SENAI CIMATEC

QUANTUM COMPUTING CENTER
LATIN AMERICA

Objetivos

1. Conhecer as reais ameaças da computação quântica aos sistemas de criptografia atuais;
2. Entender a diferença entre a criptografia quântica e a criptografia pós quântica;
3. Conhecer os principais protocolos de distribuição quântica de chaves de criptografia;
4. Conhecer as vantagens e limitações dos protocolos de distribuição quântica de chaves;
5. Conhecer o que vem sendo feito no mundo para que a implementação de sistemas de distribuição quântica de chaves de criptografia se torne viável em larga escala.

Nos protocolos de criptografia simétrica, quem envia a mensagem e quem a recebe utiliza a mesma chave, que deve permanecer em segurança durante todo o tempo em que for necessário manter a mensagem em segredo. Esses esquemas também são chamados de criptografia de chaves privadas.

Nos protocolos assimétricos as chaves são geradas em pares: uma chave pública e uma chave privada. Cada parte da comunicação precisar ter o seu par de chaves públicas e privadas. Se por exemplo Alice quiser envia uma mensagem para Bob ela deve receber a chave pública de Bob e utilizá-la para encriptar a mensagem. Ao enviar a mensagem para Alice, ela utiliza sua chave privada para decifrar a mensagem.

Impacto da computação quântica na criptografia atual

Figure: Análise do impacto da computação quântica nos protocolos de criptografia.

Cryptographic Algorithm	Type	Purpose	Impact From Quantum Computer
AES-256	Symmetric key	Encryption	Secure
SHA-256, SHA-3	–	Hash functions	Secure
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

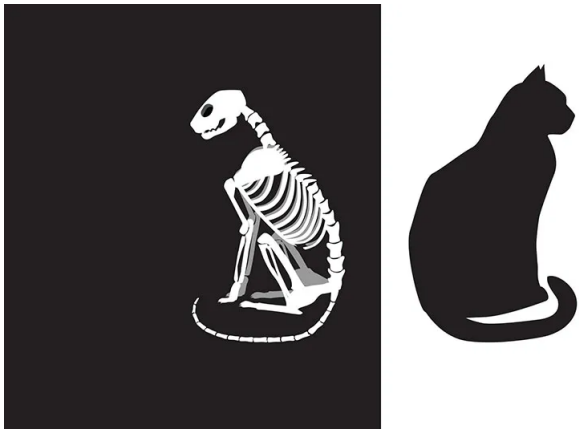
Figure: Comparação dos niveis de segurança para os protocolos de criptografia mais utilizados.

Crypto Scheme	Key Size	Effective Key Strength/Security Level (in bits)	
		Classical Computing	Quantum Computing
RSA-1024	1024	80	0
RSA-2048	2048	112	0
ECC-256	256	128	0
ECC-384	384	256	0
AES-128	**128**	**128**	**64**
AES-256	**256**	**256**	**128**

Em 2016, o NIST anunciou uma chamada para propostas de algoritmos clássicos que se acredita serem resistentes a ataques quânticos. Em 2022 quatro algoritmos foram anunciados como possivelmente resistentes.

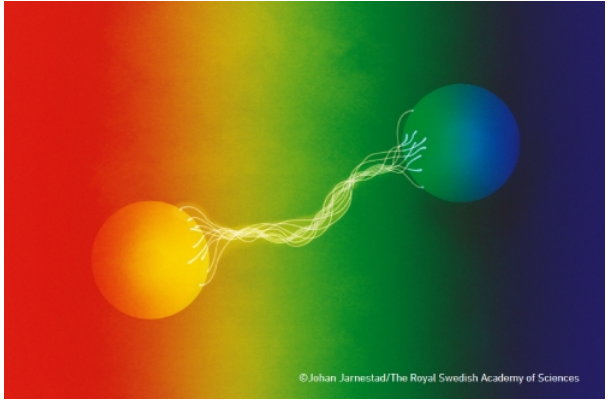
Figure: Quatro novos algoritmos estavam sendo avaliados. Entretanto um deles foi quebrado em um computador clássico.

Figure: Superposição



Emaranhamento

Figure: Emaranhamento



Comunicação superluminal

É possível utilizar comunicação quântica para transferir informação com velocidade maior que a da luz?

Clonagem

É possível copiar estados quânticos de forma eficiente?

Teorema da não clonagem

$$|\psi\rangle \otimes |0\rangle \rightarrow U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle \tag{1}$$

Se U é capaz de clonar um estado genérico $|\psi\rangle$, também deve ser capaz de clonar um estado genérico $|\phi\rangle$.

$$U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle \tag{2}$$

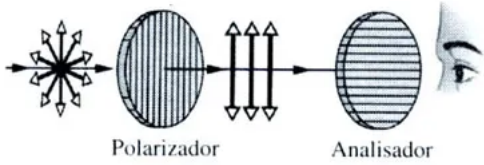
$$U(|\phi\rangle \otimes |0\rangle) = |\phi\rangle \otimes |\phi\rangle \tag{3}$$

Como o operador U é unitário e, portanto, preserva o produto interno, podemos realizar essa operação entre as supostas clonagens de ψ e ϕ:

$$\langle\psi|\phi\rangle = \langle\psi|\phi\rangle^2 \tag{4}$$

Codificação - polarização

Figure: Polarização



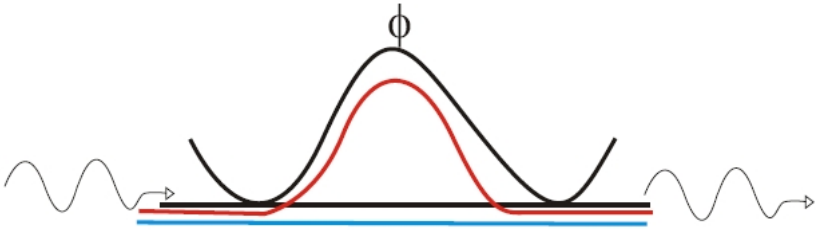
Notação

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{5}$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\leftrightarrow\rangle + |\updownarrow\rangle) \tag{6}$$

Codificação - time bin

Figure: Time bin



Criptografia Quântica

O primeiro modelo de criptografia quântica foi apresentada em 1983, por Stephen Wiesner.

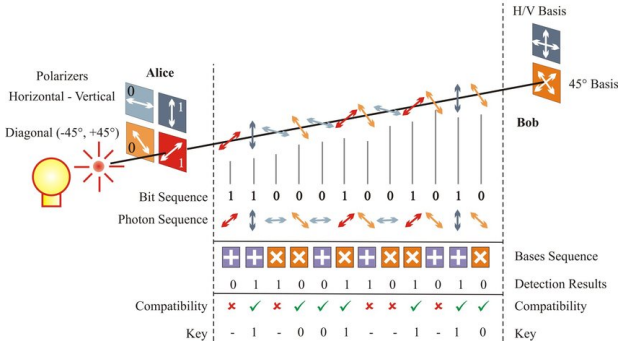
Figure: Quantum Money.

Entretanto esse modelo é impraticável mesmo nos dias atuais.

Criptografia Quântica - BB84

Em 1984 foi publicado o primeiro modelo de distribuição quântica de chaves, o BB84.

Figure: BB84.



Limite de Segurança: 11%.

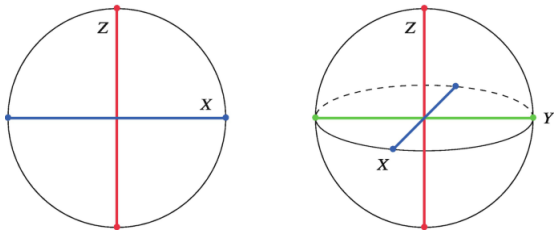
Siffting

Figure: Decoy states

Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

Protocolo de Seis Estados

Figure: Seis estados



Limite de Segurança: 12,6%.

- Alice e Bob possuem laboratórios seguros e controle dos canais de comunicação utilizados.

Figure: B92

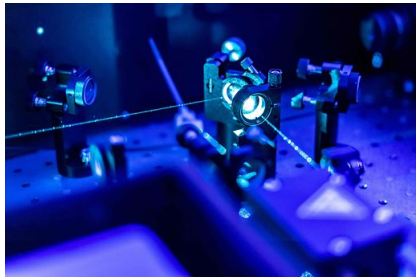
Fontes imperfeitas

Na prática, o envio de fótons únicos é impraticável devido à atenuação nos canais de comunicação.

Fontes imperfeitas

Para solucionar esse problema, lasers atenuados são utilizados no lugar das fontes de fotons únicos.

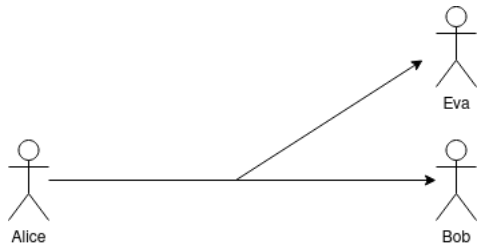
Figure: Fontes imperfeitas



Entretanto isso abre brechas de segurança.

Ataque por divisão no feixe de fótons

Figure: Ataque por divisão no feixe de fótons



Uma forma de resolver esse problema é Alice enviar pulsos com diferentes intensidades, de forma que apenas Bob saiba qual intensidade deve ser considerada.

Para resolver o problema dos ataques por PNS, o protocolo SARG04 é implementado de forma semelhante ao BB84, mas com um processo de reconciliação da informação semelhante ao B92.

Alice

$$a_1 = 0, a_2 = \pi/4, a_3 = \pi/2 \tag{7}$$

Bob

$$b_1 = \pi/4, b_2 = \pi/2, b_3 = 3\pi/4 \tag{8}$$

$$E = \langle a_1 b_1 \rangle - \langle a_1 b_3 \rangle + \langle a_3 b_1 \rangle + \langle a_3 b_3 \rangle \tag{9}$$

Se

$$-2 \leq E \leq 2 \tag{10}$$

o sistema não está completamente emaranhado e os estados devem ser descartados.
Se

$$E = -2\sqrt{2} \tag{11}$$

Então o sistema está emaranhado e Alice e Bob podem utilizar os estados que mediram na mesma base para criar a chave.

Esse protocolo guarda similaridades com o BB84 e se baseia no fato de que Eva não pode se tornar emaranhada com os qubits de Alice e de Bob sem adicionar erros nas medidas.

- Alice gera um par emaranhado e envia um dos estados para Bob;
- Alice e Bob realizam suas medidas;
- Alice compartilha quais bases utilizou para fazer suas medidas e os estados medidos na mesma base são utilizados para gerar a chave.

Figure: MDI QKD.

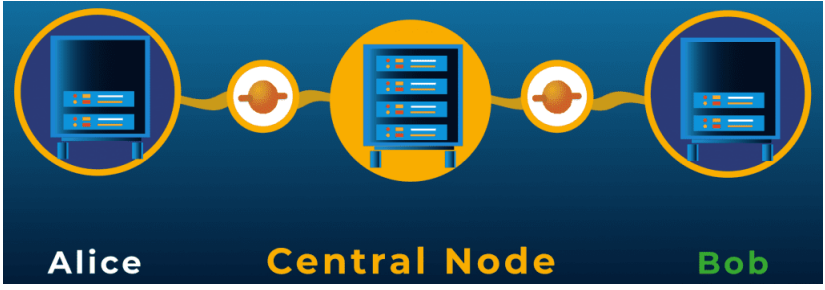


Figure: MDI QKD.

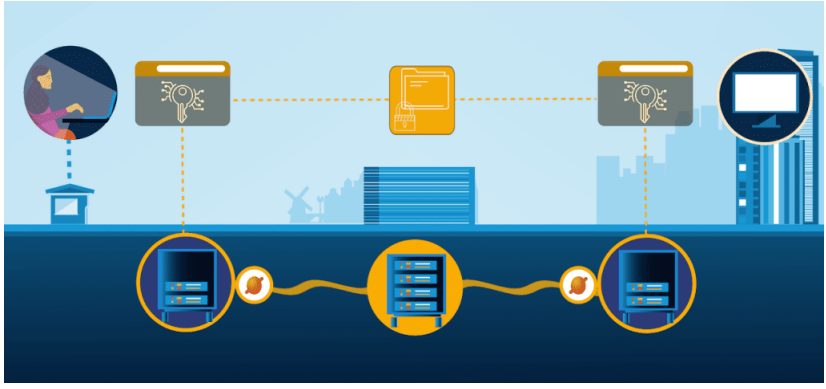
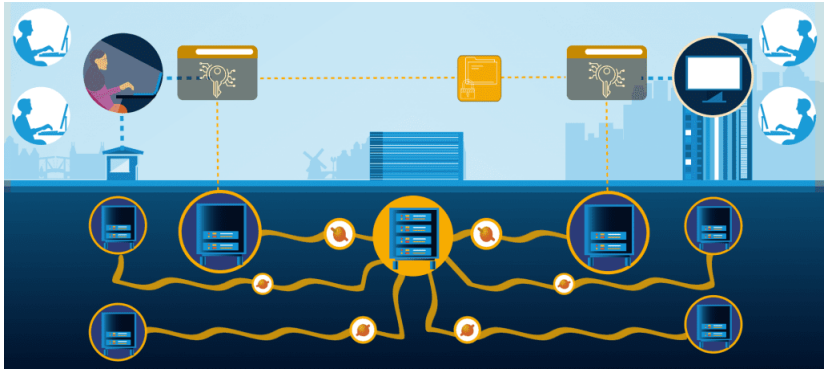


Figure: MDI QKD.



Tipo de Ataques

Existem três tipos de ataques que podem ser implementados em redes quânticas:

1. Individual
2. Coletivo
3. Coerente

Ataque individual

Em um ataque individual Eva utiliza qubits auxiliares para tentar ganhar informação dos qubits enviados e realiza medidas sobre seus qubits separadamente durante ou após o envio de todos os sinais.

Em ataques coletivos Eva também utiliza qubits auxiliares para tentar roubar informação sobre cada sinal enviado, mas a medida é realizada coletivamente e exclusivamente no final do protocolo.

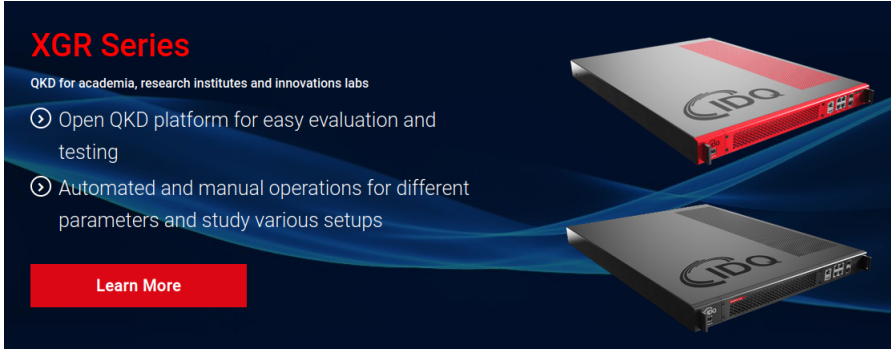
Ataque coerente

Em ataques coerentes os estados são armazenados e medidos de forma coletiva.

Se dois protocolos são provados seguros, então a segurança da combinação desses protocolos pode ser dada como segura sem a necessidade de uma prova de segurança adicional para o protocolo combinado.

Equipamentos Comerciais

Figure: IDQuantique.



Equipamentos Comerciais

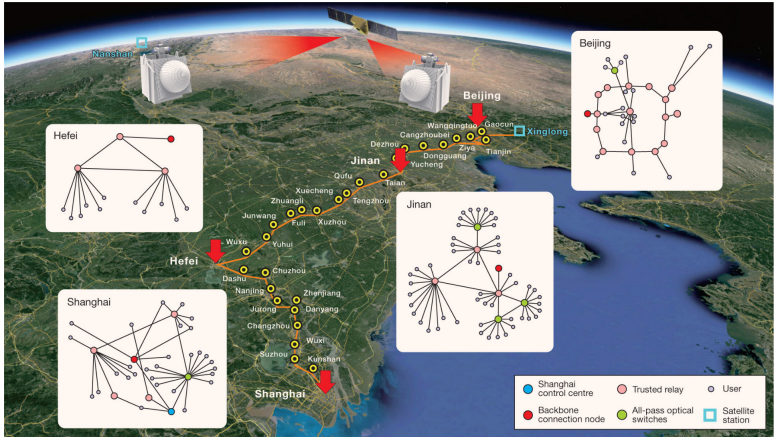
Figure: Toshiba.

Multiplexed QKD System

Long Distance QKD System

Provas de conceito - China

Figure: Rede Metropolitana Chinesa.



Europa - EuroQCI

A Europa possui ação integrada com participação dos 27 Estados-Membros e da Agência Espacial Europeia, o European Quantum Comunication Iniciative (EuroQCI).

Figure: London Network.

BT and Toshiba launch first commercial trial of quantum secured communication services

- EY becomes first commercial customer to connect quantum secure data transmission between its major London offices. -

April 27, 2022

BT Group plc
Toshiba Corporation

Japão

Uso de equipamentos comerciais.

- (aprox. 2023): Implementação na região de Kanto;
- (aprox. 2025): Implementação em todas as cidades;
- (aprox. 2030): Integração por satélite das redes terrestres (cobertura em todo o país);
- (aprox. 2035): Rede Global.

Fonte: Nacional Institute of Information and Communications Technology.

Estados Unidos

Figure: CQN - Arizona

Provas de conceito - Brasil

Figure: Rede Rio.

Referências

[1] S. Wiesner. Conjugate Coding, 1983.
[2] S. Pirandola. Advances in quantum cryptography. Optica publishing group, 2020.
[3] Y. Chen et al. An integrated space-to-ground quantum communication network over 4,600 kilometres., Nature 2021.
https://www.idquantique.com/
https://www.global.toshiba
[] https://rederio.br.