REVISTA DE COMPUTAÇÃO E SISTEMAS (RCS)
ISSN XXXX-XXXX
VOLUME 1 – NÚMERO 1 – ABRIL/2016
http://www.revistacomputacaoesistemas.net

Fortalecimento Do Protocolo De Criptografia Quântica BB84

Nathália Costa e Silva, Rafael Hissato Minomiya, Luciano Silva

Faculdade de Computação e Informática, Universidade Backenzie, São Paulo
nat.thalia.cs@gmail.com, minomiyarafael@gmail.com
luciano.silva@mackenzie.br

Abstract. *An alternative to classical cryptography methods is the quantum cryptography, whose security is assured by quantum physics laws, and it can be simulated in optical fiber. The BB84 protocol is a quantum distribution key protocol which uses two bases for polarization of photons, providing half of the information for an eavesdropper on each measure. In order to reduce the information intercepted by the eavesdropper, it was proposed a strengthening for this protocol, and, to achieve the proposed objectives on this project, there were added two new bases for polarization in order to complicate the eavesdropper's measurements, reducing the information acquired by him. To avoid damaging the protocol, it was necessary to introduce a different method to do the measurements and polarizations of the photons using a cyclic key, composed by pairs of the bases. The results were satisfactory, since the goal of strengthening the security of BB84 protocol was achieved by decreasing the amount of information that an eavesdropper is able to get without being detected, and it wasn't necessary neither to increase the quantity of information which goes by the quantum channel, nor to decrease the information the receiver acquires on his measurements.*

Resumo*. Uma alternativa aos métodos de criptografia clássica é a criptografia quântica, cuja segurança é garantida pelas leis da física quântica, e pode ser simulada em fibra ótica. O protocolo BB84 é um protocolo de distribuição de chaves quântica que utiliza duas bases para polarização dos fótons, fornecendo, assim, metade da informação para um intruso a cada medida. Com a finalidade diminuir a informação interceptada por um intruso, foi proposto um fortalecimento deste protocolo, e, para alcançar os objetivos propostos neste trabalho, foram adicionadas duas novas bases para polarização, para dificultar as medições de um intruso, diminuindo, assim, a informação adquirida por ele. Para não prejudicar o protocolo, foi necessário introduzir um método diferente para realizar as polarizações e as medições dos fótons, utilizando uma chave cíclica, formada por pares de bases. Os resultados foram satisfatórios, uma vez que o objetivo de reforçar a segurança do protocolo BB84 foi alcançado, diminuindo a quantidade de informação que um intruso pode adquirir sem ser detectado, sem a necessidade de aumentar a quantidade de informação que trafega no canal quântico, nem diminuir a informação que o receptor adquire com suas medições.*

1 Introdução

A Criptografia é a ciência cujo objetivo é proteger informações privadas e assegurar a integridade dos dados e a autenticidade das partes envolvidas. A segurança dos métodos clássicos de criptografia é garantida pela dificuldade de problemas matemáticos, como a fatoração de números inteiros, utilizada pelo RSA, e o problema do logaritmo discreto, usado em curvas elípticas. Com o surgimento da computação quântica e dos algoritmos quânticos de Shor para fatoração de números inteiros e cálculo de logaritmos discretos, a criptografia clássica ficou, pelo menos em teoria, vulnerável. Ainda que não exista um computador quântico para quebrar os métodos de criptografia clássica, alternativas já são estudadas (BRUSS *et al*., 2007).

Uma alternativa é a criptografia quântica, ou distribuição de chaves quântica. Segundo Marquezino (2003), é provadamente segura a distribuição de chaves quânticas utilizando estados não-ortogonais, com um protocolo como o BB84, e se houver espionagem, o canal será perturbado, causando um aumento detectável na taxa de erro. Além disso, na mecânica quântica, não é possível clonar um *qubit*, portanto a segurança da criptografia quântica é garantida pelas leis da física quântica (BRUSS *et al*., 2007).

O protocolo BB84 é um protocolo no qual Alice utiliza um canal quântico para enviar *bits* codificados utilizando fótons polarizados na base retilínea (0º ou 90º) ou diagonal (45º ou 135º), aleatoriamente, para Bob, que faz medições nos *qubits* em alguma das duas bases, também aleatoriamente. O protocolo consiste em garantir que Alice e Bob obtenham uma chave única e que um intruso seja detectado (MARQUEZINO, 2003).

O objetivo deste trabalho é propor uma forma de fortalecer o protocolo de distribuição de chaves quântica BB84 acrescentando duas bases para polarização além das bases retilínea e diagonal, sem diminuir a quantidade de informação obtida por Bob, porém diminuindo a informação que um possível intruso pode conseguir.

O artigo está dividido em computação quântica, informação quântica, protocolo BB84, fortalecimento do protocolo BB84, conclusões e trabalhos futuros. Nos dois primeiros tópicos foram definidos conceitos relevantes sobre computação quântica e informação quântica para, em seguida, explicar o funcionamento do protocolo BB84, no terceiro tópico. A seção do fortalecimento do protocolo BB84 esclarece e justifica a proposta do trabalho e as decisões tomadas em relação a ela. Por fim, o tópico conclusões e trabalhos futuros mostra se o objetivo do trabalho foi alcançado e sugere pesquisas posteriores possíveis sobre o fortalecimento.

2 Computação Quântica

A computação quântica refere-se ao processamento de computadores quânticos, os quais utilizam a álgebra quântica, baseada na teoria da mecânica quântica. Uma das diferenças entre a computação clássica e a computação quântica é a unidade de informação utilizada: na clássica, utiliza-se o *bit (binary digit)*, representado numericamente por "*0*" ou "*1*", que podem ser interpretados respectivamente como tensão baixa ou alta, desligado ou ligado, etc.; já na computação quântica, é utilizado o *qubit (quantum bit)*, que, diferente do *bit*, pode ser interpretado como $|0\rangle$ ou $|1\rangle$, análogos aos estados clássicos 0 e 1, ou uma superposição dos dois estados (MELO; CHRISTOFOLETTI, 2003). A notação padrão para estados

quânticos, representada por "| >", é chamada notação de Dirac (NIELSEN; CHUANG, 2010).

O *qubit*, que, como visto anteriormente, é usado na computação quântica como unidade de informação, é um objeto quântico e segue as leis que regem o mundo micro, da mecânica quântica. O *bit* clássico pode ser representado fisicamente pela tensão elétrica, já os *qubits* são representados por objetos quânticos com estados bem distintos, como a polarização do fóton, *spins* quânticos, átomos de dois níveis como mostrado na Figura 1, dentre outros (NIELSEN; CHUANG, 2010).

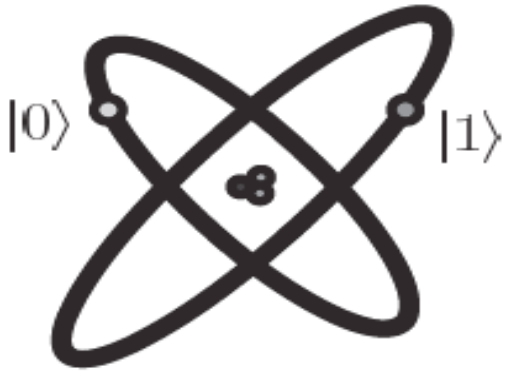

Figura 1: *Qubit* representado por dois níveis eletrônicos em um átomo.

Visto que os *qubits* são superposições de dois estados, dois *qubits* podem ser uma combinação de todos os números de dois *bits* ao mesmo tempo, três *qubits* podem ser uma combinação de todos os números de três *bits* ao mesmo tempo, e assim por diante. Com isso, têm-se o chamado paralelismo quântico (FERNANDES et al, 2007).

Formalmente, o *qubit* é um vetor em um espaço de Hilbert (GRIFFITHS, 2005) de duas dimensões, os estados |0> e |1> são denominados estados da base computacional e formam uma base ortonormal nesse espaço vetorial. O *qubit* $|\psi\rangle$ é representado da seguinte forma:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle ,$$

sendo que $\alpha, \beta \in \mathbb{C}$ e $|\alpha|^2 + |\beta|^2 = 1$, ou seja, o estado quântico $|\psi\rangle$ pode colapsar para o estado $|0\rangle$ com probabilidade $|\alpha|^2$ e para o estado $|1\rangle$ com probabilidade $|\beta|^2$. Em um *qubit*, os valores "0" e "1" podem ser armazenados ao mesmo tempo com a sobreposição. O estado de um *qubit*, expresso geometricamente, é a rotação de um vetor na esfera de *Bloch* (NIELSEN; CHUANG, 2010), como mostra a Figura 2, próxima página, e pode ser representado da seguinte maneira:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\Phi}\text{sen}\frac{\theta}{2}|1\rangle .$$

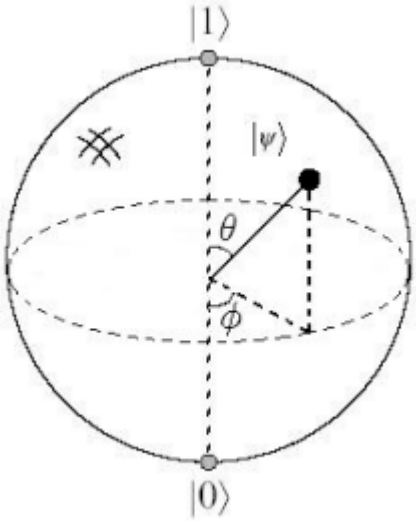

Figura 2: Representação de um *qubit* na esfera de Bloch.

Um sistema físico muda com o tempo, o mesmo acontece com um *qubit* $|\psi>$. A evolução de um sistema quântico é descrita por um operador unitário, ou seja, sendo o estado inicial do sistema $|\psi_1>$ e o estado final $|\psi_2>$, existe um operador unitário U que satisfaça $|\psi_2> = U|\psi_1>$. Um operador em um espaço de Hilbert de duas dimensões para um único *qubit* pode ser representado por uma matriz de dimensão 2x2 (KAYE et al, 2007).

Visto que os *qubits* são representados por vetores no espaço de Hilbert, as portas lógicas, que na computação clássica são circuitos, na computação quântica são operadores, isto é, matrizes, os quais são aplicados a esses vetores (FERNANDES et al, 2007).

Por outro lado, durante uma medição, o processo não é unitário. Suponha um sistema com N estados, |0>, |1>, ..., |N-1>, e um aparato que seja capaz de distingui-los. A medição é o processo pelo qual se obtém como resultado uma descrição clássica de um estado quântico, ou seja, o aparato terá como resposta *i*, com probabilidade $|\alpha_i|^2$ e o estado do sistema convergirá para |i> (KAYE et al, 2007). Em outras palavras, o simples fato de medir o estado de um *qubit* $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ destrói o estado quântico, retornando sempre $|0>$ ou $|1>$ nas medições, com as respectivas probabilidades $|\alpha|^2$ ou $|\beta|^2$, e nunca uma sobreposição dos dois estados (NIELSEN; CHUANG, 2010).

Concluindo, os três axiomas da mecânica quântica são a superposição, a qual diz que o estado quântico de um sistema é um vetor unitário em um espaço de Hilbert, a medição, a qual declara que, ao fazer uma medida, o estado colapsa para uma das bases com certa probabilidade, e a evolução unitária, a qual exprime que a evolução de um estado quântico no tempo corresponde a uma rotação no espaço de Hilbert.

Para entender a computação quântica, é preciso entender como a mecânica quântica funciona quando há um sistema em que haja interação entre dois ou mais *qubits*, isso será melhor explicado ao longo do texto. Quando dois *qubits* são tratados como um único sistema, diz-se que o espaço do sistema combinado é o produto tensorial dos dois espaços, isto é, esteja o primeiro *qubit* no estado $|\psi_1>$ e o segundo no estado $|\psi_2>$, o estado combinado é $|\psi_1> \otimes |\psi_2>$, que pode ser escrito $|\psi_1>|\psi_2>$ ou $|\psi_1\psi_2>$ (KAYE et al, 2007).

3 Informação Quântica

A informação é uma quantidade abstrata e, para processar, armazenar ou transmitir uma informação é necessário codificar o conteúdo para um sistema físico e aplicar as leis da física para processar a informação. A informação na computação clássica é codificada em *bits*, que são representadas, por exemplo, por tensão alta ou tensão baixa, e que, portanto, obedecem as leis da mecânica clássica. Para processar uma informação quântica, é necessário um objeto quântico, por exemplo os átomos, elétrons, fótons, ou qualquer outra partícula a nível atômico. Na computação quântica a informação é representada por *qubits*, apresentado no tópico anterior, que são regidos pelas propriedades da mecânica quântica.

A física clássica não é capaz de explicar a mecânica do mundo subatômico, o que torna os *qubits* diferentes dos *bits*. Por exemplo, na teoria da informação quântica, não é possível copiar o estado quântico $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ de um *qubit* e produzir duas copias $|\psi\rangle\ |\psi\rangle$ sem ter conhecimento dos valores de α e β, devido a linearidade da mecânica quântica, como será observado a seguir.

Suponha *U* como uma operação unitária que pode clonar um *qubit*. Então *U* pode clonar os estados $|0\rangle$ e $|1\rangle$:

$$U|0\rangle = |00\rangle \quad (1)$$

$$U|1\rangle = |11\rangle \quad (2).$$

Como uma operação unitária pode ser representada por uma matriz, podemos aplicar *U* em um *qubit* genérico $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ e resultará em $U|\psi\rangle = \alpha U|0\rangle + \beta U|1\rangle$. Substituindo as expressões 1 e 2, como segue:

$$U(|\psi\rangle) = \alpha|00\rangle + \beta|11\rangle \quad (4).$$

Se a operação *U* clonar um *qubit* deverá apresentar o seguinte resultado:

$$U(|\psi\rangle) = |\psi\rangle\ |\psi\rangle = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle \quad (5).$$

O resultado da expressão 4 é diferente da expressão 5, concluindo a propriedade quântica da impossibilidade de se clonar um *qubit*. Esta propriedade, chamada de teorema da não-clonagem, tem vantagens e desvantagens no processamento da informação quântica. Por não ser possível clonar um *qubit*, a transmissão de informação ganha um reforço em segurança, por outro lado, não é possível efetuar uma correção de erro em um *qubit* como nos *bits* clássicos, armazenando uma cópia de segurança, por exemplo (VENDRAL, 2006).

Outra propriedade da mecânica quântica que a mecânica clássica não está apta para responder é o fato de que as partículas ou sistemas subatômicos são capazes de se emaranhar, o que significa que se dois sistemas estiverem emaranhados, os valores de certas propriedades de um sistema estarão correlacionados com os valores que as propriedades assumirão do outro sistema, um interferindo diretamente no resultado do outro, mesmo que separados espacialmente (MCMAHON, 2008). Em outras palavras, diz-se que dois *qubits* estão emaranhados se não for possível escrevê-los como um produto tensorial de outros estados (PAPADAKOS, 2001).

O emaranhamento, por outro lado, pode ser uma alternativa para fazer uma medição em um *qubit* sem destruir seu estado quântico, pois, ao medir o primeiro *qubit*, ele converge para

um valor, e, simultaneamente, o segundo *qubit* também converge, com isso pode-se determinar seu valor sem observá-lo (FERNANDES et al, 2007).

Um exemplo de emaranhamento bastante utilizado é o estado de Bell, ou par de Bell, que possui quatro configurações diferentes, porém com as mesmas propriedades:

$$|\Phi^+> = \frac{1}{\sqrt{2}}|00> + \frac{1}{\sqrt{2}}|11>,$$

$$|\Phi^-> = \frac{1}{\sqrt{2}}|00> - \frac{1}{\sqrt{2}}|11>,$$

$$|\Psi^+> = \frac{1}{\sqrt{2}}|01> + \frac{1}{\sqrt{2}}|10>,$$

$$|\Psi^-> = \frac{1}{\sqrt{2}}|01> - \frac{1}{\sqrt{2}}|10>.$$

O estado de Bell é uma superposição com mesma amplitude para os estados |00> e |11> e tem como propriedade os resultados correlacionados, isto é, ao medir o primeiro *qubit*, sabe-se o valor do segundo *qubit* sem realizar uma medição. Em outras palavras, a probabilidade de se obter 0 é ½ e a probabilidade de se obter 1 é ½, porém, ao fazer a medição no primeiro *qubit*, se for encontrado 0, sabe-se que o segundo *qubit* será 0 com probabilidade 1 e seu estado será |00>, ou, se o resultado do primeiro *qubit* for 1, o segundo *qubit* também será 1 e seu estado será |11>. Os resultados são coordenados, independentemente da distância a que são separados os dois *qubits*. Uma das utilidades do par de Bell é o teletransporte quântico (NIELSEN; CHUANG, 2010), explicado a seguir.

Como foi demonstrado, é impossível copiar um *qubit* desconhecido segundo o teorema de não-clonagem, porém é possível transmitir um estado quântico de um lugar para outro através do teletransporte quântico.

O teletransporte quântico é um protocolo que utiliza a propriedade do emaranhamento quântico para teletransportar um *qubit* de Alice para Bob (KAYE et al, 2007), como detalhado a seguir e ilustrado na Figura 3.

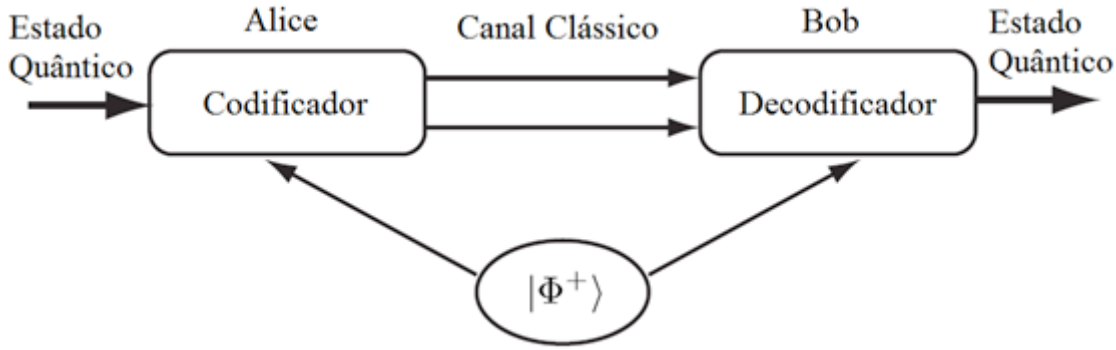

Figura 3: Teletransporte quântico.

Alice e Bob, em algum momento no passado, compartilharam um par de Bell no estado $|\Phi^+> = \frac{1}{\sqrt{2}}|00> + \frac{1}{\sqrt{2}}|11>$. Alice, então, quer enviar um *qubit* $|\psi>$ em um estado desconhecido a Bob, ou seja, um *qubit* $|\psi> = a|0> + b|1>$, entretanto ela não pode fazer uma cópia deste estado, tampouco pode medi-lo para obter os valores de a e b visto que, ao fazer a medição, obtém-se 0 com a probabilidade $|a|^2$ ou 1 com a probabilidade $|b|^2$, e não os valores desejados. Além disso, realizando a medição, o estado do *qubit* torna-se o estado para o qual ele convergiu, não sendo possível repetir o experimento.

O estado inicial dos três *qubits* obtidos por Alice e Bob é:

$$|\psi> |\Phi^+> = a|000> + b|100> + a|011> + b|111>.$$

Alice mede seus dois *qubits*, o *qubit* que deseja mandar e o seu *qubit* do par de Bell, seu estado após a medição é um entre os estados a seguir:

$$|00> (a|0> + b|1>),$$

$$|01> (a|1> + b|0>),$$

$$|10> (a|0> - b|1>),$$

$$|11> (a|1> - b|0>),$$

cada um com probabilidade $\frac{1}{4}$.

O fato de Alice ter feito a medida faz com que o estado colapse para uma das quatro possibilidades e produza dois *bits* clássicos, que são enviados a Bob. Se necessário, Bob aplica operações em seu *qubit* utilizando portas quânticas, e obtém como resultado o estado $|\psi> = a|0> + b|1>$, estado que Alice queria enviar a princípio (STEANE, 1997).

O teletransporte quântico não contradiz o teorema de não-clonagem, pois a informação original, do lado de Alice, é destruída para ser transmitida e recebida do lado de Bob (NAKAHARA; OHMI, 2008).

Concluindo, o teletransporte quântico permite que Alice envie a Bob um estado quântico apenas utilizando *qubits* emaranhados - o par de Bell -, enviando dois *bits* clássicos e fazendo medições locais, o que não exige um canal quântico de comunicação e pode ser realizado a longas distâncias. Pode-se dizer, portanto, que Alice envia para Bob um estado quântico sem enviar nenhuma informação quântica (KAYE et al, 2007).

Uma das aplicações da teoria da informação quântica é a criptografia quântica. A criptografia tem como principal função estabelecer uma comunicação segura entre duas partes, Alice e Bob, e evitar que um provável intruso, Eve, consiga obter informações dessa comunicação. A criptografia quântica utiliza a mecânica quântica para garantir uma distribuição de chaves segura em um canal público, as quais serão usadas posteriormente em métodos de criptografia de chave privada. Por isso, a criptografia quântica também é chamada de distribuição de chave quântica (FERNANDES et al, 2007).

A mecânica quântica pode ser utilizada para garantir a segurança da criptografia quântica, pois, como foi definido anteriormente, as informações não podem ser copiadas, segundo o teorema de não-clonagem, e qualquer ganho de informação de Eve pode perturbar o sistema. O primeiro protocolo de distribuição de chave quântica foi o Protocolo BB84, apresentado a seguir (PAPADAKOS, 2001).

4 Protocolo Bb84

Em 1984, foi publicado o primeiro método de criptografia quântica, ou seja, o primeiro protocolo de distribuição de chaves quântica, desenvolvido por Charles Henry Bennet e Gilles Brassard, o que originou a sigla BB84 (MARQUEZINO, 2003). Um protocolo de distribuição de chaves quântica, ou DCQ (do inglês, *quantum key distribution* ou QKD), tem a função de estabelecer uma conexão segura na qual Alice usa um canal quântico para

enviar *qubits* para Bob, os quais serão utilizados para formar chaves secretas, que serão usadas em outros métodos de criptografia, usados para o envio de mensagens (BRUSS et al, 2007).

Os protocolos de distribuição de chaves quântica, assim como o BB84, utilizam dois canais de comunicação, um canal clássico e um canal quântico, que estão ilustrados na figura 4 (NAKAHARA; OHMI, 2008).

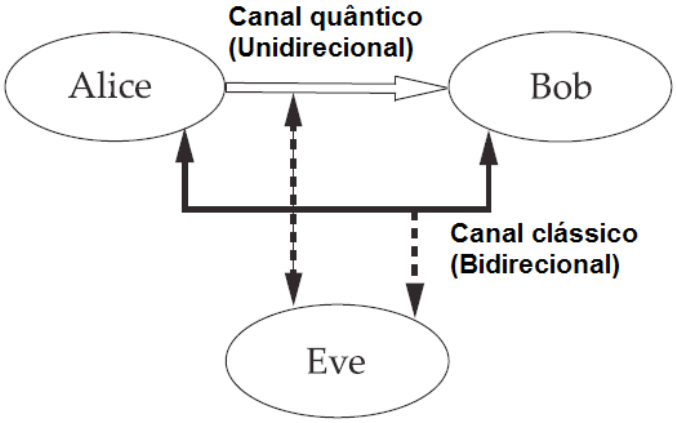

Figura 4: Canais utilizados no protocolo BB84.

O canal clássico é utilizado para transportar a mensagem criptografada, utilizando a chave estabelecida pelo protocolo BB84, por uma rede clássica como, por exemplo, a internet. Já o canal quântico se diferencia por transmitir apenas estados quânticos, como fótons polarizados, isto é, no caso de um protocolo DCQ, é utilizado para estabelecer um canal seguro para troca de chaves secretas, com a capacidade de detectar um intruso no meio da comunicação. O canal quântico não é utilizado para troca de mensagens por não ser tão eficaz em relação ao tempo e custo.

A seguir será descrito com mais detalhes o funcionamento do protocolo BB84 utilizando canais de comunicação ideais, sem ruído.

Suponha que um transmissor, Alice, queira transmitir uma mensagem secreta para um receptor, Bob, e precisa evitar que um intruso, Eve, intercepte a mensagem. Antes de iniciar o protocolo, Alice e Bob precisam ter conhecimento de uma pequena chave secreta para autenticação, para evitar que Eve tente se passar por um dos dois ao iniciar o protocolo, esta chave será usada apenas no início do protocolo e depois será descartada, o próprio protocolo ficará encarregado de gerar novas chaves de autenticação.

Após a verificação de autenticidade de Alice e Bob, usando a chave secreta para o início do protocolo, Alice irá escolher aleatoriamente uma sequência de *bits* e uma sequência de bases para polarização dos fótons, que podem ser diagonal (x) ou retilínea (+), sendo uma base para cada *bit*. Na base retilínea, os fótons são polarizados em 0 ou 90 graus e, na base diagonal, são polarizados em 45 ou 135 graus. Em seguida, Alice envia os *qubits* para Bob na forma de fótons polarizados de acordo com o valor de cada *bit* e sua respectiva base, seguindo o padrão:

- para enviar o *bit* 0, o fóton deverá ser polarizado em 0° na base retilínea ou 45° na base diagonal;
- para enviar o *bit* 1, o fóton deverá ser polarizado em 90° na base retilínea ou 135° na base diagonal.

Para efetuar a leitura de cada *qubit*, Bob deverá escolher aleatoriamente uma das bases, diagonal (x) ou retilínea (+), e guardar as informações sobre qual base foi usada e qual o resultado de cada *qubit* medido, sendo que as informações obtidas só estarão corretas quando Bob fizer a medição do *qubit* na mesma base que Alice usou para codificá-lo, caso contrário, o resultado será aleatório.

Após a medição de todos os *qubits*, Bob terá uma sequência de *bits*, chamada de "chave bruta" (*raw key*). Os *bits* enviados por Alice compõem sua chave bruta, que é diferente em 25% da chave bruta de Bob, devido aos erros das medições incorretas.

A criação da chave bruta é conhecida como o primeiro passo do Algoritmo BB84. Neste passo, verifica-se que a as chaves brutas combinam em 75% dos *bits*, porém ⅓ dos *bits* corretos foram obtidos aleatoriamente, devido às medições que foram realizadas utilizando bases erradas e geraram resultados aleatórios. Como Alice enviou para Bob apenas as bases corretas na medição, não é possível para Bob identificar os *bits* que foram obtidos corretamente por meio de bases erradas, por isso são descartados, restando 50% da chave bruta.

Em seguida, é executado o segundo passo do protocolo, a reconciliação de bases. Nesta etapa, Alice envia para Bob, utilizando o canal clássico, as bases que ela utilizou para a geração de sua chave bruta e Bob envia para Alice a sequência de polarizadores que ele utilizou nas medições dos fótons, mas sem revelar o resultado das medições. Ambos comparam as duas bases, as que Alice utilizou para polarizar os fótons e as que Bob usou para medi-los, e descartam as bases divergentes. Com isso, 50% da chave é descartada, restando apenas os valores que Bob mediu utilizando as mesmas bases de Alice. Os *bits* restantes formam a chamada "chave filtrada" (*sifted key*).

No terceiro passo do protocolo é feita a verificação de intrusos. Utilizando a chave filtrada, é possível detectar se algum intruso interceptou a comunicação verificando a taxa de erro. A taxa de erro dos *bits* quânticos (do inglês *quantum bit error rate*, ou QBER) é utilizada para verificar a porcentagem de erro entre as chaves filtradas. Alice e Bob divulgam um subconjunto aleatório da chave filtrada e calculam o QBER que, teoricamente, deveria ser zero, supondo uma comunicação ideal, sem ruído. Se Eve fizer a medição de algum *qubit* antes de Bob, Eve interferirá no sistema e introduzirá ruído nas medições de Bob, podendo, assim, ser detectado antes que Alice e Bob transmitam qualquer informação sigilosa. Se for detectado algum intruso na comunicação, Alice e Bob voltam ao início do protocolo e começam novamente. Caso contrário, os *bits* usados para verificação são descartados e o protocolo segue para o próximo passo.

No quarto passo do protocolo, é utilizada quando não há um canal de comunicação ideal, ou seja, o protocolo é realizado em um canal com ruído. Esta etapa corrige os erros encontrados na terceira etapa, aplicando algoritmos de correção de erros, com a finalidade de corrigir os ruídos introduzidos pelo canal de comunicação ou pelos equipamentos utilizados na criptografia quântica. Esses ruídos são comuns na prática, não há como garantir 100% que uma comunicação à distância não tenha ruídos. É importante salientar que, na prática, se Eve fizer medições em parte da comunicação entre Alice e Bob, a terceira etapa do protocolo pode confundir a interferência de Eve com um ruído de canal ou do sistema e, chegando na quarta etapa, esses ruídos serão corrigidos, assim Eve não será detectada.

Para garantir que Eve não consiga informação suficiente para colocar em risco a comunicação, é aplicada a quinta etapa do protocolo, denominada ampliação de privacidade. Nesta etapa, a chave é reduzida para minimizar a informação obtida por Eve (MARQUEZINO, 2003).

A segurança do protocolo BB84 é garantida pelas propriedades da mecânica quântica como o teorema da não clonagem, o que impossibilita que Eve consiga fazer uma cópia do *qubit*, além disso, se Eve fizer uma medição, ele perturbará o sistema. Outro fato que garante a segurança do protocolo é o terceiro passo, que detecta a presença de ruídos no canal quântico, acusando a intrusão de Eve e, caso não seja detectada por interceptar apenas parte da informação, o quinto passo, o qual amplifica a privacidade da chave, reduzindo a informação de Eve para valores aceitáveis (MARQUEZINO, 2003).

A Tabela 1 exemplifica o uso do protocolo BB84:

Tabela 1: Tabela para exemplificar o funcionamento do protocolo BB84.

Bits enviados	1	0	0	1	0	1	1	1	0	0	1	0	1	0	1
Base Alice	+	+	x	x	+	x	+	x	x	x	+	+	+	x	+
Base Bob	x	+	x	x	x	+	+	x	+	x	+	x	x	+	+
Chave		0	0	1			1	1		0	1				1

A Tabela 1 ilustra um exemplo simplificado do funcionamento do protocolo BB84. A primeira linha da tabela mostra a chave bruta de Alice, ou seja, a sequência de *bits* aleatórios que Alice escolheu para enviar a Bob, e a segunda linha mostra as polarizações que ela usou para codificar cada *bit*, a polarização retilínea está representada pelo símbolo + e a polarização diagonal pelo símbolo x. A terceira linha apresenta as polarizações usadas por Bob para medir cada fóton recebido. As três primeiras linhas referem-se ao primeiro passo do protocolo.

A quarta linha da tabela é correspondente ao segundo passo do protocolo, no qual Alice envia a Bob quais polarizações foram utilizadas para codificar os *bits* e Bob envia à Alice as polarizações usadas para medi-los. Com essas informações, Alice e Bob descartam os *bits* que não foram medidos na mesma base em que foram codificados, formando, assim, a chave filtrada. Neste exemplo, o primeiro, o quinto, o sexto, o nono, o décimo segundo, o décimo terceiro e o décimo quarto *bits* foram descartados por serem resultados aleatórios, resultando na chave filtrada 00111011.

Este exemplo é apenas uma ilustração simplificada. No protocolo completo, Alice e Bob ainda fariam as outras etapas, comparando parte das chaves filtradas obtidas para verificação de intrusos, correção de erros e amplificação da privacidade. Além disso, na prática o número de *bits* usados seria maior.

Pode-se observar que, sem a interferência de um intruso, Bob só obtém a informação correta nos *qubits* que forem medidos na mesma base que Alice os codificou. Caso contrário, as informações obtidas por Bob são aleatórias e, portanto, descartadas. A Figura 5, próxima página, ilustra os possíveis casos de medições realizadas.

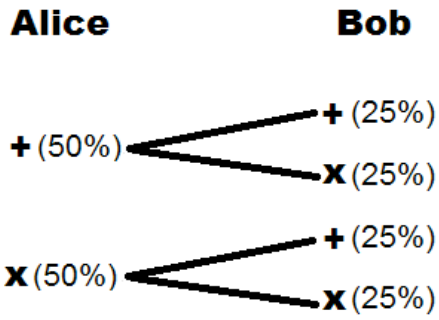

Figura 5: Casos possíveis sem interferências de um intruso.

É possível observar que metade da informação é descartada por não ter sido medida na base correta. Portanto, Alice e Bob aproveitam apenas 50% dos *bits* enviados, isto é, a chave filtrada tem metade do tamanho da chave bruta.

Supondo que não haja ruído no canal, mas que um intruso esteja fazendo uma espionagem e reenviando os *qubits* para Bob, as possibilidades de medidas são mostradas na figura 6.

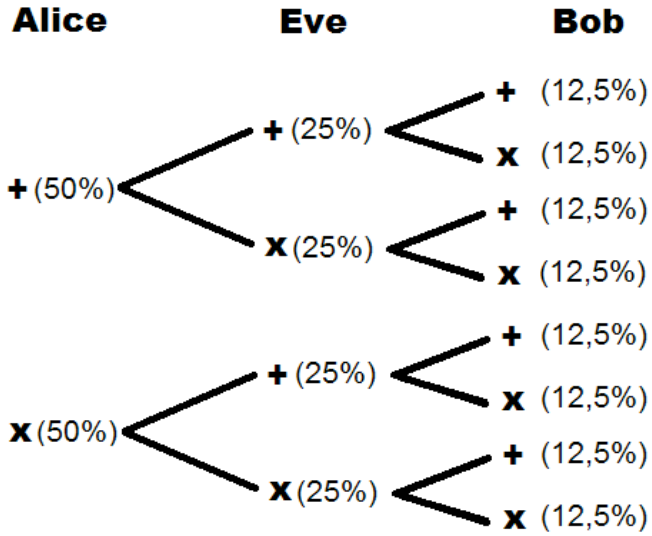

Figura 6: Casos possíveis com a interferência de um intruso.

Neste caso, Eve possui informações corretas quando suas medições forem feitas na mesma base que Alice fez as polarizações, portanto Eve consegue metade da informação. Por outro lado, quando Eve medir na base errada mas Bob fizer a medição na base correta, Bob, na verdade, estará recebendo informações aleatórias, portanto Eve acrescenta uma taxa de erro.

A chave filtrada, como dito anteriormente, é composta pelos *bits* que forem codificados por Alice e medidos por Bob nas mesmas bases, então, mesmo que Eve faça a medição em uma base diferente, esses *bits* farão parte da chave filtrada, como mostra a Tabela 2, próxima página, porém os valores serão aleatórios.

Tabela 2: Chave filtrada em caso de espionagem.

Base utilizada por Alice	+	+	x	x
Base utilizada por Eve	+	x	+	x
Base utilizada por Bob	+	+	x	x
Ocorrência na *sifted key*	25%	25%	25%	25%

Nos casos em que Eve faz medições nas mesmas bases que Alice e Bob, o resultado obtido por Bob não é alterado, porém, quando Eve introduz uma medição com uma base errada, os resultados das medições de Bob são aleatórios, portanto apenas metade dos resultados está correta. Com isso, tem-se que a taxa de erro da chave filtrada com a espionagem é de 25%, metade da segunda coluna e metade da terceira coluna da figura 8 (MARQUEZINO, 2003). Caso Alice e Bob obtenham uma taxa de erro tão alta, é interessante que eles abortem o protocolo (BRUSS *et al*., 2007).

Há, também, uma versão do protocolo BB84 baseada em emaranhamento. Essa versão utiliza ideias do protocolo BB84 com conceitos de emaranhamento vistos no teletransporte quântico. Alice e Bob compartilham um número n estado de Bell:

$$|\Phi^+>^{\otimes n} = |\Phi^+> \otimes \ldots \otimes |\Phi^+>.$$

Com isso, sabe-se que os resultados das medidas de Alice e Bob estão correlacionados, e, como esses estados são puros, não é possível para Eve emaranhá-los com outros *qubits* (BRUSS et al, 2007). O funcionamento deste protocolo, porém, não será aprofundado por não ser o foco deste artigo.

5 Fortalecimento Do Protocolo Bb84

O protocolo BB84 utiliza duas bases em todo o processo, a base retilínea com as polarizações em 0° ou 90° e a base diagonal com polarizações em 45° ou 135°. Se um intruso tentar interceptar a comunicação do protocolo BB84, em cada medição feita, o intruso terá uma probabilidade de 50% para acertar a base escolhida por Alice e obter uma parte da informação. Para minimizar a informação obtida pelo interceptador, o protocolo BB84 utiliza um passo de amplificação de privacidade, contudo esse processo não é capaz de reduzir a zero a informação obtida por Eve.

A ideia principal deste trabalho é minimizar a informação que um intruso consegue extrair ao observar o canal quântico, sem a necessidade de enviar uma quantidade maior de *qubits*, aumentando, assim, a segurança do protocolo. Primeiro será explicada a proposta de fortalecimento, depois serão mostrados os cálculos que levaram às decisões. No decorrer da explicação serão feitas comparações da proposta com o protocolo BB84 e serão apresentados alguns exemplos.

A proposta para o fortalecimento do protocolo BB84, é a inclusão de duas novas bases para a polarização e medição dos fótons sem diminuir a informação obtida por Bob. Para isso, será utilizada uma estratégia na polarização e medição dos fótons.

A estratégia adotada consiste em usar chaves cíclicas, compostas por seis pares formados pelas quatro bases. Esta chave deve ser compartilhada antes do início do protocolo, como verificador, para evitar que Eve tente se passar por Alice ou Bob e estabeleça uma comunicação falsa.

O início do fortalecimento do protocolo BB84 é semelhante, em parte, ao protocolo original, no qual Alice escolhe aleatoriamente uma sequência de *bits* que, no caso do fortalecimento, deverá ser um conjunto de seis pares, ou múltiplos de seis, isso será melhor detalhado ao longo do texto. Em seguida, Alice polarizará os fótons de acordo com o valor do *bit*. Para isso, Alice deve utilizar a sua chave cíclica compartilhada com Bob e, seguindo a ordem da

chave, ela deverá escolher aleatoriamente uma das duas bases de cada par e enviar o fóton a Bob.

Para Bob realizar as medições, ele também deverá utilizar a chave cíclica. Da mesma forma que Alice, Bob irá escolher uma entre as duas bases de cada par da chave cíclica, respeitando a ordem. Como Alice e Bob possuem as mesmas chaves cíclicas a probabilidade de Bob acertar uma medição é de 50%, a mesma proporção oferecida pelo protocolo BB84. Mas, para um intruso, as chances de interceptar uma informação com quatro bases é de 25%, ao contrário do BB84, que fornece 50%.

Após Bob realizar as medições, ele anuncia para Alice, por meio de um canal clássico, as bases que escolheu para medir os *qubits*, e Alice envia para Bob as bases utilizadas para polarizar os fótons. Ambos irão descartar as bases divergentes e, com as bases corretas, formarão a chave filtrada que, a princípio, deverá ser a mesma para ambos, considerando um canal sem ruído.

Com a chave filtrada, Alice e Bob compartilham parte da chave para verificar se houve interceptação na comunicação, calculando a taxa de erro no subconjunto da chave filtrada. Outra vantagem do fortalecimento é tornar o canal mais sensível a intrusos. No protocolo BB84, por exemplo, quando Eve intercepta todos os *qubits* e os reenvia para Bob, Eve introduz um ruído de 25% na chave filtrada, podendo, assim, ser detectado. Aplicando uma estratégia de interceptação, medindo apenas parte da informação, Eve pode não ser detectado e conseguir parte da informação. No fortalecimento proposto, entretanto, se Eve interceptar toda a comunicação o ruído introduzido será de 37,5%, o que obriga Eve a interceptar menos informações que no protocolo BB84 para não ser detectado.

A correção de erros, em caso de um canal com ruídos, e a amplificação de privacidade são realizados da mesma maneira que o protocolo BB84.

Na proposta, são adicionadas duas novas bases ao protocolo BB84, as bases M e N, aplicadas em uma estratégia de chave cíclica. As bases M e N correspondem, às polarizações em 30 ou 120 graus e 60 ou 150 graus, respectivamente, como mostrado na Figura 7. Para facilitar a nomenclatura, a base retilínea será chamada de base R e a base diagonal será chamada de base D.

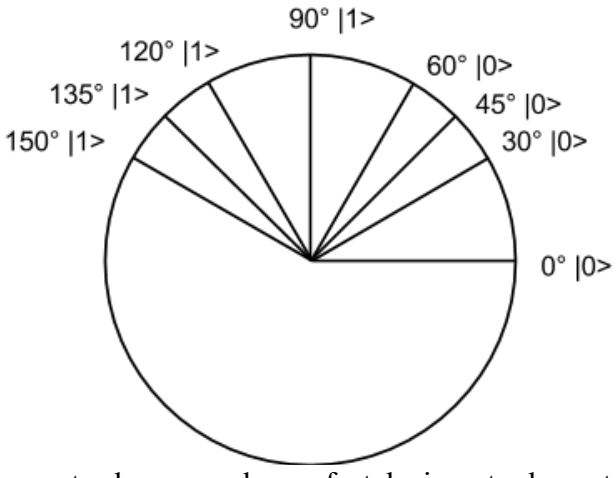

Figura 7: As quatro bases usadas no fortalecimento do protocolo BB84.

Simbolicamente:

- A base R representará os eixos de 0° e 90°;
- A base M representará os eixos de 30° e 120°;
- A base D representará os eixos de 45° e 135°;
- A base N representará os eixos de 60° e 150°.

Abaixo será descrito como aplicar o fortalecimento ao protocolo sem prejudicar a quantidade de informação que Bob consegue medir no protocolo BB84 nem a quantidade de *qubits* que trafegam no canal quântico.

Para iniciar o protocolo BB84, Alice e Bob devem ter conhecimento de uma chave secreta, compartilhada previamente, para evitar que Eve tente se passar por um dos dois. No fortalecimento do protocolo BB84, esta chave secreta deverá ser uma sequência de pares aleatórios, formados pelas quatro bases descritas acima, e o comprimento da chave é calculado e padronizado para garantir maior segurança.

O tamanho mínimo da chave deve ser de seis pares e deve crescer aritmeticamente com razão seis. A quantidade mínima de pares da chave foi calculado de acordo com o número mínimo de comutações das quatro bases, sem privilegiar nenhuma, evitando uma perda maior de informação para Eve, como mostram os cálculos abaixo:

- Há quatro bases diferente, R, D, M e N;
- Deve-se formar a maior sequência de pares possíveis, sem repetição;

Aplicando a fórmula de combinação simples de análise combinatória:

$$\frac{n!}{k!(n-k)!} = \frac{4!}{2!2!} = 6.$$

Onde n é o número de elementos diferentes e k é a quantidade de elementos em cada subconjunto, no caso $k = 2$, pois são pares de bases. Este resultado representa o número de pares diferentes que compõem uma chave. Resultando em seis combinações possíveis de pares de quatro bases distintas, sem repetição:

$$RD, NM, RN, DM, RM, DN.$$

As seis variáveis da chave resultam em 6! combinações, ou seja, 720 chaves diferentes. A probabilidade de Eve acertar aleatoriamente a sequência de uma chave de seis pares é de $1/6!$ = 0,139% para acertar a chave inteira e conseguir medir 50% da informação, ou 1/(6*5*4) = 0,83% de acertar metade da chave e conseguir medir 25% da informação. Portanto, não é interessante para Eve tentar adivinhar a chave pelo desconhecimento do tamanho da chave e porque para cada aumento de seis posições na chave há uma diminuição de cinco casas decimais na probabilidade de Eve acertá-la, como ilustrado no exemplo a seguir :

- A probabilidade de acertar uma chave com seis pares é:

  chave $\{RD, NM, RN, DM, RM, DN\}$

  $$1/6 * 1/5 * 1/4 * 1/3 * 1/2 * 1 = (1/6!)^1 = 0{,}139\%;$$

- A probabilidade de acertar uma chave com doze pares é:

chave $\{RD, NM, RN, DM, RM, DN, RD, NM, RN, DM, RM, DN\}$

$$1/6 * 1/6 * 1/5 * 1/5 * 1/4 * 1/4 * 1/3 * 1/3 * 1/2 * 1/2 * 1 * 1 =$$

$$= 1/6! * 1/6! = (1/6!)^2 = 0{,}193 * 10^{-7} = 0{,}193 * 10^{-5}\% .$$

- A probabilidade de Eve acertar uma chave diminui exponencialmente:

$$(1/6!)^n,$$

onde o aumento de n significa aumentar a chave em $6n$ posições.

Com a inclusão das duas bases, a quantidade de informação que Eve consegue extrair do canal quântico cai de 50% para 25%, ou seja, a quantidade de informação que Eve conseguiria obter no protocolo BB84 é reduzida pela metade com a introdução dessas duas novas bases.

Se, ao invés de tentar descobrir a chave, Eve empregar uma estratégia na medição, como, por exemplo, utilizar apenas uma das bases para aumentar a quantidade de informação extraída, levando em conta que qualquer uma das quatro bases aparecem em metade dos pares da chave, Eve pode escolher uma única base para medir todos os *qubits*. Supondo R como a base escolhida, para cada *qubit* polarizado em um dos três pares RN, RD ou RM, em uma chave de qualquer tamanho ou ordenação, Eve terá 50% de acerto em 50% das medições, o que resulta em 25% da informação, como mostrado na tabela 3. A mudança de estratégia rendeu a Eve 25% da informação, porém, se compararmos ao protocolo BB84, que fornece 50% da informação, esta estratégia melhora em 50% a segurança do protocolo.

Tabela 3: Comparação dos dados obtidos por Eve no protocolo BB84 e no fortalecimento proposto

Bits aleatorios de Alice	*1*	*1*	***0***	*1*	*0*	*0*	***0***	*0*	*1*	*1*	***0***	*1*
Chave inicial de tamanho 12	***RN***	*NM*	***RD***	*DM*	***RM***	*DN*	***RD***	*DN*	***RN***	*DM*	***RM***	*NM*
Base escolhida por Alice no fortalecimento do protocolo BB84	*N*	*M*	***R***	*D*	*M*	*N*	***R***	*D*	*N*	*D*	***R***	*M*
Base escolhida por Alice no protocolo BB84	*R*	*D*	***R***	*D*	*D*	*D*	***R***	*R*	*R*	*D*	***R***	*D*
Base escolhida por Eve	*R*	*R*	***R***	*R*	*R*	*R*	***R***	*R*	*R*	*R*	***R***	*R*
Informação interceptada por Eve no fortalecimento do protocolo BB84			***0***				***0***				***0***	
Informação interceptada por Eve no protocolo BB84	***1***		***0***				***0***	***0***	***1***		***0***	
Informação protegida pelo reforço do protocolo BB84	***1***							***0***	***1***			

Com Alice e Bob compartilhando a mesma chave, $\{RD, NM, RN, DM, RM, DN\}$, pode-se dar início ao fortalecimento do protocolo BB84. Inicialmente, Alice escolhe aleatoriamente uma sequência de *bits*, da mesma forma que no protocolo BB84, porém a quantidade de *bits* deve

ser um múltimplo de 6. A diferença neste primeiro passo é a forma de escolher as bases para a

polarização dos *qubits*. Suponha que Alice escolheu aleatoriamente a sequência de *bits* 010111001010. Alice, então, aplica a sua chave no início da sequência de *bits* e a repete até cobrir todos os *bits*, como ilustrado na Tabela 4.

Tabela 4: Montagem da chave cíclica

Bits de Alice	0	1	0	1	1	1	0	0	1	0	1	0
Chave compartilhada	RD	NM	RN	DM	RM	DN						
Aplicar a chave até o fim da sequência							RD	NM	RN	DM	RM	DN

Seguindo o padrão do protocolo BB84, Alice irá escolher aleatoriamente uma entre as duas bases, de acordo com a sequência da chave pré-estabelecida, e enviará a Bob os fótons polarizados, como mostra a Tabela 5.

Tabela 5: Utilização da chave cíclica para a polarização dos fótons

Bits de Alice	0	1	0	1	1	1	0	0	1	0	1	0
Chave cíclica	RD	NM	RN	DM	RM	DN	RD	NM	RN	DM	RM	DN
Base escolhida por Alice aleatoriamente baseado no par da chave	R	M	N	D	M	N	R	M	N	D	R	D
Polarização dos fótons	0°	120°	60°	135°	120°	150°	0°	30°	150°	45°	90°	45°

Bob, por sua vez, utilizará o mesmo método de Alice para fazer as medições. Aplicando a sua chave cíclica, ele escolhe aleatoriamente qual das duas bases será utilizada. Em seguida, Bob anuncia para Alice as bases que foram utilizadas para fazer as medições e Alice envia para Bob quais bases foram utilizadas para polarizar cada fóton. Com isso, ambos terão a mesma sequência de *bits*, que compõe a chave filtrada, caso não haja interceptação na comunicação e o canal seja um canal quântico ideal, como demonstrado na Tabela 6, próxima página.

Tabela 6: Utilização da chave cíclica para a medição dos fótons

Bits de Alice	0	1	0	1	1	1	0	0	1	0	1	0
Base escolhida por Alice aleatoriamente	R	M	N	D	M	N	R	M	N	D	R	D
Base escolhida por Bob aleatoriamente	R	M	M	D	N	D	D	M	N	N	R	R
Bits obtidos pelas medições de Bob	0	1		1				0	1		1	

No fortalecimento, assim como no protocolo BB84, após Alice e Bob criarem a chave filtrada, é aplicado o passo de verificação de erro para detectar se houve interceptação de informação ou não, dando continuidade ao protocolo. Sem a presença de um intruso, a quantidade de informação da chave filtrada deve refletir em 50% da chave bruta em um canal ideal. A figura 8 mostra que a informação de Bob estará correta apenas quando ele fizer as medições nas mesmas bases que Alice. A chave cíclica direciona Bob a medições mais precisas, dando duas opções de bases para efetuar cada medida, o que equivale a 50% das medições em cada base, mantendo a mesma proporção que o protocolo BB84.

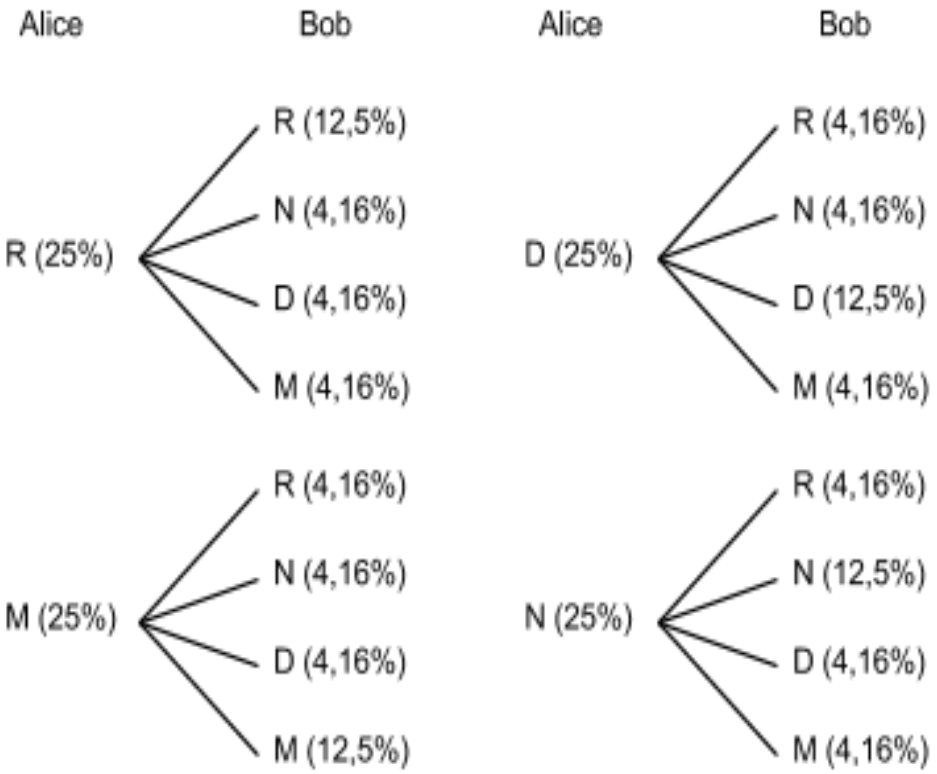

Figura 8: Casos possíveis sem interferências de um intruso.

Quando Eve intercepta toda a comunicação, interceptando e reenviando os *qubits* para Bob, Eve introduz um ruído de 25% na chave filtrada no protocolo BB84, podendo, assim, ser detectado. Com o fortalecimento, se Eve utilizar o mesmo método de interceptação e reenvio, a diferença entre as chaves filtradas sobe para 37,5% e, com um ruído maior, torna-se mais evidente a sua intrusão na comunicação. Como Eve não sabe em qual base medir, ele terá que escolher uma base entre quatro, enquanto Bob escolhe uma entre duas. Isso diminui as chances de Eve de acertar uma medição ao repassar a Bob, que antes era de 50% e agora é 25%.

Pelo fato de a chave cíclica compartilhada entre Alice e Bob antes do início do protocolo ser composta por quantidades iguais de cada base, a probabilidade de Bob medir cada base é a mesma. Ou seja, de todos os fótons polarizados por Alice, metade serão medidos pelas bases corretas e as outras serão medidas pela outra base do par na chave cíclica de Bob. Como Eve não tem conhecimento da chave cíclica, ele terá que medir aleatoriamente em uma das

quatro bases dividindo a probabilidade de cada base em quatro e distorcendo as medições de Bob, como mostra o esquema da figura 9:

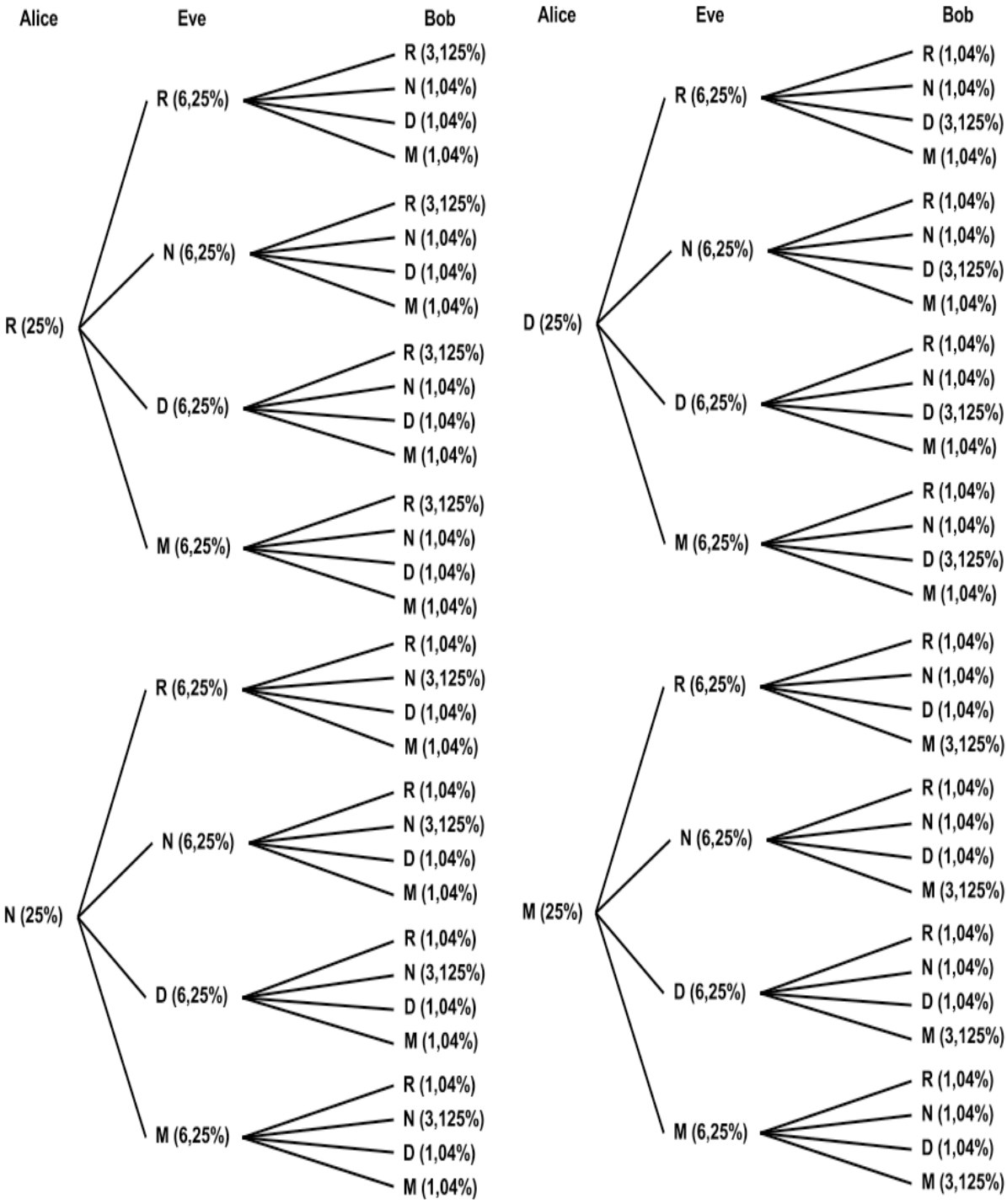

Figura 9: Casos possíveis com a interferência de um intruso.

As medições de Bob, seguindo a chave cíclica, correspondem a 50% nas bases corretas e os outros 50% serão distribuídos nas demais bases. Com a interceptação de Eve, os resultados das medições de Bob dependem das bases que Eve utilizou para medir os *qubits* antes de reenviá-los para Bob, lembrando que, quando Eve introduzir uma base errada e reenviar o *qubit* para Bob, suas medições tornam-se aleatórias, corrompendo metade dessas medições.

A Tabela 7 representa a análise do resultado da chave filtrada, indicando a quantidade de informação que Bob terá com a intrusão de Eve. Para cada base errada que Eve utilizar, Bob terá uma redução de metade da informação correta daquela base, e para cara base correta que Eve utilizar Bob não terá seu resultado alterado.

Tabela 7: Análise da chave filtrada

Base de Alice	R	R	R	R	N	N	N	N	D	D	D	D	M	M	M	M
Base de Eve	R	N	D	M	R	N	D	M	R	N	D	M	R	N	D	M
Base de Bob	R	R	R	R	N	N	N	N	D	D	D	D	M	M	M	M
Chave Filtrada (%)	6,25	6,25	6,25	6,25	6,25	6,25	6,25	6,25	6,25	6,25	6,25	6,25	6,25	6,25	6,25	6,25
Informação correta de Bob (%)	6,25	3,125	3,125	3,125	3,125	6,25	3,125	3,125	3,125	3,125	6,25	3,125	3,125	3,125	3,125	6,25
Informação roubadas por Eve	6,25					6,25					6,25					6,25

Desta forma, é possível calcular a taxa de erro da chave filtrada da seguinte forma:

Informação que Eve utilizou a base correta:

$$4 * 6{,}25 = 25\%.$$

Informação que Eve utilizou uma base incorreta, reduzindo a informação de Bob:

$$12 * 3{,}125 = 37{,}5\%.$$

Observando que a informação que Bob perdeu, não é a informação que Eve ganhou. Sendo assim, a interceptação de Eve introduziu no sistema uma taxa de erro de 37,5%, entretanto, em um canal ideal não deveria haver erros. Neste caso, o procedimento é o mesmo do protocolo BB84, interromper a comunicação e voltar para o início do fortalecimento do protocolo BB84.

Caso não seja detectada a presença de nenhum intruso na comunicação de Alice e Bob, no fortalecimento do protocolo, os passos seguintes são os mesmos do protocolo BB84, correção de erros usando o canal clássico e amplificação de privacidade, para reduzir ainda mais a informação obtida por Eve.

6 Conclusões E Trabalhos Futuros

Este artigo definiu conceitos importantes sobre computação quântica e informação quântica para explicar o funcionamento do protocolo BB84 e sugerir uma forma de fortalecê-lo. O fortalecimento propôs a adição de duas bases além das já existentes para diminuir a informação adquirida por um possível intruso, porém sem comprometer a informação obtida pelo receptor. Cálculos mostram que o método de fortalecimento manteve a porcentagem de informação obtida pelo receptor e aumentou a taxa de erros introduzidos pelo interceptador,

o que, consequentemente, reduz a quantidade de informação que o intruso pode adquirir sem ser detectado pelo protocolo.

Este trabalho tem uma contribuição não só no aumento da segurança do protocolo, que é um dos protocolos de distribuição de chaves quântica mais estudados, mas também no desenvolvimento desta área, ainda pouco trabalhada.

Por ser uma área pouco trabalhada, uma das dificuldades encontradas neste trabalho foi a baixa quantidade de materiais atualizados referentes ao assunto de mecânica quântica e sobre a linguagem de programação quântica QCL (do inglês, *Quantum Computing Language*), se comparados com mecânica clássica e uma linguagem de programação clássica como Java.

Como trabalhos futuros, tem-se a opção de desenvolver um algoritmo do fortalecimento do protocolo BB84, na linguagem QCL (do inglês, *Quantum Computer Language*), e analisar o seu comportamento e desempenho comparado ao protocolo BB84 sem o fortalecimento, com o intuito de adicionar e promover alternativas no ramo da criptografia quântica, e, assim, expandir as opções de protocolos para garantir a segurança da informação na computação quântica, tanto utilizada em fibra ótica, quanto em computadores quânticos, quando forem desenvolvidos.

Outra possibilidade de um trabalho futuro seria o estudo mais aprofundado dos protocolos de distribuição de chave, buscando outra forma de melhorar outros protocolos existentes ou de desenvolver um novo protocolo, mais seguro e eficiente, dando, assim, continuidade ao desenvolvimento e acrescentando material no ramo da computação quântica, para evitar que a segurança da informação quântica seja comprometida com a quebra de um protocolo.

Referências Bibliográficas

BRUSS, D. et al. Quantum cryptography: a survey. Eletronic Colloquium on Computational Complexity, 2006.

FERNANDES, S. R. et al. Criptografia quântica, uma abordagem introdutória. XI Encontro de Modelagem Computacional, 2007.

GRIFFITHS, D. J. Introduction to quantum mechanics. Upper Saddle River: Pearson Prentice Hall, 2005.

KAYE, P. et al. An introduction to quantum computing. New York: Oxford University Press Inc., 2007.

MARQUEZINO, F. L. Estudo introdutório do protocolo quântico BB84 para troca segura de chaves. Revista Eletrônica de Iniciação Científica, 2004.

MCMAHON, D. Quantum computing explained. Hoboken: John Wiley & Sons, Inc., 2008.

CHRISTOFOLETTI, T. V. D.; MELO, B. L. M. Computação quântica: estado de arte. Monografia, Santa Catarina: INE/UFSC, 2003.

NAKAHARA, M.; OHMI, T. Quantum computing: From linear algebra to physical realizations. Boca Raton: CRC Press, 2008.

NIELSEN, M. A.; CHUANG, I. L. Quantum computation and quantum information. Cambridge: Cambridge University Press, 2010.

OLIVEIRA, A. G. Criptografia usando protocolos quânticos. Monografia, Lavras: Universidade Federal de Lavras, 2004.

PAPADAKOS, N. P. Quantum information theory and applications to quantum cryptography. Individual Study Option for the Department of Computing, Imperial College, UK. 2001.

STEANE, A. Quantum computing. Reports on Progress in Physics 61: p 117-173, 1997.

VENDRAL, V. Introduction to quantum information science. New York: Oxford University Press Inc., 2006.