Fundação Educacional do Município de Assis
IMESA - Instituto Municipal de Ensino Superior de

Marcos Patricio do Nascimento

Criptografia Quântica

Novas Tecnologias na Segurança de Dados e Telecomunicações

Assis
2014

Marcos Patricio do Nascimento

Criptografia Quântica

Novas Tecnologias na Segurança de Dados e Telecomunicações

Trabalho de conclusão de
Curso apresentado ao Instituto
Municipal de Ensino Superior
de Assis, como requisito do
curso de Graduação.

Orientador: Luiz Ricardo Begosso

Área de Concentração: Criptografia Quântica

Assis
2014

FICHA CATALOGRÁFICA

Nascimento, Marcos Patricio
Criptografia Quântica – Novas Tecnologias na Segurança de Dados e Telecomunicação / Marcos Patricio do Nascimento: Fundação Educacional do Município de Assis, 2014.
00p.

Orientador: Dr. Luiz Ricardo Begosso.
Trabalho de Conclusão de Curso – Instituto Municipal de Ensino de Assis – IMESA

1. Criptografia 2.Quântica 3.Segurança

CDD: 001.6
Biblioteca da Fema

Assis
2014

CRIPTOGRAFIA QUÂNTICA - NOVAS TECNOLOGIAS NA SEGURANÇA DE DADOS E TELECOMUNICAÇÕES

MARCOS PATRICIO DO NASCIMENTO

Trabalho de conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do curso de Graduação, analisado pela seguinte comissão examinadora.

Orientador: Luiz Ricardo Begosso

Avaliador: Diomara Martins Reigato Barros

Assis
2014

Agradecimentos

Primeiramente a Deus por ter me abençoado nessa caminhada ao longo desses 4 anos, por ter me dado discernimento, tranquilidade, força de vontade e determinação.

Ao meu orientador Luiz Ricardo Begosso, pela disposição e atenção no acompanhamento das diversas etapas desta pesquisa e que nunca deixou de acreditar em mim, sempre me incentivando.

Aos professores Curso de Bacharelado em Ciências da Computação que não pouparam esforços para me ensinar.

Ao demais colegas de graduação, pelas críticas e sugestões.

À minha esposa pelo apoio e compreensão durante o desenvolvimento deste trabalho, e à minha família em geral, responsável pela essência de minha formação e sempre fonte de apoio incondicional.

Assis
2014

Resumo

Este trabalho apresenta o conceito da utilização de técnicas da Criptografia Quântica, no compartilhamento de dados visando a segurança e confiabilidade das informações, bem como ameaças potenciais. Com o objetivo de aprender novas técnicas de segurança da informação com a utilizando de aplicação da criptografia quântica.

Palavras-chave: Criptografia Quântica, Segurança, Fibra Óptica

Assis
2014

Abstract

This paper presents the concept of using techniques of quantum cryptography in data sharing for the security and reliability of the information, as well as potential threats. Aiming to learn new techniques of information security with the use of application of quantum cryptography.

Keywords: Quantum Cryptography, Security, Fiber Optic

Assis
2014

Lista de Ilustrações

Lista de Tabela

Assis
2014

SUMÁRIO

Assis
2014

1. INTRODUÇÃO

De acordo com MENEZEZ; OORSCHOT; VANSTONE, 2001, pág. 4, 246, o termo criptografia pode ser definido como:

> *A criptografia pode ser dividida em duas áreas principais, a criptografia e criptoanálise. A primeira desta abrange todo o esforço de se estabelecer transmissão segura de informações viabilizando diferentes características como confidencialidade, integridade de dados, autenticação e irretratabilidade. A última reúne todas as técnicas que tem como objetivo obter de forma não autorizada mensagens geradas por algum processo de criptografia.*

Com o aumento de novas tecnologias, a comunicação passou a ser um ponto bastante visado. Grandes organizações, procuram recursos para proteger seus dados e com isso empresas de comunicação e armazenamento elaboram meios para dar a seus clientes essa segurança com sistemas criptográficos mais potentes, mas nem sempre isso acontece.

Os meios atuais são baseados em cálculos matemáticos e dão certo sigilo e segurança, mas nada que não possa ser decifrados, e essa fragilidade aumenta com o avanço das pesquisas de computadores quânticos.

Uma codificação nos dias de hoje, que nos tradicionais computadores atuais levariam até quatro dias, num computador quântico, esse intervalo é reduzido para aproximadamente 34 segundos, mostrando sua vulnerabilidade frente à tecnologia de maior poder de processamento. Os métodos atuais são alicerçados em problemas matemáticos que tem soluções difíceis. Tais problemas referem a funções que é de fácil argumento para obtenção de resultados, porem imensamente complicado indícios pelo resultado da função.

Uma tecnologia ainda em desenvolvimento poderá auxiliar esta necessidade das empresas, trata-se da Criptografia Quântica. A comunicação quântica envolve criptografar informação em estados quânticos, ao invés dos bits usados na comunicação clássica. Um registrador habitual de 8 bits pode armazenar um número

de 0 a 255. Já um de 8 qubits (quantumbits) não só guarda os mesmo 0 a 255, e sim todos eles simultaneamente. De outro modo, um registrador de n qubits pode acumular 2^n valores distintos. Particularidade, denominada paralelismo quântico, evidencia que a memória quântica é relativamente maior que sua memória física.

Ela não se baseia numa simples chave matemática, se guia no Princípio da Incerteza de Heisenberg - a base da mecânica quântica. Essa ciência revela que não existe um estado especifico, mas vários estados simultaneamente.

Os estados mais utilizados são base retilínea vertical de 0º e horizontal de 90º, base diagonais de 45º e 135º e base circulares de direita e esquerda, utilizando o protocolo BB84, que ficou conhecido com essa nomenclatura devido a seus inventores e ano da publicação, Charles Bennett e Gilles Brassard em 1984.

Esse protocolo permite que duas partes, o emissor conhecido como Alice e o receptor Bob conectados por um canal de comunicação, fibra ótica, telefone ou internet, fazem uma transmissão de estados quânticos. Sem qualquer segurança, o protocolo é escrito assumindo-se que um espião (chamado de Eva) pode interferir de qualquer maneira com qualquer um dos canais.

A IBM já realizou a criptografia quântica, porém sem resultados satisfatórios para distâncias superiores a 70 quilômetros, apenas distâncias curtas conectadas via fibra ótica, mais que isso resultou em inconsistências nos dados causados pelo Princípio da Incerteza de Heisenberg.

Sendo está uma área recente e em expansão possui muitos desafios teóricos e práticos que necessitam ser enfrentados para que as comunicações quânticas possam crescer.

1.1. OBJETIVOS

Este trabalho tem por objetivo o estudo da empregabilidade de chave criptográfica, para troca de informação, preservando o sigilo do conteúdo transmitido entre o emissor e o receptor. Os meios atuais proporciona certa segurança, porém programas maliciosos demonstram cada vez mais a fragilidade desse sistema *One Time Pad* (criada em 1917, por Gilbert Vernam) ou a atual *Data EncryptionStandat*,

que é utilizada desde 1976. Será abordada a utilização da criptografia quântica na comunicação entre dois pontos, como ferramenta para maior segurança de dados em organizações que privam por sigilo de suas informações. Com o avanço das pesquisas do Computador Quântico, os métodos atuais de criptografias poderão ser decifrados em questões de horas. Baseado na Mecânica Quântica, uma ferramenta de segurança que não apresenta lacunas para violações.

1.2. JUSTIFICATIVA

A pesquisa surgiu com intuito de conhecer novos meios de segurança. Com aumento de recursos para acesso à rede mundial de computadores por simples usuários e com o hábito de manter dados nos vários tipos de dispositivos, como também empresas que utilizam essa rede para transmissões de informações particulares e/ou dados de seus clientes e parceiros. Com isso usuários mal intencionados, utilizam meios para suprimir essas informações e utiliza-las em proveito próprio ou apenas por hobby.

A Criptografia Quântica vem para suprir essa falha. Essa nova tecnologia aborda meios que mesmo com utilização de computadores potentes, não consegue acessar os dados, e mesmo que consiga cruzar a comunicação, não poderá ler as informações coletadas, pois a transmissão será interrompida ao que se perceba ruídos na mesma.

1.3. ESTRUTURA DO TRABALHO

O capítulo 1, esta introdução, apresenta uma breve visão sobre Criptografia Quântica, os objetivos deste trabalho, as justificativas para pesquisa. O Capitulo 2 apresenta a utilização da Criptografia Atual, introdução à criptografia, utilização da Criptografia Simétrica e Criptografia Assimétrica. No Capitulo 3, comenta-se sobre a Computação Quântica, Modelos de Computadores Quânticos, Circuito Quântico, Computador Quântico de Sentido Único, Computadores Quânticos à base de uma Rede Óptica, Empresa D-Wave. E no Capitulo 4, explana Criptografia Quântica, Protocolo BB84, Funcionamento do protocolo BB84 sem tentativa de espionagem, Protocolo BB84 na tentativa de espionagem, Estimativa de Erro, Provas de

segurança do protocolo BB84, Ataque ao protocolo BB84, Criptografia quântica em comunicação por fibra óptica

2. Criptografia Atual

Tomar posse de informações alheia pode definir o destino de empresas ou de países num guerra, como foi o caso da Segunda Guerra Mundial, com a aquisição da máquina alemã Enigma. Com o aumento dos sistemas de comunicações, essas informações trafegam por sistema de cabeamento, ondas de rádio, que deixam certa brecha para possíveis interceptações.

Nesse capitulo estudaremos as atuais técnicas empregadas na segurança de dados, suas vantagens e desvantagens, na seção 2.1 uma descrição sobre criptografia, a seguir uma introdução aos sistemas utilizados nesses conceitos, na seção 2.2 os fundamentados em chaves simétricas e na seção 2.3 chaves assimétricas.

2.1 Introdução à Criptografia

De acordo com o dicionário Aurélio, criptografia é um sinônimo físico referente a "Arte de escrever secretamente por meio de abreviaturas ou de sinais convencionados entre duas ou mais pessoas ou partes. / Codificação de um artigo ou outra informação armazenada num computador, para que só possa ser lido por quem detenha a senha de sua decodificação" (Dicionário Aurélio).

Segundo Costa (2008, p.29), como é habitual nas publicações sobre criptografia, o conceito de transmissão de dados segura, utiliza três personagens para compor a sua demonstração: Alice, Bob e Eva. Como protótipo, Alice quer enviar uma mensagem segura para Bob, antecedendo que Eva intercepte a mensagem ou envie mensagens a Bob como se fosse Alice.

Alice então efetua a encriptação da informação original, referente a uma mensagem simples, gerando uma mensagem tal que

$$E=e_B(P), \qquad 2.1$$

sendo que *P* faz referência a mensagem simples, $e_B(.)$ a função de encriptação de Alice no momento que se comunica com Bob e *E* é a mensagem codificada. Assim a encriptação é referente à codificação das informações, e por sua vez, a desencriptação refere-se a decodificação. Bob recebe *E* por uma conexão de dados e utilizando a função de desencriptação $d_B(.)$ obtem a mensagem original tem se então,

$$P=d_B(E). \qquad 2.2$$

O sigilo do envia dos dados, nesse caso, é realizada pelas funções $e_B(.)$ e $d_B(.)$. Mas este metodo não supri todos os requisitos, pois requer uma vasta quantidade de diferentes funções para seu uso real.

Segundo Costa(2008, pg30), uma solução para esse problema que ao inves de manter um função como informação sigilosa, utiliza-se argumentos para função utilizada por ambos interlocutores na transmição dos dados e esses argumentos utilizados como mensagem secreta compartilhada. E esse argumento faz mensão como chave criptgrafica na critptafia e as funções 2.1 e 2.2, se convertam em

$$E=e(P,K_B), \qquad 2.3$$

$$P=d(E,L_B), \qquad 2.4$$

as chaves de entrada K_B e L_B corresponde as funções de encriptação e desencriptação, respectivamento, adotada pelas pares implicados na transmição. Esse metodo gera uma vantagem mas nem sempre, o digrama da figura 1 demostra as operações mencionas em 2.3 e 2.4.

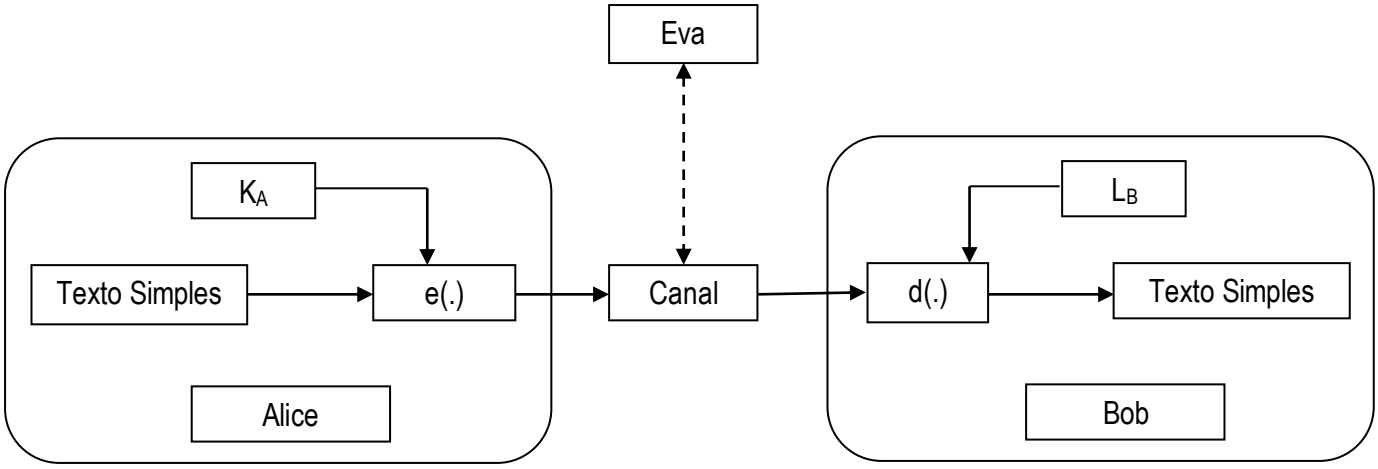

Fig.1: Conceito básico de comunicação segura de dados

2.2 Criptografia de Chave Simétrica

Segundo Galvão Junior, na criptografia de chave simétrica utiliza-se a mesma chave para realizar a criptografia quanto a descriptografia. Os algoritmos em si são bem mais modestos dos que os utlizados na criptografia assimétrica. E o fato de utililzar a mesma chave é umas das sua principais desvantagens, facilitando interpretação as informações sigiliosas quando interceptadas por terceiros. Uma vez que ambos pares enviam e recebem as informações devem ter acesso a chave criptografia.

Se ponderarmos o esboço de encriptação constituindo de um conjunto de funções de encriptação e desencriptação $\{E_e : K \in \mathbb{K}\}$ e $\{D_d : L \in \mathbb{K}\}$, $\mathbb{K}$ representa o espaço de chaves. A chave simétrica é expressa pelo par de chaves (K, L), é facilmente determinar *d(.)* a partir de *e(.)* e *e(.)* de *d(.)*.

O sistema conhecido como chave de uso único ou Cifra de Vernam, é determinado sobre o alfabeto A = {0,1}. Uma informação binaria m_1, m_2... m_t é executada por uma chave k_1, k_2...k_t de tamanho igual, criando um dado cifrado c_1, c_2...c_t ou seja

$$c_i = m_i \oplus k_i, \; 1 \leq i \leq t.$$

Seguindo a proposta de Costa (2008, p.32), Alice e Bob prepara para transmissão de informações por um rede segura. Por tanto, previamente ambos estabelecem chaves secretas semelhantes. Alice por sua vez introduz aos símbolos da informação simples, os símbolos da chave sigilosa, introduzidos no modulo *N*, sendo que *N* refere-se ao tamanho do alfabeto adotado. Resultando na seguinte mensagem encriptada

$$E[k] = e(P[k],K_B) = (P[k]+K_B[k]) \mod N, \qquad 2.5$$

no qual *E[k]* destina-se ao *k*-ésimo símbolo da mensagem encriptada e *P[k]* e $K_B[k]$ a informação simples e a chave secreta respectivamente. A primazia desta técnica está na operação de cifragem, que é bem singular, no que resulta na redução do perídio de inativada de entre um envia e resposta. A desencriptação que Bob ira proceder após o recebimento das informações é realizar pela operação inversa, ou

seja na subtração do modulo *N*. De posse da mesma chave envia por Alice, a informação simples é obtida pela operação

$$P[k] = d(E[k], L_B) = (E[K] - L_B[k]) \bmod N = (E[K] - K_B[k]) \bmod N. \quad (2.6)$$

A Cifra de Vernam se utilizada na prática, devido a sua simplicidade, resulta em algumas dificuldades devido a alguns problemas, no que se destaca se aplicada a um grande número de usuários que mantém um trafego de comunicação entre si.

2.3 Criptografia de Chave Assimétrica

Na criptografia assimétrica utiliza-se duas chaves distintas, mas relacionadas matematicamente, no processo de encriptação e desencriptação. E as mesma são denominadas com o chaves privadas e chaves públicas. É estimada como mais segura que a chave simétrica pelo fato de utilizar chaves distintas no processo de encriptação e desencriptação das informações partilhadas entre os pares. O uso de algoritmos mais complexos e de um par de chaves, o processo é mais demorado.

Para uma compreensão da encriptação de chave pública na comunicação realizada entre Alice e Bob. Bob determina sua chave secreta L_B no intuito de decifrar a informação enviada por Alice e expõe uma chave K_B que poderá ser utilizada por Alice para realizar a encriptação das informações que pretende compartilhar com Bob. Informações esta apoderada por Alice através da função

$$d(e(P,K_B),L_B) = P. \quad (2.7)$$

Como não há a obrigatoriedade de troca de chaves ao mesmo tempo, isso é que diferencia a criptografia de chave pública em relação ao sistema simétrico, ou seja, $L_B \neq K_B$.

O que se dever atentar quando utilizado na chave pública no compartilhamento das chaves

$$d(e(P,L_B),K_B) = P, \quad (2.8)$$

devem ser inversa entre si. Particularidade essencial ao adquirir algumas características dos protocolos assimétricos.

Utilizando o exemplo já relatado anteriormente, um espião interceptador, no nosso caso Eva, transmite informações à Bob, personificando como Alice. Isso acontece devido que K_B é publicamente compartilhada, obtida inclusive por Eva, que pode se passar por Alice, no intuito de enganar Bob.

O protocolo sugerido por Diffie-Hellman, para sua eficiência, exige da complexidade de cálculos do algoritmo para execução da tarefa de encriptação e desencriptação que composto em duas etapas e ter em vista que ambos interlocutores tenham suas próprias chaves públicas e privada $\{L_A, K_A\}$ e $\{L_B, K_B\}$. Primeiramente Alice faz uma encriptação de um dado simples usando sua respectiva chave L_A. Em seguida efetua uma nova encriptação utilizando a chave pública de Bob K_B nos dados cifrados anteriormente. Isso resulta nos dados cifrados E, no qual:

$$E = e(e(P,L_A)\ K_B. \qquad 2.9$$

Para tomar posse dos dados Bob realiza outra operação:

$$d(d(E,\ L_B)\ K_A) = d(d(e(e(P,L_A),K_B),K_A = d(e(P,\ L_A),\ K_A) = P, \qquad 2.10$$

que realiza a desencriptação de posse da chave privada L_B seguidamente uma desencriptação empregando a chave pública de Alice K_A.

A ação executada por Alice, compreendido como processo de autenticação, consenti a Bob de verificar a veracidade do emissor, se é realmente Alice, e não Eva se passando por Alice. O diagrama apresentado na figura 2, dá um bom entendimento quanto a utilização do algoritmo Diffie-Hellman.

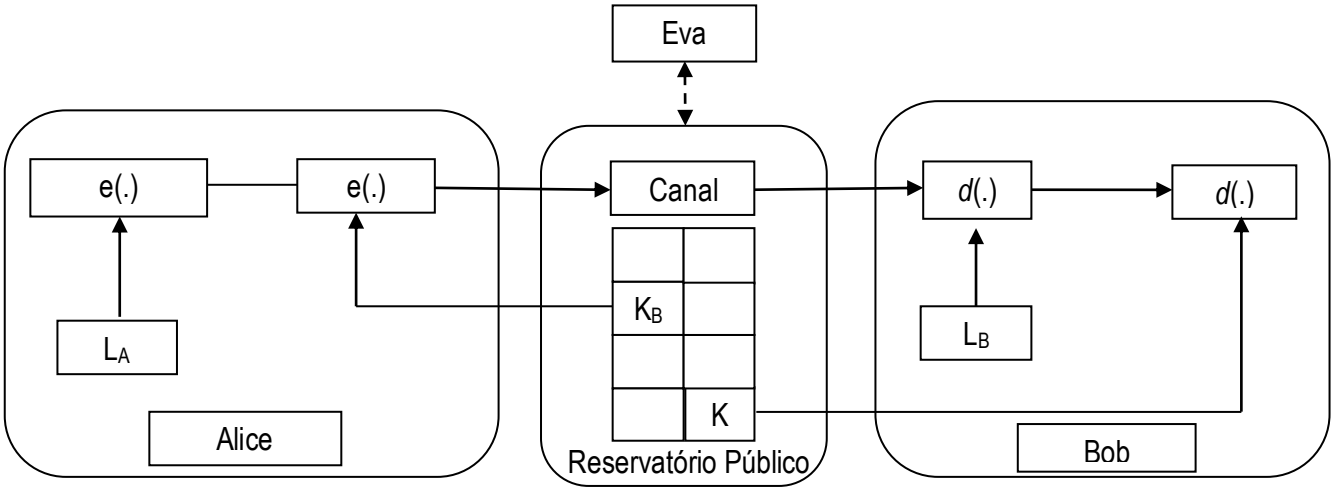

Fig.2: Diagrama de implementação do conceito de Diffie-Hellman.

3. Computador Quântico

A arquitetura dos computadores, por anos se baseia na teoria da Lei de Moore, onde prevê a cada ano um aumento no número de transistores por volta de 60%, aumentando a desempenho desses mesmos chips.

Segundo Tanenbaum, (2007, pg16), a lei de Moore não é real, mas uma observação de quão rápida do estado sólido. Essa consideração deve ser válida até 2020, ou um pouco mais. Ao ponto que os transistores reduzidos abaixo de um determinado mínimo muito pequeno para garantir a confiabilidade, passam a estar submetido a efeitos do túnel quântico, contudo outros efeitos podem aparecer e causem sérios problemas que necessitam de resolução, como a fuga de corrente.

Encontrar a alternativas para a clássica arquitetura dos computadores, uma saída são os computadores quânticos, que se beneficiam de propriedades da mecânica quântica, como à superposição quântica e o entrelaçamento quântico.

Segundo Figueiredo, (2012, pg4), a computação quântica é uma área recente e de rápido desenvolvimento. Contudo existem desafios a serem transpostos para tornar o computador quântico viável, organizações em vários países já começaram a desenvolver laboratórios de computação quântica.

3.1 Modelos de Computadores Quânticos

Segundo Figueiredo (2013, p.05), uma sucinta descrição dos principais modelos que se distingue pelos elementos básicos de computação quântica.

Na computação quântica, um qubit se assemelha a um bit da computação clássica. O qubit pode encontrar-se no estado 1(um) ou 0(zero), ou em sobreposição de estado 1’ s (uns) e 0’ s (zeros) ao mesmo tempo.

Um registrador clássico de 8 bits pode armazenar um número de 0 a 255. Um registrador de 8 qubits além de conter os mesmo números de 0 a 255, mas todos eles simultaneamente. Isto é, um registrador de n qubits pode armazenar 2n valores diversos. Particularidade essa denominada como paralelismo quântico, indica que a memória de um computador quântico é exponencialmente maior que sua memória física. De acordo com o físico David Deutsch, esse paralelismo permite que um computador quântico realize 1 milhão de cálculos ao mesmo tempo, enquanto que o seu PC faz apenas um. Um computador quântico de 30 qubits deve igualar a potência de um computador convencional a 10 teraflops (trilhões de operações de ponto flutuante por segundo). Os computadores pessoais de hoje rodam a velocidades medidas em gigaflops (bilhões de operações de ponto flutuante por segundo).

Empregando a notação de ket, os qubits são representados na forma vertical.

Dando-se a representação matemática do estado por: $\alpha|0> + \beta|1>$ onde α e β representam probabilidades e por isso $|\alpha|^2 + |\beta|^2 = 1$.

3.2 Circuito Quântico

Segundo Figueiredo (2013, p.05), um circuito quântico se assemelha a um computador tradicional quanto a utilização de portas lógica, para realização de suas operações como as AND, OR e NOT.

Uma porta quântica imediata seria análoga a porta clássica NOT, que leva o bit clássico 0 →1 e 1→0. Todavia, ao contrário das portas lógicas convencionais, as portas lógicas quânticas tem que ser reversíveis, ou seja, dado a informação na saída da porta, tem que existir uma operação que permita obter a entrada. O que não se aplica a porta AND, já que não é possível com a saída, obter entradas. Aguarda-se da ação da porta quântica negação que esta, leve o estado |0>→|1> e |1>→|0>. A mais, a porta NOT quântica deve agir sobre estados superpostos de forma a inverter os coeficientes, tal que o estado:

$$|\psi >= \alpha|0 > +\beta|1 >, \qquad 2.11$$

torne-se:

$$|\psi >= \alpha|1 > +\beta|0 >. \qquad 2.12$$

Os circuitos quânticos tem o análogo representado pela porta de dois qubits NOT-controlada CNOT. A porta CNOT atua em dois ou mais qubits e funciona similar a porta NOT convencional, entretanto um dos qubits serve de controle, executando a função NOT somente se o qubit esteja |1>.

Do qual a matriz é CNOT = $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

e sua representação é

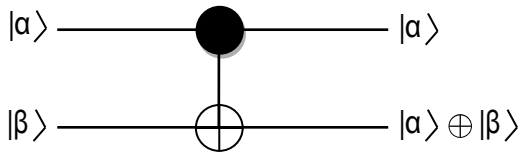

Fig.3: Porta quântica CNOT.

Na representação da figura 2, $|\alpha\rangle$ é o qubit de controle e $|\beta\rangle$ o qubit alvo. A notação utilizada é a mais recorrente na literatura para descrever a ação da porta CNOT para dois qubits.

3.3 Computador Quântico de Sentido Único

Segundo Figueiredo (2013, p.07), A computação quântica de sentido único (one-way quantum computing) foi proposta em 2001 por Robert Raussendorf e Hans J. Briegel na Universidade de Munique, na Alemanha. Este modelo requer que os qubits sejam inicializados num estado de elevado entrelaçamento quântico, como o estado aglomerado (cluster state). Em seguida, entra-se num ciclo onde é feita uma medida a um único qubit, obtendo-se um resultado clássico e a destruição do qubit medido, daí o nome “computação de sentido único”. Finalmente, utiliza-se esse resultado clássico para determinar o algoritmo a seguir. O ciclo é repetido, fazendo-se uma nova medição para saber o novo algoritmo a seguir. Assim, todas as partículas que restam no final de todas as medições transportam o resultado do cálculo.

Fig.4 - Computação quântica de sentido único[1]

3.4 Computadores Quânticos à base de uma Rede Óptica

Segundo Figueiredo (2013, p.10), Uma rede óptica é formada pela interferência de feixes de laser criando uma polarização, obtendo assim poços de potencial. Em seguida, os átomos são resfriado de modo a resultar num ponto de potencial mínimo. São empregados nêutrons ao invés de íons, para impedir que eles interajam, indesejadamente, com as forças eletromagnéticas do ambiente devido à

[1] Fonte: www.portasaber.org

sua cargas. Posteriormente, é utilizado um outro grupo de lasers para controlar o estado dos átomos, os qubits, de modo a realizar as operações do computador quântico.

Na Fig.5 uma representação de uma rede óptica, a área verde simula os poços de potencial que prende os átomos, os pontos castanhos.

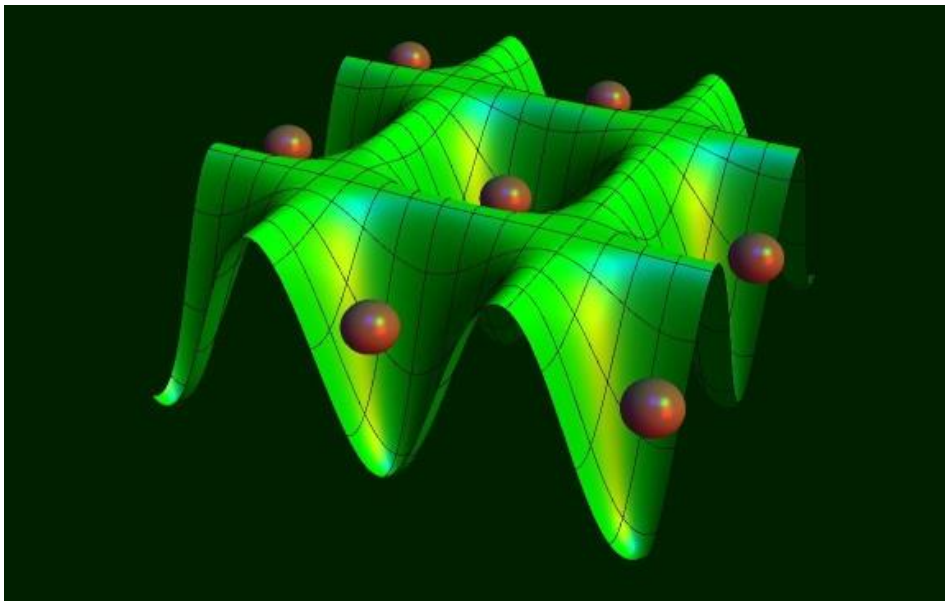

Fig.5 – Representação de uma Rede Óptica[2]

3.5 Empresa “D-Wave”

Segundo Tarantola do site Gizmodo, em 2010, a empresa norte-americana D-Wave, lançou o primeiro computador quântico o D-Wave One ™, com um processado de 128 qubits que utiliza o modelo adiabático quântico para resolver de otimização discreta, sendo implementado fisicamente com supercondutores. Dobrando a cada ano o número de qubits, em 2013 foi lançando o D-Wave Two ™, com o sistema de 512 qubits, cada qubits se comunica diretamente com outros sete qubits, são blocos que formam a estrutura de 8 em qubits. Por isso é até 300.000 vezes mais rápido que seu antecessor.

[2] Fonte: Figueiredo ,2012, p.11

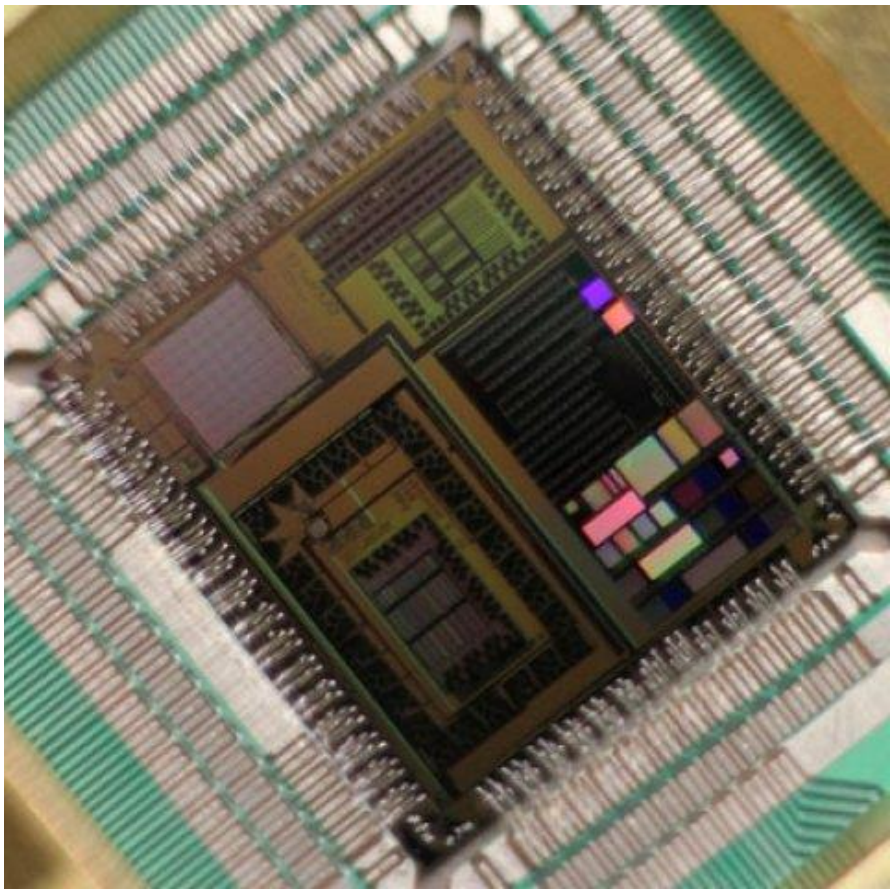

Fig.6 – Processador D-Wave Two™ [3]

Para tirar proveitos dos efeitos quânticos, o D-Wave Two ™, requer condições extremas e muito especificas. Ele opera a 0.02 Kelvin, ou seja -273,13º C, 150 vez mais frio do que a profundeza do espaço interestelar. E requer uma blindagem para se proteger contra interferências magnéticas.

[3] Fonte: www.dwavesys.com/d-wave-two-system, 2014

Fig.7: Sistema de Blindagem e Refrigeração[4]

Segundo Figueiredo (2013, p13) o D-Wave One ™, foi vendido inicialmente por US$ 10 milhões, por ser diversas vezes mais rápido que os computadores atuais, foi logo adquirido por laboratórios de pesquisas e pelo Departamento de Defesa Americano.

Segundo Mansfield do site BBC News, D-Wave Two custa até US$ 15 milhões e foi adquirido pela Google, NASA e a Associação das Universidades para Pesquisa Espacial, para uso compartilhado, pois se mostrou eficiente no teste de *benchmarking*, que exigido pela NASA e Google, em um dos casos retornou resultado em menos de meio segundo fazer algo que um convencional demoraria até 30 minutos.

[4] Fonte: www.dwavesys.com/d-wave-two-system, 2014

Fig.8: D-Wave Two[5]

4. Criptografia Quântica

Segundo Costa (2008, p.79), e como mencionado anteriormente, com problemas de segurança introduzido na criptografia atual pela computação quântica, dispomos de várias soluções, sendo que uma das delas é apresentada por uma nova área, a criptografia quântica, mais especificamente a distribuição de palavras-chaves quânticas.

Esta proposta baseia-se no sistema de palavras-chaves privadas, ou seja, as entidades que desejam manter uma comunicação com segurança e privacidade, pré-estabelecem uma palavra-chave entre si, por meio de uma via que considerem segura. Determinado a palavra-chave podem encriptar os dados e transmiti-los com segurança por qualquer meio de comunicação, pois só é possível desencriptar de posse da palavra-chave correta. Mas se uma terceira entidade estiver infiltrada no canal de comunicação, no momento em que se compartilhava a palavra-chave, poderá ter acesso a palavra-chave e decifrar todos os dados que possam vir a ser transmitidos e comprometendo assim a segurança da mesma.

[5] Fonte: www.dwavesys.com/d-wave-two-system, 2014

O compartilhamento de palavra-chave quânticas, utiliza das propriedades quânticas, para realiza-la com segurança. Um dos protocolos que possibilita essa distribuição, apresentado em 1984 denominado BB84, descrito da seguinte maneira.

O emissor gera um bit clássico aleatório e em seguida, escolhe da mesma maneira, entre duas bases diferentes, para gera um qubit em um dos quatro estados seguintes:

Base	**Bit**	
	0	1
X	$\psi_{X0} = \|0\rangle$	$\psi_{X1} = \|1\rangle$
Y	$\psi_{Y0} = \frac{\|0\rangle + \|1\rangle}{\sqrt{2}}$	$\psi_{Y1} = \frac{\|0\rangle - \|1\rangle}{\sqrt{2}}$

Tabela 1: Preparação do qubit para envio no protocolo BB84.

Como se percebe, os estados não são octogonais e por isso, não é possível medi-los com exatidão por meio da mesma chave.

Este processo é executado, seguidamente, várias vezes para *n* qubit, e são envido para o receptor. Enquanto o emissor não revela em que base gerou os qubit, o receptor analisa aletoriamente em uma das duas bases, para medir cada qubit, armazenando cada valor de 0 e 1 obtido.

Ao concluir a medição, o receptor, se comunica com o emissor, por um canal clássico e o informa da conclusão. Emissor e receptor partilham as base que utilizaram, mas sem revelar os qbits que obtiveram. Dessa maneira, após eliminarem os valores divergentes e armazenarem apenas os correspondente, terão os a confirmação que estão de posse da mesma chave

Caso haja uma espião na rede no mesmo canal, mas não tiver de posse da chave previamente estabelecida, a medição se dará incorreta e um interferência ocorrera no qubit, e dará erro na comunicação.

Deste modo, emissor e receptor distribui apenas parte da sequência conseguida por um meio público, para averiguar autenticidade dos códigos. Se coincidirem, então empregam o restante do código para elaboração da palavra chave, caso contrário, a presença de um espião é detectada, então se realiza o mesmo processo, pela mesma ou outra via, até que se confirme a segurança da privacidade.

Mesmo não podendo evitar que espiem o canal, mas detectando sua presença, só fazem a transmissão dos dados após terem assegurado a privacidade da palavra-chave.

4.1. Protocolo BB84

Seguindo a proposta de Costa (2008, p.83), o protocolo BB84 consiste numa distribuição de chave sessão ou parte única. Este é um processo não-determinístico, convenientemente a natureza dos sistemas quânticos, não sendo possível empregar para partilhar os dados. Todavia, o processo consenti instituir uma chave de maneira segura, aplicando diferentes algoritmo simétrico para realizar a criptografia e enviar os dados. Sendo essencial para o protocola a utilização de um canal quântico e um público, importante que o canal quântico não deve incluir erros acima de entrada e preciso que o canal público deve ser validado. Com a utilização do protocolo, qualquer tentativa de invasão, seja identificada.

A utilização de estado quânticos do protocolo BB84 para cifrar dados, aplicando os estados quânticos representados pela polarização de fótons em duas bases, sendo capaz dos bits clássicos 0 e 1 serem descritos em ambos os casos e do qual vale o princípio da incerteza de Heisenberg e o teorema da não-clonagem.

As duas bases de polarização são a base retilínea ($\oplus$) e a base diagonal ($\otimes$). Na base retilínea o bit 0 é relacionado a direção de polarização 0, que forma o estado quântico$|0>$, e o bit 1 é associado a direção de polarização $\pi/2$, que o forma o

estado |1 >. Já a base diagonal o bit 0 é relacionado a direção de polarização + π/4, que forma o estado quântico (|0 > + |1 >)/√2 (por maio de facilitar ao entendimento será denominado por |0′ >), e o bit 1 é relacionado a direção de polarização -π/4, formando o estado (|0 > - |1 >)/√2 (da mesma maneira será denominado por |1′ >).

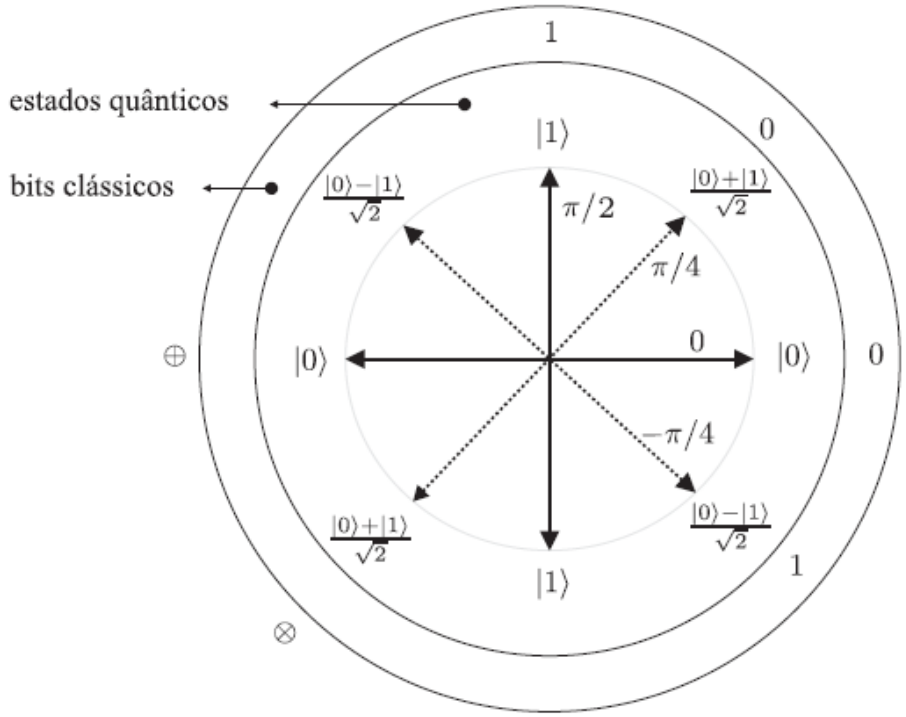

Fig.9: Bases de codificação para o Protocolo BB84.[6]

4.2 Funcionamento do protocolo BB84 sem tentativa de espionagem

O processo de para elaboração de uma chave por meio do protocolo BB84, pode ser explanado em poucos processos.

Inicialmente Alice, cria um conjunto binário *(ca)* por meio de uma algoritmo aleatório. Para fins explicativo, suponhamos o seguinte conjunto de 8 bits *ca* = [01100101]. Em seguida ela criptografa o conjunto empregando as bases $\oplus$ e $\otimes$ (serão empregados 0 e 1 paras bases respectivamente) aleatoriamente, gerando o conjunto correspondente para polarização *pa* = [10111100]. Os qubits criados são compartilhados com Bob por meio de um canal público.

[6] Fonte: Costa ,2008, p.84

Bob aufere os qubits sem a noção do conjunto de bases *pa* empregado por Alice. Ele seleciona, então aleatoriamente, um conjunto de bases para aplicar a medica em cada qubits passado por Alice, empregando por exemplo o conjunto de bases *pb* = [00101010], conseguindo o conjunto de bits *cb*. Se por acaso o conjunto selecionado por Bob se equipare ao de Alice, *pa*, o conjunto enviado será restaurado na integra e por sua vez *cb* = *ca*. Entretanto, a estimativa de Bob empregara a base certa em 50% das vezes, e se levar em conta que medição de um qubit com a base errada acarretara em 0 ou 1 com 50% de chance de cada valor, a cota de erros averiguados (*Quantum Bit Error Rate,* QBER) entre os conjuntos de Alie e Bob será de $\approx 25\%$.

Por meio de um canal público, Alice e Bob compartilham os conjuntos *ca* e *cb*, proporcionando a Bob averiguar quais os bits logrou êxito.

Enfim, Alice e Bob definem os bits compatíveis em *pa* e *pb* como sua chaves criptográfica k_A e k_B, que me uma via sem interferência serão iguais e terão, aproximadamente, o tamanho de *ca*/2.

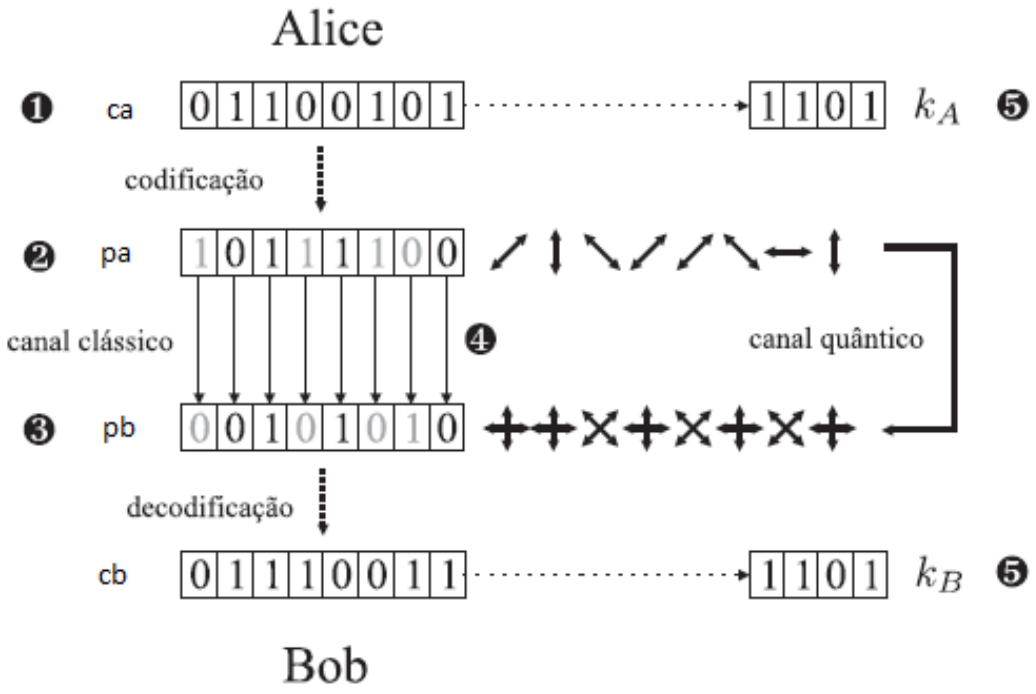

Fig.10: Passo da execução do Protocolo BB84.[7]

4.3 Protocolo BB84 na tentativa de espionagem

Seguindo a proposta de Costa (2008, p.86), Para se ter uma noção mais real, suponhamos que Eva é um intruso espião que tem por objetivo tomar posse dos dados do canal de comunicação entre Alice e Bob. Levando em conta o protocolo utilizado, Eva por meio do canal quântico se apossar dos qubits compartilhados por Alice com a intenção de adquirir a chave de acesso k_A=k_B que será empregada para comunicação posterior. Eva não consegue ter conhecimento de um qubit e aplicar medição posteriormente devido ao método de não clonagem, apenas executar a mesma operação como Bob. Para efeito de entendimento, deduz que Eva aplique o referido procedimento de posse da base *me*=[10001011], interpretando o conjunto *se*=[01010010]. Todavia, para ocultar a ação Eva precisa encaminhar a Bob os qubits que obteve com sua medição, lembrado que pelo postulado da mecânica quântica conhecido como colapso de superposição o qubit encaminhado por Eva, uma vez medido e conseguido o valor do dado, acarretara sempre no valor igual independente de outra medida aplicada sequentemente.

Sendo que Eva não tem conhecimento do conjunto de bases *pa* aplicado por Alice, ela somente pode aplicar seu conjunto de bases para conseguir a serie s_E . Estatisticamente, *pa* e s_E são idênticos para metade dos valores, resultando que *se* terá metade dos bits em acordo com *pa*. Entretanto, ao reencaminhar destes bis não sugerira a Bob a espionagem. Com tudo, para 25% bits encaminhado a Bob, o valor restaurado por ele estará em desconcerto com o que foi codificado por Alice devido a interceptação de Eva. Adicionando uma nova etapa no protocolo, no qual Alice e Bob divulgam e averiguam entre si uma parte de k_A e k_B, que de início deveriam ser iguais, esse podem detectar a interferência de um espião por meio da certificação de uma taxa de erros.

[7] Fonte: Costa ,2008, p.86

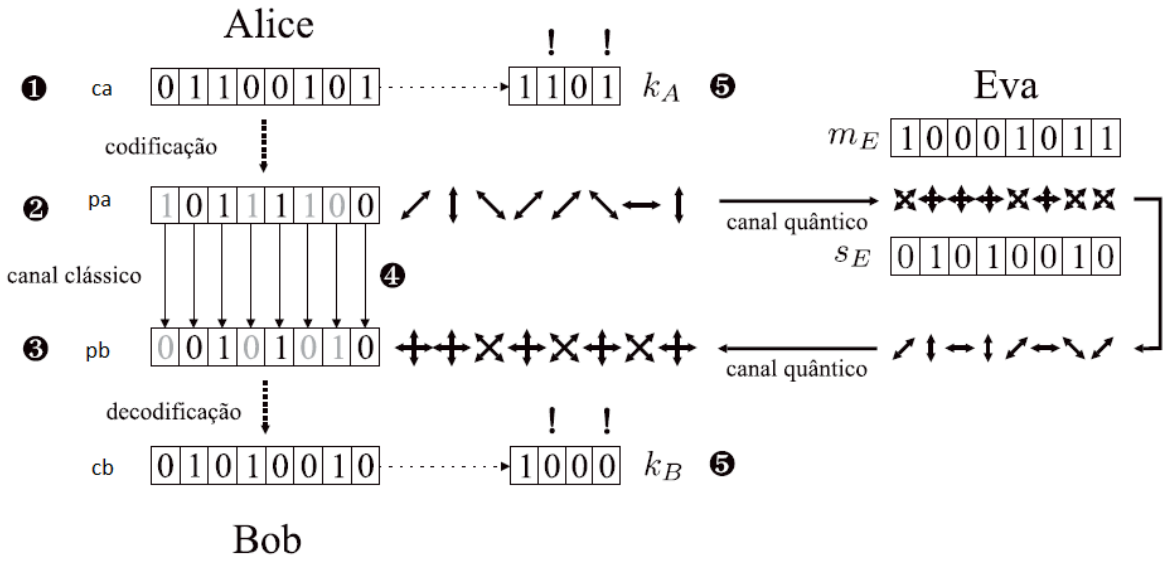

Fig.11: Passo da execução do Protocolo BB84 com a interferência de Eva.[8]

4.4 Estimativa de Erro

Segundo Costa (2008, p.87), evidentemente, para uma extensa chave, a probabilidade de Bob obter todos os bits corretamente na possibilidade de Eva espionar o canal é $(0,5)^K$, todavia que *K* o número de vezes que a base errada foi utilizada por Eva. Isso ocorre já que Eva, provavelmente, utiliza a base errada em 50% dos casos, e para uma base equivocada Eva obtém os valores 0 e 1 com estimativa de 50% acerto. Essa ação resulta em erro de 25%, no qual a interceptação é detectada pela utilização através da comparação entre parte estimativamente grande das chaves k_A e k_B.

A checagem de erros entre k_A e k_B pode ser realizada pelo seguinte procedimento: Alice retira um fragmento da chave estabelecida na utilização do protocolo e compartilha com Bob. Alice comunica a Bob um subconjunto de posições de comprimento *N* e o valor do bit nessas posições na chave. Alice e Bob averiguam a taxa de erros *e* então prossegue a comunicação caso fique abaixo do limite estipulado (valor esse que é definido de acordo com canal quântico que será

[8] Fonte: Costa, 2008, p.87

empregado pela implementação utilizada), todavia, venha *e* maior que o limite determinado a comunicação será encerrada.

4.5 Provas de segurança do protocolo BB84

A proposta apresentada por Costa (2008, p.100), um protocolo de criptografia é declarado integralmente seguro quando é permitido comprovar matematicamente que, uma vez que satisfaz as exigências da execução do protocolo, esta é inviolável para qualquer ataque. Esta é a situação proposta pela Cifra de Vernam.

O protocolo BB84 é referido constantemente como um protocolo de criptografia completamente seguro. Todavia, o protocolo BB84 é na realidade casualmente seguro, sendo possível tornar a possibilidade de falhas deste tendendo a zero. Ainda assim, com a efetividade de algumas técnicas de ataque conhecidas. Isso demonstra que o protocolo é essencialmente seguro contra qualquer ataque permitidos pela mecânica quântica.

4.6 Ataque ao protocolo BB84

Segundo Costa (2008, p.94), todo o conceito explanado demonstrar que protocolo BB84 é seguro em seu fundamento teórico, lacunas podem ocorrer durante a implementação do mesmo, abrindo brechas a possíveis ataques.

Segundo Costa (2008, p.96), Uma das estratégias de ataque utiliza um circuito quântico determinístico que atua em cima de dois qubits existente num único fóton. Predições teóricas conhecida como informação de Rényi para obter dados das chaves compartilhadas por Alice e Bob adquirida na existência de erros no canal quântico.

Apesar de indicar que a criptografia quântica pode sofrer interceptações, a técnica se emprega em caso bem especifico. A empregabilidade da técnica se fundamenta no fato que Eva obtenha acesso físico ao modulo receptor de fótons de Bob. Tal condição que não se emprega a um caso prático, todavia que fato que Eva obtenha

acesso físico ao equipamento de Bob resulta numa vulnerabilidade que vai além das propriedades da mecânica quântica.

Sendo assim, a técnica de ataques colaboram na averiguação dos limites essenciais da segurança no protocola BB84 na presença de espionagem e erros físicos reais. Criar uma caso adicional para ser considerado na elaboração de técnicas de averiguação de dados e aumento da privacidade. Assim resultados não inviabiliza o protocolo BB84 do mesmo modo como técnicas anteriores.

4.7 Criptografia quântica em comunicação por fibra óptica

A aplicação de protocolo de criptografia quântica por meio da transmissão de fótons por fibra óptica é uma investida confiante quando se avaliada a extensa infraestrutura de fibra óptica e fontes de luz como Leds e Lasers e o respectivo baixo custo de operação desse ambiente quando confrontado outras técnicas de comunicação. Entretanto, alguns inconveniência são averiguadas nessa abordagem. Primeiramente tem-se complexidade da obtenção de fontes de luz aptos de gerarem fótons únicos com a confiabilidade admissível, e a taxa de geração de fótons satisfatórios para as necessidades de desempenho averiguadas pelos sistemas de telecomunicações modernos. Compreende-se que os estados de polarização de fótons compartilhado por fibra óptica são modificados no decorrer da trajetória, igualmente como sua intensidade, pelo motivo da atenuação intrínseca criada pela fibra, o que resulta em erros na geração de protocolo de criptografia quântica. Por esse motivo a requisita fibras ópticas especifica para esse recurso, além de aplicação de técnicas aptas de restaurar a polarização inicial de um fóton.

Segundo Costa (2008, p.104), mesmo com as dificuldades na execução dos protocolos de criptografia quântica por meio de fibra, essa é o tratamento mais avançado atualmente. Aperfeiçoamento de técnicas de melhoramento das dificuldades associadas a manipulação de fótons polarizados em fibra, tanto como a aquisição de fontes de luz mais especificas e garantido, tem tornado possível a fabricação de equipamentos comerciais de compartilhamento de chaves quânticas. Alguns exemplos comercializado pelas empresas MagiQ, Q-Box Workbench, com

alcance 50km, é um sistema ponto-a-ponto à base de fóton único, desenvolvido para cientistas em organizações acadêmicas, governamentais e comerciais para realizar pesquisa relacionada ou utilizando QKD e com uma configuração base do protocolo BB84 para distribuição de chaves simétricas entre Alice e Bob e idQuantique, IDQ's Cerberis, que suporta dois protocolos, ou seja, o BB84 para distância até 20km e o SARG para comunicações superiores a 20km, em combinação com a técnica QKD para distribuição de chaves convencias. O QKD é uma tecnologia ponto a ponto, onde duas partes estão ligados por uma fibra escura, com alcance aproximado de 80 km.

Fig.12: Cerberis Quantum Key Distribution (QKD) Server.[9]

Segundo Costa (2008, p.105), Progressos explanados previamente, como outro não relatados, demonstram que a implantação do protocolo BB84 por fibra óptica tem atingido indícios consideráveis para a utilização em algumas execuções praticas. No entanto, uma aplica num cenário de uma rede quântica de abrangência global, ainda se demonstra algo ainda muito distante quando estimado os milhares de quilômetros de fibras ópticas empregadas nas redes de telecomunicações mundiais atuais. Ainda assim, é uma área em desenvolvimento sem resultado prático.

[9] Fonte: http://www.magiqtech.com/Products.html, 2014

5. Conclusão

Como a mudanças na rotina das pessoas no mundo inteiro são constantes estímulos para o aperfeiçoamento de técnicas mais seguras. Alguns anos atrás, para se realizar uma transação financeira, compartilhar pesquisas novas, dentre outras tarefas, tudo era registrada em várias páginas e contavam com sistema de escolta para serem enviada em segurança. Nos dias atuais, com um simples clique de mouse, todas essas informações são encaminhas por meio virtual. Contudo esse recurso, a segurança virtual transpassou de um complemento essencial a algo indispensável independente das área aplica.

Num mundo onde quem tem posse informações, que pode favorecer sobre organizações, ou por outro lado, deixar que a própria informação fossem interceptadas por concorrentes, poderia levar a ruina uma organização inteira ou até mesmo iniciar guerras entre nações, pelo o que foi obtido, muitas vezes, por fragilidade na transmissão, armazenamento dos dados sigilosos, uma vez se utilizam técnicas antigas.

A criptografia clássica empregada nos dias de hoje, e os resultados apresentados pelo progresso da teria da computação quântica, demonstram que algumas técnicas da criptografia clássicas empregadas necessitam de serem reavaliadas quando confrontada a computação quântica demonstram-se vulnerável. Como apresentado no capitulo 3.5, demonstra essa conquista no avanço da computação quântica, inicialmente para um grupo privilegiado devido ao valor ainda não acessível a todos.

A vontade associada a fragilidade do conceitos utilizados atualmente da criptografia levou a pesquisa de meios para técnicas renovadas, como apresentada no capitulo 4. A pesquisa dos elementos teóricas da criptografia quântica, investigação de protocolos para criptografia quântica disponíveis, explanado na seção 4.1, induziu a escolha do protocolo BB84 como possibilidade que melhor se ajusta em caso reais. Por meio dos conceitos de aplicação teórico do protocolo BB84 em ambiente de compartilhamento entre duas partes, foi possível verificar pontos debilitáveis, que pudessem ser uma brecha para qualquer espião se apoderar de parte da informação transmitida, ainda assim não comprometeria a segurança pois a presença de um terceiro elemento seria detectada ao aplicar a averiguação das chaves.

Mesmo com pouco alcance, como mencionado seção 4.7, avanço tem sido obtido para uma maior cobertura por meio da fibra óptica com menos ruído, e maior percepção em caso de qualquer interceptação por alguém não autorizado.

A elaboração desse trabalho mostrou que os protocolos de criptografia quântica podem ser bem-conceituados como possíveis recurso para renovação das técnica criptográficas clássicas aplicadas nas redes de comunicações. Entretanto este trabalho é apenas um início no aperfeiçoamento de uma análise mais profunda na execução de protocolo quânticos, em rede crítica, para o aumento de sua confiabilidade e segurança.

REFERÊNCIAS BIBLIOGRÁFICAS

ALBUQUERQUE, Luciana Carreiro; Barnabé, Anderson; Ferreira, Claudemberg; Raupp, Ronny. Criptografia Quântica. 2005. 8p. Trabalho de MBA. Universidade Católica de Brasília, Brasília, 2005.

COSTA, Carlos Henrique Andrade. Criptografia Quântica em Redes de Informação Critica – Aplicação a Telecomunicações Aeronáuticas. 2008. 191p. Dissertação (Mestrado) – Escola Politécnica da Universidade de São Paulo, São Paulo, 2008.

DIFFIE, Whitfield; Hellman, Martin E. - New Directions in Cryptography, IEEE Transactions on Information Theroty, IT-22, n.6, 1976.

FIGUEIREDO, Filipe Seabra. Simulador de Circuito Quânticos, 2013. 81p. Dissertação (Mestrado) – Faculdade de Engenharia da Universidade do Porto, Porto, 2013

GALVÃO JUNIOR, Pedro - Diferenças entre chaves simétrica e assimétrica para criptografia. Disponível em <http://pedrogalvaojunior.wordpress.com/2007/11/16/diferencas-entre-chaves-simetrica-e-assimetrica-para-criptografia >. Acessado em 14 abr.2014.

IDQ's, CERBERIS QUANTUM KEY DISTRIBUTION (QKD) SERVER – Disponível em <http://www.idquantique.com/network-encryption/products/cerberis-quantum-key-distribution.html#overview>. Acessado em 14 ago.2014.

MagiQ, Q-Box Workbench™ Quantum Key Distribution (QKD) System - <http://www.magiqtech.com/Products_files/QBox%20Datasheet-2011.pdf>.Acessado em 14 ago.2014.

MANSFIELD, Alex - NASA buys into 'quantum' computer. Disponível em <http://www.bbc.com/news/science-environment-22554494>. Acessado em 27 jun.2014.

MENEZES, A. J.; Oorschot, P. C. van; Vanstone, S. A. – Handbook of Applied Cryptography. [S.1], CRC Press, 2001.

STEINER, Barbara - Computação Quântica, já ouviu falar?. Disponível em <http://www.ssbrasil.com.br/blog/computacao-quantica-ja-ouviu-falar-2/>. Acessado em 01 jun.2014.

TANEMBAUM, Andrew S. – Organização Estrutura de Computadores, 2007. 5º Edição.

TARANTOLA, Andrew - Baseado em teoria quântica, D-Wave 2 pode ser mais rápido que um supercomputador. Disponível em <http://gizmodo.uol.com.br/d-wave-2-quantico>. Acessa em 25 jun.2014.