SCIENTIA PRIMA

CRIPTOGRAFIA PÓS-QUÂNTICA: PROTOCOLO DENTE DE LEÃO

HENRIQUE GUERRA
Colégio Dante Alighieri, São Paulo, SP, Brasil, 01420-002,
henrique.guerra@colegiodante.com.br
CRISTIANE RODRIGUES CAETANO TAVOLARO
Colégio Dante Alighieri e PUC-SP, São Paulo, SP, Brasil, 02202-000,
cristiane.tavolaro@cda.colegiodante.com.br

RESUMO

Desde a invenção do computador e da internet, a transmissão de informações ganhou escalas significativas, assim como os códigos que as protegem. Atualmente, o método mais usado de criptografia é o RSA, cuja segurança é fundamentada na dificuldade de fatorar um número. Contudo, o desenvolvimento das tecnologias quânticas viabilizaria o uso do Algoritmo de Shor, que usa propriedades quânticas para realizar a tarefa muito mais rapidamente do que os algoritmos vigentes, comprometendo a segurança dos dados online. Já existem protocolos clássicos de criptografia seguros e capazes de superar esse obstáculo; o intento desse trabalho, entretanto, é fornecer uma alternativa quântica a esses protocolos, através do aprimoramento dos métodos criptográficos resistentes ao Algoritmo de Shor e que já são usados comercialmente (em pequena escala), nomeadamente BB84 e E91, e discutir maneiras de utilizá-los nas redes de fibra óptica presentes nas cidades, com alterações mínimas.

Palavras-chave: Física Quântica. Emaranhamento Quântico. Criptografia.

POST QUANTUM CRYPTOGRAPHY: DANDELION PROTOCOL

ABSTRACT

Since internet and computer's invention, information's transmission has gained significant scales, aswell as the codes that protect it. Currently, the most used cryptography protocol is RSA, whose safety underlies on the difficulty of factorizing a number. However, quantum technologies' development would make the use of Shor Algorithm - which uses quantum properties to do the factorization task way faster than the current algorithms - viable, compromising online data's safety. There already exist classic protocols which are safe and able to overcome this obstacle; this work's intent, however, is to develop a quantum alternative to these protocols, through improvement of Shor-resistant cryptographic methods that are already used commercially (in small scale), namely BB84 and E91, and to discuss ways to use them in present cities optic fibre networks, with little to no modifications.

Keywords: Quantum Physics. Quantum Entanglement. Cryptography.

INTRODUÇÃO

A segurança de informações privadas e/ou confidenciais é um dos principais pilares que norteia a organização de nossa sociedade, pois, segundo a ONU (1948), **privacidade é um direito humano**. Isso não pode ser diferente no âmbito virtual, de forma que é fundamental que existam sistemas de criptografia seguros e eficientes protegendo a informação, respeitando o conceito de segurança da informação, que é fracionado nos seguintes tópicos, segundo Simião (2009, apud LEITE, 2016, p.3):

1. Confiabilidade: para que um sistema seja confiável, é necessário que se tenha a certeza de que somente pessoas previamente autorizadas vão ter acesso às informações ali armazenadas. Assegurando dessa maneira, que não haja a possibilidade de acesso de terceiros, sem o devido consentimento.
2. Integridade: assegura a intangibilidade, ou seja, garante que a informação não seja modificada, seja essa modificação uma alteração, gravação ou exclusão, acidental ou não, mantendo as características originais estabelecidas pelo proprietário dela.
3. Disponibilidade: garante que a informação esteja sempre disponível para consulta daqueles que têm acesso a ela.

4. Autenticidade: certifica a genuinidade da informação, verificando a pessoa ou entidade que fornece a informação.

5. Auditabilidade: é a possibilidade de auditoria de um sistema, que por sua vez, deve registrar os acessos às informações.

6. Não repúdio: propriedade em que se é garantido a impraticabilidade da negação de uma transação anteriormente feita por alguém.

7. Legalidade: o sistema deve estar de acordo com as leis e regulamentos aplicáveis ao uso da informação.

Com o desenvolvimento das tecnologias quânticas, no entanto, os sistemas de criptografia atuais perderiam sua confiabilidade em cerca de 10 anos (MOSES, 2009); estimativas utilizando a lei de Moore sugerem um prazo mais curto, entre 5,5 e 7,5 anos. Isso ocorre devido à natureza das operações por trás desses sistemas, que será exposta a seguir.

1.1 CRIPTOGRAFIA CLÁSSICA

Segundo Ekert (1991, p. 1, tradução nossa), "a criptografia pode ser concisamente definida como um sistema matemático de transformação de informação tal que ela é ininteligível, e consequentemente inútil, para aqueles que não devem ter acesso a ela". Ela se baseia em um campo da Ciência da Computação chamado de "classe de problemas NP (Não Polinomiais)": os problemas que podem ser verificados em tempo polinomial – ou seja, o algoritmo consome $a_1N^{a2}+b_1N^{b2}+...+z$ tempo para verificar uma solução de N bits - , mas são resolvidos em tempo exponencial – um consumo de tempo de a^N+z $(a>1)$ - e portanto dados como intratáveis, isto é, consomem uma grande quantidade de tempo para serem solucionados. É possível visualizar a diferença entre tempo polinomial e exponencial na Figura 1.

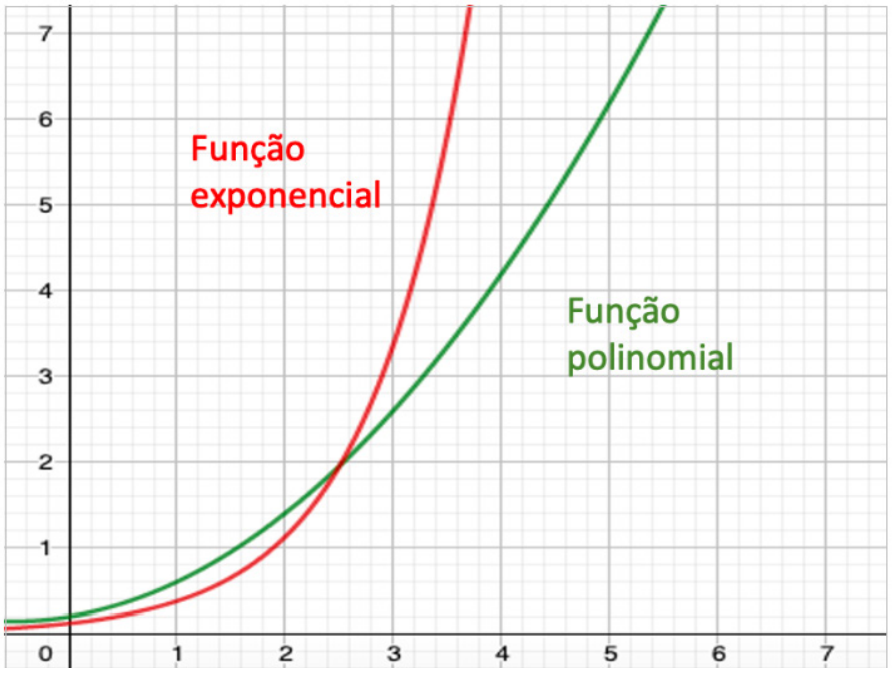

figura 1. Gráficos de uma função exponencial (vermelho) e uma função polinomial (verde); é possível observar que, embora a função verde seja mais íngreme inicialmente, a vermelha rapidamente a passa.

Desta forma, informações podem ser codificadas de tal forma que decodificá-las pode levar anos ou até décadas – isto é, até que um algoritmo que resolva o problema em tempo polinomial seja desenvolvido.

1.1.1 RSA

O RSA é um método de criptografia usado na transmissão de informação em toda a internet. Segundo Milanov (2009), ele funciona a partir do seguinte algoritmo (todas as variáveis e funções pertencem ao conjunto dos números naturais):

- Escolhem-se dois números primos p, q;

- computa-se $N = pq$ e $\phi(N) = (p-1)(q-1) = 20$

- escolhe-se e, que deve ser coprimo a $\phi(N)$ e menor que ele, além de ser maior do que 1;

- escolhe-se tal que $de \equiv 1 (mod\ \phi(N))$;

- descarta-se $p, q, \phi(N)$. d é mantido privado, e os demais parâmetros são anunciados publicamente.

Assim, alguém que deseja enviar uma mensagem a outra pessoa terá a mesma codificada em bits, obtendo m, e calculará $k = m^e (mod\ N)$ que anunciará publicamente; o destinatário então calculará $k^d = m^{ed} \equiv m^1 (mod\ N)$, e obterá a mensagem original. A segurança do sistema reside em d, cuja obtenção exige a fatoração de N que é extremamente trabalhosa (MILANOV, 2009).

1.1.2 Algoritmo de Shor

O Algoritmo de Shor integra "um algoritmo probabilístico eficiente para encontrar um fator de N" (FREITAS, 2010, p.68). Diferentemente dos demais algoritmos de fatoração atual, ele realiza a tarefa em tempo polinomial, embora com uma pequena margem de erro (pertence à classe de complexidade BQP, ou tempo polinomial quântico limitado ao erro (BERNSTEIN; VARIZANI, 1997), tornando muito mais eficiente do que seus predecessores (Figura 2).

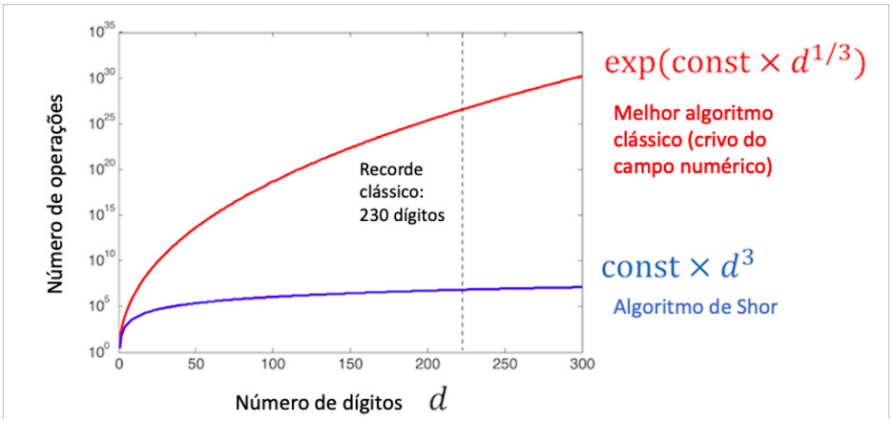

figura 2. Gráfico comparativo entre o Algoritmo de Shor e o Crivo do Campo Numérico (o melhor algoritmo de fatoração clássico para números de mais de 100 dígitos, até 2003 (CASE, M., 2003).

Disponível em: https://quantum-computing.ibm.com/composer/docs/iqx/guide/shors-algorithm. Acesso em 11/06/2020.

De forma resumida, este algoritmo calcula a ordem r de um inteiro x tal que $1<x<N$; esta ordem será usada para o cálculo de $mdc\left(x^{\frac{r}{2}}+1, N\right)$ e $mdc\left(x^{\frac{r}{2}}-1, N\right)$ (mdc é a sigla para maior divisor comum), dos quais um deles retornará um fator de N não trivial (isto é, diferente de 1 e de N) com probabilidade maior que ½ (FREITAS, 2010). Para tal, ele se apoia nos recursos oferecidos pelos computadores quânticos, que são capazes de realizar diversos cálculos ao mesmo tempo e, se manipulados de forma correta, podem produzir resultados valiosos – a ciência por trás dessas propriedades é explicada na seção 1.2. Vale ressaltar que isso não significa que os computadores quânticos são mais poderosos do que os clássicos (BERNSTEIN; VAZIRANI, 1997), mas apenas que eles nos oferecem possibilidades computacionais diferentes (DEUTSCH, 1985).

O Algoritmo de Shor já vem sendo implementado e testado em experimentos pioneiros, fazendo uso de números pequenos como 15, 21 e 35, e obtendo inclusive resultados livres de ruído (veja em 2.2.3) com versões escaláveis do algoritmo (MARTÍN-LÓPEZ *et al.*, 2012), e outros, quânticos (LI; PENG; SUTER, 2012) ou clássicos (BARBULESCU et al., 2014) e capazes de resolver certos processos utilizados em criptografia assimétrica, comprometem-na ainda mais; simplesmente aumentar o tamanho da chave usada não resolveria o problema, já que a quantidade de bits adicionada à uma chave não é proporcional aos ganhos obtidos em segurança, que se torna marginal após chaves de 4096 bits (GnuPG, entre 2012 e 2018). A

Criptografia de Curva Elíptica, dada como sucessora do RSA, é ainda mais vulnerável à invenção de Shor (PROOS; ZALKA, 2004); assim, foi comprometida grande parte dos algoritmos criptográficos de chave pública (responsáveis pelo estabelecimento de uma comunicação de forma segura), conforme evidencia-se na Tabela 1.

tabela 1. Impacto da Computação Quântica em algoritmos criptográficos populares.

Fonte: CHEN, L. et al., 2016. Report on Post-Quantum Cryptography. NIST.

Algoritmo Criptográfico	Tipo	Propósito	Impacto de computadores quânticos de grande escala
RSA	Chave pública	Assinaturas, estabelecimento de chave	Não mais seguro
ECDSA, ECDH (Criptografia de Curva Elíptica)	Chave pública	Assinaturas, estabelecimento de chave	Não mais seguro
DSA (Criptografia de Campo Finito)	Chave pública	Assinaturas, estabelecimento de chave	Não mais seguro

Existem propostas criptográficas imunes a essas tecnologias (NIST, 2017); no entanto, a análise e escolha de um protocolo definitivo e sua normatização só será completa por volta de 2024, segundo Dustin Moody, do NIST (2020)[1]. As propostas são baseadas em três tipos de problemas, que se acredita serem da classe NP (BASU *et al*., 2019). Ao desenvolver-se uma criptografia orientada na Física Quântica em detrimento da Matemática, pretende-se oferecer uma solução diversa das demais, dando alternativas caso as outras sejam ameaçadas, além de oferecer um tipo diferente de segurança: enquanto os protocolos clássicos oferecem segurança da chave baseada em tempo (BENNETT, 1992), os quânticos oferecem uma chave absolutamente inquebrável, uma vez implantada – embora a implantação dessa chave não seja uma certeza, diferentemente do que ocorre no análogo clássico. Alguns esforços já foram feitos nesse sentido, sendo o mais famoso deles a "competição" promovida pelo Instituto Nacional (americano) de Padrões e Tecnologia (2019); objetiva-se aqui

1 E-mail recebido, na íntegra:

(nome omitido)
If you look at some of our presentations on our webpage, you'll see that we estimate the 3rd round to conclude sometime about 2022, or thereabouts. It might be a little later. That's when the algorithms that will be standardized will be announced. It will then take us a year or two to write the standard, put it out for public comment, and get it finalized.

We don't control people implementing the algorithms. That runs its own course. It can take years.

Dustin (DUSTIN, 2020)

desenvolver tal criptografia por vias quânticas em detrimento das clássicas, de forma a oferecer uma solução diversa e segura caso as demais venham a perder sua segurança. O desenvolvimento dessa criptografia, logicamente, é indissociável de seu suporte teórico e dos outros protocolos que a inspiraram.

1.2 FÍSICA QUÂNTICA

Física Quântica é a ciência que estuda matéria e energia em escala atômica. Uma propriedade marcante de entidades quânticas (como fótons e elétrons) é a que eles podem se comportar tanto como partículas, interagindo com a matéria de forma localizada, ou como ondas, interagindo de forma dispersa (EISBERG; RESNICK, 1983; SHANKAR, 1994). Assim, os resultados de uma medida quântica não podem ser descritos *a priori* senão por uma soma de probabilidades atribuídas a diferentes resultados potenciais (SHANKAR, 1994), conhecida como "superposição de estados". Ao ser medida, a entidade se manifestará em um dos estados que contêm, produzindo o resultado observado; isto é, a medição de uma entidade afeta suas propriedades (EISBERG; RESNICK, 1983), o que faz com que seja impossível, por exemplo, medir a polarização de um fóton sem alterar este estado de polarização.

Daqui em diante, será abordado especificamente essa entidade – fóton - visto que ela é hegemônica em se tratando de transmissão de informação quântica Os trabalhos de Ursin e colegas (2007) e o de Kurtsiefer e colegas (2002) são dois dos muitos exemplos de artigos no campo nos quais fótons são utilizados sem muita discussão sobre os motivos para tal. Isso ocorre porque fótons, as partículas associadas às ondas eletromagnéticas, são por natureza entidades que viajam a altas velocidades e usadas para transmitir informação classicamente, através de fibras ópticas (SEARCHNETWORKING, 2019). Apesar disso, a maior parte do raciocínio desenvolvido no decorrer deste texto pode ser generalizado para as demais entidades quânticas (como, por exemplo, elétrons).

A polarização de um fóton é o ângulo no qual ele está orientado, mas esse conceito faz mais sentido quando se pensa no fóton como uma onda eletromagnética que vibra numa direção específica. O aparato de medida relativo à polarização é denominado polarizador; caso um fóton atravesse um polarizador, isso significa que a probabilidade de ele assumir a polarização medida pelo polarizador era maior do que 0 e que essa possibilidade se concretizou. A chance de um fóton atravessar um polarizador é dada pela Lei de Malus:

$Is = Ie \cdot \cos^2\theta$ (Equação 1), sendo Is a intensidade de saída do feixe, Ie sua intensidade de entrada e θ a defasagem entre os ângulos do polarizador e da polarização da onda.

Repare que esta lei muitas vezes contradiz a lógica clássica: um feixe de fótons orientado a 0°, por exemplo, após atravessar polarizadores 0°, 45° e 0°, por exemplo, teria ¼ de seu tamanho original (Figura 3), enquanto a lógica clássica nos diria que todo o feixe seria eliminado pelos polarizadores. Isso ocorre justamente porque, ao passar por um polarizador, o

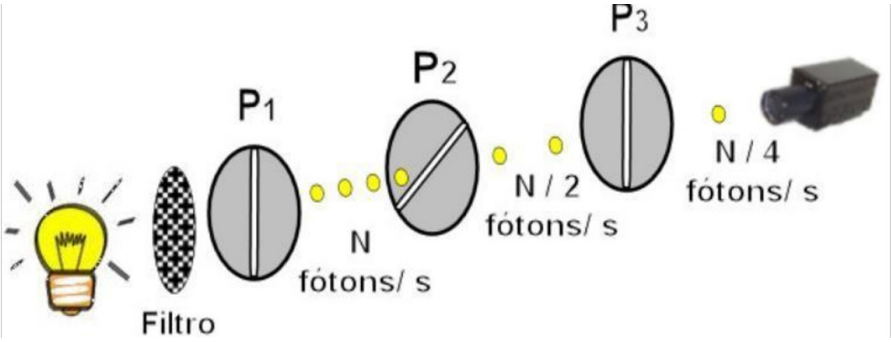

figura 3. Intensidade de um feixe de fótons após ser submetido a polarizadores a 0°, 45° e 0°, respectivamente.

Fonte: JONATHAN, Daniel. Rumo à mecânica quântica, via fótons polarizados. Curso de Licenciatura em Física. Universidade Federal Fluminense, 2006.

fóton tem sua polarização alterada.

Esta lei, entretanto, não se aplica a uma situação específica da física quântica: quando dois fótons estão emaranhados, o comportamento de um fóton enquanto interagindo com um polarizador está diretamente correlacionado ao comportamento de seu par emaranhado no mesmo processo (BES, 2012). Um exemplo de comportamento emaranhado é: se um fóton passa por um determinado polarizador, seu par emaranhado também passará por ele, e vice-versa. Assim, a chance de dois fótons emaranhados dessa forma passarem por um polarizador a 60° é de 0,25, contra 0,0625, caso eles não estivessem emaranhados.

Pode-se testar o emaranhamento entre conjuntos de fótons a partir de testes de Bell, que foram inicialmente desenvolvidos para provar que o emaranhamento era um fenômeno real (BES, 2012), e atualmente são usados para testar a correlação entre entidades quânticas. Nesse trabalho, utilizou-se o teste CHSH de um canal, derivado da desigualdade na Equação 2:

$$\left|P(a,b)-P(a,c)\right|+P(b,d)+P(c,d)\leq 2$$ (Equação 2) (CLAUSER; HORNE; SHIMONY; HOLT, 1969)

Experimentalmente, $P(x,y)$ representaria o número de medições coincidentes entre polarizadores de ângulos x e y, dividida pelo número total de fótons que interagiu com cada um dos polarizadores. A dedução da Equação 2 não será explicada aqui; basta saber que ela testa se o sistema que está sendo medido pode ser descrito como dois sistemas independentes (isto é, não correlacionados) ou não (CLAUSER; HORNE; SHIMONY; HOLT, 1969); em caso negativo, as inequações serão violadas.

O emaranhamento quântico é parte chave não só desse trabalho, mas

também de grande parte da criptografia quântica. A segurança desta se deve a dois princípios quânticos: o comportamento único e probabilístico das entidades, que não está presente na física clássica (ŠUPIĆ; BOWLES, 2020) e o fato de que medir uma entidade muda seu estado (conforme explicado anteriormente). Essas características únicas criam um canal de comunicação no qual "espionagem passiva é inútil, enquanto qualquer tentativa de manipulação ativa tem alta chance de ser detectada" (BENNETT; BRASSARD, 1984, p. 1).

1.3 PROTOCOLO DENTE DE LEÃO

Propõe-se um método criptográfico, cunhado Dente de Leão (em alegoria ao emaranhamento quântico), no qual utilizar-se-ia o uso de feixes emaranhados para evitar que a informação caia em mãos de terceiros. Isso ocorreria através de um sistema que funcionaria seguindo o seguinte algoritmo (Figura 4):

- A cria os feixes emaranhados f_1 e f_2;

- A armazena f_1 em uma memória EIT (descrita em HEINZE; HUBRICH; HALFMANN, 2013) e manda f_2 a B, por um canal público;

- B mede parte de f_2 em diferentes polarizações (visando realizar o teste CHSH posteriormente) e anuncia publicamente o trecho editado;

- A tira f_1 da memória EIT e mede o trecho correspondente em diferentes polarizações (novamente, visando realizar o teste CHSH);

- B edita (classicamente) o trecho quanticamente incólume de f_2, e o anuncia publicamente;

- A compara f_1 e f_2; se o resultado do teste CHSH implicar em feixes

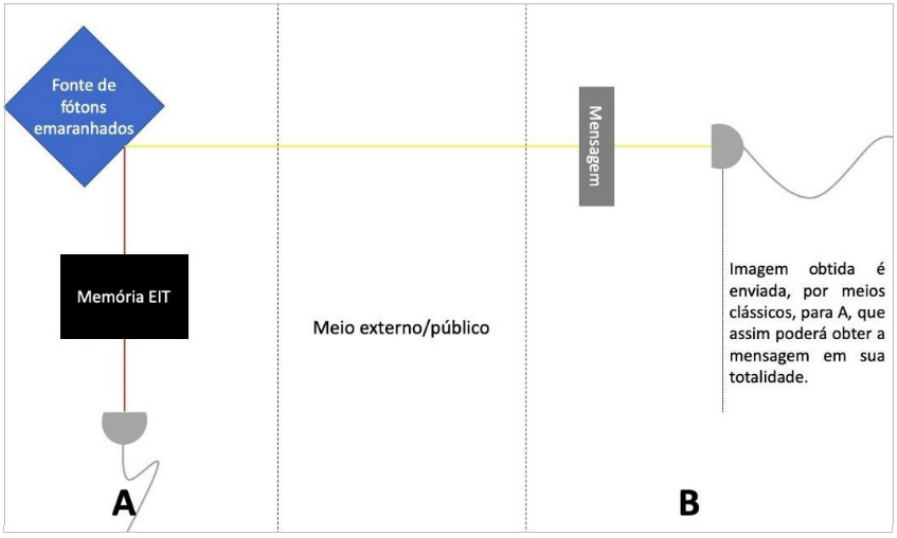

figura 4. Ilustração do protocolo.

emaranhados (para mais informações, veja o tópico 7.1), a chave é adotada; caso contrário, a chave é abortada.

Dessa forma, somente A teria acesso aos dois feixes e, portanto, à informação que foi introduzida por B neles. Isso ocorre porque, embora a informação em f_2 seja totalmente aleatória, ela está diretamente correlacionada àquela em f_1, e, portanto, quaisquer modificações realizadas classicamente seriam notadas pela comparação entre os feixes.

1.4 COMPARAÇÃO ENTRE PROTOCOLOS

O método neste texto configuraria uma alternativa aos protocolos BB84 e E91, que já são usados comercialmente desde 2004, mas pecam em alguns quesitos, como será visto a seguir.

1.4.1 BB84

O BB84, que deve seu nome aos seus criadores Charles Bennet e Gilles Brassard, é um dos pioneiros de seu ramo (Figura 5). Nele, a informação a ser transmitida é preparada em um eixo 0°/90° ou -45°/45°, e enviada ao destinatário, que medirá cada um dos *bits* em um eixo; caso o *bit* seja medido no eixo errado, sua informação se perderia, uma vez que a

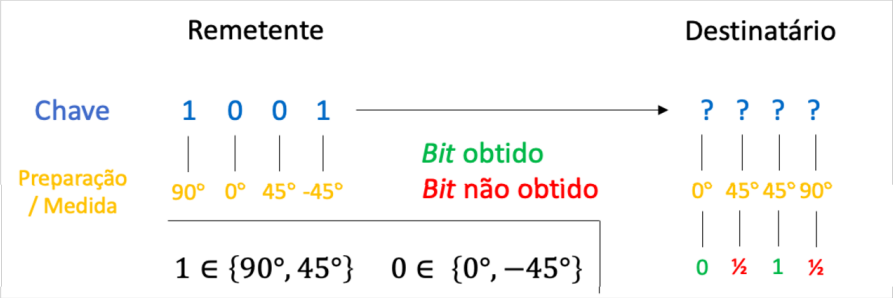

figura 5. Esquema de funcionamento do protocolo BB84

medição sempre retornaria ½ (de acordo com a Lei de Malus, descrita na seção 1.2).

Então, a mensagem é reenviada para que o destinatário obtenha a chave em sua totalidade; caso um terceiro esteja tentando obtê-la, a informação será deformada, o que será percebido pelo destinatário, e a preparação dos *bits* será mudada. O terceiro possui chances ínfimas de obter a informação em apenas uma interceptação (e assim poder retransmití-la, obtendo a chave sem o conhecimento de A ou B), dadas por

$P(n)=\left(\cos\frac{\pi}{8}\right)^{2n}\approx 0{,}8534^{n}$ (Equação 3), para uma mensagem de n bits.

A tentativa de interceptação poderia ser evitada caso o tempo de transmissão da mensagem fosse utilizado como parâmetro, porém, as diferenças entre fibras ópticas e a quantidade de variáveis envolvidas provavelmente tornaria isso inviável.

No entanto, o protocolo desqualifica-se pela ampla margem que dá para que o terceiro interrompa a comunicação pela observação contínua dela, além de duas possibilidades de ataque: introduzindo fótons extras na preparação dos estados, fazendo com que mais de um fóton seja preparado com a mesma informação, e depois retirando o excedente, obtendo informação de forma indetectável (SPEKKENS; RUDOLPH, 2002); ou "cegando" o detector do receptor, desviando os fótons e medindo-os.

1.4.2 E91

Publicado por Arthur Ekert em 1991, consiste de dois feixes emaranhados produzidos por um terceiro, que são filtrados aleatoriamente pelos interlocutores, em 3 ângulos previamente combinados. De acordo com Ekert (1991), A usaria 22,5°, 45° e 67,5°, enquanto B usaria 45°, 67,5 ° e 90°. Através desse padrão, alguns fótons seriam medidos por ambos os interlocutores no mesmo ângulo, e, por estarem emaranhados, produziriam a mesma medida; outros seriam medidos em ângulos diferentes – esses seriam anunciados publicamente, possibilitando a A e B realizarem o teste CHSH (descrito em 5.1.3) e concluindo se os feixes medidos foram ou não manipulados por "espiões" (em caso positivo, o emaranhamento se dissiparia).

Por mais que seja interrompível por terceiros, o E91 dá uma menor margem para tal do que o BB84, mas exige a presença de um agente externo produzindo partículas emaranhadas. Ele é mais seguro que seu predecessor, por não permitir ataques por introdução de fótons.

1.4.3 B92

Proposto por Bennet em 1992, o protocolo assemelha-se ao BB84; entretanto, após a primeira medição, B declararia publicamente os fótons que conseguiu medir e descartaria os demais, juntamente a A. Esse protocolo está sujeito aos mesmos ataques de seu predecessor e possui uma chave reduzida sem reduzir a probabilidade descrita na Equação 3, além de, segundo Sasaki, Matsutomo e Uyematsu (2015), exigir uma precisão maior do que o BB84; dessa forma, sua aplicação não será sequer discutida, e sua descrição é meramente informativa.

1.5 DISCUSSÃO DA VIABILIDADE

A transmissão de feixes de luz pelo planeta é feita através de cabos de fibra óptica, que consistem em quatro elementos, de acordo com Byju's (201-, tradução nossa):

- O Transmissor – Ele produz os sinais de luz e codifica-os para possibilitar a transmissão.

- A Fibra Óptica – O meio de transmissão para o pulso (sinal) de luz.
- O Receptor Óptico – Ele recebe o pulso de luz transmitido e o decodifica para uso.
- O Repetidor Óptico – Necessário para transmissão de informação a longas distâncias.

De acordo com SearchNetworking (2019), a fibra óptica é comumente dividida em dois tipos primários: modo único, que transmite apenas um sinal de luz por vez por longas distâncias, e multimodo, que é capaz de transmitir múltiplos sinais, mas devido à sua grande taxa de perda de sinal, apenas em distâncias curtas. Nessa discussão, apenas o primeiro tipo será referido.

O maior obstáculo para o uso prático da criptografia pós-quântica na atualidade é a fragilidade da informação, o que impede a transmissão de dados em longas distâncias. Até 07/02/2020, a maior distância de transmissão de informação quântica já obtida era 50km (KRUTIANSKYI et al., 2020); isso ocorre porque há perda de informação durante a transmissão, devido a impurezas na fibra óptica. Para propósitos clássicos, um repetidor é usado, habilitando deslocamentos maiores, mas seu uso na informação quântica não é possível, pois a medição e retransmissão de um estado implica na perda de suas propriedades e informações. Uma possível solução seria um sistema que fizesse uso de conexões terceiras para transmitir informações, sem que fosse possível aos donos delas acessá-las; também está em desenvolvimento uma espécie de repetidor quântico, que já possibilitou transmissão de fótons entre memórias quânticas através de 22km (YU et al., 2020).

Como já discutido anteriormente, fibras ópticas imperfeitas também impedem o uso do tempo e de graus de precisão muito altos em protocolos; tais contratempos, entretanto, são inevitáveis do ponto de vista prático. Coube à metodologia desenvolvida no decorrer deste trabalho concluir se esses e outros problemas são ou não impeditivos à execução do Protocolo Dente de Leão; nela, verificou-se e mensurou-se a influência do erro prático em algumas situações distintas de processos quânticos.

2 HIPÓTESE

Ao invés de investir em novos códigos algébricos que poderão ser decodificados por algoritmos aliados à computação quântica ou a supercomputadores, acredita-se que seria eficaz usar sistemas quânticos para a codificação da informação. Este sistema não pode se fundamentar em nenhum algoritmo ou processo clássico, de forma a garantir sua imunidade à computação quântica e diversidade em relação aos demais protocolos, e será, portanto, baseado no sistema de *qubits*, que por

sua vez explora a polarização dos fótons, o *quanta* de energia de onda eletromagnética.

3 OBJETIVO

Criar um método criptográfico resistente aos novos métodos de decodificação e/ou otimizar os atuais, criando um sistema viável que possa ser utilizado a curto prazo; e analisar, a partir de comparação com rede interuniversitária parceira (RNP, 2007), as adaptações necessárias no sistema atual de fibras ópticas de São Paulo para permitir o seu uso para sistemas quânticos, procurando minimizá-las. Dessa forma, pretendemos resolver os seguintes problemas, expostos pela BBC (2017):

- Fazer computadores quânticos se comunicarem entre si;

- garantir a proteção contra hackers;

- transmitir mensagens por longas distâncias sem perder parte delas;

- direcionar mensagens por uma rede quântica.

4 METODOLOGIA

Para a realização deste trabalho foram, e serão, realizados experimentos que abordam medidas de características quânticas da luz, empregando a infraestrutura do laboratório de óptica quântica da instituição de nosso coorientador, sob a sua tutela. Em paralelo a eles, será realizada a ideação dos sistemas que visamos desenvolver, e suas qualidades serão testadas.

4.1 EXPERIMENTO 1

Foram observados e analisados casos quânticos de dois sistemas de dois níveis (2 qubits), em que um laser incide em dois cristais, que os absorvem e, em uma taxa extremamente baixa, produzem pares de fótons emaranhados (Figura 6). Esses pares emaranhados foram submetidos a polarizadores de graus diferentes, de forma que cada partícula possui uma probabilidade de atravessá-lo ou não de acordo com a Lei de Malus (ver seção 1.2). Caso atravesse o polarizador, ela é medida por um sensor, que mede o número de fótons captados em cada polarização na qual o polarizador é ajustado. Essas medidas são utilizadas por uma CPU para

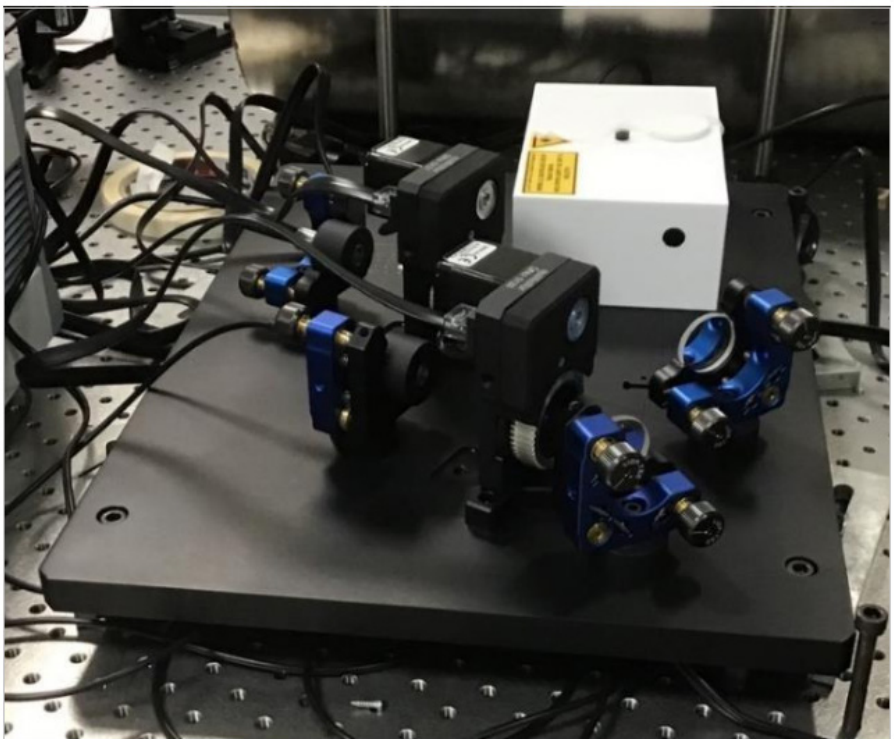

figura 6. Estrutura experimental mostrando o emissor laser, os cristais e os polarizadores (laboratório de óptica quântica – instituição parceira).

o cálculo do coeficiente de correlação entre os fótons, a partir do teste CHSH (QUINTINO; ARAUJO, 2011) e da correção dos valores observados.

4.2 EXPERIMENTO 2

Comprovado o emaranhamento entre os pares de fótons (no experimento anterior), foram observados e analisados casos quânticos de um sistema simples (de 1 *qubit*), no qual fótons foram submetidos a diferentes polarizações, e a congruência dos resultados em relação a Lei de Malus foi analisada. O equipamento utilizado foi o mesmo do Experimento 1 (Figura 6).

4.3 EXPERIMENTO 3

Foi realizado o teste de canal do BB84, isto é, provou-se praticamente que sua execução é plausível. Para tal, foram utilizados uma fonte de luz clássica, uma placa de onda (uma lente que determina a polarização

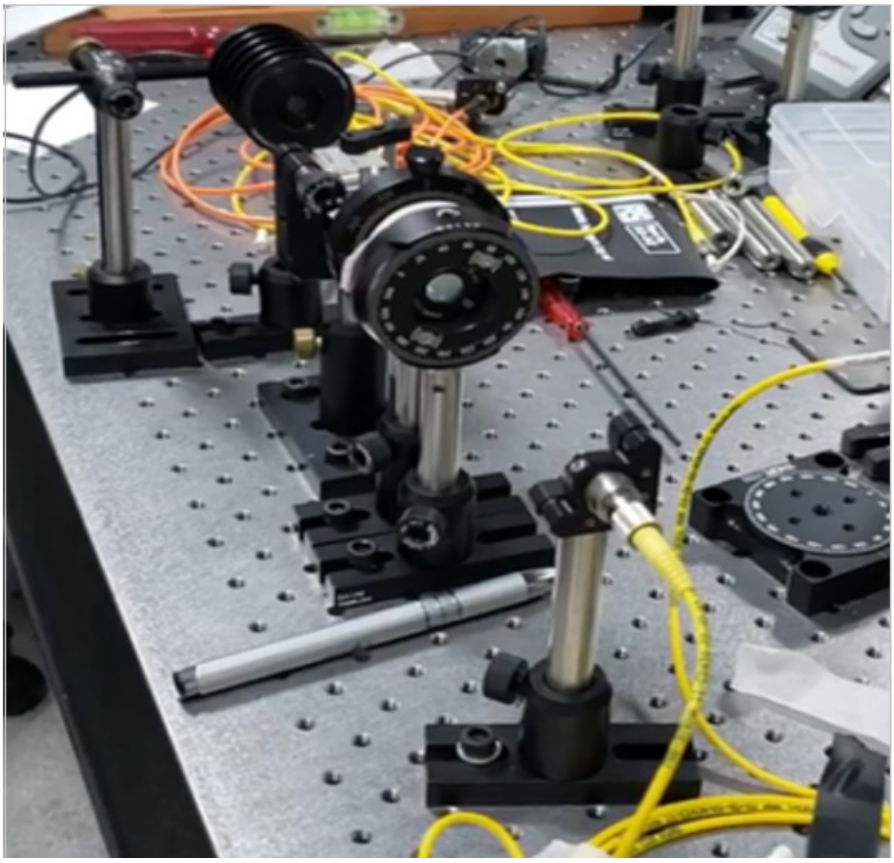

figura 7. Estrutura experimental mostrando a uma fonte de fótons, uma placa de onda, o cubo divisor polarizador e o detector (laboratório de óptica quântica – instituição parceira).

da luz sem filtrá-la), um cubo divisor polarizador (uma espécie de polarizador horizontal que reflete a luz que não o atravessa) e um detector (Figura 7).

4.4 EXPERIMENTO 4

Foi realizado o teste de canal do E91. A estrutura experimental utilizada foi a mesma do experimento 1 (Figura 6).

5. RESULTADOS

5.1 EXPERIMENTO 1

As duas primeiras colunas da Tabela 2 indicam a polarização utilizada em cada uma das lentes, e a terceira o número de coincidências.

POLARIZADOR 1 (X)	POLARIZADOR 2 (Y)	COINCIDÊNCIAS
0°	22,5°	63675
0°	112,5°	11099
90°	22,5°	16442
90°	112,5°	91337
0°	67,5°	12521
0°	157,5°	63387
90°	67,5°	90847
90°	157,5°	16906
45°	22,5°	68366
45°	112,5°	23773
135°	22,5°	9347
135°	112,5°	82321
45°	67,5°	81911
45°	157,5°	10982
135°	67,5°	24314
135°	157,5°	68678

tabela 2. Dados coletados no Experimento 1 (Os ângulos foram escolhidos visando maximizar a Desigualdade de Bell)

Ao serem submetidas ao protocolo CHSH, essas medidas retornaram um valor corrigido de 2,638 para o software que realiza o experimento e um valor "bruto" de 2,719 a partir de nossos cálculos; ambos os valores, portanto, indicam emaranhamento entre as partículas (descrito em 1.2).

Para a realização do protocolo CHSH, as medidas foram agrupadas de 4 em 4 de acordo com os ângulos utilizados nelas (tal agrupamento já foi realizado na Tabela 2); elas são somadas, cada uma delas é associada a um sinal positivo ou negativo a partir de seus ângulos (ângulos menores ou iguais a 90° recebem o sinal +, aquelas entre 90° e 180° recebem um sinal de -, e os sinais são somados) e normalizadas (divididas pela soma das medidas do grupo).

$$E = N_{++} - N_{--} - N_{+-} - N_{-+}$$ (Equação 4)

Os valores obtidos foram aproximados em 3 casas decimais e somados; assim, cada grupo possuía um valor entre -1 e 1 associado a ele (correspondente a E, na Equação 4). Esses valores são utilizados para obter S, que é o resultado do teste CHSH:

$$S = E(a_1 b_1) + E(a_2 b_1) + E(a_1 b_2) - E(a_2 b_2)$$ (Equação 5)

No caso, os valores obtidos pelo autor foram de 0,779, -0,68, 0,64 e 0,62, respectivamente, resultando em um valor S de 2,719. Observe que, em um sistema clássico, o seu valor máximo seria de 2, quando $a_1 = a_2 = b_1 = b_2 = 1$. Quanticamente, o valor máximo é $2\sqrt{2}$ (cerca de

2,82).

5.2 EXPERIMENTO 2

As duas primeiras colunas da Tabela 3 indicam as polarizações às quais os fótons foram submetidos, e a última, o número de coincidências (quando os dois sensores detectam fótons simultaneamente) contabilizadas.

tabela 3. Dados coletados no Experimento 2

Polarizador 1	Polarizador 2	Contagens
0°	0°	62934
0°	45°	32709
0°	90°	3025
0°	135°	33149
45°	0°	32268
45°	45°	78658
45°	90°	52372
45°	135°	4529
90°	0°	2968
90°	45°	51122
90°	90°	99885
90°	135°	48729
135°	0°	32033
135°	45°	5389
135°	90°	52877
135°	135°	78855

Como os pares de fótons emaranhados devem ter a mesma polarização (que não é definida, no entanto, até que seja medida), o número de contagens deve ser equivalente ao previsto pela Lei de Malus (descrita na seção 1.2). Comparando os dados experimentais com as previsões matemáticas, foi obtido um desvio-padrão médio para as medidas de σ = 13208,445, ou cerca de 13,2% das medidas. A distorção inviabiliza propostas que exijam grandes precisões; os resultados, no entanto, são qualitativamente condizentes com as previsões matemáticas da lei.

As distorções observadas se devem a diversos fatores, como a calibragem dos aparelhos, a pequena margem de entrada dos sensores, a luz ambiente e o fato de que os fótons gêmeos são produzidos em cristais diferentes (Figura 8), de acordo com o manual da fabricante (Figura 9) do equipamento (QUEDL, 2017, tradução nossa):

A informação distintiva, que pode evidenciar os processos de emissão e, consequentemente, reduzir sua coerência mútua, pode ser de caráter temporal ou espacial. O último caso ocorre sempre que os modos de emissão são espacialmente distinguíveis. Para evitar essa situação, os cristais não lineares devem ser suficientemente finos e a conversão dos fótons em sinais eletrônicos deve ser feita através de canais monomodo, como pares de fibra óptica monomodo. [...] [como ambas as medidas são adotadas,] não há maneira, mesmo a princípio, de distinguir espacialmente se os fótons medidos vieram do primeiro ou do segundo cristal e assim pares de fótons puramente emaranhados quanto à polarização podem ser detectados.

No domínio do tempo, a birrefringência dos cristais [isto é, um raio que atinge o cristal é dividido em dois] em combinação com a dispersão levam a um efeito indesejado. Os tempos de chegada dos fótons à face produtora de fótons do segundo cristal depende de seus comprimentos de onda e polarizações, o que revela a posição original dos fótons-pares. Isso leva a uma perda parcial de coerência entre os dois processos de emissão, e consequentemente a uma qualidade de emaranhamento reduzida.

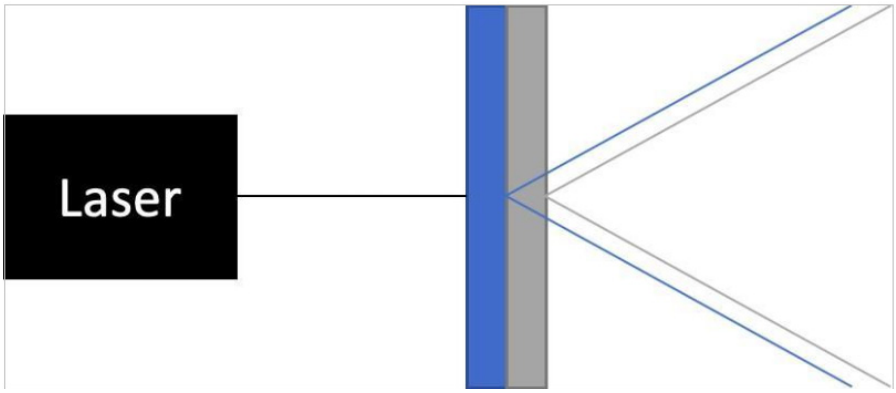

figura 8. Esquema (nossa autoria) da produção dos pares de fótons gêmeos (fora de escala). A diferença de posição entre cada par (que deveria constituir um único feixe) é uma das causas das distorções nos resultados das medições.

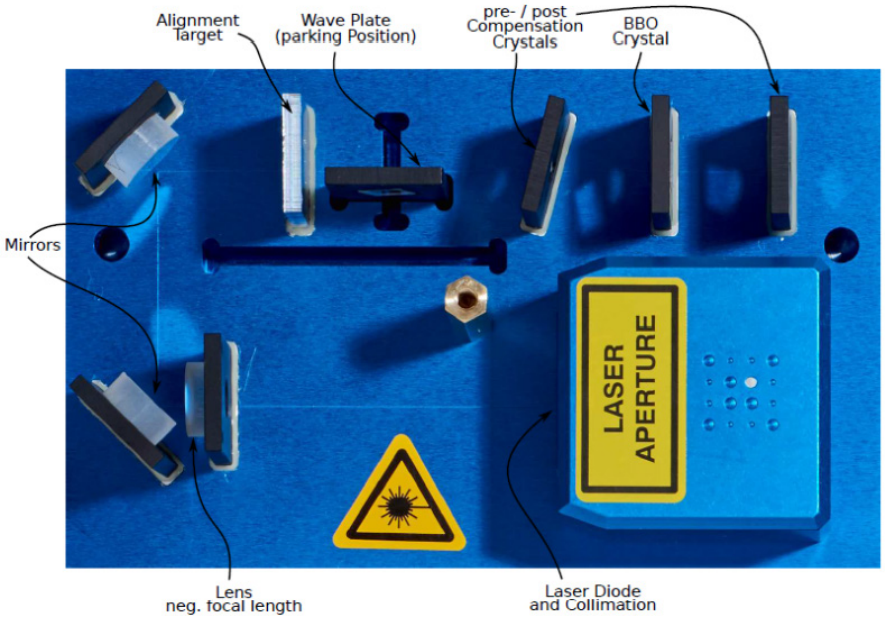

figura 9. Detalhes internos da fonte de fótons emaranhados.
Fonte: QUEDL. Entanglement demonstrator. 1 ed. [S.l.]: Qutools, 2017, p. 7.

Note que, embora lide-se com 2 feixes de fótons, trata-se de um sistema de 1 *qubit*, pois um deles apenas define a polarização do outro.

5.3 EXPERIMENTO 3

Quando a placa de onda foi ajustada a 0°, foram obtidas medidas de cerca de 0,8 milliwatts; e entre 45° e -45°, os valores aproximaram-se de 0,46 milliwatts; e, a 90°, os resultados foram perto de 30 microwatts. Embora a fonte utilizada tenha potência de 3 a 5 miliwatts, há dissipações no processo experimental, o que pode explicar a potência medida a 0°. Na Figura 10, há um gráfico que compara os resultados obtidos com a previsão matemática da Lei de Malus, admitindo-se uma potência de 0,85 miliwatts quando nenhuma medida é feita.

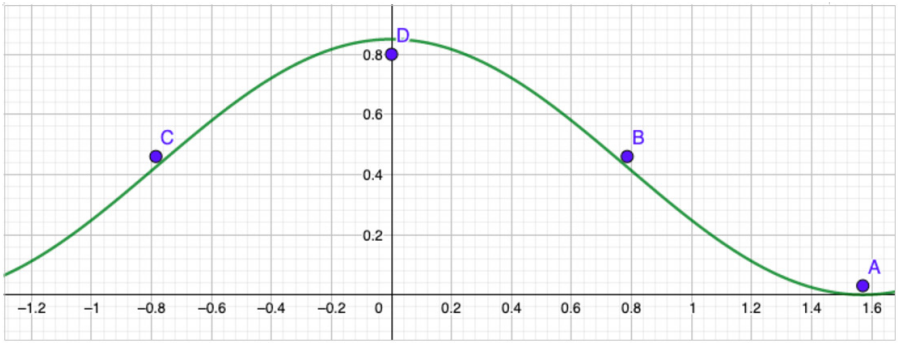

figura 10. Comparação entre as medidas obtidas (pontos A, B, C, D) e a previsão matemática da Lei de Malus, ajustada.

O experimento busca uma situação análoga àquela proposta pelo BB84. Aqui, a placa de onda representa fótons preparados em um eixo determinado, enquanto o divisor de feixe representa o destinatário da mensagem, que nesse caso apenas realiza medições em um eixo. Note que

a analogia é imperfeita, porque a simulação não prepara fótons um por um, como requerido pelo protocolo.

Os resultados mostram clara distinção entre medições no eixo certo, possibilitando a identificação dos *bits* apesar de uma pequena margem de erro - que deve ser maximamente de 16,5% (SASAKI, H; MATSUMOTO, R.; UYEMATSU, T., 2015) -, enquanto as feitas no eixo errado são indistinguíveis. Assim, a viabilidade do método criptográfico foi corroborada.

5.4 EXPERIMENTO 4

Os resultados estão organizados na Tabela 4 de acordo com os parâmetros utilizados.

Polarizador 1	**Polarizador 2**	**Coincidências**
0°	0°	7100
0°	90°	240
0°	45°	3600
0°	-45°	3700
45°	0°	3800
45°	90°	3700
45°	45°	7050
45°	-45°	350
90°	0°	300
90°	90°	7500
90°	45°	4000
90°	45°	3700
-45°	0°	3300
-45°	90°	4300
-45°	45°	400
-45°	-45°	7200

tabela 4. Dados coletados no Experimento 4

Taxas de erro variaram entre 0,6% e 5,2%, e eram baixas o suficiente para possibilitar a identificação de espionagem, já que elas não inviabilizam o teste CHSH (as medidas do Experimento 1 tiveram taxas de erro maiores do que as desse). Assim, a viabilidade do método está confirmada.

6. CONSIDERAÇÕES FINAIS

É possível concluir a partir do trabalho realizado que o protocolo ideado é viável e seguro, visto que ele faz uso dos mesmos mecanismos que o BB84 e o E91, cuja viabilidade foi assegurada nos experimentos 3 e 4. Além disso, o experimento 2 oferece dados valiosos para o desenvolvimento desse protocolo, pois delimita as possibilidades práticas de sua execução.

A próxima etapa para o desenvolvimento do protocolo é a comparação teórica entre ele e os demais protocolos quânticos – o que não foi possível a partir da metodologia desenvolvida nesse trabalho até o ponto da publicação - com o objetivo de assinalar vantagens e desvantagens desse protocolo e determinar se ele é competitivo em relação aos demais. Em caso positivo, é necessário determinar quais são os requisitos práticos para a execução – por exemplo: quais comprimentos de onda podem ser usados no protocolo? A quais distâncias ele é efetivo? Que margem de erro ele pode suportar? Que adaptações nas redes de fibra óptica são necessárias para sua execução? Respondidas essas questões, o protocolo Dente de Leão estaria pronto para o uso prático, e se tornaria mais uma alternativa segura para futuras aplicações da criptografia quântica.

REFERÊNCIAS BIBLIOGRÁFICAS

BARBULESCU, R. *et al*. A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In: **EUROCRYPT**, 33, 2014, Copenhague.

BARKER, E.; ROGINSKY, A. Transitioning the Use of Cryptographic Algorithms and Key Lengths. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf, acesso em 26/06/2020.

BASU *et al*. NIST Post-Quantum Cryptography- A Hardware Evaluation Study. Disponível em https://eprint.iacr.org/2019/047, acesso em 26/06/2020.

BENNETT, C. Quantum Cryptography Using Any Two Nonorthogonal States. **Physical Review Letters**, v. 68, n. 21, p. 3121-3124, 05/1992.

BENNETT, C.; BRASSARD, G., 1984. An Update on Quantum Cryptography. Disponível em https://link.springer.com/content/pdf/10.1007/3-540-39568-7_39.pdf, acesso em 12/07/2021.

BERNSTEIN, E.; VARIZANI, U. Quantum Complexity Theory. **Society for Industrial and Applied Mathematics**, v. 26, n. 5, p. 1411-1473, 10/1997.

BES, D. Quantum Mechanics: A Modern and Concise Introduction. 3 ed. Berlim: Springer, 2012.

BYJU`S. What is optical fiber?. Disponível em https://byjus.com/physics/what-is--optical-fiber/, acesso em 26/02/2020.

CASE, M. Beginner's Guide To The General Number Sieve. Disponível em https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.219.2389&rep=rep1&type=pdf, acesso em 26/06/2020.

CLAUSER, J.; HORNE, M.; SHIMONY, A.; HOLT, R. Proposed experiment to test local hidden-variable theories. **Physical Review Letters**, v. 23, 1969.

DEUTSCH, D. Quantum theory, the Church-Turing principle and the universal quantum computer. **Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences**, v. 400, n. 1818, p. 97-117, 06/1985.

EISBERG, R.; RESNICK, R. Física Quântica, 2 ed. Rio de Janeiro: Campus, 1983.

EKERT, A. Quantum Cryptography based on Bell's Theorem. **Physical Review Letters**, v. 67, n. 6, 08/1991.

FREITAS, A. Algoritmo de Shor e sua aplicação à fatoração de números inteiros. 2010. 78f. Dissertação (Mestrado em Matemática) - Universidade Federal de Minas Gerais, Belo Horizonte, 2010.

GNUPG. FAQ. Disponível em https://www.gnupg.org/faq/gnupg-faq.html#no_default_of_rsa4096, acesso em 20/06/2020.

HEINZE, G.; HUBRICH, C.; HALFMANN, T. Stopped Light and Image Storage by Electromagnetically Induced Transparency up to the Regime of One Minute. **Physical Review Letters**, v. 111, 06/2013.

KRUTYANSKYI, V.; MERANER, M.; SCHUPP, J.; KRCMARSKY, V.; HAINZER, H.; LANYON, B. Light-matter entanglement over 50 km of optical fibre. **npj Quantum Information**, v. 5, 08/2020.

KURTSIEFER, C.; ZARDA, P.; HALDER, M.; WEINFURTER, H.; GORMAN, P.; TAPSTER, P.; RARITY, J. A step towards global key distribution. **Nature**, v. 419, 2002.

LEITE, H. **A Importância da Privacidade na Internet**. 2016. 61 f. TCC (Graduação) – Tecnologia em Análise e Desenvolvimento de Sistemas, Departamento de Tecnologia da Informação, Faculdade de Tecnologia de São Paulo, São Paulo, 2016.

LI, J.; PENG, X.; SUTER, D. Efficient Exact Quantum Algorithm for the Integer Square-free Decomposition Problem. **Scientic Reports**, v. 2, 02/2012.

MARTÍN-LÓPEZ, E.; LAING, A.; LAWSON, T.; ALVAREZ, R.; ZHOU, X.; O`BRIEN, J. Experimental realization of Shor's quantum factoring algorithm using qubit recycling. **Nature Photonics**, v. 6, 10/2012.

MILANOV, E., 2009. The RSA Algorithm. Disponível em https://pdfdirectory.com/702-tutorial-the-rsa-algorithm.pdf, acesso em 12/07/2021.

MOODY, D. **Post-Quantum Cryptography Implementation**. Mensagem recebida pelo autor em 07/02/2020.

MOSES, T. Quantum Computing and Cryptography: Their impact in cryptographic practice. Disponível em: https://www.entrust.com/wp-content/uploads/2013/05/WP_QuantumCrypto_Jan09.pdf, acesso em 26/06/2020.

NIST. Post-Quantum Cryptography. Disponível em: https://csrc.nist.gov/Projects/post-quantum-cryptography, acesso em 26/06/2020.

ONU. Universal Declaration of Human Rights. Disponível em: https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf, acesso em 26/02/2020.

PROOS, J. & ZALKA, C. Shor's discrete logarithm quantum algorithm for elliptic curves. Disponível em: https://arxiv.org/pdf/quant-ph/0301141.pdf, acesso em 01/07/2020.

QUEDL. QuED: Entanglement demonstrator. Munique: Qutools GmBH, 2017, 26 p.

QUINTINO, M.; ARAÚJO, M. Desigualdades de Bell: Uma introdução à não-localidade quântica. Disponível em: https://www.academia.edu/4199782/Desigualdades_de_Bell_Uma_introdução_à_não-localidade_quântica, acesso em 01/07/2020.

RNP. Fibra ótica. Disponível em: https://bit.ly/2tSzRwa, acesso em 07/02/2020.

RUSSON, M. Computação quântica: como será a internet super-rápida do futuro. Disponível em https://www.bbc.com/portuguese/amp/geral-41697094, acesso em 19/06/2020.

SASAKI, H; MATSUMOTO, R.; UYEMATSU, T. Key Rate of the B92 Quantum Key Distribution Protocol with Finite Qubits. Disponível em https://arxiv.org/pdf/1504.05628.pdf, acesso em 01/07/2020.

SEARCHNETWORKING. Optic fiber (optical fiber). Disponível em: https://searchnetworking.techtarget.com/definition/fiber-optics-optical-fiber, acesso em 26/02/2020.

SHANKAR, R. Principles of Quantum Mechanics, 2 ed. Nova Iorque: Springer, 1994.

SPEKKENS, R. W.; RUDOLPH, T. Optimization of coherent attacks in generalizations of the BB84 quantum bit commitment protocol. Disponível em: https://www.researchgate.net/publication/220436086_Optimization_of_coherent_attacks_in_generalizations_of_the_BB84_quantum_bit_commitment_protocol, acesso em 01/07/2020.

ŠUPIĆ, I.; BOWLES, J. Self-testing of quantum systems: a review. **Quantum**, v. 4, 2020.

URSIN, R.; TIEFENBACHER, F.; SCHMITT-MANDERBACH, T.; WEIER, H.; SCHEIDL, T.; LIDENTHAL, M.; BLAUENSTEINER, B.; JENNEWEIN, T.; PERDIGUES, J.; TROJEK, P.; ÖMER, B.; FÜRST, M.; MEYENBURG, M.; RARITY, J.; SODNIK, Z.; BARBIERI, C.; WEINFURTER, H.; ZEILINGER, A. Entanglement-based quantum communication over 144km. **Nature Physics**, v. 3, 2007.

YU, Y.; MA, F.; LUO, X.; JING, B.; SUN, P.; FANG, R.; YANG, C.; LIU, H.; ZHENG, M.; XIE, X.; ZHANG, W.; YOU, L.; WANG, Z.; CHEN, T.; ZHANG, Q.; BAO, X.; PAN, J. Entanglement of two memories via fibres over dozens of kilometers. **Nature**, n. 578, p. 240-245, 02/2020.

HENRIQUE VIEIRA DOS SANTOS GUERRA

Aluno do 3º ano do Colégio Dante Alighieri (SP); tem interesse em Ciências Exatas, Letras, e especialmente em Matemática Aplicada. Começou a pesquisa em Física Quântica em 2018, e desde então expôs seu trabalho em diversas feiras de ciências, como a FEBRACE 2020, a ISEF 2020 e a MOSTRATEC 2020. Foi bolsista ICJ do CNPq.

CRISTIANE RODRIGUES CAETANO TAVOLARO

Graduada em Física e Mestre em Instrumentação para Física Nuclear pela PUC-SP. Professora da Faculdade de Ciências Exatas e Tecnologia da PUC-SP atuando nos cursos de Física, Engenharia de Produção, Civil e Biomédica. Membro fundadora do GoPEF - Grupo de Pesquisa em

Ensino de Física da PUC-SP, certificado pelo CNPq (www.pucsp.br/gopef). Coautora do livro paradidático “Física Moderna Experimental” editado pela Manole. Profa. Do Programa de Iniciação Científica Junior Cientista Aprendiz e do departamento de física do Colégio Dante Alighieri. Especialista em ensino de física com foco em física moderna e novas tecnologias para o ensino.

submetido
13.04.2021

reapresentado
12.07.2021

aprovado
16.07.2021

Contribuição de autoria. Henrique Vieira dos Santos Guerra participou da elaboração do estudo, da investigação de dados, do levantamento bibliográfico e da redação do artigo. Cristiane Rodrigues Caetano Tavolaro orientou todas as etapas e participou da revisão final e da edição do artigo.

Apoio. ICJ/CNPQ.