Estudo Introdutório do Protocolo Quântico BB84 para Troca Segura de Chaves

F.L. Marquezino[1]*, J.A. Helayël-Neto (Orientador)[1]

[1]Centro Brasileiro de Pesquisas Físicas
CCP - Coordenação de Campos e Partículas
Av. Dr. Xavier Sigaud 150
22.290-180 Rio de Janeiro (RJ)

franklin@serraon.com.br,helayel@cbpf.br

Abstract. *This article presents a review on the BB84 quantum protocol, used for secure key distribution. The BB84 protocol uses Quantum Mechanics properties and is unbreakeable. A brief explanation on Classical Cryptography and the Vernam cipher is presented, as well as the mechanism of BB84 protocol. Some Cryptoanalysis techniques are described. The present situation of experimental Quantum Cryptography is also briefly commented. The article aims at a better comprehension of Quantum Cryptography amongst brasilian students of Computer Science. Ideal conditions shall be considered, with perfect equipments and noiseless channels. However, further references shall be given, so that the reader may understand the general case.*

Resumo. *Este artigo apresenta um estudo do protocolo quântico BB84 para troca segura de chaves criptográficas. O protocolo BB84 utiliza propriedades da Mecânica Quântica, o que o torna inviolável. Uma breve explicação sobre a Criptografia Clássica e sobre o cifrador de Vernam é apresentada, assim como o funcionamento do protocolo BB84. Algumas estratégias de espionagem são descritas. Também é feito um breve comentário da situação experimental da Criptografia Quântica atualmente. O artigo visa a uma maior divulgação da Criptografia Quântica entre os estudantes brasileiros de Ciência da Computação. Serão consideradas condições ideais, com equipamentos perfeitos e canais sem ruído. No entanto, dar-se-ão referências suficientes para que o leitor possa se aprofundar no caso mais geral.*

1. Introdução

O protocolo BB84 foi criado por Charles Bennett e Gilles Brassard em 1984 [6], daí o seu nome. Trata-se de utilizar propriedades da Mecânica Quântica para fazer uma Criptografia completamente segura. Enquanto na Criptografia Clássica[1] a segurança é baseada

*Bolsista PIBIC-CNPq no CBPF/MCT. Estudante do curso de Bacharelado em Ciência da Computação da Universidade Católica de Petrópolis (http://www.inf.ucp.br). Membro do Grupo de Física Teórica José Leite Lopes.

[1]Entender-se-á Criptografia Clássica por Criptografia "Não-Quântica", ou seja, sujeita às leis da Mecânica Newtoniana. Da mesma forma, por Computação Clássica, entender-se-á toda forma de computação que não utiliza propriedades da Mecânica Quântica.

em problemas computacionais que não possuem solução eficiente hoje, mas que um dia poderão ter, na Criptografia Quântica a segurança é baseada nas leis da Física Quântica.

Apesar de o nome "Criptografia" Quântica já ter se tornado comum entre os pesquisadores da área, o protocolo BB84, na realidade, serve para troca segura de chaves. Este protocolo permite que duas partes (Alice e Beto) gerem uma chave secreta comum, sem a necessidade de um canal secreto previamente estabelecido. Após ser aplicado o protocolo quântico, deve-se utilizar algum algoritmo clássico para troca da mensagem propriamente dita. Entretanto, neste caso, poder-se-ia utilizar o algoritmo de Vernam [13] (também chamado de *one-time pad*), impossível de ser violado, segundo Claude Shannon [3, 4], desde que a chave tenha o mesmo tamanho da mensagem e seja utilizada somente uma vez.

Neste artigo será explicado o funcionamento do protocolo em condições ideais, em que o emissor consegue emitir fótons isolados em cada pulso, com polarização exatamente conforme previsto pelo protocolo, sendo medido na base exata pelo receptor e, não menos importante, em canais sem ruído. A análise do protocolo em canais com ruído e com equipamentos imperfeitos não é trivial, e não será relevante para os propósitos deste artigo. Breves comentários serão feitos neste sentido, mas a leitura de [16] pode ser útil para maiores detalhes.

Na seção 2 estuda-se a Criptografia Clássica e sua segurança [1]. Também apresenta-se o algoritmo de Vernam. Na seção 3 são explicados os postulados da Mecânica Quântica e é feita uma breve demonstração do *no-cloning theorem*. Na seção 4, apresenta-se o protocolo BB84. Na seção 5 são tratados alguns casos simples de espionagem. Na seção 6, é feito um breve comentário sobre a parte prática e experimental da Criptografia Quântica.

2. Criptografia Clássica

A Criptologia é uma ciência que aqui será dividida em duas outras áreas: a Criptografia e a Criptoanálise. A Criptografia é a ciência que estuda formas de ocultar uma informação, codificando-a para que só possa ser compreendida por pessoas autorizadas. Por outro lado, alguém pode estar interessado em decodificar essa informação mesmo sem autorização. A área da Criptologia que estuda os métodos utilizados para alcançar esse objetivo chama-se Criptoanálise.

Nos problemas estudados pela Criptografia existem dois personagens que desejam comunicar-se através de um canal inseguro. Toda a comunicação, entretanto, pode ser interceptada por um terceiro personagem (chamada Eve[2], neste artigo), que não deveria tomar conhecimento da informação trocada. Para cifrar uma mensagem precisa-se de um algoritmo, e uma certa informação adicional (chamada chave), além, é claro, da própria mensagem. Para um sistema de Criptografia ser seguro ele deve ser tal que seja impossível decifrar a mensagem cifrada (criptograma) sem a posse da chave. O criptograma pode até ser lido, mas não pode, em hipótese alguma, ter revelado seu conteúdo original. Na prática, como esse requisito é muito difícil de ser alcançado, aceita-se que o sistema seja

[2]Em inglês existe a palavra *eavesdropper*, que significa algo como "bisbilhoteiro", e cuja pronúncia lembra o nome da vilã Eve.

muito difícil de ser quebrado, permitindo que a mensagem permaneça oculta pelo menos enquanto aquela informação for importante.

Os algoritmos criptográficos podem ser divididos em duas categorias: os simétricos (ou de chave secreta) e os assimétricos (ou de chave pública). Os primeiros são aqueles nos quais Alice e Beto compartilham a mesma chave. Possuem porém o inconveniente de ser necessário um mensageiro de confiança para que Alice e Beto troquem a chave. Os algoritmos assimétricos são aqueles nos quais Alice publica uma chave que serve para cifrar as mensagens a ela enviadas, mas ao mesmo tempo possui uma chave privada, somente com a qual ela pode decodificar as mensagens recebidas. Estes, funcionam como uma caixa postal, onde qualquer pessoa pode colocar um envelope, mas somente o dono da caixa pode abri-la para ler a carta.

O único algoritmo perfeitamente seguro conhecido até hoje é o Cifrador de Vernam. Deve-se a Claude Shannon a prova da inviolabilidade deste procedimento, além do próprio conceito de segurança perfeita [3].

2.1. Cifrador de Vernam

Tem-se uma mensagem p, representada por uma sequência de dígitos binários. A chave utilizada, k, é do mesmo tamanho que a mensagem, e é também representada por dígitos binários, porém estes devem ser aleatórios. A mensagem cifrada, c, é dada por:

$$c = p \oplus k, \tag{1}$$

onde $\oplus$ representa soma módulo 2. Isto é equivalente a fazer um *XOR* (OU-exclusivo) bit a bit entre a mensagem e a chave.

Assim, como a chave é aleatória, a mensagem cifrada também o será. As únicas restrições ao algoritmo são, em primeiro lugar, usar uma chave do mesmo tamanho que a mensagem a ser cifrada, e em segundo lugar, utilizar a chave somente um vez, trocando de chave a cada vez que uma nova mensagem for transmitida. Se a chave for utilizada mais de uma vez, Eve pode armazenar várias mensagens e obter informações delas. Sejam c_i, p_i e k as mensagens cifradas, mensagens abertas (não-codificadas) e a chave, respectivamente.

$$c_1 \oplus c_2 = p_1 \oplus p_2 \oplus k \oplus k = p_1 \oplus p_2, \tag{2}$$

onde foi utilizada a propriedade comutativa de $\oplus$, bem como a propriedade do elemento neutro, $x \oplus 0 = x$, e a identidade $x \oplus x = 0$.

É importante observar que, utilizando duas mensagens cifradas com a mesma chave, Eve conseguiu obter informação sobre as mensagens que não depende da chave, portanto, não é aleatória.

As restrições tornam o cifrador de Vernam impraticável para boa parte das aplicações realísticas, já que para cada mensagem trocada é necessária uma nova chave (que pode ser bastante grande), e para trocar essa chave é necessário um mensageiro confiável. Não adianta utilizar um algoritmo de chave assimétrica para trocar a chave, já que este não seria infalível, e quebrando-se este algoritmo, o Cifrador de Vernam já estaria condenado.

Entretanto, o protocolo BB84 permite a troca segura de chaves criptográficas quaisquer, e combinando-se isso com o algoritmo de Vernam, obtém-se uma Criptografia absolutamente livre de espionagem. Classicamente isto não é possível, já que, apesar de existirem métodos clássicos para distribuição de chaves em canais inseguros, nenhum destes pode impedir a cópia da chave transmitida publicamente em um canal de comunicação. O funcionamento do protocolo BB84 será exposto na seção 4.

2.2. Segurança Perfeita e a Inviolabilidade do Cifrador de Vernam

Nesta seção serão mostrados elementos que permitirão ao leitor provar a inviolabilidade do Cifrador de Vernam. Em primeiro lugar, deve-se definir o conceito de "sistema criptográfico".

Definição 1 *Um sistema criptográfico é um quintupleto $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ que satisfaça: i) $\mathcal{P}$ é o espaço das mensagens, ou seja, o conjunto finito de todas as mensagens possíveis; ii) $\mathcal{C}$ é o espaço dos criptogramas, ou seja, o conjunto finito de todos os criptogramas possíveis; iii) $\mathcal{K}$ é o espaço das chaves, ou seja, o conjunto finito de todas as chaves as possíveis; iv) para cada $k \in \mathcal{K}$ existe uma regra de cifragem $e_k \in \mathcal{E}$ e uma regra de decifragem correspondente $d_k \in \mathcal{D}$, tal que $e_k : \mathcal{P} \to \mathcal{C}$, $d_k : \mathcal{C} \to \mathcal{P}$ e $d_k(e_k(x)) = x, \forall x \in \mathcal{P}$.*

Claude Shannon definiu o conceito de "segurança perfeita" baseado na probabilidade de ocorrência dos elementos nos conjuntos $\mathcal{P}$, $\mathcal{C}$ e $\mathcal{K}$. Com isso a Criptologia, que antes era considerada pura arte, pode hoje ser considerada uma ciência.

Definição 2 *Para um sistema criptográfico possuir segurança perfeita é necessário que*

$$p(x \mid y) = p(x), \quad \forall x \in \mathcal{P}, \quad \forall y \in \mathcal{C} \tag{3}$$

onde $p(x)$ é definido por $Prob(\mathcal{P} = x)$ e $p(x \mid y)$ é definido por $Prob(\mathcal{P} = x \mid \mathcal{C} = y)$.

Ou seja, um sistema criptográfico possui segurança perfeita se a probabilidade *a posteriori* de uma mensagem x (quando observado seu criptograma y) é igual à probabilidade *a priori* de x.

Teorema 1 *Um sistema criptográfico possui segurança perfeita se e somente se*

$$p(y \mid x) = p(y), \quad \forall x \in \mathcal{P} \quad \forall y \in \mathcal{C} \tag{4}$$

onde seja, para todo $x \in \mathcal{P}$ e $y \in \mathcal{C}$, $P(y \mid x)$ deve ser independente de x.
Prova *Pelo teorema de Bayes e pela definição de segurança perfeita, tem-se que*

$$\frac{p(y \mid x)p(x)}{p(y)} = p(x) \Leftrightarrow p(y \mid x) = p(y) \tag{5}$$

desde que $p(y) \neq 0$.

Teorema 2 *O sistema criptográfico $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, onde $\|\mathcal{K}\| = \|\mathcal{C}\| = \|\mathcal{P}\| = n$ é perfeitamente seguro se e somente se cada chave é utilizada com probabilidade $\frac{1}{n}$.*

Prova *Como $\|\mathcal{K}\| = \|\mathcal{C}\|$, para cada par (x_i, y), onde $x_i \in \mathcal{P}$ e $y \in \mathcal{C}$, existe apenas uma chave k, tal que $y = e_k(x_i)$, onde $e_k \in \mathcal{E}$. Aplicando (3) e o teorema de Bayes, tem-se:*

$$p(x_i \mid y) = \frac{p(y \mid x_i)p(x_i)}{p(y)} \tag{6}$$

$$p(x_i) = \frac{p(y \mid x_i)p(x_i)}{p(y)}, \tag{7}$$

onde (6) $\Leftrightarrow$ (7).

Fixando um y constante, pode-se definir $p(k_i) = p(y \mid x_i) = p(y)$, como a probabilidade de ocorrência da chave k_i, que transforma a mensagem x_i no criptograma y. Como y é constante, $p(k_i)$ também tem que ser constante, para $1 \leq i \leq n$. Dessa forma, $p(k_i) = \frac{1}{\|\mathcal{K}\|} = \frac{1}{n}$.

3. Alguns *Flashes* de Mecânica Quântica

Nesta seção serão mencionados os postulados da Mecânica Quântica, fazendo ao final uma simples demonstração do *no-cloning theorem*.

O primeiro postulado, sobre o espaço de estados, ou espaço das configurações, diz que um sistema físico isolado tem associado um espaço de Hilbert. O sistema físico é totalmente descrito por um vetor de estado unitário nesse espaço de Hilbert. Esses vetores normalmente são representados na notação de Dirac, onde um vetor do tipo $\vec{v_i}$ é escrito como $|v_i\rangle$ (sem a seta), ou simplesmente, $|i\rangle$ (utilizando apenas o índice, subentendendo-se o nome). Estes são chamados *kets*. O vetor transposto conjugado, por sua vez, é representado por $\langle i|$. Dá-se o nome a estes, de *bras*. O produto escalar entre vetores, que equivale a multiplicar o transposto conjugado de um vetor por outro vetor, pode ser escrito $\langle a||b\rangle$, ou de forma mais simples, $\langle a|b\rangle$.

Assim, para um estado quântico de dois níveis (os chamados qubits), onde pode-se considerar a base computacional $\{|0\rangle, |1\rangle\}$, os vetores de estado podem ser representados por $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, onde $\alpha, \beta \in \mathbf{C}$, e são chamados de "amplitudes". O quadrado do módulo da amplitude corresponde a probabilidade de um resultado quando for feita uma medição. Fica claro então que, $\|\alpha\|^2 + \|\beta\|^2 = 1$. No exemplo anterior, existe uma probabilidade $\|\alpha\|^2$ de obter o resultado $|0\rangle$ na medição. O terceiro postulado irá falar sobre medições, formalizando estes conceitos.

A interpretação é que enquanto um bit clássico só pode estar em um estado de cada vez, um bit quântico pode estar em uma superposição de estados, como se valesse zero e um ao mesmo tempo, com suas probabilidades relativas.

O segundo postulado, sobre a evolução temporal, diz que a evolução de um sistema quântico fechado é descrita por uma transformação unitária. Se em t_1 o estado é $|\psi\rangle$ e em t_2 é $|\psi'\rangle$, então existe U unitário tal que $|\psi'\rangle = U|\psi\rangle$. U depende apenas de t_1 e t_2. Assim são representadas as "portas lógicas" em Computação Quântica. Por exemplo, o operador unitário equivalente a porta NOT clássica é a matriz de Pauli σ_x, pois $\sigma_x|0\rangle = |1\rangle$ e $\sigma_x|1\rangle = |0\rangle$. Em um estado genérico,

$$\sigma_x(\alpha|0\rangle + \beta|1\rangle) = \sigma_x(\alpha|0\rangle) + \sigma_x(\beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle \tag{8}$$

Em [8, 12] há estudos introdutórios sobre portas lógicas quânticas e circuitos quânticos. Em [9, 15] encontram-se explicações sobre a *Equação de Schrödinger*, utilizada para descrever a evolução de um sistema quântico em tempo contínuo.

Uma medição se caracteriza por um observável M, tal que $M = M^\dagger$. Logo, existe a decomposição espectral de M.

$$M = \sum_m mP_m \tag{9}$$

O terceiro postulado diz que os valores possíveis da medição de M são seus autovalores m, com a probabilidade $p(m) = \langle\psi|P_m|\psi\rangle$.

Além destes postulados, é importante conhecer o *no-cloning* theorem, para uma boa compreensão dos protocolos quânticos para Criptografia. Este teorema foi publicado por W.K.Wooters e W.H.Zurek, em um artigo da revista Nature de 1982 [17]. Aqui será mostrada apenas a impossibilidade de clonagem de estados quânticos genéricos. Para uma análise completa do caso, recomenda-se a leitura do artigo da Nature. Inicia-se a prova supondo que seja possível criar uma máquina que receba dois qubits, nomeados A e B. O qubit A, recebe um estado quântico desconhecido, $|\psi\rangle$, e o qubit B inicialmente está em um estado puro padrão, $|s\rangle$ (como se fosse uma folha em branco em uma máquina de cópia xerográfica). Deseja-se copiar esse estado $|\psi\rangle$ para o qubit B. O estado inicial da máquina é então

$$|\psi\rangle \otimes |s\rangle \tag{10}$$

onde $\otimes$ representa produto tensorial.

O cálculo o produto tensorial não será abordado em detalhes, aqui. Basta, por enquanto, saber que um registrador quântico é o produto tensorial entre dois ou mais qubits [3]. Para a cópia ser possível, segundo o segundo postulado da Mecânica Quântica, deve haver um operador unitário U que satisfaça: $U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$. Mas para a máquina ser genérica, ela deve servir para outro estado $|\phi\rangle$. Ou seja, $U(|\phi\rangle \otimes |s\rangle) = |\phi\rangle \otimes |\phi\rangle$. Fazendo o produto interno entre essas duas equações surge o importante resultado:

$$\langle\psi|\phi\rangle = (\langle\psi|\phi\rangle)^2. \tag{11}$$

É fácil perceber que as únicas soluções para essa equação são $\langle\psi|\phi\rangle = 1$ e $\langle\psi|\phi\rangle = 0$, ou seja, quando $|\phi\rangle = |\psi\rangle$, ou quando $|\phi\rangle$ e $|\psi\rangle$ são ortogonais. A primeira solução é trivial. Logo, foi provado que uma máquina de clonagem quântica só é capaz de clonar estados ortogonais. O protocolo BB84 utiliza fótons polarizados em bases não ortogonais, portanto eles não podem ser clonados.

[3] Há registradores quânticos que não podem ser escritos como produto tensorial de seus qubits. Diz-se que estes qubits estão emaranhados, pois estão de tal forma correlacionados, que não podem ser descritos individualmente.

4. Protocolo BB84

É bastante óbvia a idéia de que a informação clássica pode ser copiada facilmente. Basta que se pense em cópias de CDs e fitas K7, bastante comuns hoje em dia. Porém uma das propriedades mais importantes da Mecânica Quântica é a **impossibilidade** de cópia da informação quântica, segundo o *no-cloning theorem* (vide seção 3). **Não** se pode nem mesmo obter informação de um estado quântico genérico, do qual não se tenha conhecimento *a priori*, sem que se perturbe o sistema. Pode-se citar, ainda, o Princípio da Incerteza de Heisenberg, segundo o qual **não** é possível medir, com precisão infinita, certas grandezas complementares, como momento e posição. Qualquer estudante de Mecânica Quântica necessariamente se depara com uma série de propriedades impondo restrições à forma de observar ou manipular a natureza. A idéia da Criptografia Quântica está justamente na utilização desta propriedades.

Para simplificar, o protocolo BB84 será dividido em várias etapas. Na **primeira etapa**, Alice irá enviar uma sequência de bits[4] aleatórios para Beto. Esse bits serão enviados através de fótons, que poderão estar em duas polarizações diferentes: retilínea (+) ou diagonal ($\times$). Na base retilínea, os fótons podem ser polarizados em 0 ou 90 graus. Já na base diagonal, os fótons são polarizados em 45 ou 135 graus. Associam-se valores lógicos aos fótons polarizados. Por exemplo, zero para fótons polarizados em 0 ou 45 graus, e um para fótons polarizados em 90 ou 135 graus. Para medir o fóton, Beto escolhe uma base aleatoriamente, sendo que ele só vai obter a informação correta na medição se escolher a base certa (a mesma em que Alice polarizou o fóton). Se ele utilizar a base errada, o resultado obtido será aleatório. Essa sequência de bits obtidos por Bob, da mesma forma que a sequência de bits enviados por Alice, é chamada freqüentemente de *raw key* [5]. Naturalmente, a chave inicial de Alice é diferente da chave inicial de Bob, devido às medições incorretas. De fato, a discrepância, sem espionagem, é de 25% de bits incorretos.

A **segunda etapa** do protocolo, chamada de reconciliação de bases, é uma comunicação pública. Beto divulga as bases escolhidas por ele, sem revelar o resultado de sua medição. Alice, então, informa para Beto qual polarizador ela utilizou em cada fóton, mas não qual o qubit que ela enviou. Alice e Beto mantêm os bits cujas bases corresponderam, e formam uma chave com eles (normalmente chamada de *sifted key*, ou "chave filtrada").

Esta etapa reduz a chave inicial pela metade. Apesar de 75% da chave inicial estar correta, somente 50% representa informação, pois o restante corresponde a resultados aleatórios de quando Beto usou bases erradas para medir. Isso ainda ficará mais claro até o final do artigo, especialmente depois da seção sobre técnicas de espionagem.

Finalmente, deve-se aplicar algoritmos clássicos para detectar a presença de Eve, e para corrigir possíveis erros. Assim sendo, existe uma **terceira etapa**, para verificar se houve interceptação da comunicação por Eve, quando eles divulgam um subconjunto aleatório da chave e comparam, verificando a taxa de erro. Essa taxa de erro é chamada QBER (*quantum bit error rate*). Qualquer tentativa de captura da informação, por parte de Eve, implica em mudanças nesta informação, segundo a Teoria da Medida. Se for

[4] Ou melhor, *qubits*, do inglês: *quantum bits*, bits quânticos

[5] Literalmente, chave "crua". Neste artigo, será chamada de "chave inicial"

constatado que alguém tentou espionar a chave de Alice e Beto, eles podem voltar ao início do protocolo e fazer uma nova tentativa. Se não for constatada espionagem, eles descartam os bits utilizados na verificação, e continuam o protocolo.

Neste artigo, para simplificar, é dada ênfase ao protocolo sob condições ideais. No entanto, em situações práticas o canal poderia ter ruído, ou os equipamentos utilizados poderiam ter pequenos defeitos, de forma que o qubit chegasse a Beto um pouco diferente do qubit pretendido por Alice, introduzindo uma pequena taxa de erro. Para corrigir isso, dever-se-ia utilizar algum algoritmo de correção de erros no final. Esta seria a **quarta etapa**. Além disso, Eve poderia aplicar alguma estratégia de espionagem apenas em parte da comunicação, obtendo uma pequena quantidade de informação sobre a chave, mas induzindo uma taxa de erro menor ainda. Possivelmente, a chave iria passar pela terceira etapa, confundindo-se a espionagem maligna de Eve com o inocente ruído da natureza. Na **quinta etapa**, essa pequena informação obtida por Eve deve ser reduzida a zero em um processo chamado "amplificação de privacidade" (privacy amplification).

Assim como na terceira etapa, a quarta e a quinta também implicam redução da chave. Então é evidente que o número de fótons emitidos por Alice deve ser bem maior que o tamanho da chave desejada. Claro que não é obrigatória a utilização do cifrador de Vernam. Existem outros cifradores bastante eficientes que poderiam ser utilizadas, sendo que, neste caso, a criptografia deixaria de ser infalível.

Com o exemplo a seguir, o funcionamento do protocolo ficará mais claro.

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 Beto	x	+	x	x	x	+	+	x	+	x	+	x	x	+	+
Chave		0	0	1			1	1		0	1				1

Tabela 1: Exemplo de distribuição de chaves

Na tabela acima, pode-se ver na primeira linha a sequência de bits aleatórios que Alice resolveu enviar para Beto. Na segunda linha, estão as polarizações que ela decidiu usar. Na terceira linha, as polarizações com as quais Beto mediu cada fóton recebido. Após Beto comunicar em um canal público as bases utilizadas para medição, e Alice confirmar em quais casos ela utilizou a mesma base para polarizar o fóton, eles podem montar uma chave somente com as medições corretas. No caso da tabela 1, ela será 00111011. Alguns bits, no entanto, são perdidos nas próximas etapas, de correção de erros e amplificação de privacidade (quando se consideram canais com ruído). Naturalmente, em situações práticas, a quantidade de fótons enviados seria muito maior que a do exemplo.

Se Eve tentar interceptar os fótons enviados por Alice e medi-los, irá perturbar o sistema, e reenviará qubits danificados para Beto. É importante lembrar que Eve não pode fazer cópias dos fótons antes de medir, e ao fazer uma medição escolhendo a base errada, ela não irá obter informação. Eve também não pode adivinhar que polarizador será usado por Alice, pois estas escolhas são totalmente aleatórias.

No final do protocolo, quando Alice e Beto compararem um subconjunto de sua *sifted key*, eles irão perceber que alguns bits estão errados, mesmo Beto tendo medido na mesma base que Alice usou para polarizar o fóton. Isso significa que alguém inter-

ceptou o qubit, mediu na base errada, e reenviou para Beto. Alice e Beto podem então descartar a chave e repetir o protocolo, até que consigam uma chave segura. Uma vez que tenham conseguido trocar uma chave segura, eles podem utilizar o algoritmo de Vernam, e a mensagem estará infalivelmente cifrada. A vantagem é que percebe-se a presença de intrusos antes que alguma mensagem valiosa seja trocada. Aliás, é por isso que o protocolo BB84 serve apenas para distribuir chaves, e não para trocar mensagens: a verificação de segurança só pode ser feita no final do protocolo.

4.1. Comentários adicionais sobre o protocolo

Todo sistema de distribuição de chaves precisa ter autenticação. Caso contrário, Eve poderia mentir para Alice, passando-se por Beto, e da mesma forma, mentir para Beto, passando-se por Alice[6]. O protocolo quântico quântico também requer certos cuidados. Uma possível solução, para evitar ataques *man-in-the-middle* no protocolo BB84, seria admitir que Alice e Beto compartilham um pequeno segredo inicialmente (uma pequena sequência de zeros e uns). Esse segredo é usado para autenticação no início do protocolo, quando então uma grade chave é gerada. Uma pequena parte dessa chave é guardada para a próxima seção. Sob este ponto de vista, o protocolo quântico de distribuição de chaves funciona como um "aumentador de segredo". Algumas outras estratégias de espionagem serão comentadas mais adiante.

É interessante, ainda, citar uma aplicação interessante para o *one-time pad*: o teletransporte clássico. Supondo que Alice possua um sistema clássico qualquer, deseja-se transportá-lo para Beto através de um canal inseguro, sem que Eve tome conhecimento de seu estado. Se Alice e Beto inicialmente compartilharem uma chave arbitrariamente grande, isso seria possível. Alice pode medir o sistema com precisão arbitrária, e enviar o resultado dessa medição através do *one-time pad*. Beto, a partir dessa informação, poderia reconstruir o sistema.

O teleporte quântico [7], descoberto em 1993, é uma técnica que permite mover um estado quântico mesmo na ausência de um canal de comunicação quântico. Assim como no parágrafo anterior foi feita uma comparação entre o cifrador de Vernam e um teletransporte clássico, pode-se também fazer uma analogia entre o teletransporte quântico e uma espécie de Cifrador de Vernam Quântico.

Inicialmente, Alice e Beto devem compartilhar uma quantidade arbitrariamente grande de qubits emaranhados. Esses qubits são análogos à chave do cifrador de Vernam clássico. Supõe-se que Alice tenha uma sequência de qubits representando uma informação, a qual deve ser enviada para Beto de forma segura. Ela não pode medir o sistema para extrair informação clássica, pois fazendo isso os qubits sofreriam um colapso (vide seção 3). No entanto, Alice pode teletransportar esses estados para Beto, de forma que Eve não tenha acesso. Beto, ao receber esses estados pode medi-los e obter a informação, ou talvez realizar alguma operação no sistema antes.

5. Estratégias Básicas de Espionagem

Este artigo é um estudo, voltado para estudantes de Ciência da Computação, do protocolo criado em 1984 no Canadá. Mesmo assim, convém mencionar algumas técnicas de espi-

[6]Na literatura em inglês este tipo de ataque é conhecido como *man-in-the-middle attack* [14].

onagem, para que se tenha uma noção da segurança real do protocolo. Para ser seguro o protocolo deve, em qualquer situação, gerar uma chave segura ou informar a existência de espionagem aos usuários, antes da troca da mensagem.

As técnicas estudadas serão a Interceptar-Reenviar e a de medição na base intermediária.

5.1. Interceptar-Reenviar

Nesta estratégia, Eve intercepta todos os qubits vindos de Alice e os mede, escolhendo uma base aleatória. Depois disso, ela reenvia o qubit para Beto. Isto está representado no diagrama da (Fig. 1), na página 10.

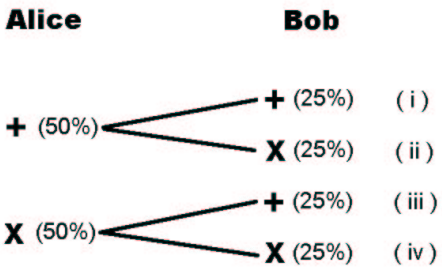

Figura 1: Casos possíveis no BB84 sem espionagem

Nele está representado o caso trivial, onde não há espionagem. Na reconciliação de bases, Alice e Beto irão concordar somente nos casos (i) e (iv), onde ambos usam a mesma base. Em (ii) e (iii) metade dos bits estarão corretos, mas mesmo assim serão descartados, pois a informação é aleatória.

A *sifted key*, então, terá a metade do tamanho da chave inicial, e ao medir a taxa de erros, obter-se-á zero ($QBER = 0$). A partir da (Fig. 2) pode-se analisar as possibilidades quando existe espionagem.

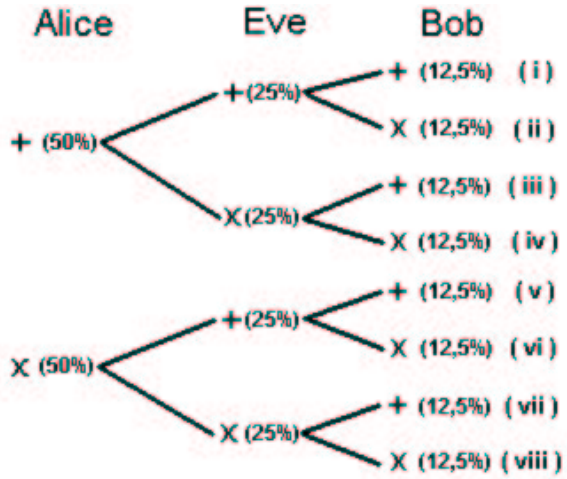

Figura 2: Casos possíveis no BB84 com espionagem

Na reconcilização de bases, Alice e Beto concordam em (i), (iii), (vi) e (viii). Os outros bits são todos descartados. Os bits restantes correspondem à tabela 2.

Base utilizada por Alice	+	+	x	x
Base utilizada por Eve	+	x	+	x
Base utilizada por Bob	+	+	x	x
Situação correspondente	i	iii	vi	viii
Ocorrência na *sifted key*	25%	25%	25%	25%

Tabela 2: Composição da *sifted key* em uma situação de espionagem Interceptar-Reenviar

Portanto, nesta estratégia, Eve obtém 50% de informação (para cada 2 bits da *sifted key* ela consegue 1 bit de informação), correspondendo à primeira e à quarta coluna da tabela. Enquanto isso, introduz uma taxa de erros de 25% ($QBER = 0.25$), que corresponde às metades da segunda e terceira coluna da tabela.

Claro que Eve poderia aplicar a estratégia Interceptar-Reenviar em apenas alguns fótons. Nesse caso, ela obteria menos informação, mas introduziria uma pertubação ainda menor, podendo até ser confundida com o ruído do canal. Para evitar esse tipo de problema, Alice e Beto utilizam algum processo de amplificação de privacidade, conforme mencionado anteriormente.

5.2. Medição na Base Intermediária

Nesta estratégia, em vez de Eve escolher as bases aleatoriamente, ela mede sempre em uma mesma base, que não é nenhuma das mencionadas anteriormentes, mas sim uma base intermediária (Fig. 3). Para simplicar, as bases estão representadas graficamente, levando-se em conta apenas valores reais. Porém no caso mais genérico, em que as amplitudes dos estados podem assumir valores complexos o método funciona da mesma forma[7]. Além disso, é importante ressaltar a convenção feita aqui, segundo a qual $|\alpha\rangle$ representa o zero lógico da base intermediária e $|\beta\rangle$, o um lógico.

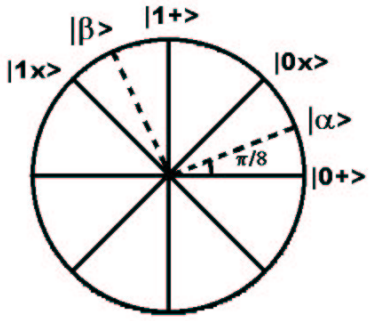

Figura 3: Base intermediária $\{|\alpha\rangle, |\beta\rangle\}$

Mostrar-se-á que essa técnica não apresenta vantagem para Eve, em comparação com o método Interceptar-Reenviar. Mesmo assim, é muito interessante teoricamente.

Reescrevendo as quatro bases tradicionais do BB84 na nova base $\{|\alpha\rangle, |\beta\rangle\}$, vista na (Fig. 3), tem-se:

[7]Mesmo no caso geral, em que as amplitudes do qubit são números complexos, pode-se representá-lo graficamente através da "esfera de Bloch". No entanto, esta representação não é utilizada aqui por questões didáticas.

$$|0_x\rangle = \cos\frac{\pi}{8}|\alpha\rangle + \sin\frac{\pi}{8}|\beta\rangle \tag{12}$$

$$|0_+\rangle = \cos\frac{\pi}{8}|\alpha\rangle - \sin\frac{\pi}{8}|\beta\rangle \tag{13}$$

$$|1_x\rangle = -\sin\frac{\pi}{8}|\alpha\rangle + \cos\frac{\pi}{8}|\beta\rangle \tag{14}$$

$$|1_+\rangle = \sin\frac{\pi}{8}|\alpha\rangle + \cos\frac{\pi}{8}|\beta\rangle \tag{15}$$

Conclui-se que a probabilidade de Eve acertar o valor enviado por Alice, utilizando a base intermediária para medir seria:

$$p = \left(\cos\frac{\pi}{8}\right)^2 \approx 0.854 \tag{16}$$

Calculando a probabilidade de Beto obter um resultado errado mesmo usando a base supostamente correta (a mesma usada por Alice), encontra-se o QBER produzido por Eve ao utilizar essa estratégia de espionagem. Não é difícil perceber que $QBER = 2p(1-p) = 0.25$.

Até aqui pode parecer que esta estratégia é mais eficiente (sob o ponto de vista de Eve). Afinal, o QBER produzido é o mesmo, e Eve tem uma probabilidade maior de acertar a medição (cerca de 85% contra 75% do Interceptar-Reenviar). Porém a análise do ganho de informação por bit da *sifted key* revela que:

$$I = H_{\text{a priori}} - H_{\text{a posteriori}} \tag{17}$$

$$I = 1 - H(p) \approx 0.399 \tag{18}$$

onde H é a função de entropia. Esta, é definida como uma função de uma distribuição de probabilidades, $p_1, p_2, \ldots, p_n$, da forma:

$$H(p_1, p_2, \ldots, p_n) = -\sum_x p_x \log p_x, \tag{19}$$

convencionando-se que $0 \log 0 \equiv 0$. Pode-se notar que $\lim_{x\to 0} x \log x = 0$.

A entropia de Shannon é um conceito importantíssimo para a Teoria da Informação, e serve para medir a incerteza acerca de um determinado sistema físico, ou, equivalentemente, a quantidade de informação ganha ao medir este sistema.

Então, este método não traz vantagens para Eve, já que ela ganharia 0.399 bit de informação por bit da *sifted key*, contra 0.5 do método Interceptar-Reenviar. Há uma diferença sutil entre acertar a medição e obter informação.

Deve-se notar que se Eve utiliza o método Interceptar-Reenviar, em 50% dos casos não há informação (os resultados são aleatórios). Entretanto, nos outros casos (50% da *sifted key*) a informação é determinística. Por outro lado, ao medir na base intermediária o resultado é sempre probabilístico.

6. Questões Tecnológicas

A primeira experiência em Criptografia Quântica foi realizada em um laboratório da IBM, em 1990, com os resultados sendo publicados somente em 1992 [5]. A distância era de apenas 30cm, mas ainda assim o resultado foi muito importante.

Na prática, o que se procura são distâncias muito maiores (da ordem de km), ou muito menores que 30cm. Esta última situação não é muito óbvia, porém o artigo [2] mostra aplicações para Criptografia Quântica onde Alice e Beto devem estar muito próximos, como é o caso de um cartão de crédito e a máquina ATM, por exemplo.

Os experimentos em Criptografia quântica podem ser realizados com espaço livre ou fibras óticas, sendo as últimas o caso mais comum atualmente. Tendo escolhido o canal quântico, deve-se escolher o comprimento de onda dos fótons que serão utilizados, para haver compatibilidade entre os emissores e os detectores.

Existem duas opções: fótons com 800nm, ou fótons na faixa de 1300 até 1500nm. Os primeiros apresentam a vantagem de serem compatíveis com contadores de fótons eficientes já disponíveis no mercado, mas têm a desvantagem de precisarem de fibras especiais ou espaço livre, já que não são compatíveis com as fibras óticas mais comuns. Os últimos têm compatibilidade com as fibras óticas utilizadas atualmente em telecomunicações, mas precisam que sejam desenvolvidos contadores de fótons mais eficientes. Também têm a vantagem de possuírem uma atenuação bem menor. Enquanto os fótons com comprimento de onda na faixa dos 800nm têm sofrem atenuação de 2 dB/km, os fótons com cerca de 1300nm sofrem atenuação de 0.20 até 0.35 dB/km. Caso desejese utilizar espaço livre, o melhor comprimento de onda é 800nm, que neste caso coincide com uma baixa atenuação.

Atualmente a distribuição quântica de chaves atinge distâncias consideráveis. Na Suíça foi realizado um experimento sob o lago de Genebra, trocando chaves entre os 23km que separam as cidades de Nyon e Genebra. Para isso foi utilizada fibra ótica da empresa de telecomunicações Swisscom, do mesmo tipo usado em telefonia convencional. Recentemente, também na Suíça, foi realizado um experimento ligando dois pontos separados por 67km [11]. Algumas empresas, como a suíça Id Quantique e a americana MagiQ Technologies, já estão até mesmo começando a explorar a Criptografia Quântica comercialmente.

7. Conclusões

Neste artigo, o protocolo BB84 foi apresentado de forma resumida e voltada para estudantes de Ciência da Computação. Mostrou-se como o protocolo pode ser usado por duas partes, Alice e Beto, para derivar uma chave secreta comum, sem a necessidade de estabelecer um canal secreto *a priori*. Claramente, o protocolo BB84 funciona com absoluta segurança sob condições ideais, onde Beto e Alice possuem equipamentos perfeitos e se comunicam em um canal sem nenhum ruído. Além disso, o emissor deve ser capaz de enviar um único fóton por pulso. Se ele enviar um feixe com pelo menos dois fótons, existe a possibilidade de que Eve possua uma tecnologia mais avançada, que permita dividir o feixe, medindo um *qubit* e enviando outro inalterado para Beto.

Estas restrições são muito difíceis de serem satisfeitas na prática. Por isso,

procura-se entender o comportamento do protocolo mesmo em condições não ideais, estudando várias formas de criptoanálise. Para cada forma de criptoanálise que se descobre, tenta-se solucionar o caso adicionando processos extras ao protocolo, como códigos de correção de erro e amplificaçao de privacidade, por exemplo. Mesmo com estas difuldades técnicas, decorrentes do desafio inerente à manipulação de sistemas quânticos, pode-se constatar que a Criptografia Quântica tem tido grades avanços nos últimos anos, cada vez mais deixando os laboratórios para, efetivamente, servir à sociedade.

Análises mais profundas da Criptografia Quântica em canais com ruído, ou com equipamentos imperfeitos, fogem do escopo deste texto. O artigo [16] pode ser de grande utilidade para quem pensa em se aprofundar nessa área, e o artigo [10] pode ser igualmente interessante, por mostrar técnicas para se provar segurança incondicional em Criptografia Quântica.

Agradecimentos

Este trabalho teve o suporte financeiro do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), através de uma bolsa de Iniciação Científica no Centro Brasileiro de Pesquisas Físicas (CBPF). O autor agradece ao Prof. J.A. Helayël-Neto e ao Dr. J.L. Acebal pelo trabalho de orientação e pelas discussões. Especiais agradecimentos também são feitos ao Prof. R. Portugal (LNCC) pelos cursos, pelas discussões e pelo incentivo.

Referências

[1] A. Menezes, P. van Oorschot and S. Vanstone, "Handbook of Applied Cryptography". CRC Press, Inc (1996). Disponível em <http://cacr.math.uwaterloo.ca/hac>.

[2] B. Huttner, N. Imoto and S.M. Barnett, "Short distance applications of quantum cryptography", J. Nonlinear Opt. Phys. Mater. **5**, (1996) pp.823-832.

[3] C.E. Shannon, "A Mathematical Theory of Communication", Bell System Technical Journal, July (1948) p.379; October (1948) p.623.

[4] C.E. Shannon, "Communication Theory of Secrecy Systems". Bell System Technical Journal, vol.28-4, (1949) pp.656-715.

[5] C.H. Bennett, F. Bessette, *et al.*, "Experimental quantum cryptography". J. Cryptology, **5** (1992) 3-28.

[6] C.H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India. (1984) pp.175-179.

[7] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W.K. Wooters, "Teleporting an unknown quantum state via dual classical and Einsteins-Poldosky-Rosen channels", Phys. Rev. Lett. **70** (1993) pp.1895-1899.

[8] C. Lavor, L.R.U. Manssur and R. Portugal, "Grover's Algorithm: Quantum Database Search". (2003) Disponível em <http://www.arxiv.org/quant-ph/0301079>.

[9] C.P. Williams and S.H. Clearwater, "Explorations in Quantum Computing", The Electronic Library of Science, California (1997).

[10] D. Mayers, "Unconditional Security in Quantum Cryptography", Journal of the Association for Computing Machinery. Vol.48, No.3, (2001) pp.351-406.

[11] D. Stucki, *et al.*, "Quantum Key Distribution over 67km with a plug&play system". New Journaul of Physics, No.4, (2002) p.41.

[12] F.L. Marquezino and R.R. Mello Junior, "An Introduction to Logical Operations on Classical and Quantum Bits". (2004) Disponível em <http://www.arxiv.org/physics/0404134>.

[13] G.S. Vernam, "Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications", Journal American Institute of Electrical Engineers, v.XLV, (1926) pp.109-115.

[14] K.G. Paterson, F. Piper and R. Schack, "Why Quantum Cryptography?". (2004) Disponível em <http://www.arxiv.org/quant-ph/0406147>.

[15] M.A. Nielsen and I.L. Chuang, "Quantum Computation e Quantum Information", Cambridge University Press (2000).

[16] N. Gisin, G.Ribordy, W. Tittel and H.Zbinden, "Quantum Cryptography", Reviews of Modern Physics, **74**, (2002) pp.145-195.

[17] W.K. Wooters and W.H. Zurek, "A single quantum cannot be cloned", Nature, **299**, (1982) pp.802-803.