Estudo Introdutório do Protocolo Quântico BB84 para Troca Segura de Chaves

F.L. Marquezino[*]
CBPF - Centro Brasileiro de Pesquisas Físicas
CCP - Coordenação de Campos e Partículas
(Bolsista PIBIC no CNPq)
Av. Dr. Xavier Sigaud 150 - CEP 22.290-180 Rio de Janeiro (RJ)
e-mail: franklin@serraon.com.br

Resumo

Este artigo tem como objetivo fazer uma revisão do protocolo quântico BB84 para troca segura de chaves criptográficas. O protocolo BB84 foi criado em 1984 e utiliza propriedades da Mecânica Quântica, o que o torna inviolável. Após uma breve explicação sobre a criptografia clássica e sobre a cifra de Vernam, o funcionamento do protocolo BB84 é explicado, e são fornecidos exemplos. 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.

Palavras-chave. Criptologia, Segurança de Dados, Mecânica Quântica, Informação Quântica.

[*]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 Introdução

O protocolo BB84 foi criado por Charles Bennett e Gilles Brassard em 1984 [7], 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 em algoritmos 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. 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[2], impossível de ser violado segundo a Teoria de Shannon, desde que a chave tenha o mesmo tamanho da mensagem e seja utilizada somente uma vez.

Neste artigo será explicadoo 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, o mais importante, em canais sem ruído. O caso do protocolo em canais com ruído e com equipamentos imperfeitos é um problema ainda não resolvido completamente [15].

Na seção 2 será estudada a criptografia clássica e sua segurança [2]. Também será apresentado o algoritmo de Vernam. Na seção 3, será apresentado o protocolo BB84. Na seção 4 são tratados alguns casos simples de espionagem. Na seção 5, é feito um breve comentário sobre a parte prática e experimental da criptografia quântica. No apêndice A apresentar-se-á algumas noções de entropia de Shannon, importante para que se entenda a inviolabilidade do algoritmo de Vernam. No segundo apêndice são explicados os postulados da Mecânica Quântica e faz-se uma breve demonstração do *no-cloning theorem*.

2 Criptografia Clássica

A Criptologia é uma ciência composta basicamente de 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 mesma informação. A área da Criptologia que estuda métodos para alcançar esse objetivo chama-se Criptoanálise.

Nos problemas estudados pela criptografia, existem dois personagens (chamaremos de Alice e Beto), que desejam comunicar-se através de um canal inseguro. Mas toda informação para por um terceiro personagem (normalmente Eve[3]), que não deveria tomar conhecimento da informação trocada. Para criptografar 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 absolutamente seguro deve ser tal que seja

[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

[2] Também chamado de *one-time pad*

[3] Eve é um nome feminino equivalente a Eva, em português. Em inglês temos a palavra *eavesdropper*, que significa algo como "bisbilhoteiro", e cuja pronúncia lembra o nome de nossa vilã.

impossível decifrar a mensagem sem a posse da chave[4]. Na prática, como esse requisito é muito difícil de ser alcançado, aceita-se que o sistema seja 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 privada) 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 encontro, ou um canal seguro para que Alice e Beto troquem a chave. Os algoritmos assimétricos são aqueles nos quais Alice publica uma chave que serve para criptografar as mensagens a ela enviadas, mas ao mesmo tempo possui uma chave secreta, somente com a qual ela pode decodificar as mensagens recebidas. Estes algoritmos 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.

Normalmente os algoritmos de chave assimétrica são bem mais lentos, então eles não são utilizados para trocar a mensagem em si, mas para a troca da chave. Utiliza-se assim algum algoritmo de chave assimétrica, como o RSA por exemplo, para transmitir a chave de algum algoritmo de chave simétrica, como por exemplo, o DES. O único algoritmo conhecido até hoje que é absolutamente seguro, de acordo com a Teoria da Informação, de Shannon, é a Cifra de Vernam.

2.1 Cifra de Vernam

Tem-se uma mensagem m, representada por uma seqüência 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 criptografada, c, é dada por:

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

onde $\oplus$ representa soma módulo 2, sem o chamado "vai-um".

Isso é equivalente a fazer um *XOR* bit a bit entre a mensagem e a chave. Assim, como a chave é aleatória, a mensagem cifrada também o será. Segundo a teoria de Shannon, a mensagem criptografada tem entropia máxima neste caso (ver apêndice A). A entropia mede o grau de "desconhecimento", ou de "desordem", de um sistema. Como a mensagem está escrita em um alfabeto binário, em que cada letra ocorre com a mesma probabilidade, temos que a entropia será:

$$H(c) = -\left(\frac{1}{2}\log_2\frac{1}{2} + \frac{1}{2}\log_2\frac{1}{2}\right) = 1 \tag{2}$$

Os computadores atuais utilizam alfabeto binário, porém é fácil perceber que a mensagem continuaria tendo entropia máxima se utilizássemos um alfabeto de n letras, fazendo soma módulo n, sem vai-um. 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

[4]Repare que a mensagem criptografada pode até ser lida, mas não pode em hipótese nenhuma ter revelado seu conteúdo original.

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 criptografadas, mensagens planas (não-codificadas) e a chave, respectivamente.

$$c_1 \oplus c_2 = p_1 \oplus p_2 \oplus k \oplus k = p_1 \oplus p_2 \tag{3}$$

Foi utilizada a propriedade comutativa de $\oplus$, bem como a identidade $x \oplus x = 0$. Repare que utilizando duas mensagens criptografadas com a mesma chave, Eve conseguiu obter informação sobre as mensagens que não depende da chave, portanto, não é aleatória. Na prática, alguém poderia aceitar utilizar a mesma chave poucas vezes, sob o custo de uma perda tolerável na segurança.

Mesmo assim, as restrições tornam a cifra 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 canal seguro. Não adianta utilizar um algoritmo de chave assimétrica para trocar a chave, já que este não seria infalível, e quebrando-se este algoritmo, a Cifra de Vernam já estaria condenada.

Entretanto, o protocolo BB84 permite a troca segura de chaves criptográficas quaisquer, e combinando-se isso com o algoritmo de Vernam, teríamos uma criptografia absolutamente livre de espionagem. Classicamente isso não é possível, já que não existe nenhum método clássico para distribuição de chaves em canais inseguros. E trocar uma chave criptográfica simétrica em um canal inseguro é tão imprudente quanto não utilizar criptografia nenhuma. Na seção (3) veremos o funcionamento do protocolo BB84.

2.2 Teletransporte Clássico

Uma aplicação interessante para o *one-time pad* seria o teletransporte clássico. Suponha que Alice tenha um sistema clássico qualquer. Deseja-se transportar este sistema para Beto através de um canal inseguro, sem que Eve tome conhecimento do estado deste sistema. 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 medida através do *one-time pad*. Beto, a partir dessa informação, poderia reconstruir o sistema.

3 Protocolo BB84

É bastante óbvia a idéia de que a informação clássica pode ser copiada facilmente. Basta pensarmos 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* (veja o segundo apêndice). Não se pode obter informação de um estado quântico genérico, do qual não se tenha conhecimento *a priori*, sem que se perturbe o sistema. A idéia da criptografia quântica está justamente na utilização desta propriedade.

Para simplificar, irei dividir o protocolo em várias etapas. Na **primeira etapa**, Alice irá enviar uma seqüência de bits[5] aleatórios para Beto. Esse bits serão enviados através de fótons, que poderão estar em duas polarizações diferentes: retilínea (+) ou diagonal

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

(×). 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 seqüência de bits obtidos por Bob, da mesma forma que a seqëncia de bits enviados por Alice, é chamada freqüentemente de raw key [6]. 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 que foram lidos corretamente, e formam uma chave com eles (normalmente chamada de *sifted key*[7]).

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.

Na última parte do protocolo, deve-se aplicar algoritmos clássicos para detectar a presença de Eve, e para corrigir possíveis erros. Na **terceira etapa**, para verificar se houve interceptação da comunicação por nossa vilã Eve, 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*). Se for 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, estamos dando ênfase ao protocolo sob condições ideais. No entanto, em situação 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 da cifra de Vernam. Outras cifras, como o DES por exemplo, são bastante eficientes (apesar de não serem infalíveis), e poderiam ser utilizados.

[6] Literalmente, chave "crua". Chamaremos de "chave inicial"

[7] Algo como "chave selecionada".

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, vemos na primeira linha a seqüência de bits aleatórios que Alice resolveu enviar para Beto. Na segunda linha, temos 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 interceptou 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 criptografada. 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.

3.1 Crescimento de segredo quântico

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. Uma possível solução seria admitir que Alice e Beto compartilham um pequeno segredo inicialmente (uma pequena seqüência de zeros e uns). Esse segredo é usado para autenticação no início do protocolo BB84, 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".

3.2 Analogia entre Teletransporte Quântico e *One-Time Pad*

O teleporte quântico [8] foi descoberto em 1993 por um número relativamente grande de pesquisadores, entre os quais, C. Bennett, um dos criadores do protocolo BB84. Assim como na subseção 2.2 comparamos a cifra de Vernam a um teletransporte clássico, podemos fazer uma analogia entre o teletransporte quântico e uma espécie de cifra de Vernam quântica.

Inicialmente, Alice e Beto devem compartilhar uma quantidade arbitrariamente grande de qubits emaranhados. Esses qubits são análogos à chave da cifra de Vernam clássica. Digamos que Alice tenha uma seqüência 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 iriam colapsar (veja apêndice sobre Mecânica Quântica). 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.

4 Estratégias Básicas de Espionagem

Este artigo é uma revisão, voltada para estudantes de Ciência da Computação, do protocolo criado em 1984 no Canadá. Mesmo assim, convém mencionar algumas técnicas de espionagem, 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.

4.1 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. Vejamos o diagrama (Fig 1) na página 6.

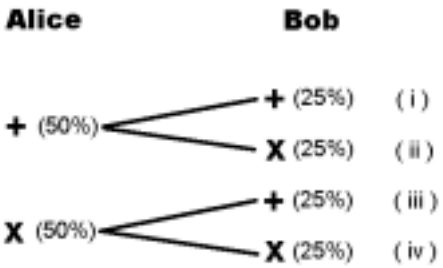

Figura 1: Casos possíveis no BB84 sem espionagem

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 ($QBER = 0$). Vejamos a (Fig. 2) e analisemos as possibilidades quando existe espionagem.

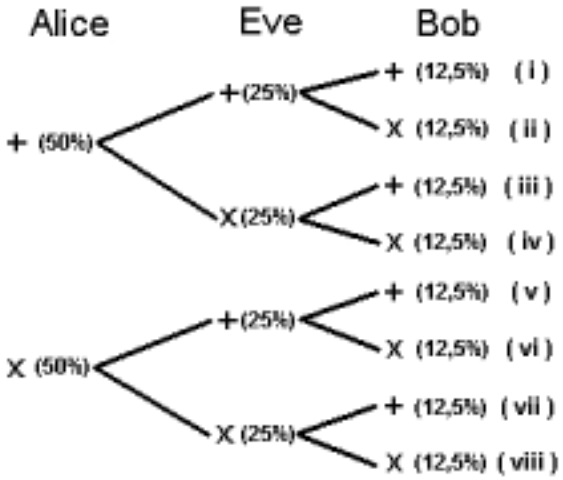

Figura 2: Casos possíveis no BB84 com espionagem

Na reconcilização de bases, Alice e Beto concordam em (i), (iii), (vi) e (viii). Os outros bits serão todos descartados. Os bits restantes corresponderão 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 confunfida com o ruído do canal. Para evitar esse tipo de problema, Alice e Beto utilizam algum processo de amplificação de privacidade, conforme mencionado anteriormente.

4.2 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[8]. Além

[8]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

disso, é importante ressaltar que convencionamos $|\alpha\rangle$ representando o zero lógico da base intermediária e $|\beta\rangle$, o um lógico.

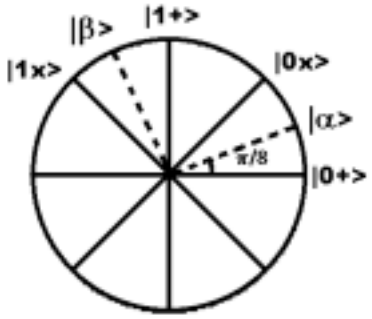

Figura 3: Base intermediária $\{|\alpha\rangle, |\beta\rangle\}$

Mostrarei 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), temos:

$$|0_x\rangle = \cos\frac{\pi}{8}|\alpha\rangle + \sin\frac{\pi}{8}|\beta\rangle \tag{4}$$

$$|0_+\rangle = \cos\frac{\pi}{8}|\alpha\rangle - \sin\frac{\pi}{8}|\beta\rangle \tag{5}$$

$$|1_x\rangle = -\sin\frac{\pi}{8}|\alpha\rangle + \cos\frac{\pi}{8}|\beta\rangle \tag{6}$$

$$|1_+\rangle = \sin\frac{\pi}{8}|\alpha\rangle + \cos\frac{\pi}{8}|\beta\rangle \tag{7}$$

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

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

Se calcularmos a probabilidade de Beto obter um resultado errado mesmo usando a base supostamente correta (a mesma usada por Alice), encontraremos 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 se analisarmos o ganho de informação por bit da *sifted key*, veremos que:

$$I = H_{\text{a priori}} - H_{\text{a posteriori}} \tag{9}$$

$$I = 1 - H(p) \approx 0.399 \tag{10}$$

onde H é a função de entropia (ver apêndice).

didáticas.

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.

Repare 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.

5 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 [6]. 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 isso. Esta última situação não é muito óbvia, porém o artigo [4] mostra aplicações onde Alice e Beto devem estar muito próximos, como é o caso de um cartão de crédito e a máquina, 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 deseje-se 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 [12]. Algumas empresas, como a suíça iD Quantique e a americana MagiQ Technologies, já estão até mesmo começando a explorar a criptografia quântica comercialmente.

6 Conclusões

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. Por equipamento perfeito, entende-se um emissor que consiga emitir os fótons na exata polarização descrita pelo protocolo, e um detector que mede na base exata que se

deseja. Caso contrário existiria uma probabilidade não nula de Beto medir (ou pensar medir) um fóton na mesma base que Alice polarizou (ou pensava ter polarizado) o fóton, e mesmo assim obter um resultado errado. Além disso, o emissor deve ser capaz de enviar um único fóton por pulso. Se ele enviar um feixe com pelo menos dois ftons, 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. Dessa forma sua presença não poderia ser detectada. Canal sem ruído significa que o qubit não sofre nenhuma alteração no percurso: ele chega a Beto da mesma forma que saiu de Alice.

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 que possa existir em cada situação. 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. Porém uma análise completa da criptoanálise em situações não-ideais ainda não foi alcançada.

Em 1992, Charles Bennett publicou outro artigo [5] com um novo protocolo quântico para troca de chaves, que ficou conhecido como B92. A idéia desse protocolo é bem semelhante ao anterior: em vez de utilizar quatro estados não-ortogonais, utilizam-se apenas dois. Desde que eles não sejam ortogonais entre si, Eve não pode copiá-los. Outro protocolo importante é o EPR (Einstein-Poldosky-Rosen), desenvolvido por Arthur Ekert, da Universidade de Oxford, em 1991 [3]. Ele é baseado no BB84, e tem esse nome por estar diretamente relacionado com o famoso debate filosófico sobre a desigualdade de Bell. Einstein, Poldosky e Rosen, três grandes físicos do século passado, propuseram um paradoxo em 1935 [1], criticando a Mecânica Quântica. Este paradoxo ficou conhecido como o "paradoxo EPR".

O objetivo deste artigo é fazer uma breve revisão, em língua portuguesa, desta área relativamente nova da criptologia. Portanto, análises mais profundas da criptografia quântica em canais com ruído, ou com equipamentos imperfeitos, fogem do escopo deste texto. O artigo [15] pode ser de grande utilidade para quem pensa em se aprofundar nessa área, e o artigo [11] pode ser igualmente interessante, por mostrar técnicas para se provar segurança incondicional para a 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.

Apêndices

A Entropia de Shannon

O conceito de entropia de Shannon é importantíssimo para a Teoria da Informação. Ele serve para medir a incerteza que temos acerca de um determinado sistema físico, ou, equivalentemente, a quantidade de informação que ganhamos ao medir esse sistema. Se temos uma variável aleatória X, a entropia de Shannon irá nos dizer a quantidade de informação que ganhamos ao conhecer o valor de X.

A entropia de Shannon é definida como uma função de uma distribuição de probabilidades, $p_1, p_2, \ldots, p_n$, da forma:

$$H(X) \equiv H(p_1, p_2, \ldots, p_n) \equiv -\sum_x p_x \log p_x \tag{11}$$

Neste caso, convenciona-se $0 \log 0 \equiv 0$. Note que $lim_{x \to 0}(x \log x) = 0$. A entropia de Shannon pode ser utilizada para mensurar a quantidade mínima de recursos necessária para codificar determinada informação (compressão de dados).

A.1 Justificativa Intuitiva para a Definição de Entropia

O seguinte exercício é proposto em [14] como forma de justificar o conceito de entropia. Nesta seção, apresentarei o problema, bem como sua solução.

Suponhamos que estejamos medindo a quantidade de informação ganha através de um evento E, o qual ocorre em um experimento probabilístico. Utilizaremos para isso uma função I(E). Afirmaremos o seguinte sobre a função:

- I(E) é função somente do evento E, então podemos escrever $I = I(p)$, onde p é a probabilidade do evento E;
- I é uma função suave de probabilidade, derivável em todo seu domínio;
- $I(pq) = I(p) + I(q)$ quando $p, q > 0$, ou seja, a informação ganha quando dois eventos independentes ocorrem com probabilidades individuais p e q é a soma da informação ganha por cada evento isoladamente.

Deseja-se mostrar que $I = k \log p$, para alguma constante k. Partindo da terceira condição do problema:

$$I(pq) = I(p) + I(q) \tag{12}$$

$$q = 1 \Rightarrow I(p) = I(p) + I(1) \Rightarrow I(1) = 0 \tag{13}$$

$$\frac{dI(pq)}{dp} = I'(p) \tag{14}$$

$$\frac{dI(pq)}{d(pq)} \cdot \frac{d(pq)}{dp} = I'(p) \tag{15}$$

$$I'(pq) \cdot q = I'(p) \tag{16}$$

$$I'(pq) \cdot q = I'(p) \tag{17}$$

$$p = 1 \Rightarrow I'(q) \cdot q = I'(1) \tag{18}$$

Como sabemos que $I(1) = 0$, podemos afirmar que $I'(1) = k$, para k constante.

$$I'(q) = \frac{k}{q} \tag{19}$$

$$I(q) = \int \frac{k}{q} dq \tag{20}$$

$$I(q) = k \log q \tag{21}$$

Assim, mostra-se que a função $I(p)$ surge naturalmente e satisfaz às três condições do problema. A função $I(p)$, no entanto, representa a quantidade de informação ganha por um evento de probabilidade p. Estaríamos interessados em conhecer a informação média, ou seja, a entropia. A média da variável $I(p)$ é:

$$H =< I >= \frac{\sum_x p_x (k \log p_x)}{\sum_x p_x} \tag{22}$$

$$H =< I >= k \sum_x p_x \log p_x \tag{23}$$

onde $k = -1$.

Em Ciência da Computação é importante estudarmos a entropia de uma variável binária. Esta entropia recebe o sugestivo nome de entropia binária, e é definida como:

$$H(p) = -p \log p - (1-p) \log (1-p) \tag{24}$$

Na equação acima, p e $1-p$ são as probabilidades de ocorrência de cada valor binário. Repare que o maior valor de H ocorre quando $p = 1/2$. De fato, a situação de maior incerteza sobre um sistema é quando todos os valores podem ocorrer com a mesma probabilidade. No caso da Cifra de Vernam, a entropia é máxima por que a chave é composta de zeros e uns aleatórios, o que significa que eles podem ocorrer com mesma probabilidade ($p = 1/2$). Assim, temos o maior grau de desconhecimento possível sobre a chave, e não podemos nem mesmo aplicar estatísticas para tentar adivinhar o valor de um determinado bit.

B Alguns *Flashes* de Mecânica Quântica

Neste apêndice irei mencionar 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: um sistema físico isolado tem associado um espaço de Hilbert (no caso da Computação Quântica, de dimensão finita). 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 $\langle i|$. Chamamos 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 temos a base $\{|0\rangle, |1\rangle\}$, nossos 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 medida. 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: 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 t1 e t2. 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,

$$\sigma_x(\alpha|0\rangle + \beta|1\rangle) = \sigma_x(\alpha|0\rangle) + \sigma_x(\beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle \tag{25}$$

Em [9] há uma boa revisão sobre portas lógicas quânticas e circuitos quânticos. Em [10, 14] encontram-se explicações sobre a *Equação de Schrödinger*, utilizada para descrever a evolução de um sistema quântico em tempo contínuo.

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

$$M = \sum_m mP_m \tag{26}$$

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

Além destes postulados, é importante conhecer o *no-cloning* theorem, para uma boa compreenção 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 irei mostrar apenas que não podemos clonar estados quânticos genéricos. Para uma análise completa do caso, recomenda-se a leitura do artigo da Nature. Suponhamos que desejamos 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

$$|\psi\rangle \otimes |s\rangle \tag{27}$$

onde $\otimes$ representa produto tensorial.

Não irei entrar em detalhes sobre como é calculado o produto tensorial, mas por enquanto basta sabermos que um registrador quântico é o produto tensorial entre dois ou mais qubits [9]. 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

[9] Há registradores quânticos que não podem ser escritos como produto tensorial de seus qubits. Dizemos

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 teremos o importante resultado:

$$\langle\psi|\phi\rangle = (\langle\psi|\phi\rangle)^2. \tag{28}$$

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 não nos interessa, então provamos que uma máquina de clonagem quântica só é capaz de clonar estados ortogonais. No nosso caso, o protocolo BB84 utiliza fótons polarizados em bases não ortogonais, então eles não podem ser clonados.

Referências

[1] A. Einstein, B. Poldosky, and N. Rosen, *Can quantum-mechanical description of physical reality be considered complete?*, Phys. Rev., **47** (1935) 777-780.

[2] A. Menezes, P. van Oorschot and S. Vanstone, *Handbook of Applied Cryptography.* CRC Press, Inc (1996). http://cacr.math.uwaterloo.ca/hac.

[3] A.K. Ekert, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett., **67** (1991) 661-663.

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

[5] C.H. Bennett, *Quantum cryptography using any two nonorthogonal states*, Phys. Rev. Lett., **6**8 (1992) 3121-3124.

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

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

[8] C.H. Bennet, 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. **7**0 (1993) 1895-1899.

[9] C. Lavor, L.R.U. Manssur and R. Portugal, *Grover's Algorithm: Quantum Database Search.* (2003) quant-ph/0301079.

[10] C.P. Willians and S.H. Clearwater, *Explorations in Quantum Computing*, The Electronic Library of Science, California (1997).

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

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

que estes qubits estão emaranhados, pois estão de tal forma correlacionados, que não podem ser descritos individualmente.

[13] J. Preskill, *Lecture Notes for Physics 229: Quantum Information and Computation.* California Institute of Technology. (1998)

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

[15] N. Gisin, G.Ribordy, W. Tittel and H.Zbinden, *Quantum Criptography*, Reviews of Modern Physics, **7**4, (2002) 145-195.

[16] S.J. Lomonaco Jr., *A quick glance at Quantum Criptography.* (1998) quant-ph/9811056.

[17] W.K. Wooters and W.H. Zurek, *A single quantum cannot be cloned*, Nature, **2**99, (1982) 802-803.