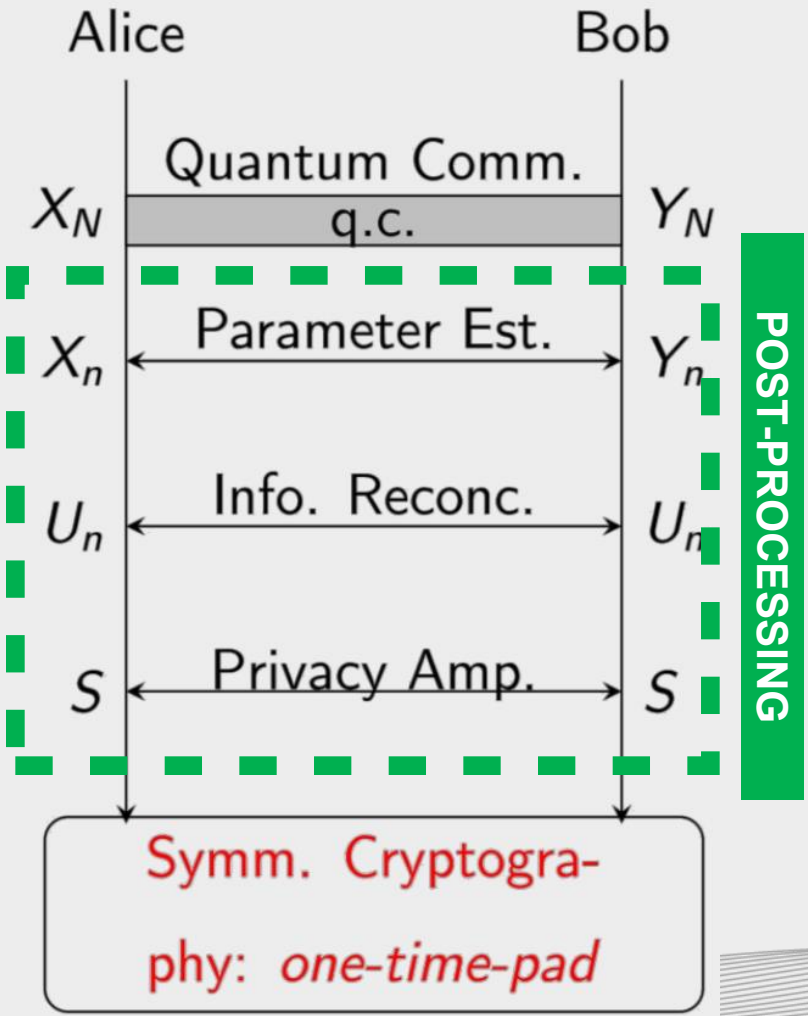


Quantum Key Distribution (QKD)

Prepare-and-measure scenario



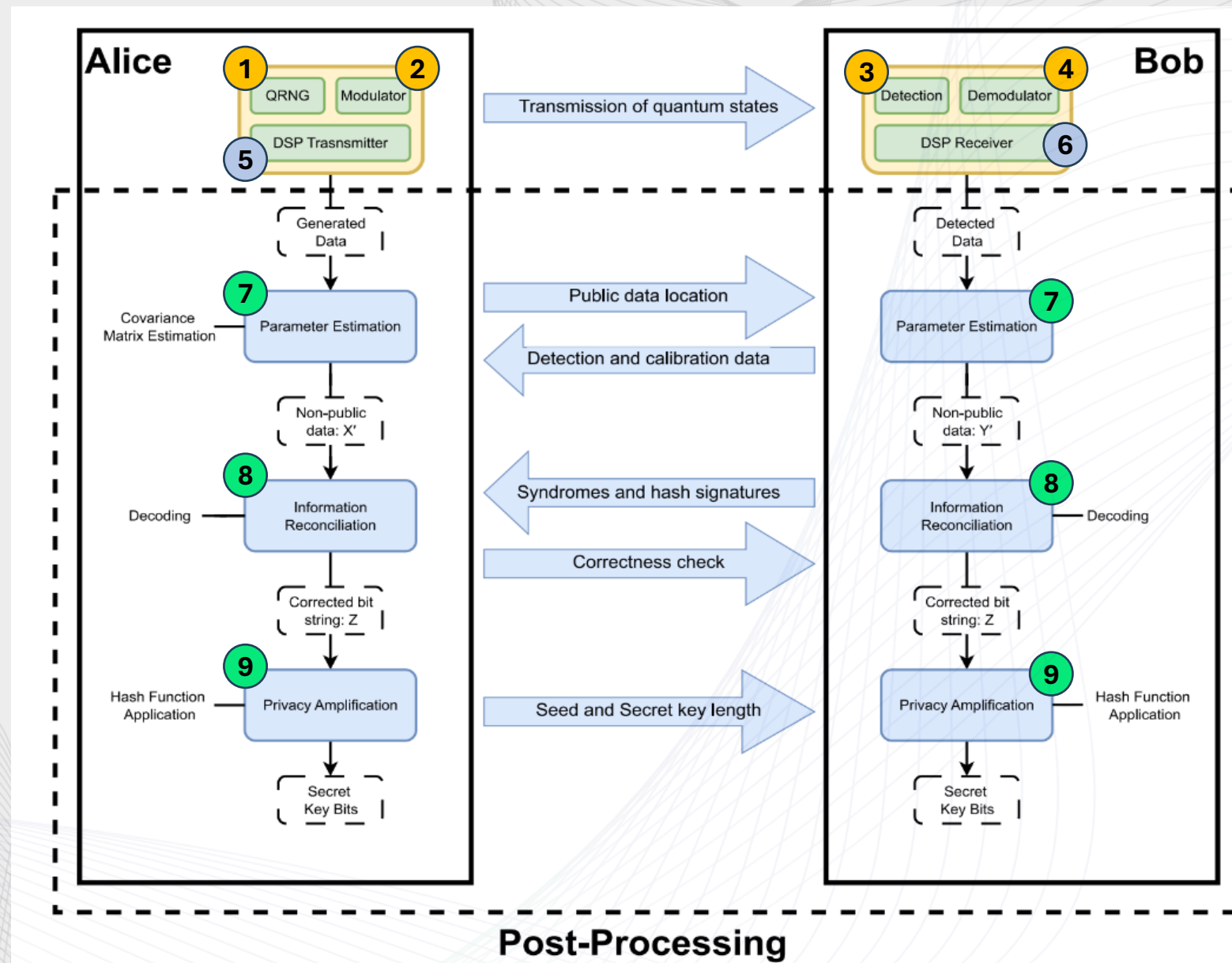
	Discrete Variables	Continuous Variables
Key encoding	Single photon polarization	Field quadrature modulation
Detection	Single photon detection	Coherent (homodyne/heterodyne)
Post processing	Low complexity	High complexity: Low SNR, DSP Stack, LDPC w/ unusual lengths



CV-QKD DSP e Pós-Processamento

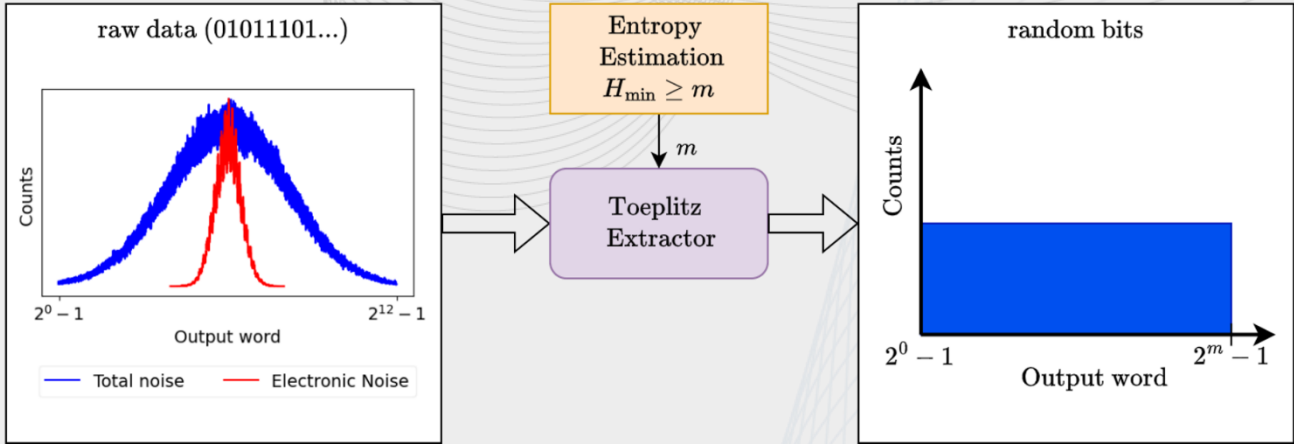


Desafio: complexidade computacional



1 QRNG

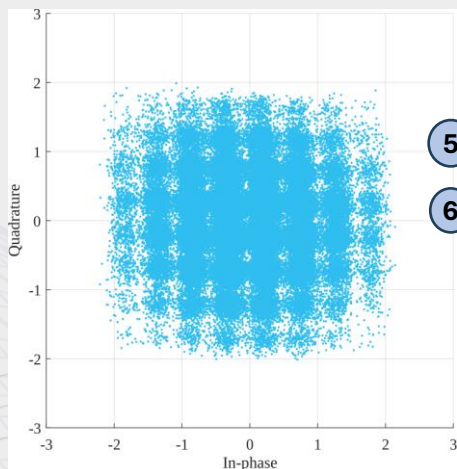
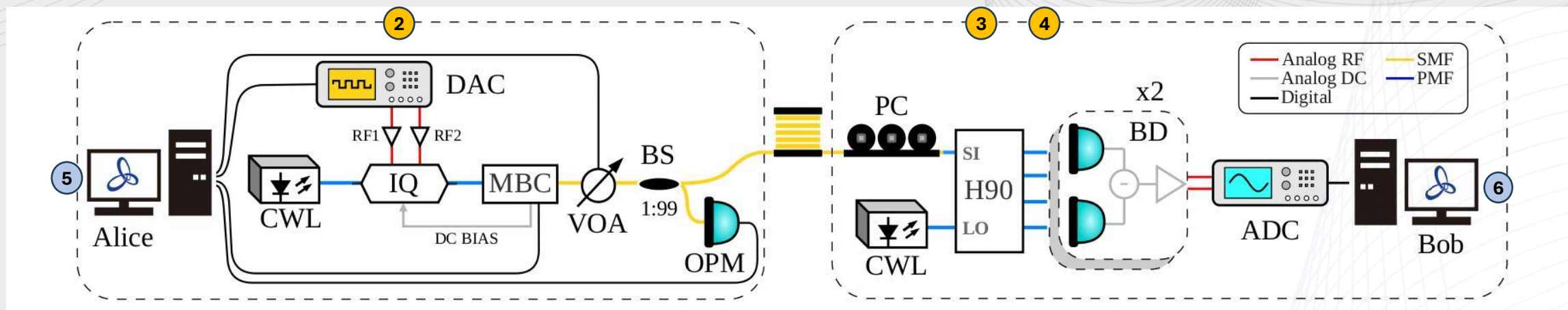
- Protótipo de bancada de gerador quântico de números aleatórios
- Batimento com vácuo
- Processamento offline
- Hmin = 10.61 bits comparado com 12 bits para cada amostra bruta



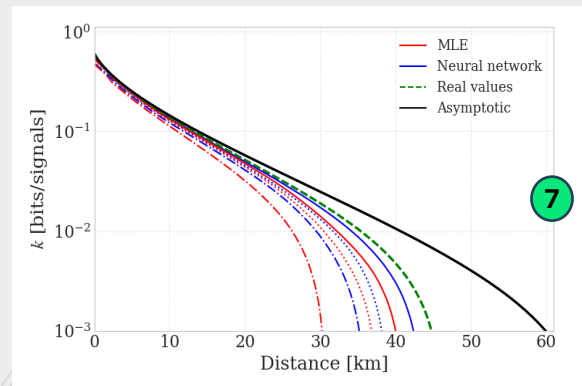
Testes de Aleatoridade do NIST

Test	Before extractor tests passed	After extractor tests passed	Test	Before extractor tests passed	After extractor tests passed
Frequency	1/1	1/1	OverlappingTemplate	0/1	1/1
BlockFrequency	0/1	1/1	Universal	1/1	1/1
CumulativeSums	2/2	2/2	ApproximateEntropy	0/1	1/1
Runs	0/1	1/1	RandomExcursions	7/8	8/8
LongestRun	0/1	1/1	RandomExcursionsVariant	18/18	18/18
Rank	1/1	1/1	Serial	0/2	2/2
FFT	0/1	1/1	LinearComplexity	1/1	1/1

CV-QKD

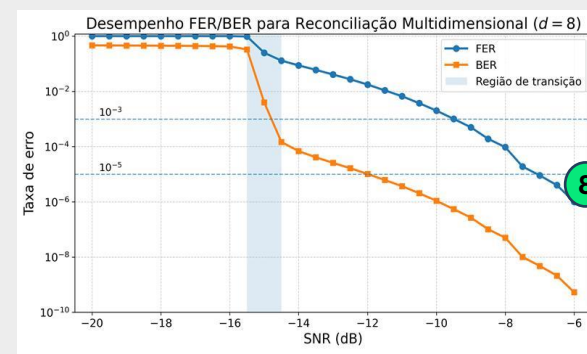


Recuperação de PCS 64-QAM constellation com DSP offline para -50 dBm e 520.83 MBd, usando piloto QPSK

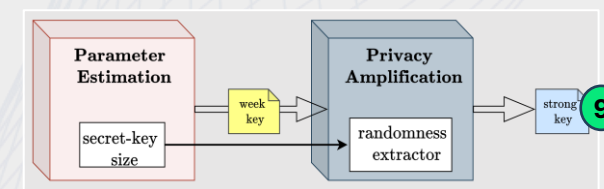


L. Galvão et al., 2026, *Quantum Sci Technol.* [10.1088/2058-9565/ae4268](https://doi.org/10.1088/2058-9565/ae4268)

Estimativa de parametros composível com redes neurais



FER/BER para Reconciliação Multidimensional com códigos MET-LDPC



BR512026004875-3
Framework

REPAQ: Randomness Extraction and Privacy Amplification for Quantum processes

TESTBED PARA APLICAÇÕES

- CV-QKD Comercial
- LuxQuanta
- 1a unidade na America Latina
- Instalada e gerando Chaves

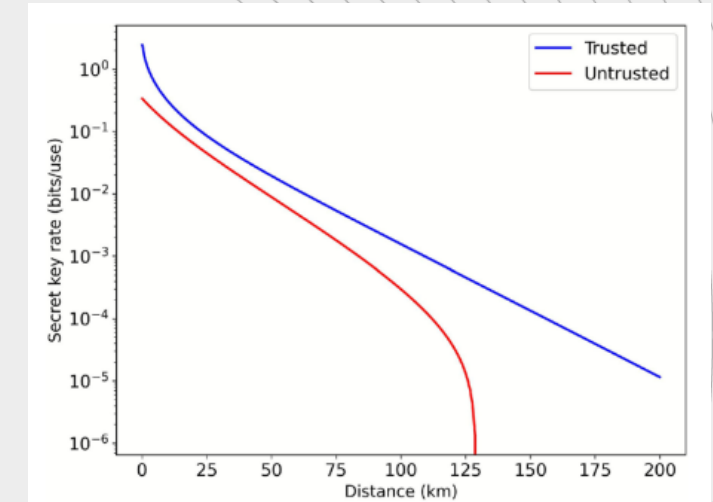
QKD: Aplicações & Casos de Uso



Redes QKD metropolitanas

Desafios

- QKD gera chaves entre 2 pontos
- Taxa de chaves cai exponencialmente com a distância
- Co-existência com canais clássicos



CV – QKD

Menor alcance – até 20 dB

Menos Sensível à presença de outros canais



Transmissão na banda C possível

DV – QKD

Maior alcance – até 30 dB

Sensível à presença de outros canais

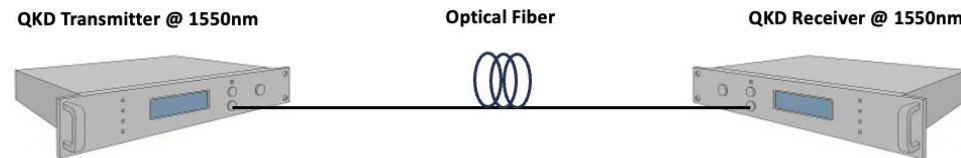


Transmissão na banda O, adição de filtros, fibras especiais (ocas e multicore) ou fibra dedicada

Alternativas

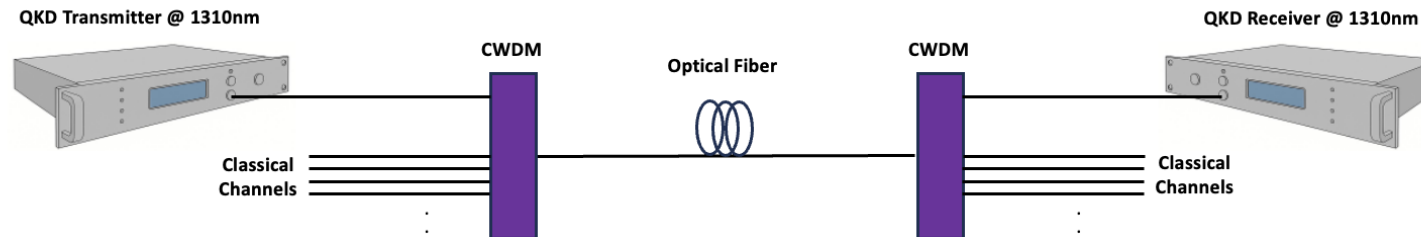
Fibra apagada @ C-band: $\sim 0,2$ dB/km

(a)



Fibra instalada @ O-band: $\sim 0,35$ dB/km + 2.0 dB

(b)



Redes quântica metropolitanas

Desafios

- QKD gera chaves entre 2 pontos
- Taxa de chaves cai exponencialmente com a distância
- Co-existência com canais clássicos

Maker	Model	Protocol		Max SKR (kbps)	Loss Budget (db)
IDQ	Clavis XG	DV-QKD	Decoy-State BB84	~50 (700,000 AES-256/h)	24 dB or 30 dB
HEQA Security	Sceptre Duo	DV-QKD	Decoy-State BB84	20 @ 1550 nm 18 @ 1310 nm	20 dB
Toshiba	Long Distance	DV-QKD	Decoy-State BB84	300 @10 dB	30 dB (150km)
Toshiba	Multiplexed	DV-QKD	Decoy-State BB84	300 @ 10 dB	30 dB (90 km)
Luxquanta	Nova LQ	CV-QKD	GG02	not publically disclosed	12 dB (old)) 20 dB (new)

Resiliência de link virtual na rede metropolitana de Salvador

Objetivo:

1. Condições de operação não ideais.
2. Entender a influência da camada de gerenciamento de chaves
⇒ BasejumpSIM da evolutionQ

Topologia: subconjunto da REMESSA (Rede Metropolitana de Salvador com 4 nós e links físicos:

Link	Capacity (keys/s)	Demand (keys/s)
100-101	39	5
100-103	17	5
101-102	44	5
102-103	21	5
100-102	0*	39

Note: keys/s denotes keys per second, where each key has a length of 256 bits. *Indirect link (no direct physical QKD link).

M. de Araujo et al, ICTON 2026
QuIN/UFBA/evolutionQ

Rotas:

- Rota primária A: 100-101-102
- Rota secundária B: 100-103-102

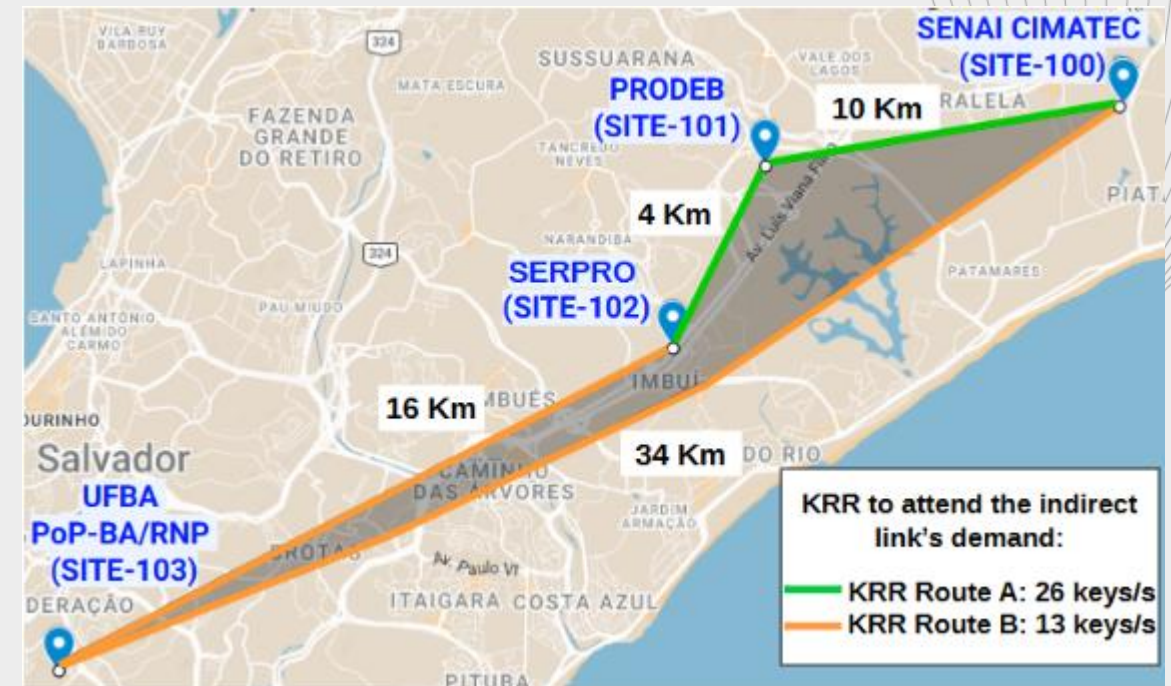
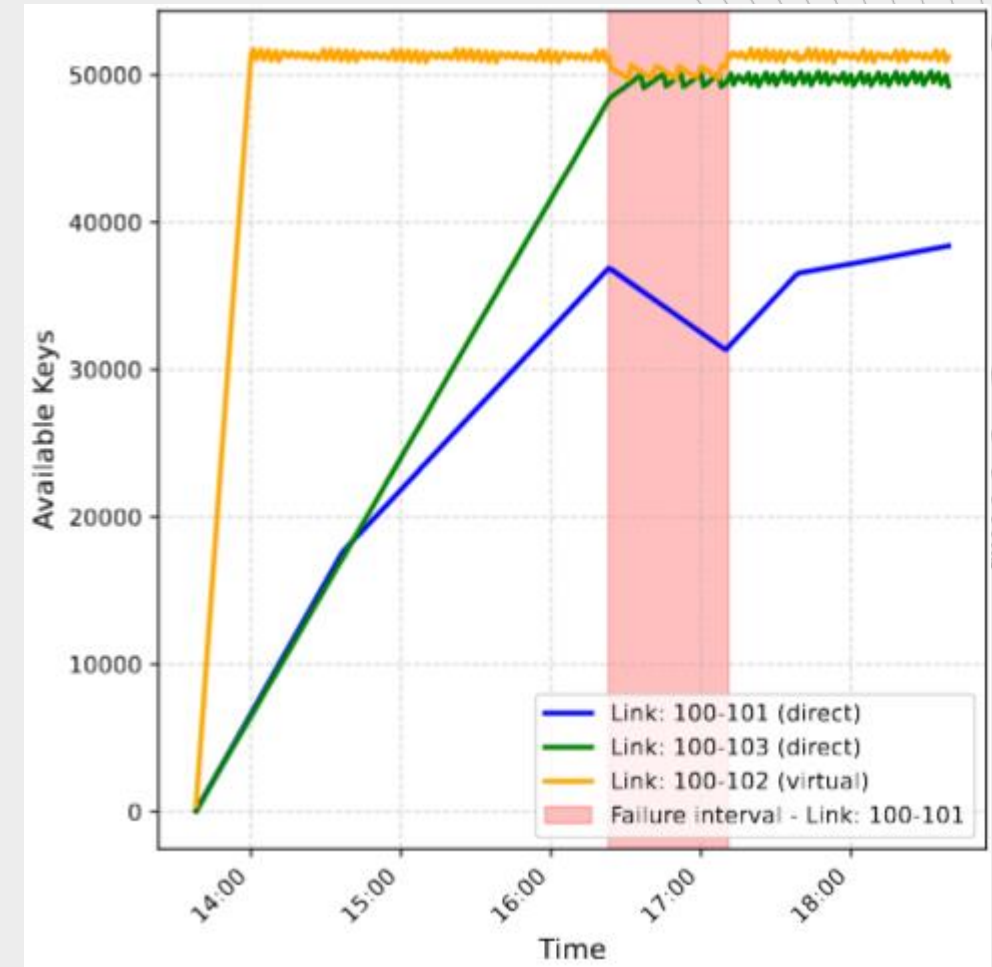
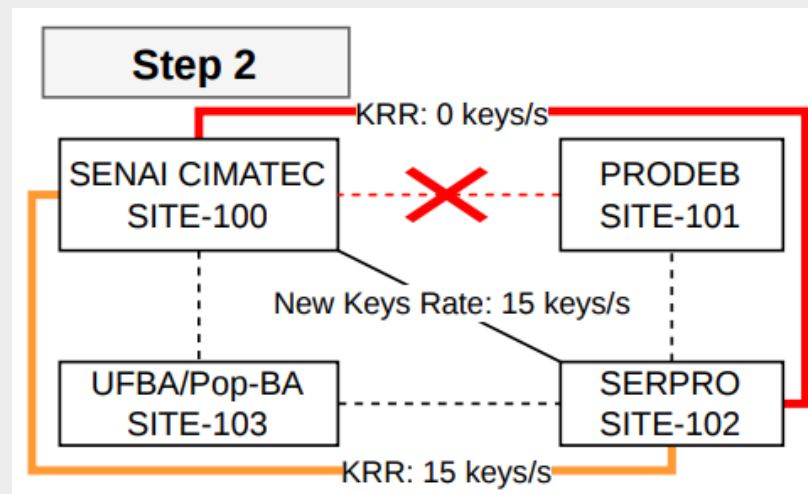
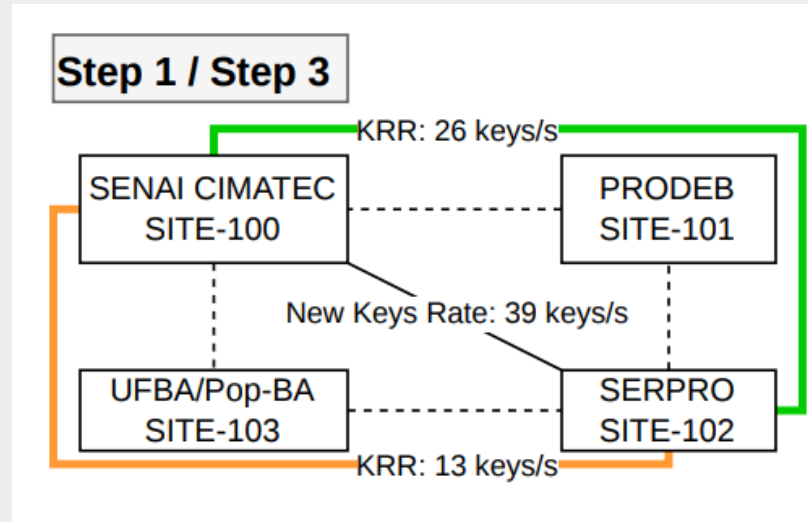


Fig.1: Há duas rotas, A e B, possíveis para conectar o link virtual, com demandas (key relay rate - KRR) de 28 e 13 chaves por segundo, respectivamente.

Quantidade de chaves disponíveis para consumo no link virtual



Oportunidades

Tecnologias Quânticas para comunicação segura estão chegando ao mercado mas ainda há muitas oportunidades

- QRNGs
 - Otimização da fonte de entropia (custo vs taxa de chaves)
 - Otimização dos extratores
 - Aceleração por hardware
 - PIC
- QKD
 - CV-QKD traz oportunidade de coexistência com tráfego clássico e potencial para integração e redução de custo
 - Sistemas híbridos podem trazer o melhor de 2 mundos
- Sistema de gerenciamento de chaves (KMS)
 - Permitem estratégias para redes resilientes a falhas e links virtuais

Visão e Futura

Criptografia Quântica | Distribuição de Chaves Quânticas | *Quantum Key Distribution (QKD)*



- DV/CV - QKD
- FSO - QKD
- QKD Network: Classical-Quantum



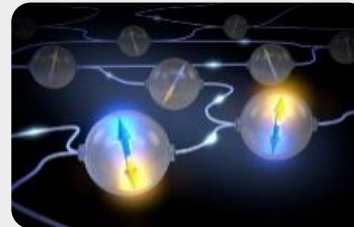
Quantum Random
Number Generation
(QRNG)



PQC: Post Quantum
Cryptography
(**mecânica quântica**)

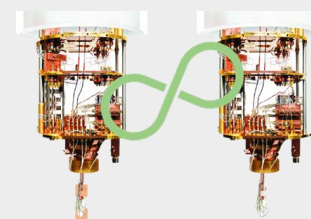
Dias de Hoje

Redes Quânticas

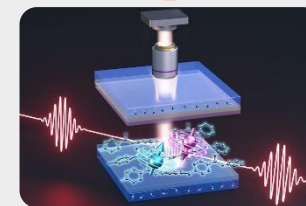


- QKD MDI (Entanglement Based)
- Entanglement Distribution
- Quantum Memories / Repeater

Computação Quântica Distribuída



Internet Quântica



**Sensores Quânticos
Distribuídos**



**Computação Quântica
em Nuvem as Cegas**



Obrigada!

Dr. Valeria Loureiro da Silva

Coordenadora

QuIIN - SENAI CIMATEC

Valeria.dasilva@fieb.org.br



**SENAI
CIMATEC**
Empresa Brasileira de Pesquisa
e Inovação Industrial

EMBRAPPI
Empresa Brasileira de Pesquisa
e Inovação Industrial

MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÃO

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO