QuIIN
Quantum Industrial Innovation

Comunicação Quântica: Oportunidades & Desafios

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

WRNP, Maio 2026

SENAI CIMATEC

EMBRAPII
Empresa Brasileira de Pesquisa e Inovação Industrial

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO

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

QuIIN & Cimatec

SENAI CIMATEC
Sede

- Fundado em 2002, localizado em Salvador, BA
- Universidade e Centro Tecnológico focado no Desenvolvimento de solutções para a industria

06
Campii

3400
Colaboradores e bolsistas

44
Areas de competência

CONFIDENCIAL
CONFIDENTIAL

QuIIN

Quantum Industrial Innovation

13
Projetos

100+
Pesquisadores, bolsistas e estudantes

8
Startups em tecnologias quânticas

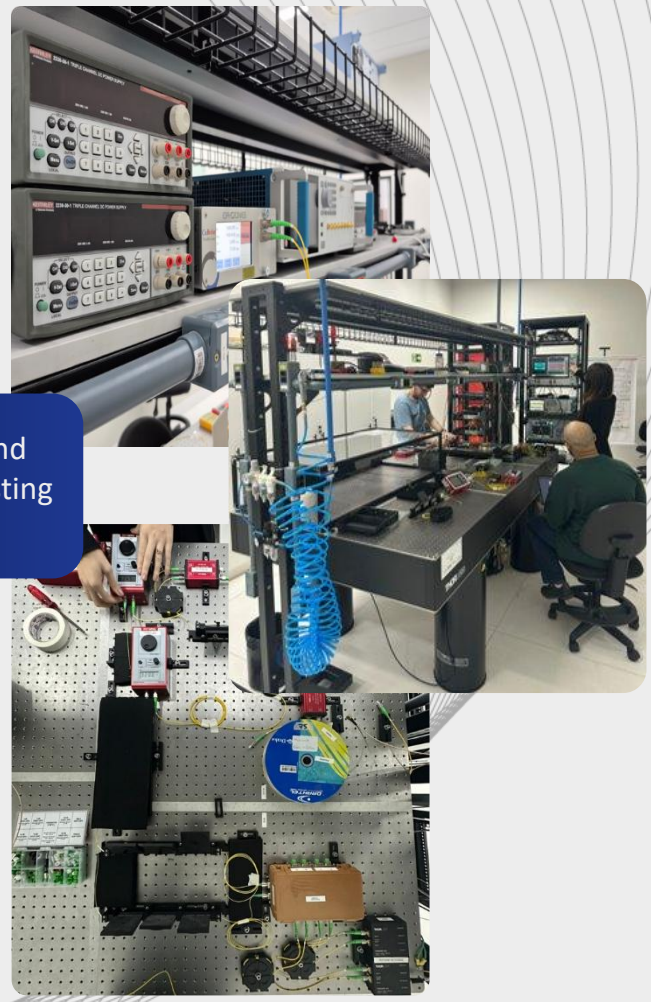
Quantum Information Theory and Security Analysis

Quantum Network Modeling and Quantum Classical Integration

CV-QKD

Coherent Communication and Optical System Design and Testing

DSP and Post-Processing Hardware



MERCADO POTENCIAL PARA TECNOLOGIAS QUÂNTICAS ATÉ 2040

USD **$198BI**

($0.9-2.0T Economic Value)

Computação Quântica

$45B – 131B*

Comunicação Quântica

$24B – 36B*

Sensores Quânticos

$18B – 31B*

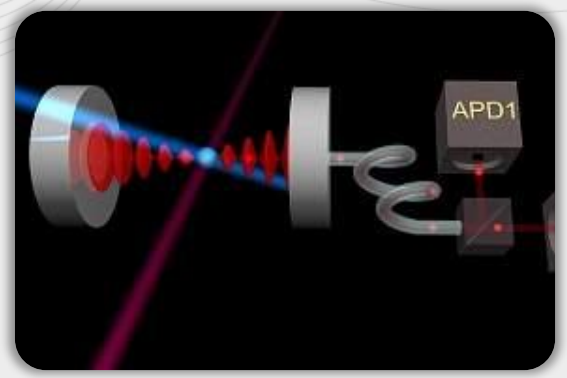
*Mercado estimado até 2040

Fonte: Quantum Technology Monitor – McKinsey & Company - June 2025

Tecnologias Quânticas 2.0

Quantum Computing

Quantum Communication and Cryptography



Quantum Sensors

QUANTUM INFORMATION & QUANTUM MECHANICS

Computação Quântica
Sonho ou Pesadelo?

Otimização

Problemas de Logística

Portfolios e Risco

Inteligência Artificial

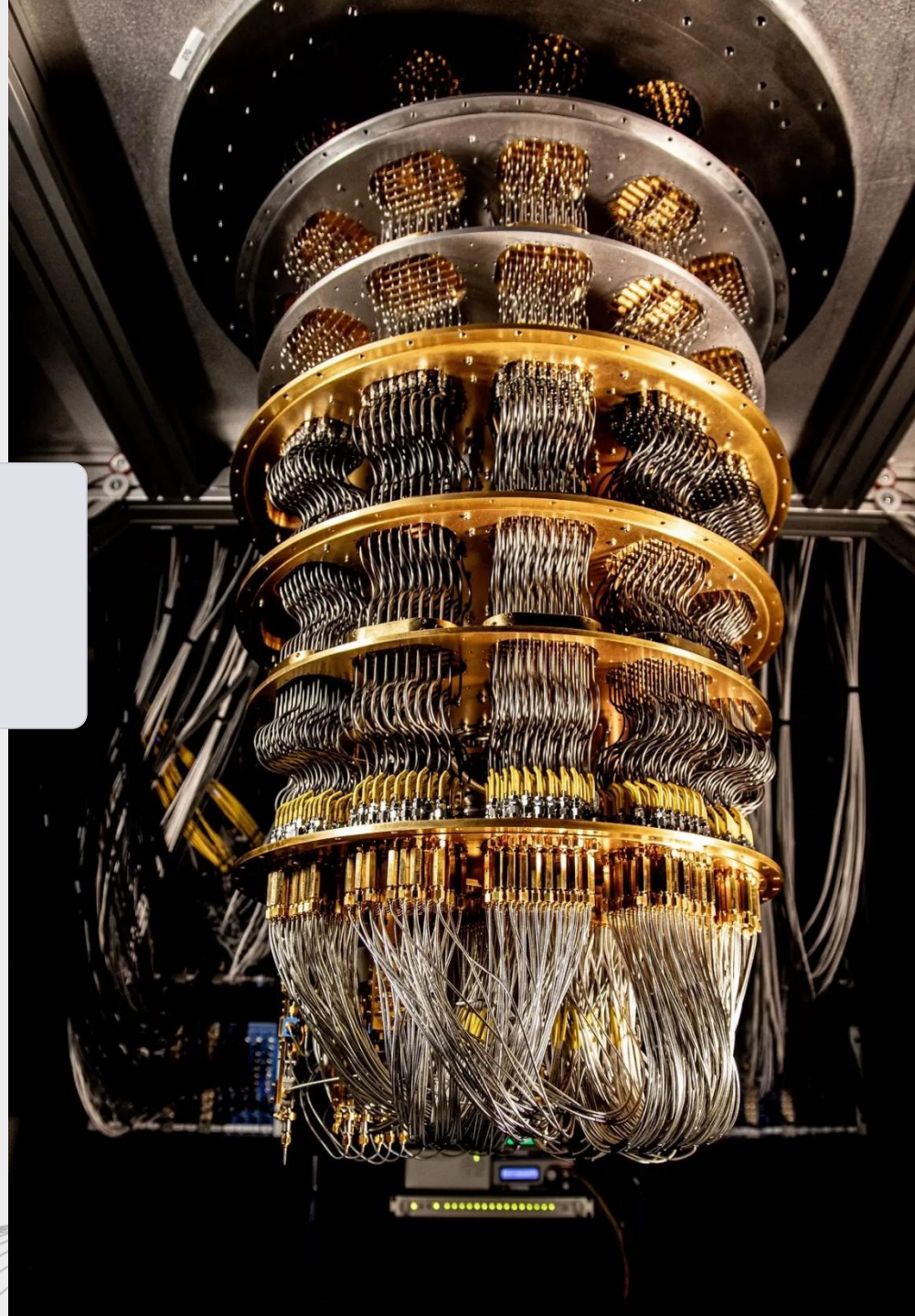
Modelos mais compactos

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

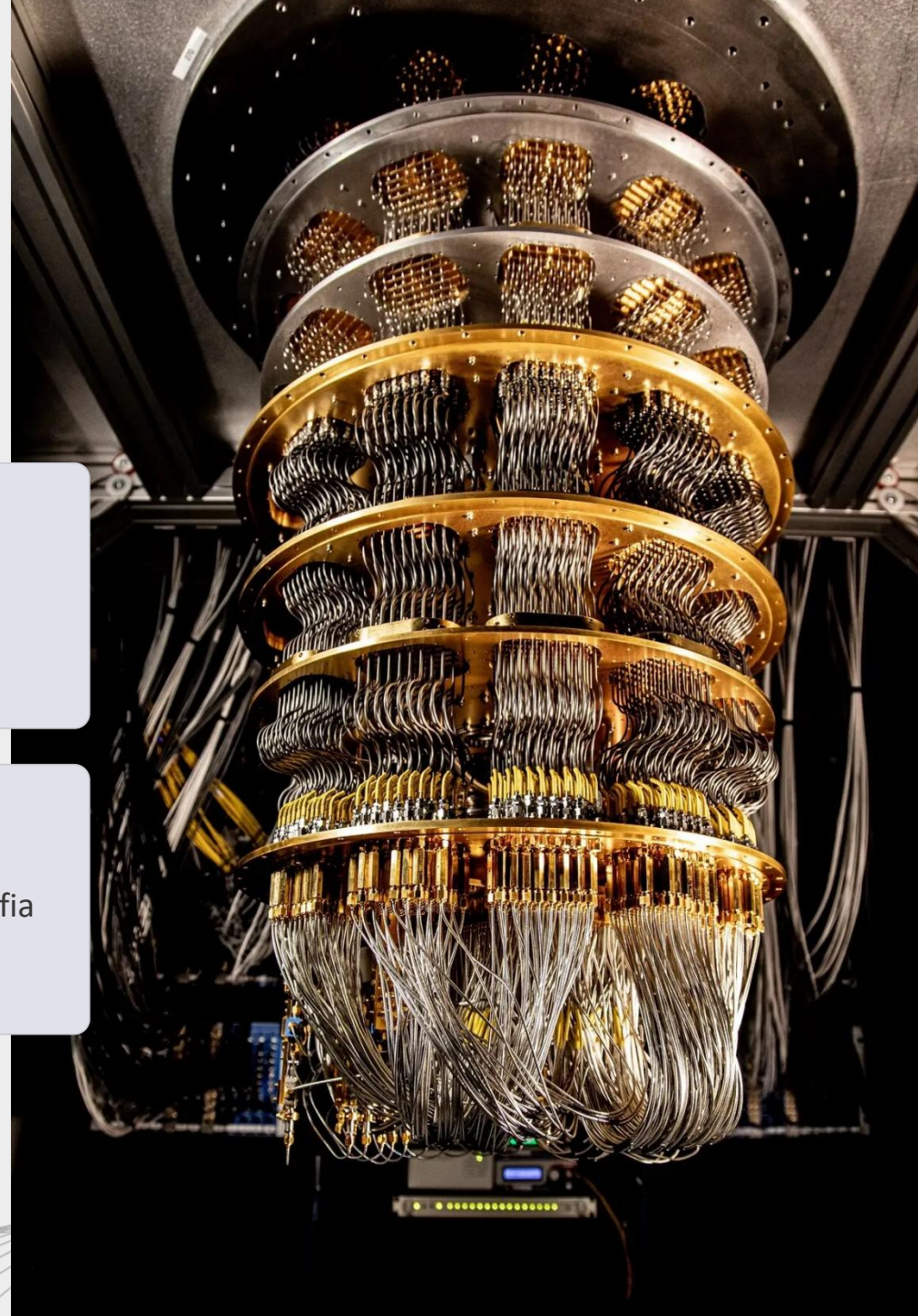
Simulações

Modelos moleculares precisos

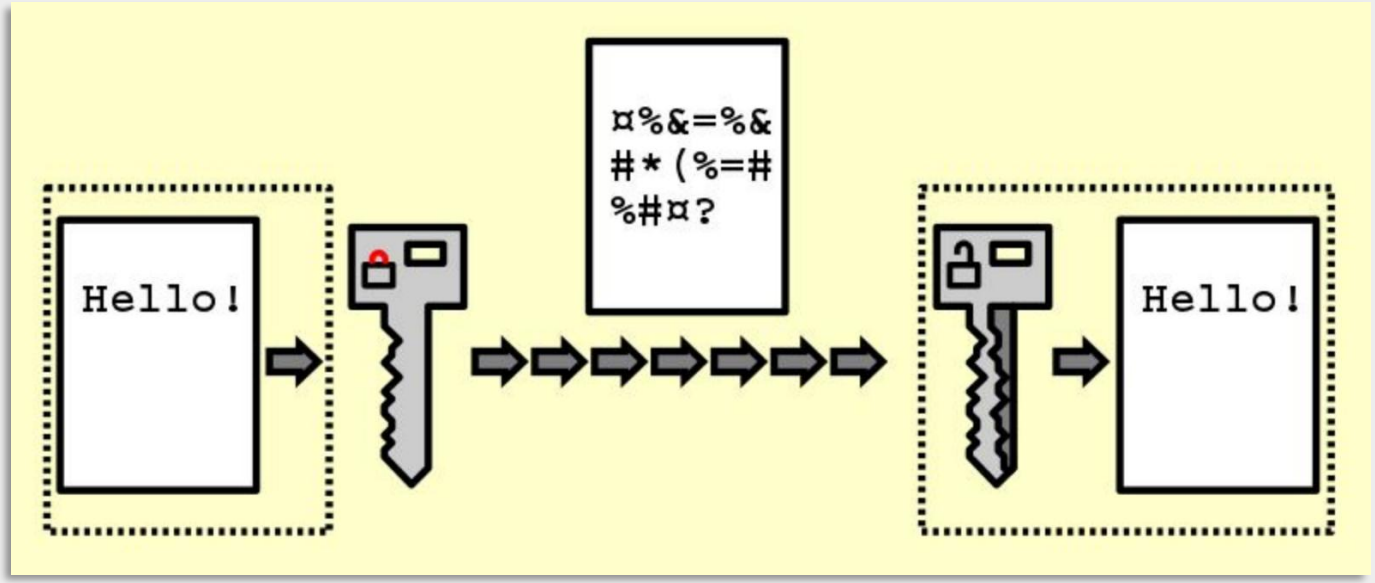
Novos materiais

Criptanálise

Quebra de chaves de criptografia



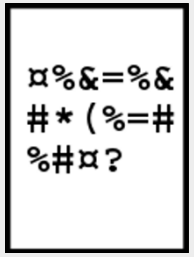
Criptografia



Source: Wikimedia Commons, Public_key_encryption_keys.png,

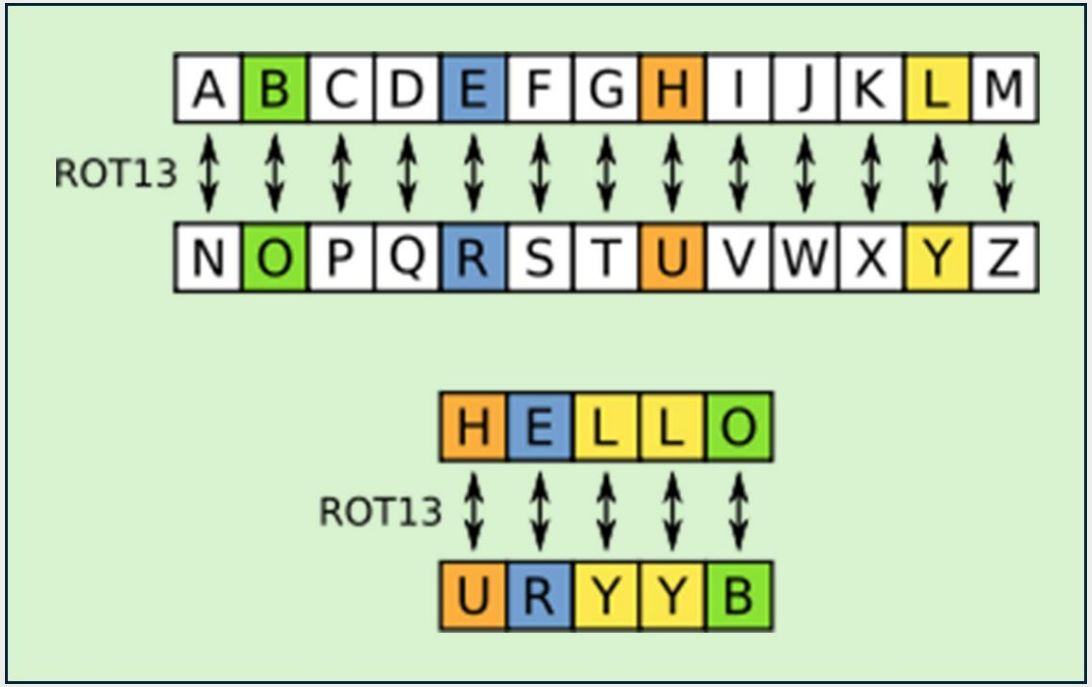
Message

Key

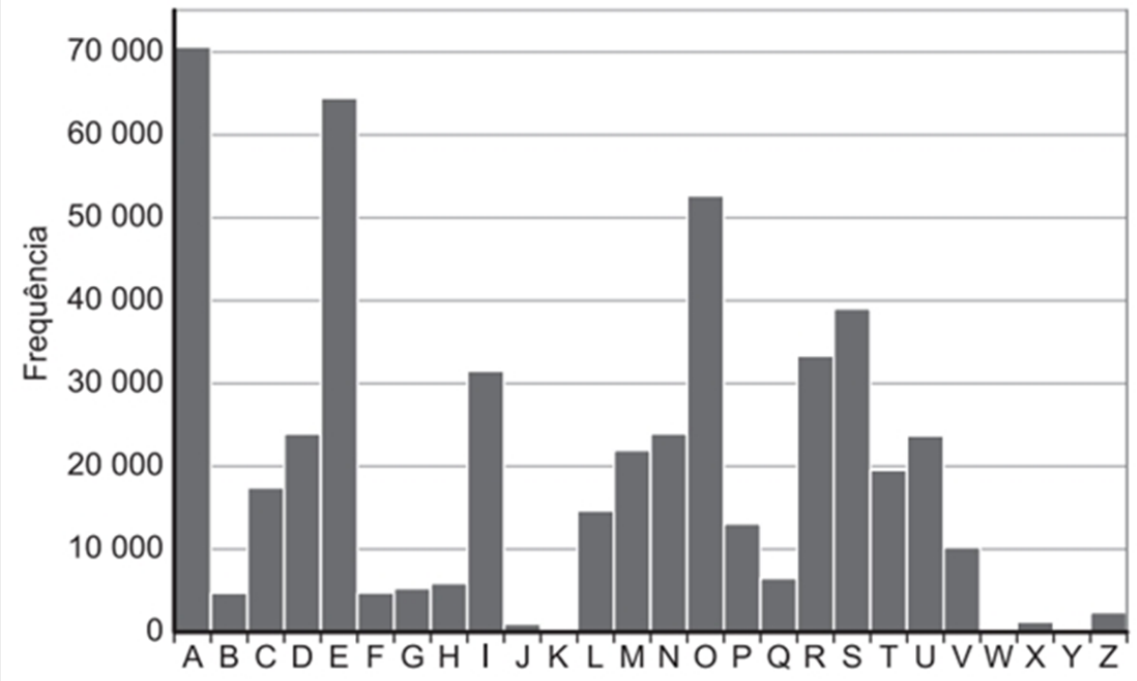


Cypher

Criptografia

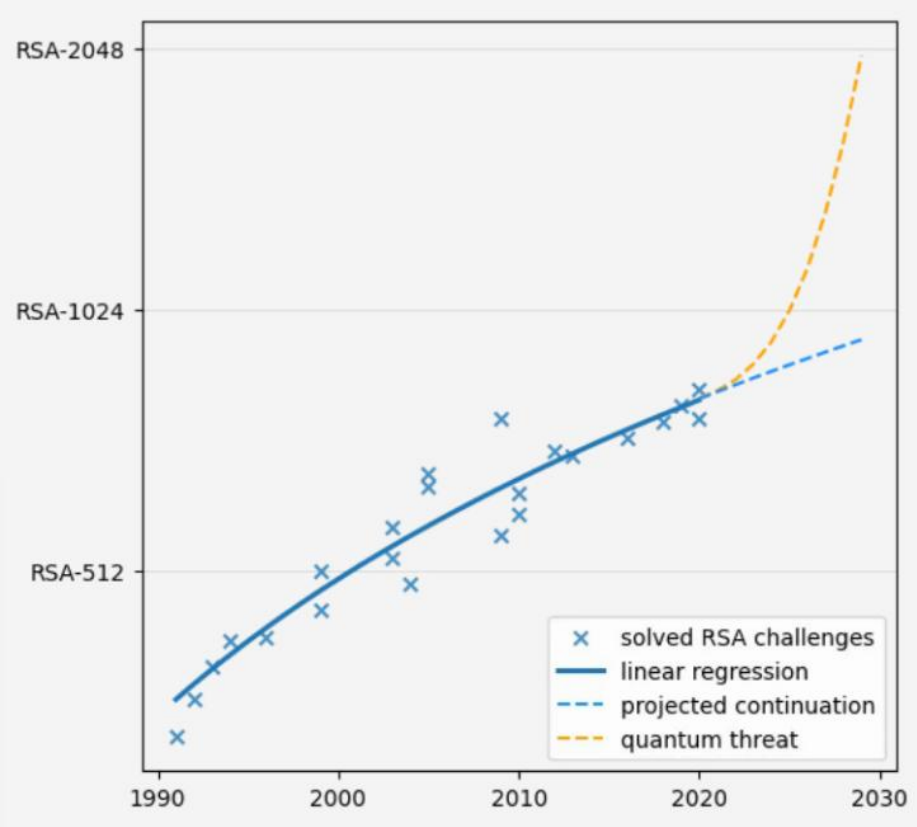


Decodificação por frequência



Criptografia segura requer técnicas mais elaboradas que eliminem padrão → Geradores de números aleatórios

Ameaça Quântica



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

Algoritmo de Shor quebra chaves assimétricas (ex: RSA)

Algoritmo de Grove enfraquece chaves simétricas (ExS: AES)

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 matemá tica
- Pode não resistir ao tempo
  - Aparecimento de algoritmos mais eficientes
  - Evolução do poder computacional.

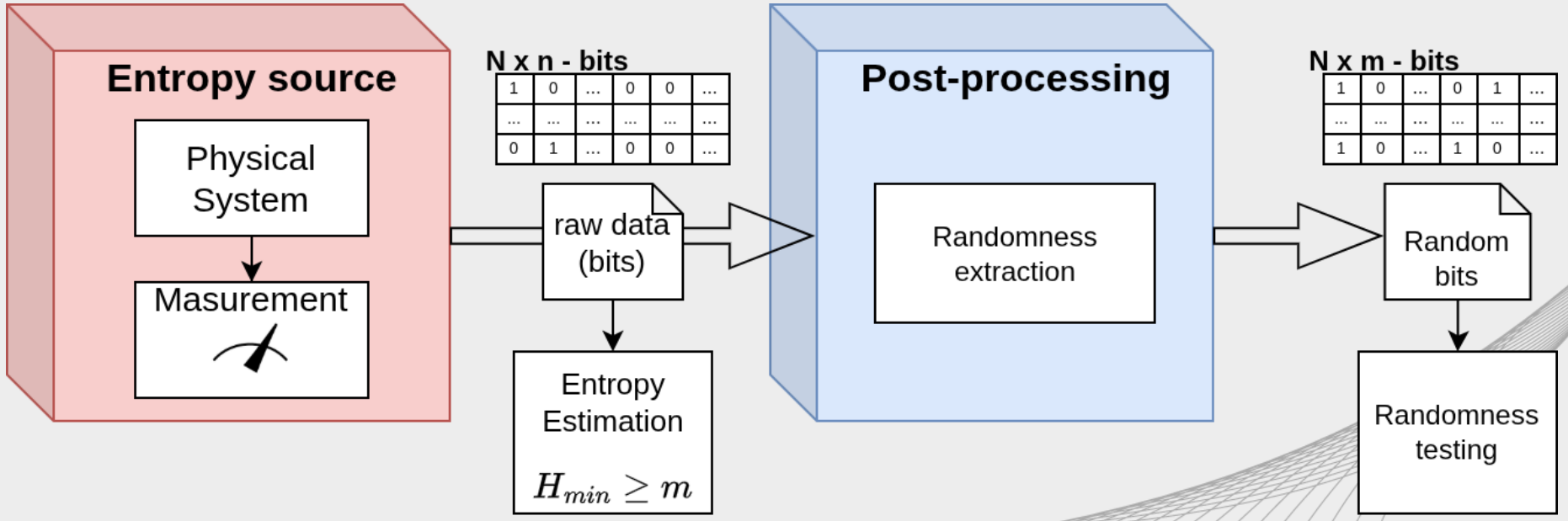
Criptografia Quântica (QKD)

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

Solução ótima utiliza combinação dessas tecnologias

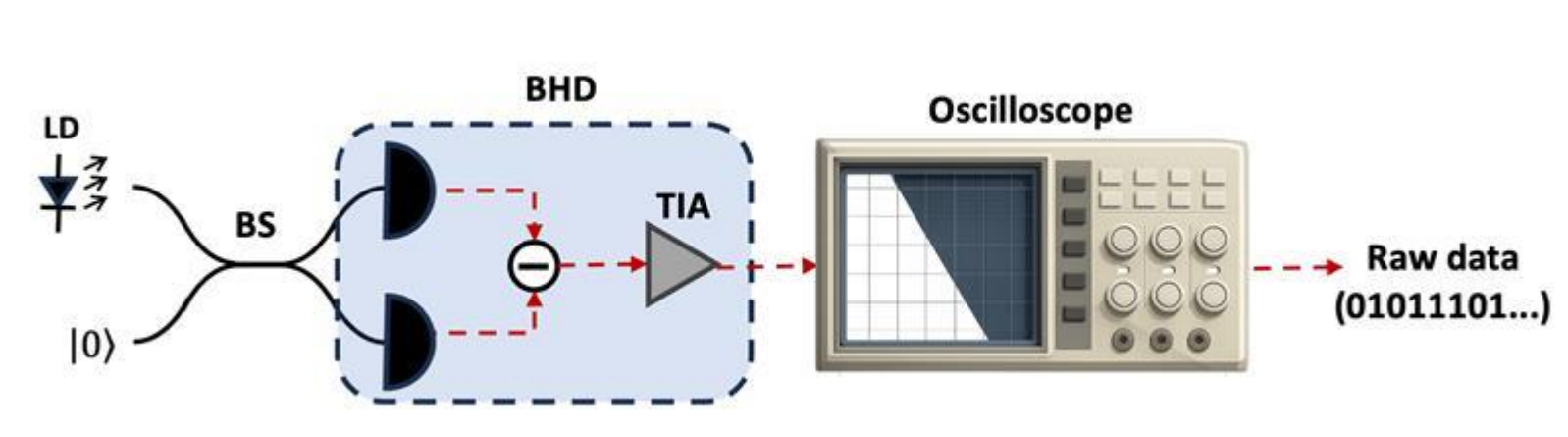
Quantum Random Number Generator

PRNGs – algoritmos determinísticos – padrão
QRNGs – usa aleatoriedade intrínseca da teoria quântica

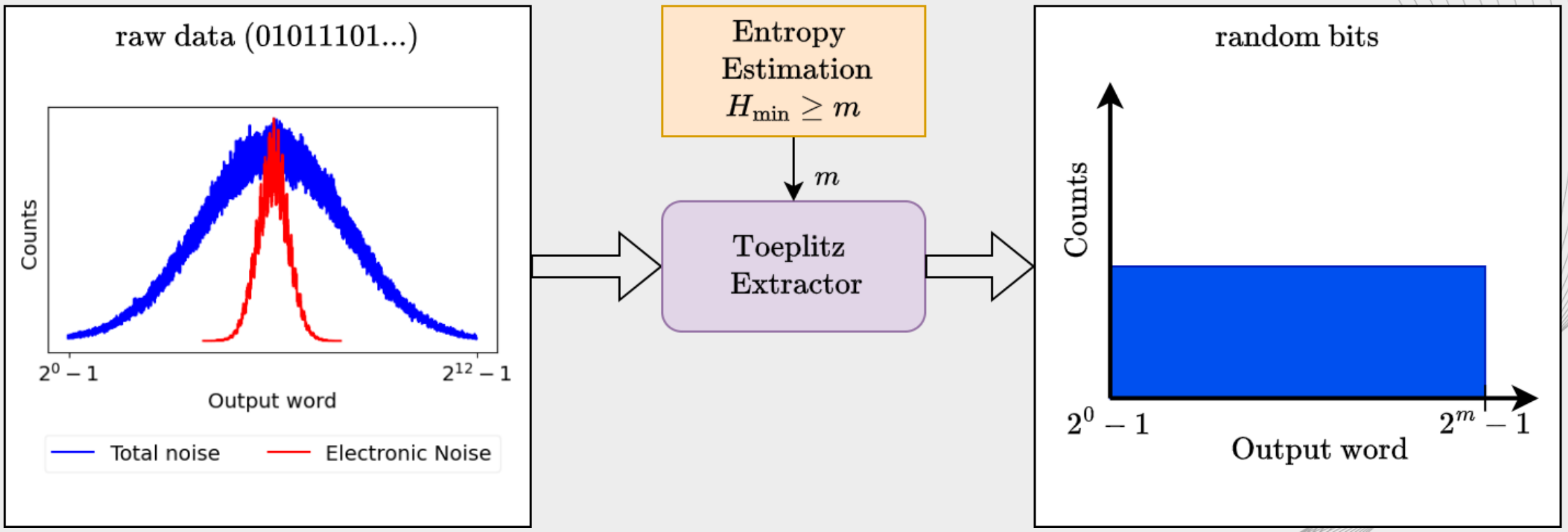


Resultados preliminares:

Batimento com o vácuo com processamento offline



Post-processing



In our setup, we achieved H_{min} = 10.61 bits compared to 12 bits for each raw sample.

Testes aleatoridade

Table 1 | Results from statistical tests NIST to analyse randomness .

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

QRNG - Desafios e oportunidades

- Proximos passos: implementação em hardware do pós-processamento

- Desafios
  - Fontes de entropia: custo x velocidade

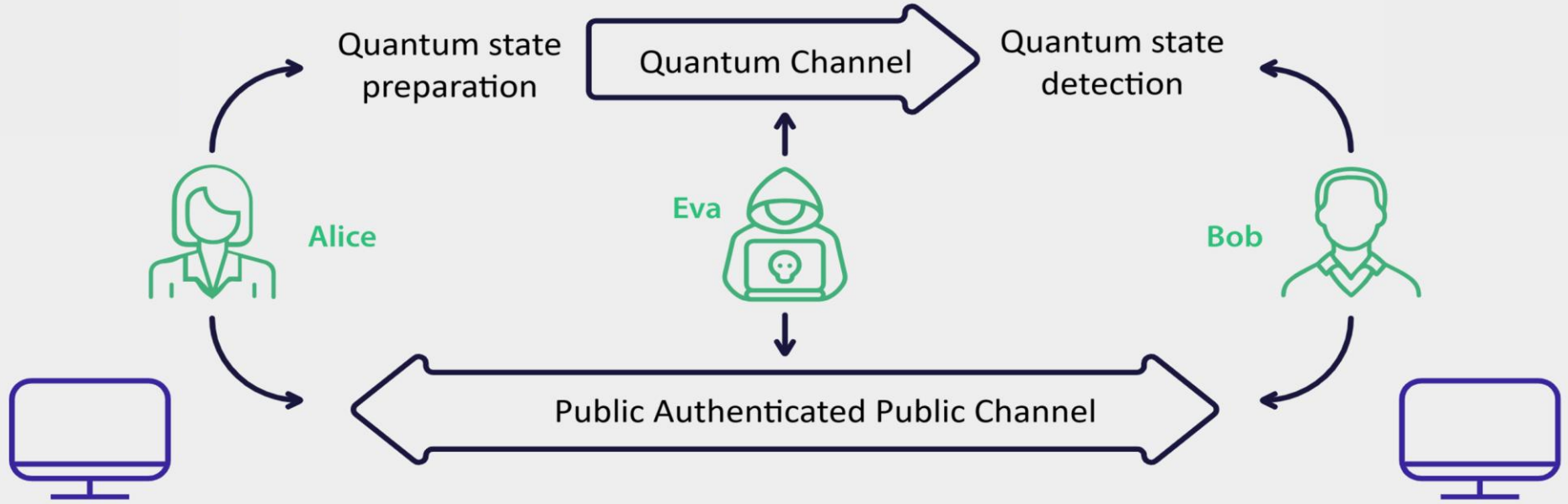
  - Extratores: eficiência computacional e aceleração de hardware

- Trabalho correlato:

⇒ paper "Análise de PRNGs em Hardware para Otimização de Memória na Amplificação de Privacidade em CV-QKD", quarta, 11h na sala Tartaruga

Quantum Key Distribution (QKD)

Cenário Prepara & Mede



0100101110110110 - Message

⊕ 1101010110101011 - Key

1001111000011101 - Cypher

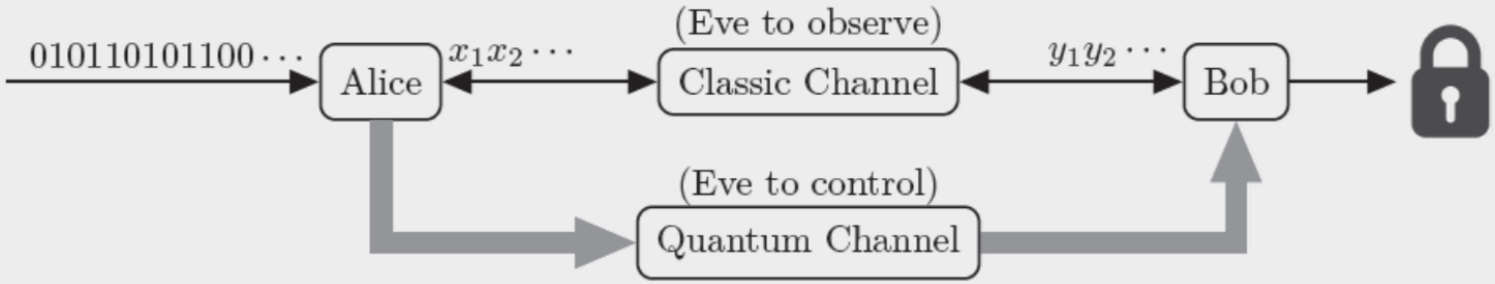
1001111000011101 – Cypher

⊕ 1101010110101011 - Key

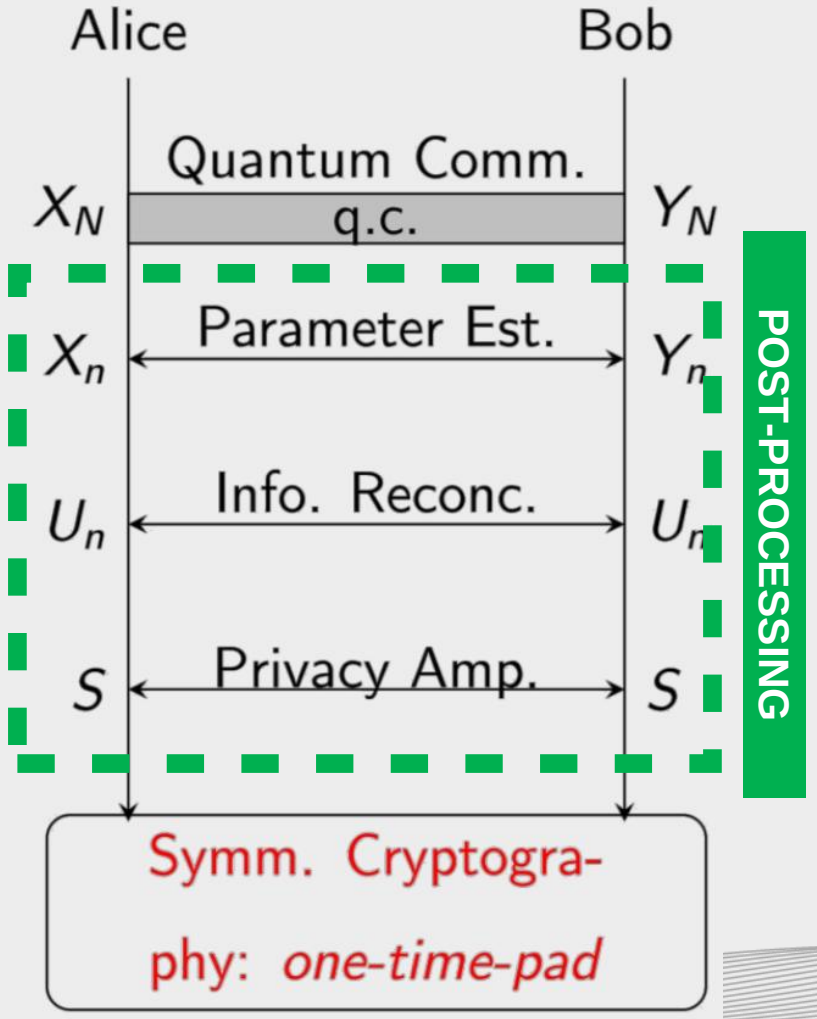
0100101110110110 - Message

Quantum Key Distribution (QKD)

Cenário Prepara & Mede



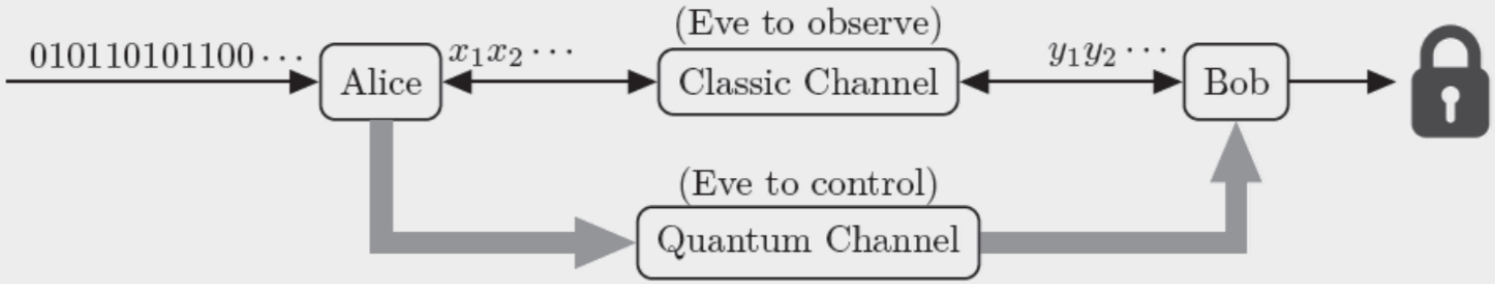
	Discrete Variables	Continuous Variables
Key encoding	Single photon polarization	Field quadrature modulation
Detection	*Single photon detecion*	Coherent (homodyne/heterodyne)
Post processing	Low complexity	High complexity: Low SNR, DSP Stack, LDPC w/ unusual lengths



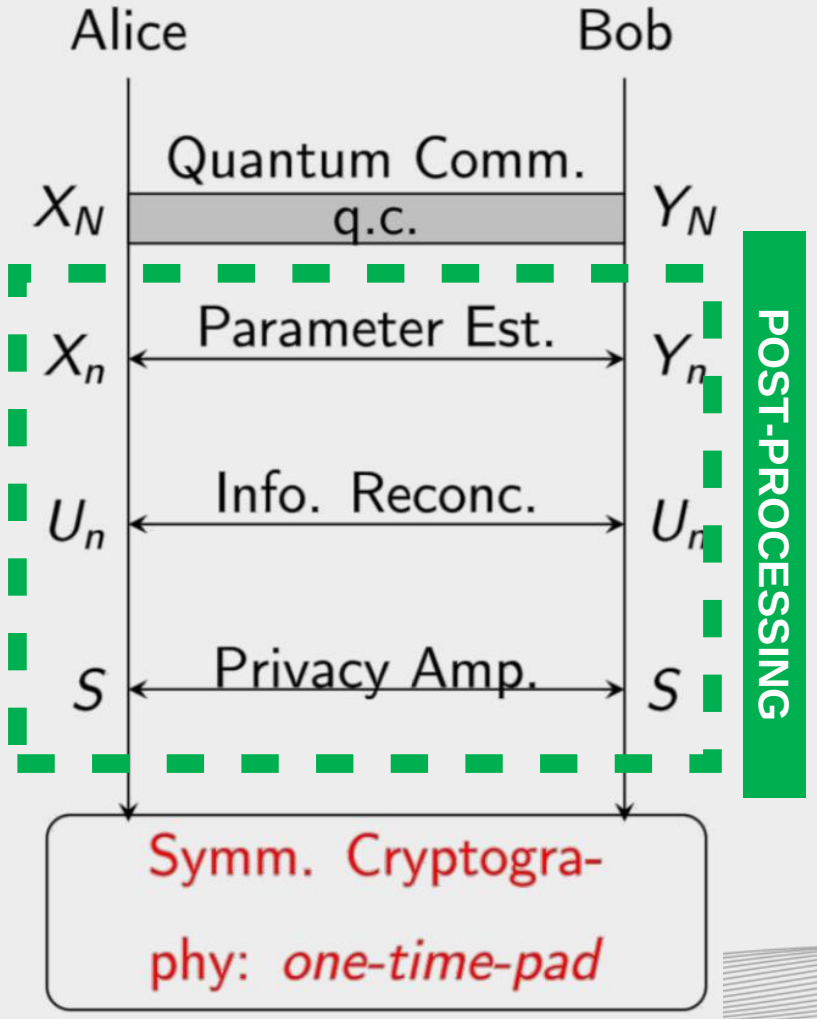
V. Da Silva et al. 2025 SBMO/IEEE MTT-S International Microwave and Optoelectronics Conference (IMOC)

Quantum Key Distribution (QKD)

Prepare-and-measure scenario



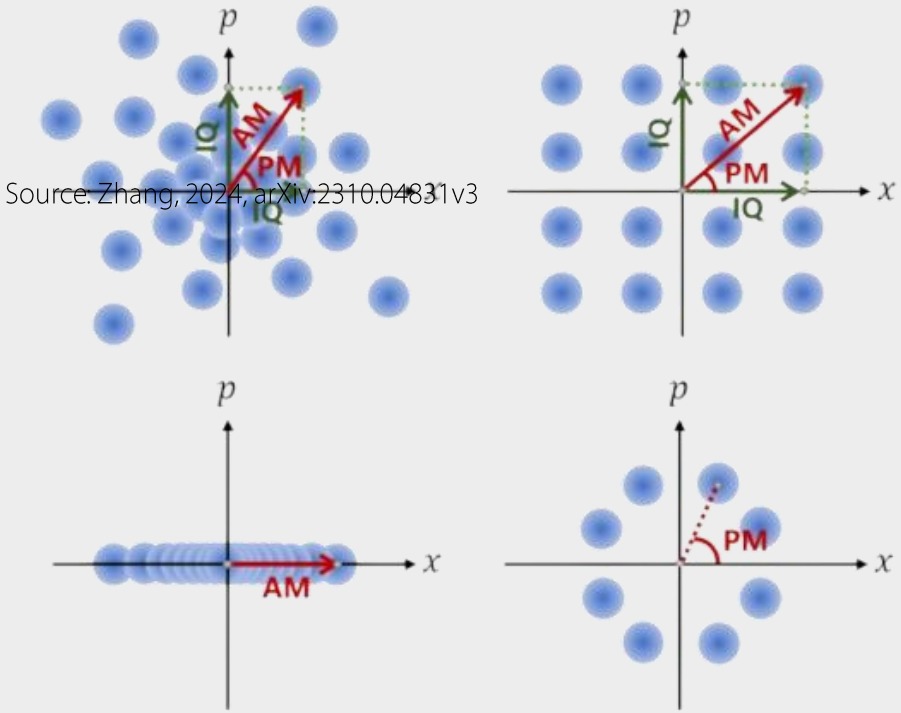
	Discrete Variables	Continuous Variables
Key encoding	Single photon polarization	Field quadrature modulation
Detection	*Single photon detecion*	Coherent (homodyne/heterodyne)
Post processing	Low complexity	High complexity: Low SNR, DSP Stack, LDPC w/ unusual lengths



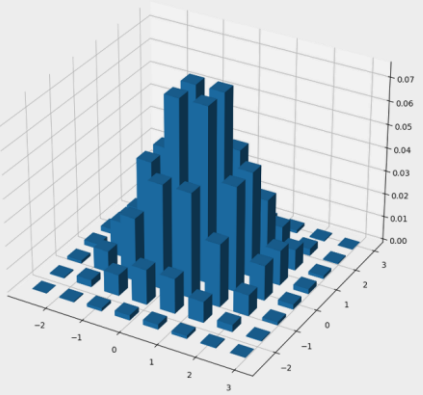
V. Da Silva et al. 2025 SBMO/IEEE MTT-S International Microwave and Optoelectronics Conference (IMOC)

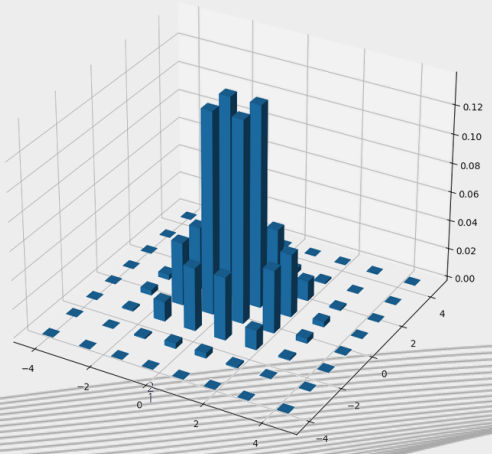
CV-QKD P&M Protocols – Essentials

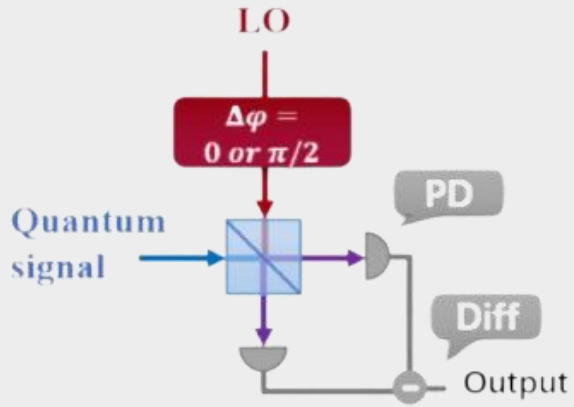
- State (coherent, squeezed, displaced thermal)
- Modulation (Gaussian or discrete–PSK, ASK, APSK, QAM)
- Detection (homodyne, heterodyne)

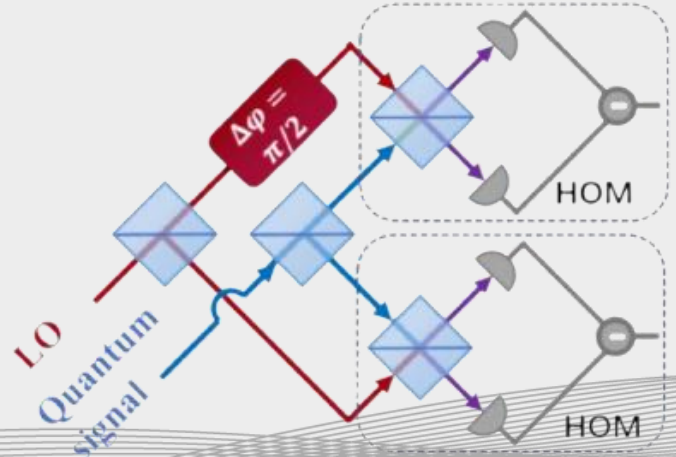


Source: Zhang, 2024, arXiv:2310.04831v3

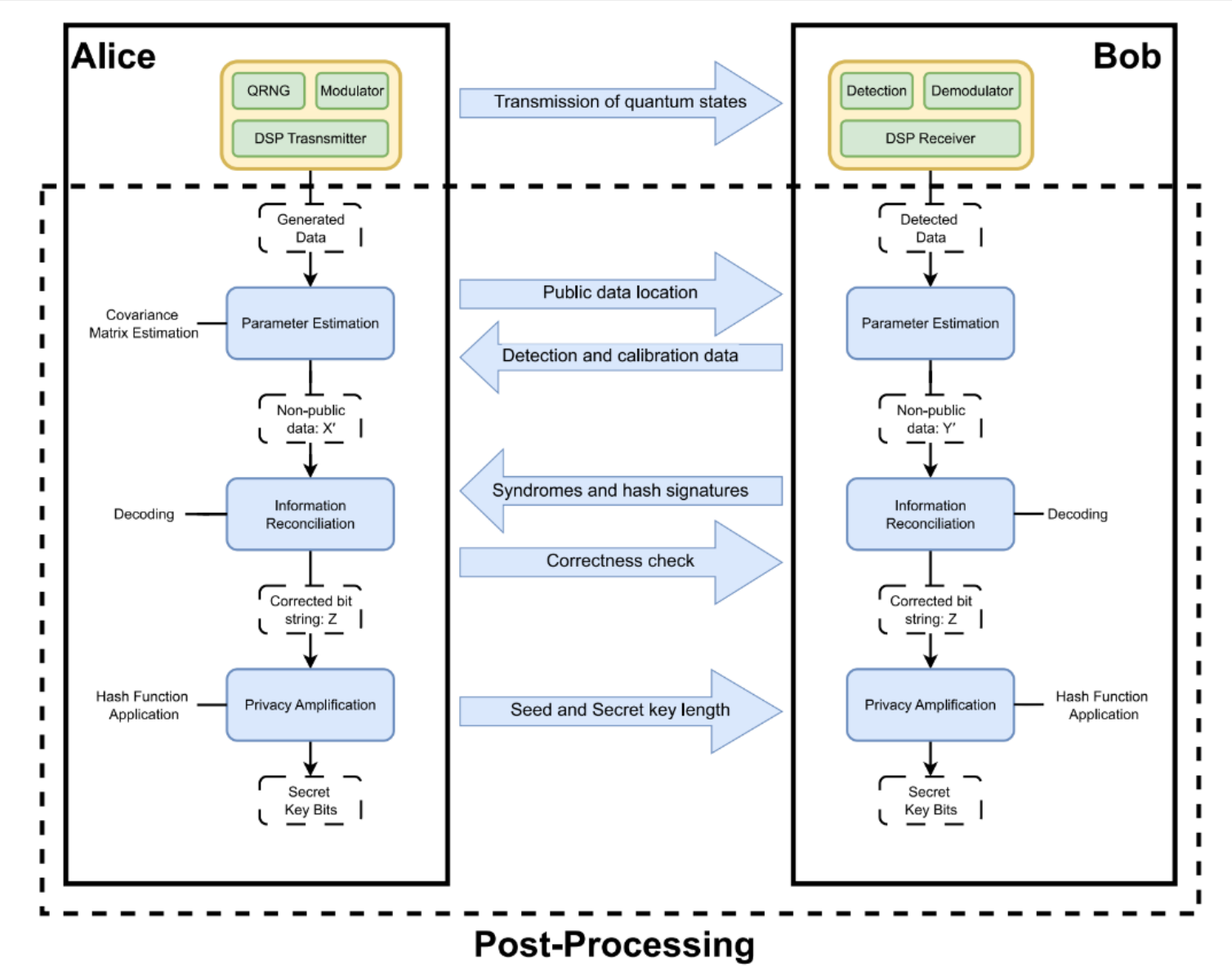






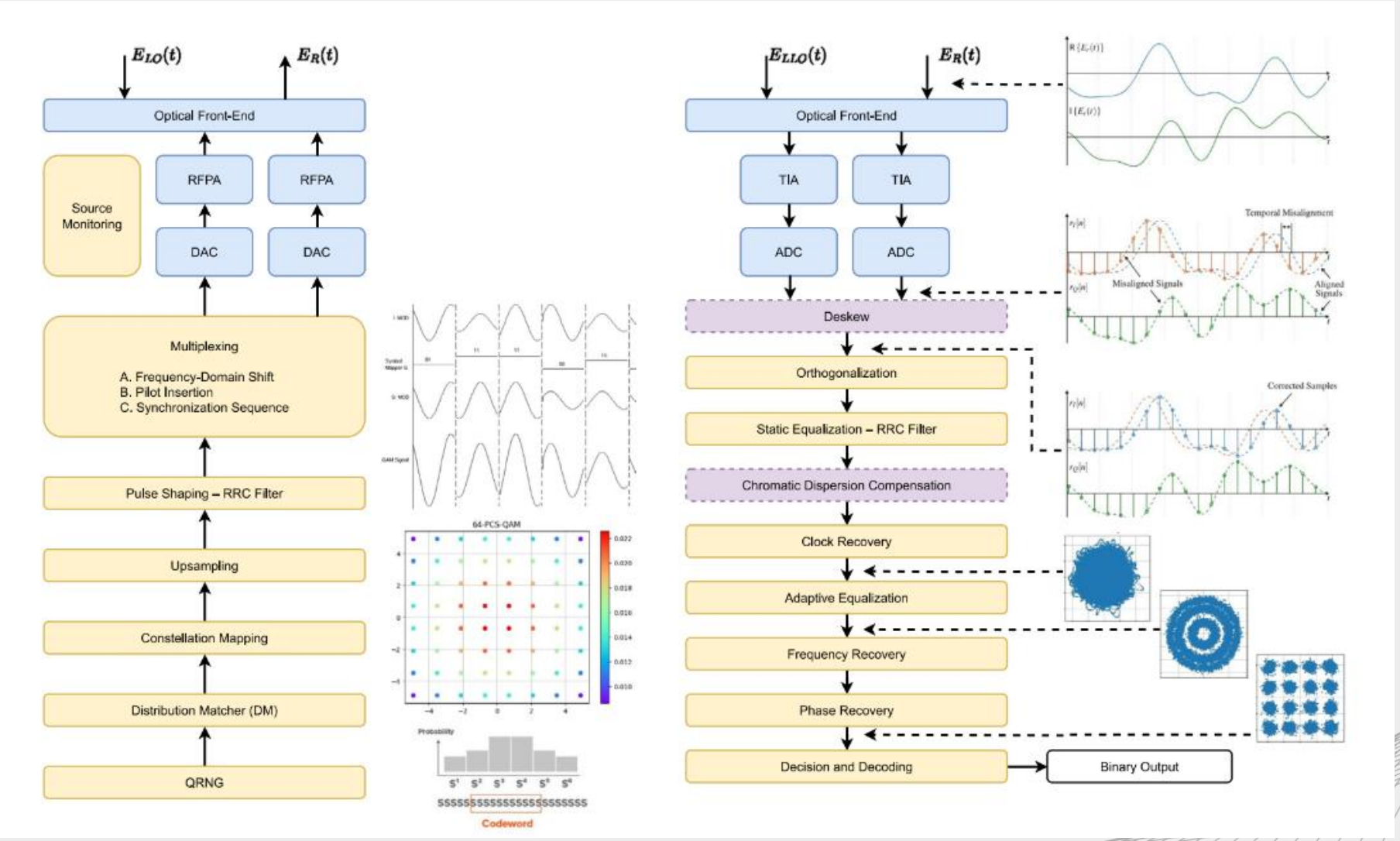


CV-QKD Post-processing



De Sousa et al., Brazilian Journal of Physics (2026) 56:106
https://doi.org/10.1007/s13538-026-02023-9

DSP Simulation Framework

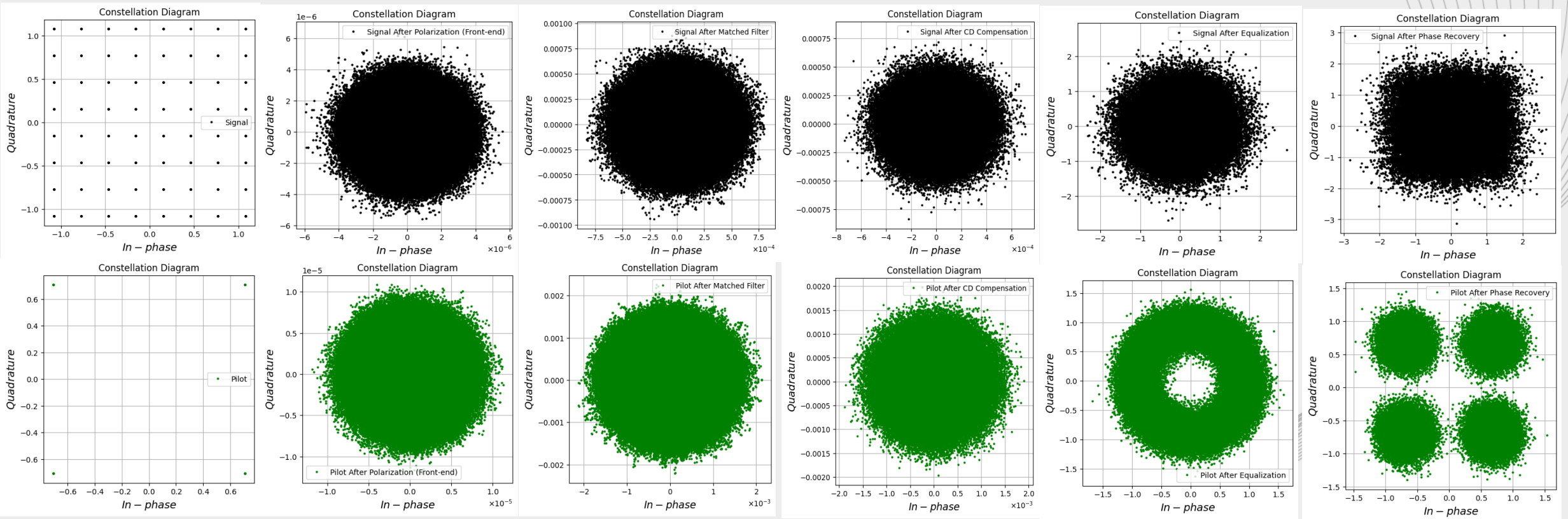


De Sousa et al., Brazilian Journal of Physics (2026) 56:106
https://doi.org/10.1007/s13538-026-02023-9

RX DSP Framework - simulation results

5km SMF-28 fiber, 1 kHz laser linewidth

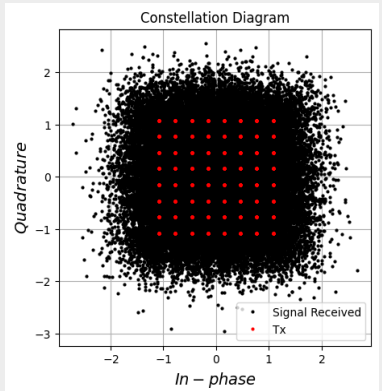
After ADC | After Matched Filter | After Disp. Comp. | After Dyn. Equal. | After Phase Recovery

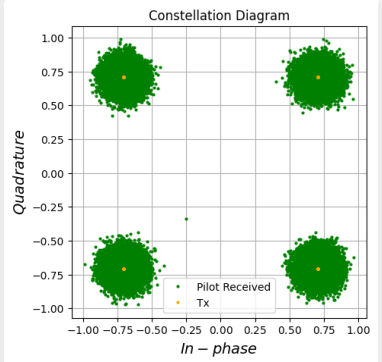


RX DSP framework - simulation results

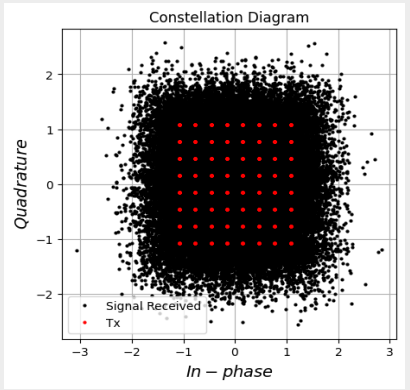
5km SMF-28

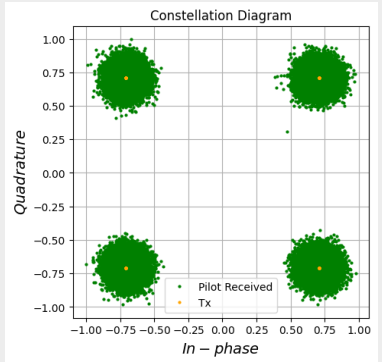
- Identical Laser Linewidth for Transmitter and LLO



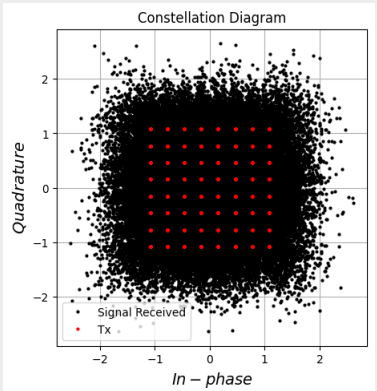


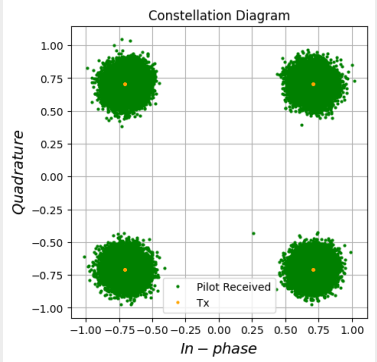
Laser Linewidth: 100 Hz



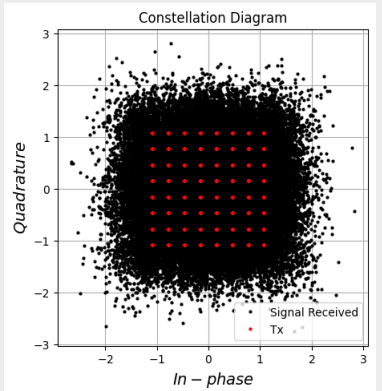


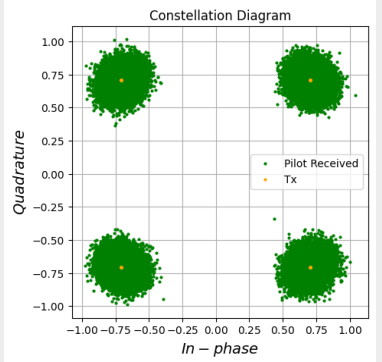
Laser Linewidth: 1 KHz



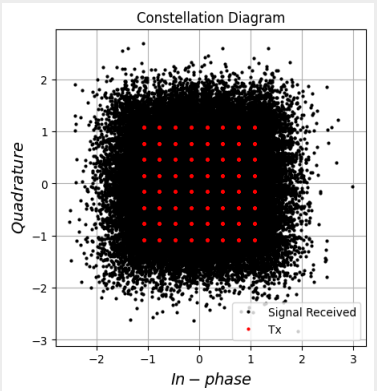


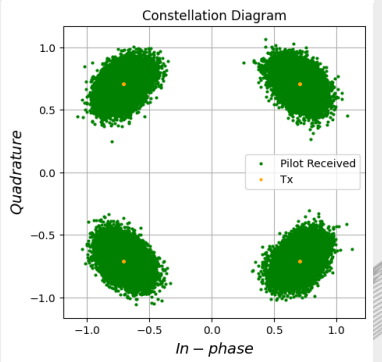
Laser Linewidth: 10 KHz





Laser Linewidth: 25 KHz





Laser Linewidth: 100 KHz

Impact on phase recovery noise vecomes significant for linewidths above 10 kHz

Tratamento do ruido na análise de segurança

- Paranoia assumes that all information losses and noises are due to Eve´s presence
- Security analysis of worst-case performance may overestimate Eve´s information access and reduce the SKR
- Trusted noise model: exclusion of detector´s noise and efficience from total excess noise attributed to Eve
- No-swithing protocol: simultaneous detection of both quadratures with double homodyne detection

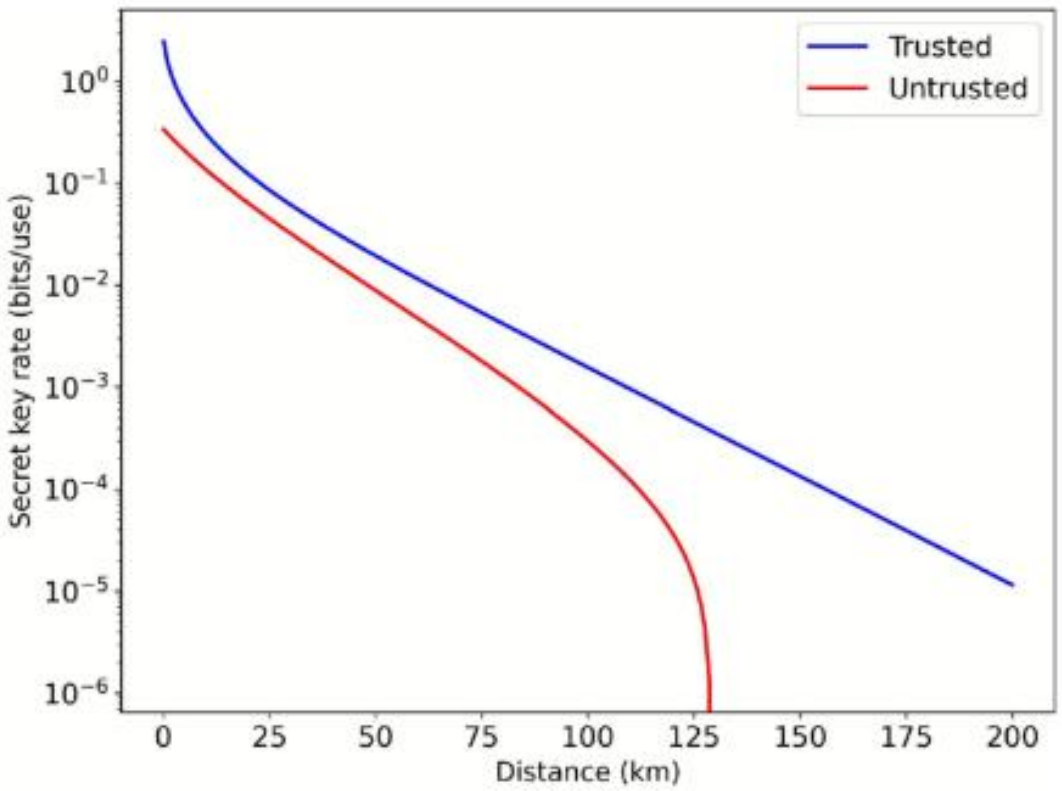


Fig. 6 Secret key rate for the No-switching protocol in both untrusted and trusted models. We used viable values for the parameters: $\beta = 0.95$ $\xi = 0.05$, $\xi_{ch} = 0.02$, $\xi_{el} = 0.03$, and $\eta = 0.6$

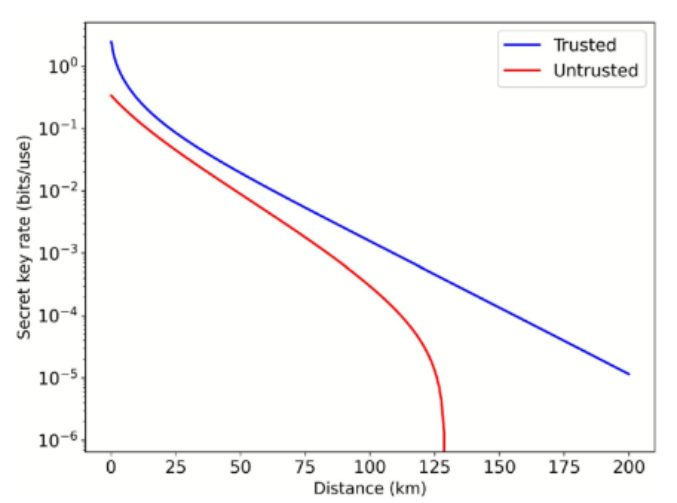
Anka et al., Brazilian Journal of Physics (2026) 56:72; https://doi.org/10.1007/s13538-025-01975-8

CV-QKD Desafios e oportunidades

- Tratamento de ruído na análise de segurança
- Otimização de algoritmos DSP (recuperação de fase e equalização)
- Otimização de algoritmos para pós-processamento
  - Estimativa de parâmetros, códigos LDPC, "distribution matcher", amplificação de privacidade
- Desenvolvimento e otimização de modelo RTL para implementação em plataforma FPGA

Apresentação de trabalhos no WquNets – quarta-feira
Modulação Gaussiana versus PCS-64-QAM em CV-QKD: Demanda por Bits Aleatórios e Desempenho em SKR
Análise de PRNGs em Hardware para Otimização de Memória na Amplificação de Privacidade em CV-QKD
Certified quantum randomness with coherent detection
Aceleração de Amplificação de Privacidade via NTT em Sistemas CV-QKD: Desafios e Tendências em Hardware
Realistic non-gaussian receivers for long distance continuous-variable quantum key distribution

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

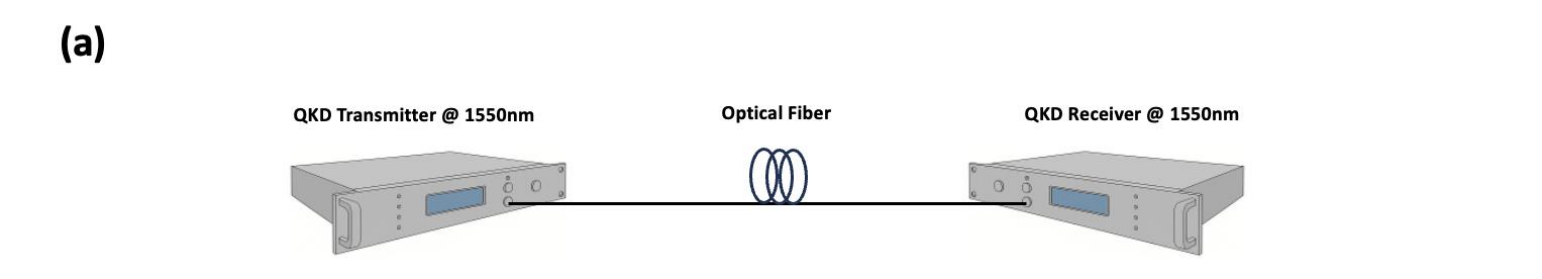
⇓

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

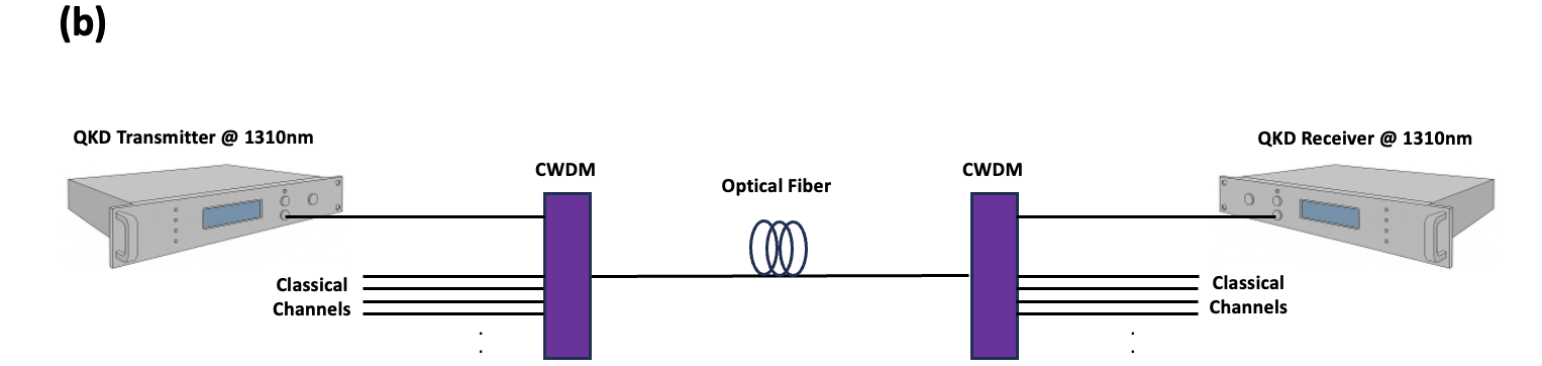
DA SILVA, VALÉRIA L et al. . Photonic Networks and Devices, 2025, p. NeM3C.1.

Alternativas

Fibra apagada @ C-band: ~0,2 dB/km



Fibra instalada @ O-band: ~0,35 dB/km + 2.0 dB



DA SILVA, VALÉRIA L et al. . Photonic Networks and Devices, 2025, p. NeM3C.1.

Redes quântica metropolitanas

Desafios

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

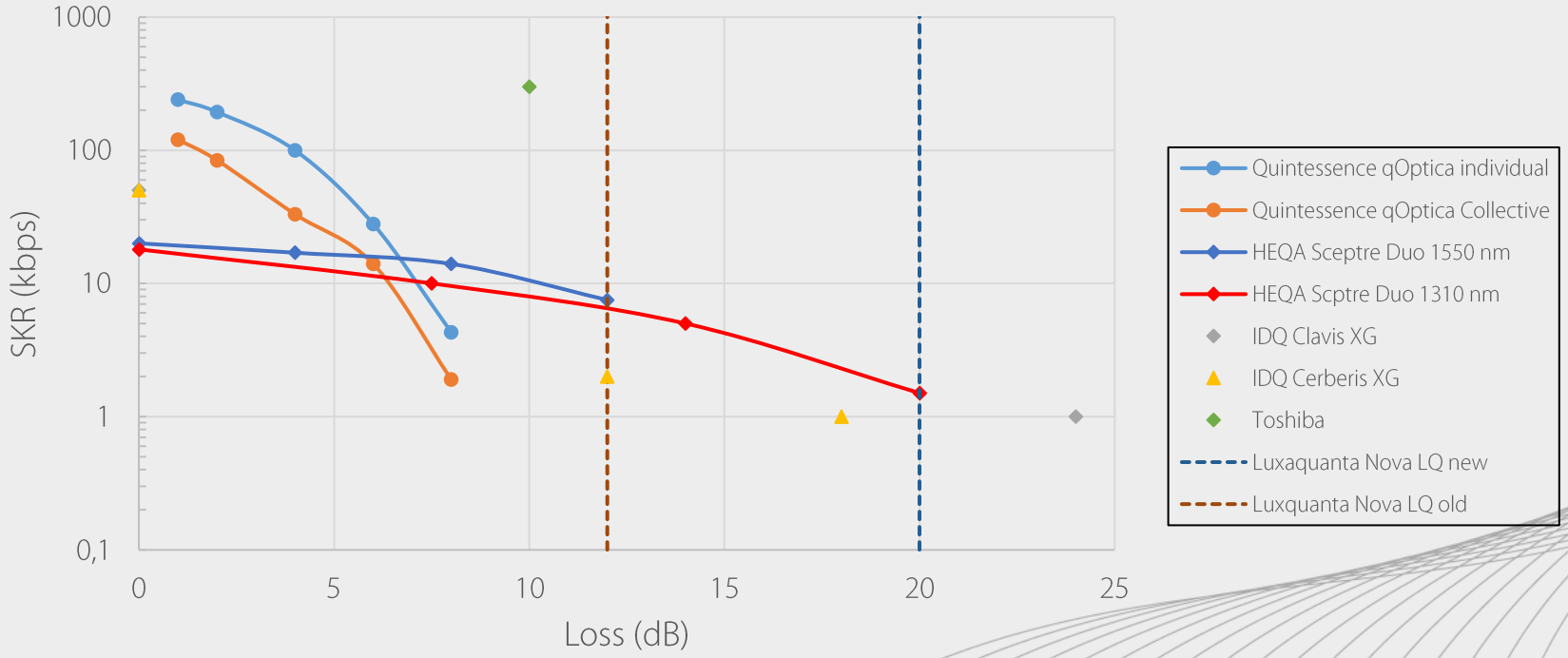
Maker	Model	Protocol		Max SKR (kbps)	Loss Budget (db)
IDQ	Clavis XG	DV-QKD	Decoy-State BB84	~50 (700,000 AES-256/h)	24 dB or 30 dB
HEQA Security	**Sceptre Duo**	**DV-QKD**	**Decoy-State BB84**	**20 @ 1550 nm 18 @ 1310 nm**	**20 dB**
Toshiba	Long Distance	DV-QKD	Decoy-State BB84	300 @10 dB	30 dB (150km)
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)
Quintessence Labs	**qOptica**	**CV-QKD**	**GG02**	**240 (individual attack) 120 (collective attack)**	**10 dB**

DA SILVA, VALÉRIA L et al. . Photonic Networks and Devices, 2025, p. NeM3C.1.

Redes quântica metropolitanas

Desafios

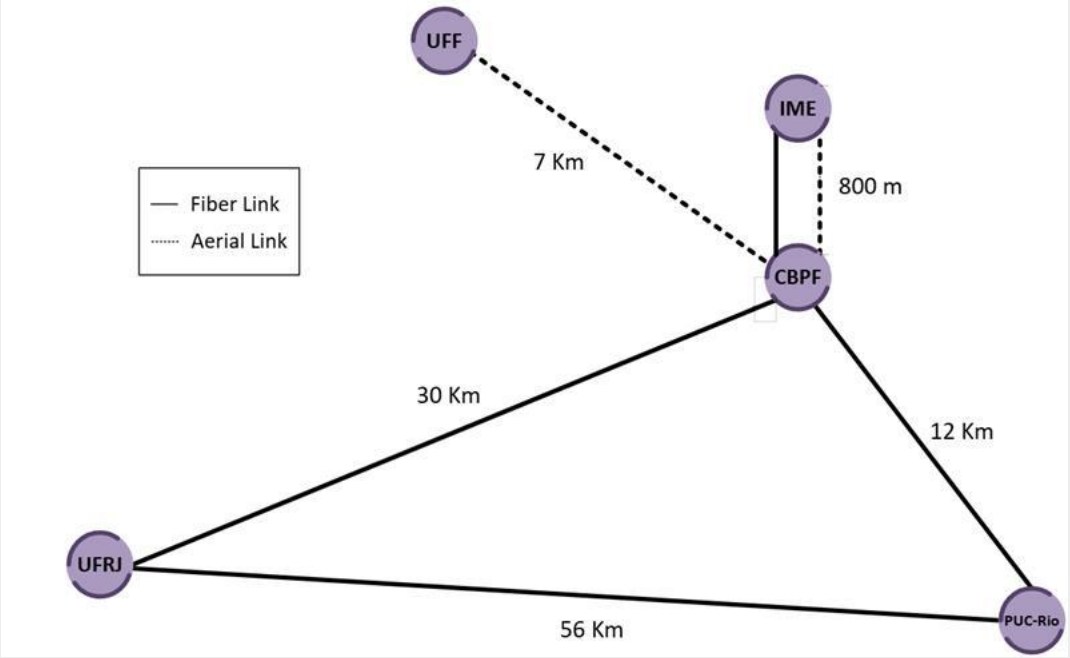
- QKD gera chaves entre 2 pontos
- Taxa de chaves cai exponencialmente com a distância
- Co-existência com canais clássicos



DA SILVA, VALÉRIA L et al. . Photonic Networks and Devices, 2025, p. NeM3C.1.

Rio Quantum Network & Dark fiber

C – band transmission over dark fiber



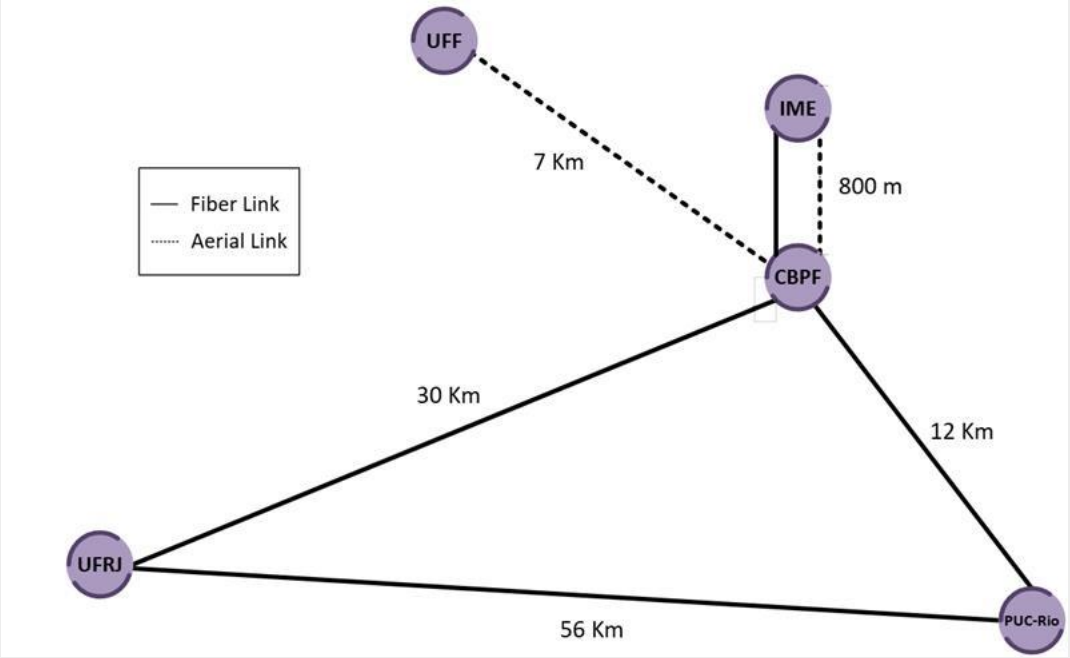
Link	Distance (km)	Loss (dB)	qOptica SKR (kbps)	Sceptre Duo SKR (kbps)	Best system
CBPF-PUC	12	2.5	69	19	CV
PUC-UFRJ	56	11	-	8,8	DV
CBPF-UFRJ	30	6	13	15	DV/CV
CBPF-IME	0,8	0,16	160	21	CV

- qOptica works for all links except PUC-UFRJ
  - Longer reach CV-QKD needed
- CBPF as a trusted node eliminates need for UFRJ/PUC-Rio direct link
  - Reduction in cost at the expense of reduced SKR

DA SILVA, VALÉRIA L et al. . Photonic Networks and Devices, 2025, p. NeM3C.1.

Rio Quantum Network & Installed fiber

O – band transmission

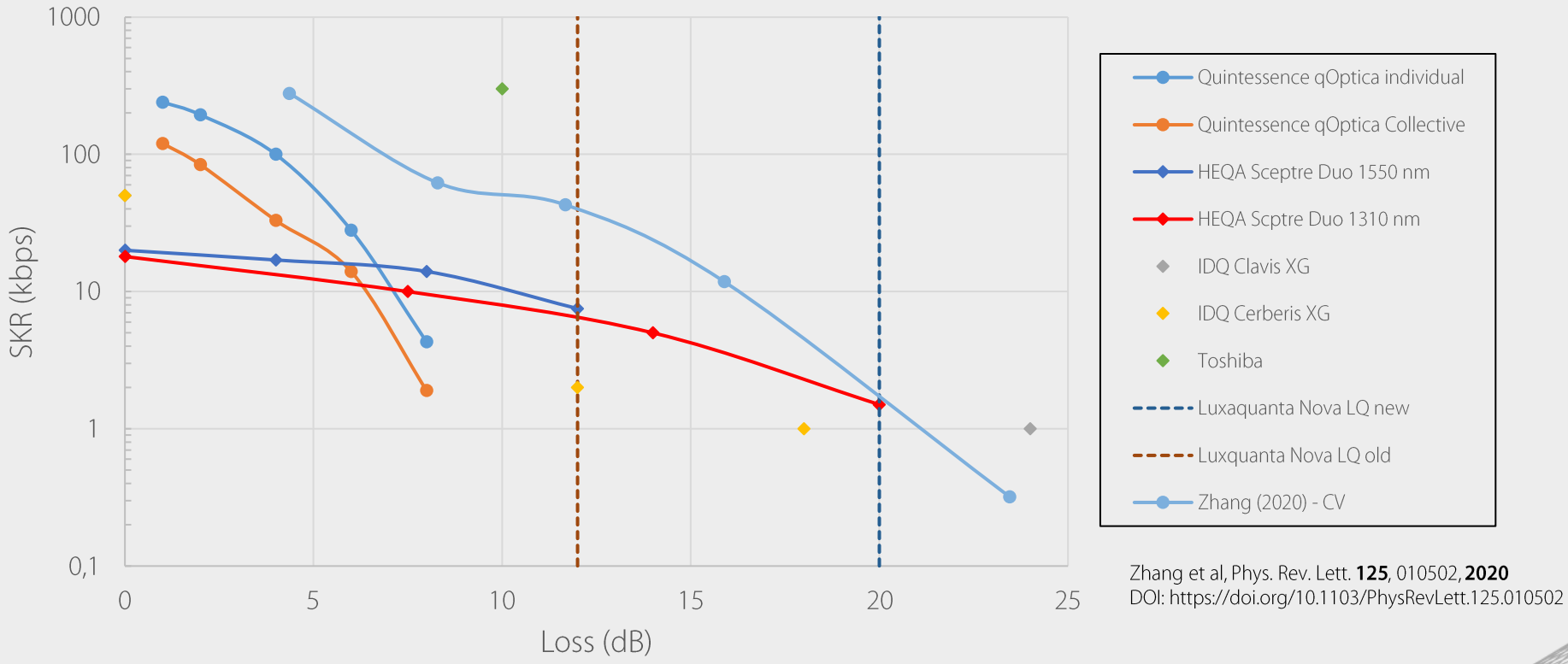


Link	Distance (km)	Loss (dB)	qOptica SKR (kbps)	Sceptre Duo SKR (kbps)	Best System
CBPF-PUC	12	6.3	11	14	DV
PUC-UFRJ	56	22	-	-	-
CBPF-UFRJ	30	12,5	-	7.3	DV
CBPF-IME	0,8	2.3	74	19	CV

- qOptica does not work for the 2 longest links
  - Longest link beyond Luxquanta specification
- Sceptre Duo also does not work for the longest link
  - Longer reach systems needed: Toshiba or IDQ
- CBPF as a trusted node is necessary unless longer reach DV systems is used

DA SILVA, VALÉRIA L et al. . Photonic Networks and Devices, 2025, p. NeM3C.1.

Can improvements in commercial equipments improve the scenario?



Zhang et al, Phys. Rev. Lett. **125**, 010502, **2020**
DOI: https://doi.org/10.1103/PhysRevLett.125.010502

- Hero experiments in CV-QKD are still limited to ~23 dB loss – satisfy needs for Quantum Rio Network for C- or O-band

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).

Rotas:

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

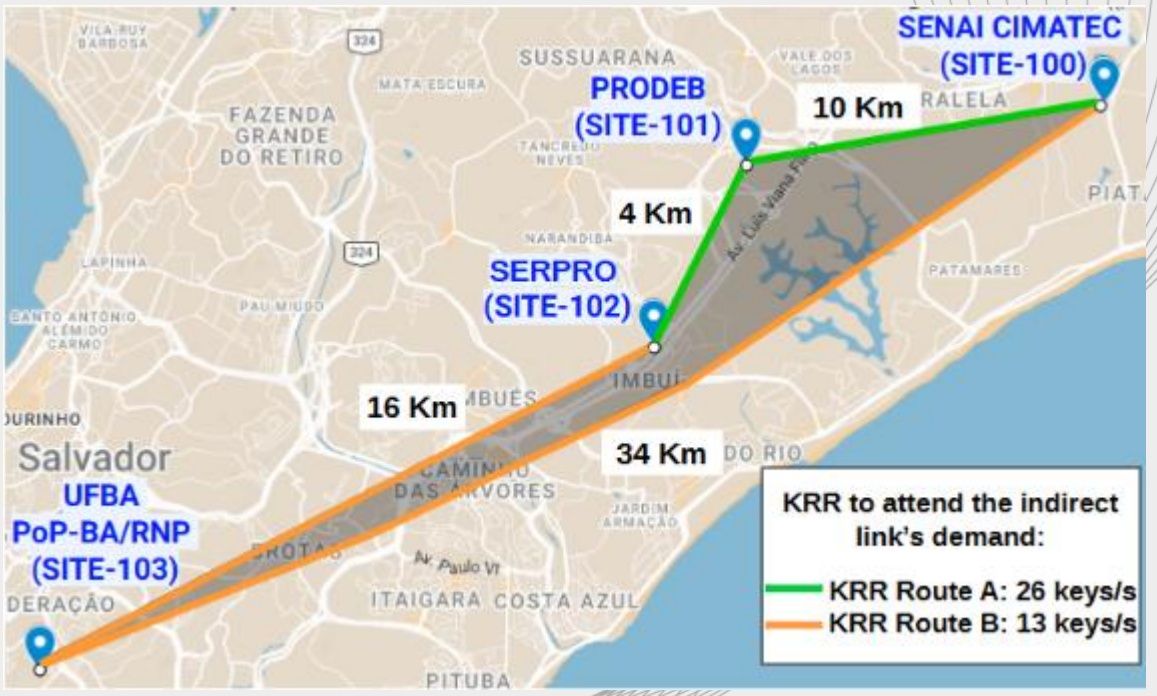
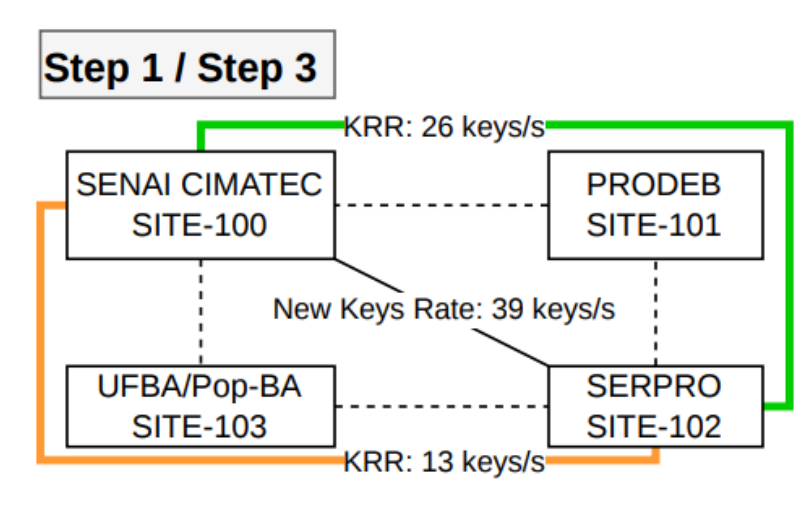
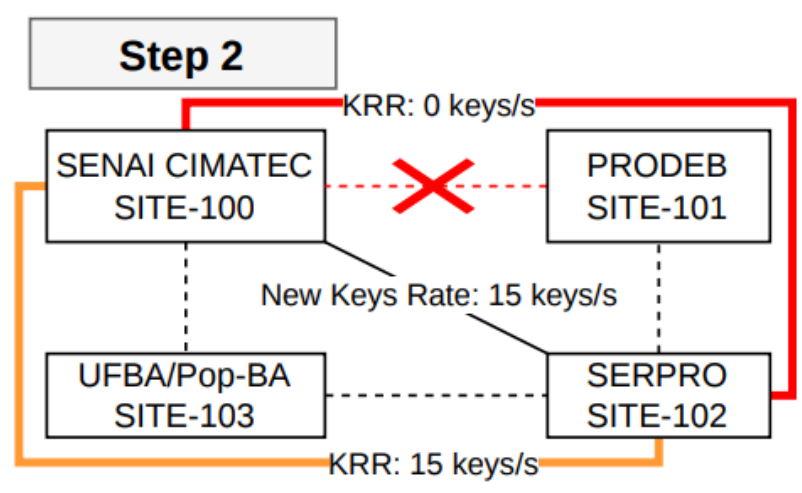
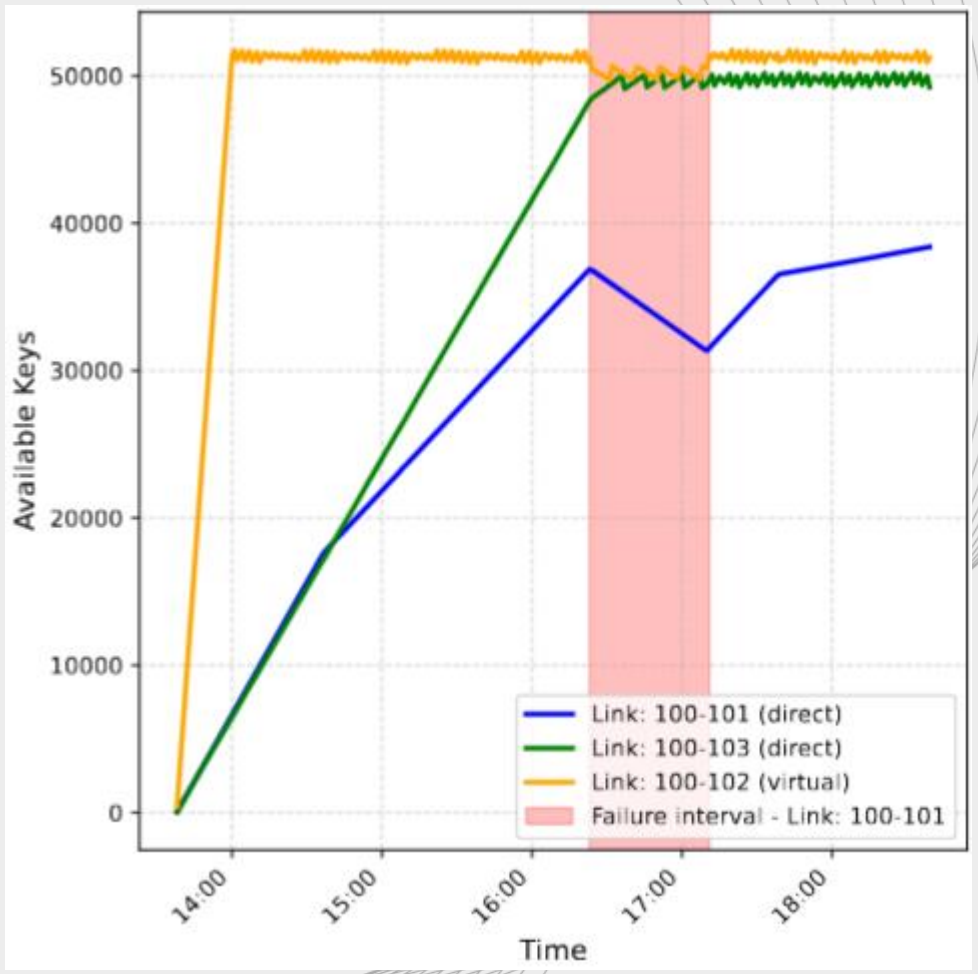


Fig.1: Há duas rotas, A e B, possíveis para conectar o link virtual, com demandas (key relay rate - KRR) de 28 e 13 chaves por segundo, respectivamente.

Quantidade de chaves disponíveis para consumo no link virtual







M. de Araujo et al, ICTON 2026

Sistema de gerenciamento de chaves (KMS)

- Trusted nodes e KMS com buffer trazem muitos benefícios
  - Conexão de link virtuais
  - Resiliência a falhas
  - Roteamento adaptativo

- Mais detalhes:
  - M. de Araujo et al, “Resilience in a Metropolitan QKDN: A Simulation Based Analysis of Brazil’s REMESSA Network” , ICTON 2026

- Outros trabalhos no ICTON:
  - Tomkelski et al., “Trusted execution environment for key relay on QKD” , QuIIN/UFBA
  - Njanda et al., “Network design in multiple non-overlapping paths within QKD networks”, UFBA/QuIIN/Un. Lisboa

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

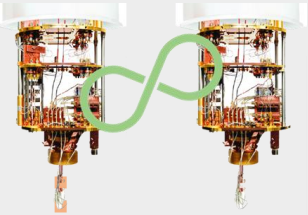
Visão e Futura

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

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

Redes Quânticas

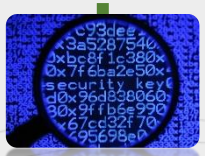
Computação Quântica Distribuída



Internet Quântica

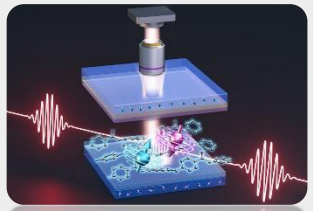
- QKD MDI (Entanglement Based)
- Entanglement Distribution
- Quantum Memories / Repeater

Dias de Hoje



Quantum Random Number Generation (QRNG)

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



Sensores Quânticos Distribuídos

Computação Quântica em Nuvem as Cegas

Img: Gimages | DBImgs

https://astrobiology.com/2023/04/tricorder-tech-quantum-sensing-in-your-pocket.html
https://mittechreview.com.br/o-que-e-comunicacao-quantica/

QuIIN
Quantum Industrial Innovation

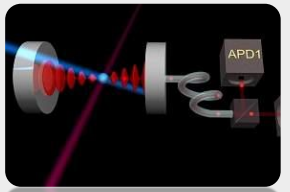
QuIIN
Quantum Industrial Innovation

SENAI CIMATEC
EMBRAPII
Empresa Brasileira de Pesquisa e Inovação Industrial
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO
GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO

Criptografia Quântica e Comunicação Quântica

Computação Quântica

Sensores Quânticos



Projetos de PD&I

Distribuição de Chaves Quânticas
e Algoritmos Quânticos

Formação & Capacitação

Do Pesquisador ao Profissional

Ecossistema de Startups

Atração e Criação de
Empreendedores

Associação Tecnológica (AT)

Integração com
Indústrias e Empresas

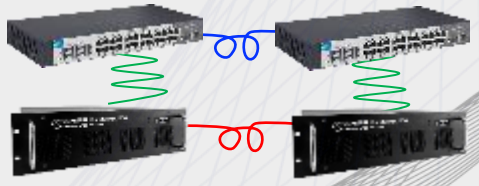
LINHAS DE PESQUISA

Como gerar chaves criptográficas?
Protocolo CV-QKD

Como utilizar chaves?

Desenvolver módulos e equipamentos próprios

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



< THE QUANTUM
FUTURE HAS
ALREADY BEGUN

Post-Graduation courses open for registration.

ESPECIALIZAÇÃO EM
COMUNICAÇÃO QUÂNTICA

ESPECIALIZAÇÃO EM
COMPUTAÇÃO QUÂNTICA

NEW CLASS 2026

ESPECIALIZAÇÃO EM TECNOLOGIAS
QUâNTICAS PARA GESTORES

QuIIN Quantum Industrial Innovation
SENAI CIMATEC
EMBRAPII Empresa Brasileira de Pesquisa e Inovação Industrial
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO
GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

QuIIN
Quantum Industrial Innovation

Obrigada!

Dr. Valeria Loureiro da Silva
Coordenadora
QuIIN - SENAI CIMATEC
Valeria.dasilva@fieb.org.br

SENAI CIMATEC
EMBRAPII
Empresa Brasileira de Pesquisa e Inovação Industrial
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO
GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO