3.
Criptografia quântica

O problema de distribuição de chaves criptográficas em sistemas simétricos pode ser solucionado empregando-se a criptografia quântica. Esta se embasa em algumas características fundamentais da física quântica, as quais asseguram sua segurança. O princípio da incerteza de Heisenberg é aqui revertido em uma característica positiva, com conseqüências interessantes. Podem-se resumir as regras que levam à formulação dos protocolos de distribuição quântica de chaves como segue [6]:

- Não se pode determinar simultaneamente a posição e o momento de uma partícula com precisão arbitrariamente alta (princípio da incerteza de Heisenberg);
- Não se pode efetuar a medição de um estado quântico sem perturbar o sistema, a não ser que a base de medição seja compatível;
- Não se pode efetuar a medição de um estado quântico em mais de uma base simultaneamente;
- Não se pode replicar um estado quântico desconhecido (teorema da não-clonagem).

A partir do princípio da incerteza, a impossibilidade de se medir um estado quântico desconhecido sem alterá-lo resulta no teorema da não-clonagem, ou seja, não se pode copiar com total precisão o que não se conhece. Como uma medição pode destruir um estado quântico, não é possível medi-lo mais de uma vez. A questão da segurança fica então evidente, pois tentativas de interceptação dos portadores de informação tendem a alterá-los. O conseqüente aumento na taxa de erro revela, por fim, o interceptador, bastando que se descarte a ainda não formada chave para que não haja ganho de informação por parte de terceiros.

3.1. Qubits

No caso clássico, a unidade fundamental de informação é o assim chamado dígito binário, ou bit (contração de *binary digit*), um sistema de dois níveis lógicos distintos representado fisicamente por um sistema com também dois níveis físicos distintos, como dois valores de tensão elétrica. Analogamente, em comunicações quânticas a entidade fundamental é chamada de bit quântico, ou qubit (*quantum bit*).

Entretanto, os qubits, apesar de também representarem dois estados lógicos distintos, 0 e 1, através dos estados quânticos $|0\rangle$ e $|1\rangle$, respectivamente, diferem do caso clássico na possibilidade de apresentarem a superposição coerente de ambos os estados, podendo existir em uma das infinitas possibilidades intermediárias entre os vetores do espaço de Hilbert que o contém.

Isso significa que uma medida realizada sobre o qubit tem probabilidade de resultar tanto em um estado quanto no outro. Dependendo do recobrimento existente ente a base de preparação do qubit e a base de medição, o resultado retornado assumirá os valores $|0\rangle$ ou $|1\rangle$ com dada probabilidade.

A probabilidade de ocorrência destes resultados é dada pelos pesos dos estados superpostos, ou seja, o estado $|\varphi\rangle$ da eq. 3.1 possui probabilidade $|\alpha|^2$ de representar o estado $|0\rangle$ e assumir o valor lógico 0, e probabilidade $|\beta|^2$ de representar o estado $|1\rangle$ e assumir o valor lógico 1, sendo que a soma das probabilidades deve ser unitária, podendo α e β ser números complexos .

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{3.1}$$

Assim, a mencionada superposição coerente significa que o qubit é codificado em uma base composta por dois estados ortogonais, de forma que é sempre possível distinguirem-se tais estados com uma medição adequada, mediante rotação do sistema no espaço de Hilbert (escolha de base). Se a base de medição tiver um máximo recobrimento com a base de codificação, o resultado será qualquer uma das duas possibilidades, com 50% cada, como no exemplo dado pela eq. 3.2.

$$|\mathrm{Y}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \tag{3.2}$$

Como mencionado, pode-se aplicar um operador unitário de rotação, a transformação de Hadamard (H), dada pelas eq. 3.3. Esta girará o sistema em 45° no espaço de Hilbert, resultando em um estado bem definido – neste caso, o estado $H|Y\rangle = |0\rangle$.

$$H|0\rangle \rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$
$$H|1\rangle \rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \tag{3.3}$$

Cabe comentar a respeito de outra transformação unitária útil, representando uma mudança de fase ϕ no estado quântico, dada pela eq. (3.4).

$$\Phi|0\rangle = e^{j\phi}|0\rangle$$
$$\Phi|1\rangle = |1\rangle \tag{3.4}$$

Fisicamente, os qubits podem ser representados por graus de liberdade de átomos ou partículas, codificados em dois níveis, como a orientação do spin de um elétron ou a polarização de um fóton. Enquanto elétrons, íons e átomos têm sido alvo de pesquisas para desenvolvimento de memórias quânticas, computador quântico e outras tecnologias locais (no sentido de estas partículas não serem enviadas à distância), os fótons destacam-se como portadores de informação para telecomunicações quânticas.

3.2. Teorema da não-clonagem

É possível demonstrar a impossibilidade de se efetuar uma cópia perfeita de um estado quântico desconhecido. Seguindo [6], uma copiadora quântica ideal deveria produzir em sua saída o próprio estado de entrada e uma cópia, como na eq. 3.5, sendo $|\psi\rangle$ o estado original do qubit a ser copiado, $|b\rangle$ representa a cópia em branco que deverá assumir o estado desejado e $|0\rangle$ representa o estado inicial da copiadora quântica, pertencente a um espaço de Hilbert arbitrário.

$$|\psi\rangle \otimes |b\rangle \otimes |0\rangle \rightarrow |\psi\rangle \otimes |\psi\rangle \otimes |f_{\psi}\rangle \tag{3.5}$$

Assim, para dois estados de uma determinada base |V⟩ e |H⟩, representando, respectivamente, os estados de polarização vertical e horizontal de um fóton, ortogonais ente si, obtém-se as eq. 3.6.

$$\begin{aligned} |V,b,0\rangle &\rightarrow |V,V,f_V\rangle \\ |H,b,0\rangle &\rightarrow |H,H,f_H\rangle \end{aligned} \tag{3.6}$$

Porém, ao se tentar copiar estados superpostos, ou seja, numa base não ortogonal à medição, como, por exemplo, uma polarização linear com ângulo de +45°, representada por |+45°⟩, o resultado, dado pela eq. 3.7, será divergente do apresentado nas eq. 3.6.

$$\begin{aligned} |+45,b,0\rangle &= \frac{1}{\sqrt{2}}\left(|V\rangle + |H\rangle\right) \otimes |b,0\rangle \\ &= \frac{1}{\sqrt{2}}\left(|V,V,f_V\rangle + |H,H,f_H\rangle\right) \neq |+45,+45,f_{45}\rangle \end{aligned} \tag{3.7}$$

Portanto, a menos que se conheça a base na qual foi preparado o estado quântico, não se pode copiá-lo com 100% de probabilidade de sucesso.

3.3. Emaranhamento e o paradoxo EPR

Em certos casos, pode-se dizer que duas partículas estão emaranhadas se apresentarem correlação tal que, ao se efetuar a medição de uma delas, o estado quântico da outra pode ser predito. Um par emaranhado pode ser representado como uma superposição de estados produto, compondo um estado não-separáveis de duas (ou mais) partículas, como na eq. 3.8, onde os sub-índices 1 e 2 as representam [9].

$$|\psi_{12}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1 |1\rangle_2 + e^{j\chi}|1\rangle_1 |0\rangle_2\right) \tag{3.8}$$

A fase χ depende das propriedades internas da fonte. Neste caso, sendo zero, os qubits assumirão valores opostos. Isso significa que, independente da distância percorrida pelos qubits em relação à fonte, esse comportamento será válido. Ao se medir a partícula 1 da eq. 3.8 em certa base, esta terá 50% de probabilidade de assumir o estado $|0\rangle$ e 50% de probabilidade de assumir o estado $|1\rangle$, já que se apresenta em uma superposição coerente. De posse deste resultado, é certo que a outra partícula assumirá o estado $|1\rangle$ ou o estado $|0\rangle$, respectivamente em cada caso, para medidas na mesma base, seja qual for.

Podem-se produzir estados quânticos emaranhados a partir de uma fonte que intrinsecamente produza estados indistinguíveis, como no decaimento de uma partícula com spin 0 para duas com *spins* ½ e -½, conservando-se o momento angular [9]. Outra possibilidade se refere a uma fonte que emita os componentes da superposição desejada, mas que podem, em princípio, ser distinguidos como, por exemplo, no caso de uma conversão paramétrica descendente tipo II (*type-II parametric downconversion*) [6]. Devido à birrefringência do cristal não-linear utilizado (eixos com índices de refração diferentes), estados com polarização vertical e horizontal possuem velocidades de propagação diferentes. Neste caso, os fótons gerados após o bombardeamento óptico do cristal, deverão ser atrasados relativamente entre si, apagando-se a ordem temporal e gerando indistinguibilidade.

O paradoxo EPR (Einstein-Podolsky-Rosen) pode ser explicado considerando-se uma fonte de pares de fótons emaranhados, cujos estados dos qubits obedecem à eq. 3.9, sendo $|H\rangle$ e $|V\rangle$ os estados de polarização ortogonais componentes de uma base. Os fótons propagam-se a partir da fonte em uma direção, cada um em um sentido, podendo ser medidos nos extremos.

$$\left|\phi^{+}\right\rangle_{12} = \frac{1}{\sqrt{2}}\left(\left|H\right\rangle_1\left|V\right\rangle_2 + \left|V\right\rangle_1\left|H\right\rangle_2\right) \tag{3.9}$$

A primeira parte da discussão EPR considera que, se os dois fótons forem medidos, independentemente da distância a partir da fonte, com a mesma base, obter-se-ão resultados anti-correlacionados, ou seja, o estado de uma partícula revelará com certeza o estado da outra, independentemente desta segunda medição. A segunda parte se refere ao conceito de localidade, isto é, a medição de um fóton deve depender de seu próprio estado e da base escolhida para esta

medição, e não da medição efetuada no outro fóton, constituindo, assim, um paradoxo.

Estando a fonte localizada entre dois pontos, em cada extremidade encontra-se um divisor de feixes ópticos por polarização (PBS – *Polarization beam-splitter*), com um detector de fótons únicos em cada um de seus dois braços. Estes podem, dependendo do estado de polarização do fóton incidente no PBS, acusar os bits 0 ou 1 em cada um. A eq. 3.10 representa a predição pela teoria quântica do número de vezes em que o ponto A obtém a medição de um bit 1 em seu aparato com orientação α e o ponto B obtém o bit 1 com orientação β, sendo N_0 o número de pares emaranhados emitidos pela fonte.

$$N(1_\alpha, 1_\beta) = \frac{N_0}{2}\cos^2(\alpha - \beta) \tag{3.10}$$

De acordo com uma teoria realista local, a desigualdade de Bell, dada pela eq. 3.11, deve ser satisfeita no caso em que as bases são escolhidas em ângulos arbitrários α, β e γ em relação aos PBS, de acordo com uma teoria realista local.

$$N(1_\alpha, 1_\beta) \leq N(1_\alpha, 1_\gamma) + N(1_\beta, 1_\gamma) \tag{3.11}$$

No caso específico em que $(\alpha-\beta) = (\beta-\gamma) = 30°$, a eq. 3.11 viola a eq. 3.10. Com isso, conclui-se que as previsões da física quântica e de teorias de realidade local diferem. As medidas recentes apontam para o prevalecimento da física quântica, refutando o realismo.

3.4. Distribuição quântica de chaves

Um sistema de distribuição quântica de chaves constitui-se basicamente de um transmissor, geralmente denominado na literatura como Alice, um receptor, chamado de Bob, um canal quântico para a transmissão da chave quântica, um canal público para a reconciliação da chave, que pode ser monitorado, mas não modificado (canal autenticado), e a possível presença de um espião, referido como Eva, que deve ser considerado como capaz de qualquer tipo de interceptação.

A chave é codificada segundo um protocolo específico utilizando-se um conjunto de estados quânticos agrupados em bases não-ortogonais, que codificam fótons simples ou emaranhados, originando os qubits.

Na recepção, os qubits são medidos e, de acordo com a base escolhida, poderão revelar claramente o bit transmitido ou gerar um resultado fruto de ambigüidade.

A escolha dos elementos do sistema de distribuição quântica de chaves deve ser feita considerando simultaneamente uma série de características, tanto restritivas quanto práticas.

Iniciando-se pela escolha do protocolo de comunicação, deve-se analisar o meio de transmissão a ser utilizado. Os canais quânticos disponíveis podem ser o espaço livre ou a fibra óptica. Pode ser vantajoso utilizar uma malha óptica já existente ou pode haver obstáculos no caminho que justifiquem um enlace não-cabeado em linha de visada. Concomitantemente à escolha do canal, deve-se optar pelo tipo de codificação, ou seja, qual característica da partícula será codificada.

3.4.1. Protocolo BB84

Inicialmente proposto por Bennett e Brassard em 1984, o protocolo BB84 utiliza quatro estados, que formam duas bases não-ortogonais em um espaço de Hilbert, para codificar a chave [3]. Essas bases devem ser maximamente conjugadas, ou seja, qualquer par de vetores, um de cada base, deve apresentar a mesma superposição [6]. A figura 1 apresenta uma representação visual dos estados, agrupados nas bases azul e vermelha.

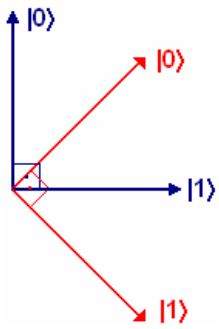

Figura 1: Bases não-ortogonais (azul e vermelha) compostas por dois estados ortogonais em um espaço de Hilbert, utilizadas no protocolo BB84.

Na transmissão, Alice escolhe aleatoriamente os bits que serão enviados e os codifica em seus fótons utilizando uma das duas bases, também escolhidas aleatoriamente para cada qubit.

Após a transmissão pelo canal quântico, Bob deve escolher, outra vez de maneira randômica, a base que utilizará para a medição de cada partícula recebida, o que encaminhará o fóton a detectores diferentes nos casos de medição dos estados $|0\rangle$ ou $|1\rangle$.

Caso a base escolhida esteja de acordo com a qual foi preparado o qubit, a projeção do estado quântico retornará o valor correto e a acusação de um dos detectores revelará o bit codificado.

Por outro lado, se Bob escolher a base errada, não-ortogonal àquela na qual foi preparado o qubit, a projeção do estado quântico nesta base resultará na obtenção de um bit 0 ou bit 1 aleatoriamente, com probabilidade de 50% para cada valor. A tabela 1 mostra o resumo das combinações de bases possíveis para cada bit codificado segundo o protocolo BB84.

Alice		**Bob**		
Base	**Bit**	**Base**	**Determinação**	**Bit**
α	0	α	Sim	0
		β	Não	0 ou 1
	1	α	Sim	1
		β	Não	0 ou 1
β	0	α	Não	0 ou 1
		β	Sim	0
	1	α	Não	0 ou 1
		β	Sim	1

Tabela 1: Possibilidades de combinações de bases para qubits codificados segundo o protocolo BB84.

Após a transmissão, em média 25% dos bits de Bob divergem dos de Alice, devido à sua escolha inadequada de base e ao resultado aleatório desses eventos. Esta chave bruta, chamada *raw key*, não pode ser utilizada, pois não seria possível a correção de erros. Logo, eles devem eliminar os resultados descorrelacionados. Para isso, devem se comunicar pelo canal público, por onde

Bob relata os instantes em que recebeu fóton, bem como as bases escolhidas para cada medição. Após a confirmação de Alice da semelhança ou não da escolha das bases, porém sem revelação dos bits, ambos descartam os qubits cujas bases divergiram. Desta forma, elimina-se, em média, metade dos qubits recebidos por Bob, obtendo-se a chave refinada, chamada *sifted key*.

A chave final será obtida após os demais passos do protocolo, ou seja, estimativa da taxa de erro da transmissão, inferência do máximo de informação que pode ter sido roubada por uma possível Eva, correção de erros e amplificação de privacidade, conforme seções seguintes.

3.4.2. Protocolo B92

Segundo o protocolo B92 (criado por Bennett em 1992) são necessários apenas dois estados quânticos não ortogonais para que se possa proceder a distribuição quântica de chaves, e não quatro como no protocolo anterior [4].

Neste protocolo, Bob deverá proceder com uma medição POVM (*positive operator valued measurement*), ou seja, para cada base escolhida para medição, ele pode obter o resultado que determina o bit recebido (0 ou 1) ou pode não obter resultado (-), ou seja, terá um sistema ternário com os bits 0 ou 1, caso a base esteja correta, ou a ausência de resultado, caso a base não esteja de acordo com a escolhida por Alice [10], como na tabela 2. Aqui, cada qubit enviado por Alice recebe a codificação em uma base que corresponde diretamente ao bit enviado.

Alice		**Bob**		
Base	**Bit**	**Base**	**Resultado**	**Bit**
α	0	α	Sim	0
		β	Não	-
β	1	α	Não	-
		β	Sim	1

Tabela 2: Possibilidades de combinações de bases para qubits codificados segundo o protocolo B92.

Este procedimento pode ser melhor explicado através da codificação de qubits por fase, aqui vista em linhas gerais (detalhes serão apresentados mais à frente). Alice pode codificar seus fótons escolhendo aleatoriamente dentre duas opções de fase para a modulação, como 0 e π, representando os bits 0 e 1, respectivamente. Na recepção, Bob também escolherá aleatoriamente um destes dois valores, 0 ou π, para modular cada qubit. A interferência poderá ser construtiva ou destrutiva, de acordo com a diferença entre as fases escolhidas pelas duas partes. Caso seja zero, a interferência será construtiva, havendo contagem no detector único de Bob que, sabendo qual fase escolheu, saberá qual bit sua detecção está acusando. Caso a diferença de fases seja igual a π, a interferência será destrutiva. Logo, não haverá contagem no detector de Bob (a menos de uma contagem de escuro), e este qubit deverá ser descartado durante a reconciliação. Detalhes da codificação por freqüência serão vistos adiante.

A chave final será obtida, assim como no protocolo BB84, após a estimativa da taxa de erro da transmissão, inferência do máximo de informação roubada, correção de erros e amplificação de privacidade.

Este protocolo apresenta a vantagem de necessitar de apenas um detector, que acusará ou não a presença de um fóton, em contrapartida ao protocolo BB84, em que dois detectores acusam bits diferentes.

Entretanto, apesar de dois estados quânticos não-ortogonais superpostos não poderem ser distinguidos de forma não ambígua sem perturbação do sistema, pode-se fazê-lo à custa de alguma perda [6]. Logo, Alice e Bob devem monitorar constantemente a atenuação do canal quântico. Ainda assim, Eva pode ser capaz de substituir o canal por um de menor perda. A presença de um pulso de referência em cada qubit pode evitar este problema do protocolo, como proposto pelo próprio Bennett [4].

3.4.3. Protocolo Ekert 1991

A QKD também pode ser efetuada utilizando estados emaranhados [9]. Deve haver uma fonte de pares de fótons emaranhados emitindo estados superpostos, assumidos como maximamente emaranhados, através de um canal quântico até Alice e Bob, recebendo, cada um, uma partícula na direção do eixo $\hat{z}$, como na eq. 3.12, onde $|V\rangle$ e $|H\rangle$ representam estados ortogonais de polarização.

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|V\rangle_1|H\rangle_2 - |H\rangle_1|V\rangle_2\right) \tag{3.12}$$

Ao receberem seus fótons, Alice e Bob podem, cada um deles independentemente, girar suas bases de medição aleatoriamente a partir do eixo x no plano xy, escolhendo, cada um, dentre os três ângulos dados na eq. 3.13, onde *a* e *b* referem-se a Alice e a Bob [11]. Assim, o protocolo Ekert, por ele criado em 1991, utiliza três bases, ao invés das duas dos protocolos BB84 e B92.

$$\begin{cases} \phi_1^a = 0 \\ \phi_2^a = \dfrac{\pi}{4} \\ \phi_3^a = \dfrac{\pi}{2} \end{cases} \qquad \begin{cases} \phi_1^b = \dfrac{\pi}{4} \\ \phi_2^b = \dfrac{\pi}{2} \\ \phi_3^b = \dfrac{3\pi}{4} \end{cases} \tag{3.13}$$

Cada medição pode originar como resultado +1, ou seja, o fóton foi medido no primeiro estado de polarização da base escolhida, ou -1, a medição foi feita no outro estado de polarização da base escolhida, podendo revelar um bit de informação.

O coeficiente de correlação das medições feitas por Alice na base girada de ϕ_n^a e por Bob na base girada de ϕ_m^b é dado pela eq. 3.14, onde $P_{\pm\pm}(\phi_n^a, \phi_m^b)$ representa a probabilidade de ocorrer o resultado ±1 com a base ϕ_n^a e ±1 com a base ϕ_m^b.

$$E\left(\phi_n^a, \phi_m^b\right) = P_{++}\left(\phi_n^a, \phi_m^b\right) + P_{--}\left(\phi_n^a, \phi_m^b\right) - P_{+-}\left(\phi_n^a, \phi_m^b\right) - P_{-+}\left(\phi_n^a, \phi_m^b\right) \tag{3.14}$$

De acordo com as leis quânticas, a eq. 3.14 resulta na eq. 3.15 [9].

$$E\left(\phi_n^a, \phi_m^b\right) = -\cos\left(\phi_n^a - \phi_m^b\right) \tag{3.15}$$

Assim, se as rotações forem idênticas, haverá total anti-correlação (resultado igual a -1) entre os resultados obtidos por Alice e Bob, como nos casos (ϕ_2^a, ϕ_1^b) e (ϕ_3^a, ϕ_2^b).

A composição dos coeficientes de correlação das medições em que Alice e Bob utilizaram rotações com ângulo diferentes (bases incompatíveis) resultará na eq. 3.16. Usando realismo local, Bell provou que o valor de S deve ser maior ou igual a -2. Entretanto, segundo a física quântica, S pode chegar até $-2\sqrt{2}$ [11].

$$S = E\left(\phi_1^a, \phi_1^b\right) - E\left(\phi_1^a, \phi_3^b\right) + E\left(\phi_3^a, \phi_1^b\right) + E\left(\phi_3^a, \phi_3^b\right) \tag{3.16}$$

Após a transmissão, as partes comunicantes anunciam, através do canal público, como nos demais protocolos, as bases de medição utilizadas para cada qubit e dividem as medições em dois grupos, um com orientações diferentes e um com orientações iguais. Após descartar os instantes em que um ou ambos não receberam fótons, eles revelam publicamente os resultados obtidos apenas no primeiro grupo. Assim pode-se estabelecer o valor de S que, caso as partículas não tenham sido perturbadas, deve resultar em $-2\sqrt{2}$. Esse resultado assegura a anti-correlação para o segundo grupo de medidas, que será convertido na chave.

Eva não pode roubar informação interceptando uma das partículas do par emaranhado, pois não há informação nas partículas até que sejam efetuadas as medições. Caso ela tente substituir uma partícula, a falta de conhecimento sobre as bases que serão utilizadas por Alice e Bob fará com que o valor da anti-correlação caia, identificando sua presença.

3.4.4. Outros protocolos

Além dos seminais BB84, Ekert91 e B92, existem diversos outros protocolos, que podem ser divididos, segundo [42], em três grupos: os de variáveis discretas – no qual aqueles se enquadram; os de variáveis contínuas; e os com referência distribuída de fase.

Nos protocolos de variáveis discretas, Alice e Bob obtém resultados discretos, sendo capazes de gerar, na ausência de erros na transmissão, uma chave diretamente. Conforme mencionado, pode-se utilizar qualquer grau de liberdade de um fóton, como polarização, fase ou fase relativa entre bandas laterais e portadora de um sinal óptico modulado.

Além dos já citados, destacam-se, nesta categoria, os protocolos SARG04 (Scarani-Acín-Ribordy-Gisin 2004) [53] e o de seis estados, proposto por Bruß em 1998 [45]. Este último apresenta grande simetria por utilizar três bases ortogonais (por exemplo, polarização H e V, +45º e -45º e σ+ e σ-), o que torna o sistema robusto em relação a ruído. Entretanto, ao requerer a utilização de elementos ópticos adicionais com perdas, sua performance geral pode ser inferior ao BB84. Já o SARG04 utiliza os mesmos estados do BB84, porém os bits são codificados nas bases não-ortogonais, e não nos estados propriamente ditos. Na reconciliação, Bob revela publicamente à Alice os resultados obtidos, e não as bases, descartando-se os casos em que se obtêm resultados idênticos. A *sifted key* é então construída de acordo com as bases utilizadas para os qubits cujos resultados da medição divergiram do estado de preparação. A vantagem deste sistema se refere à sua maior segurança em relação a ataques por divisão do número de fótons, aos quais os sistemas que valem-se de fontes coerentes fracas estão fortemente sujeitados.

Os protocolos de variáveis contínuas não serão abordados aqui por estarem além do escopo desta dissertação, devendo o leitor referir-se a [42] para detalhes.

Os protocolos com referência distribuída de fase foram criados por grupos de QKD experimental, com o objetivo de melhor explorar as propriedades do laser fortemente atenuado como fonte de fótons únicos. A chave também é gerada de forma discreta (detecção de eventos) e o canal quântico é monitorado utilizando-se as propriedades de estados coerentes, ou seja, observando-se a coerência de fase entre pulsos subseqüentes.

Como exemplo de protocolo desta categoria, tem-se o DPS (*Differential phase-shift*), em que Alice produz uma seqüência de pulsos coerentes cuja fase é ajustada aleatoriamente como 0 ou π. Com um interferômetro desbalanceado, Bob é capaz de discriminar as diferença de fase entre dois pulsos consecutivos de forma não-ambígua. Há também o protocolo COW (*Coherent one-way*), criado em 2004, no qual cada bit é codificado em uma seqüência de um pulso cheio e um pulso vazio, e a decodificação é feita com a medição do tempo de chegada entre pulsos. Para estes esquemas ainda não foi estabelecido um limiar de segurança incondicional [42].

3.4.5.
Estimativa da taxa de erro quântica

Após a transmissão dos qubits e a reconciliação de bases, para que Alice e Bob compartilhem uma seqüência de bits realmente idêntica, devem estimar a taxa de erro e corrigi-los. Cabe ressaltar que a taxa de erro de bits quânticos (QBER – *Qubit error rate*) se refere aos bits da *sifted key*, a chave provisória obtida após o anúncio público das bases. Tais erros devem-se a fatores como variações de polarização pela fibra, desestabilização de interferômetros ou filtragens imperfeitas, de acordo com o sistema em questão, e ainda à contagem de escuro dos detectores.

Por outro lado, a taxa de erro de bits clássica, a BER (*bit error rate*), apresenta o mesmo significado das comunicações tradicionais e é aplicada à chave final, após todas as etapas do protocolo, quando Alice e Bob devem possuir chaves idealmente idênticas.

Por definição, a entropia de Shannon, dada pela eq. 3.17, representa a quantidade de informação de cada palavra da fonte, que emite uma seqüência aleatória de *n* bits dada por $X=\{x_0, x_1, x_2, ..., x_{n-1}\}$, de forma que a probabilidade de ocorrer um bit 0 é dada por p_0 e a probabilidade de ocorrência de um bit 1 é dada por p_1 [12].

$$H(X) = -p_0 \log_2^{p_0} - p_1 \log_2^{p_1} \tag{3.17}$$

No caso de uma fonte aleatória equiprovável, tem-se $p_0=p_1=0,5$, resultando em uma entropia unitária, ou seja, cada palavra da fonte carrega um bit de informação.

A informação mútua entre duas variáveis aleatórias, dada em função da entropia, pode ser escrita para as *sifted-keys* de Alice e Bob em função da QBER, como na eq. 3.18. Para a estimativa da QBER, eles escolhem aleatoriamente um conjunto de bits e os comparam abertamente através do canal público [13].

$$I(A;B) = H(A) - H(A \mid B) = 1 + QBER \log_2^{QBER} + (1 - QBER) \log_2^{1-QBER} \tag{3.18}$$

Para inferir a quantidade de informação extraída por Eva, pode-se supor que toda a QBER se deve a ela. A estimativa da QBER tolerável pode ser obtida,

assumindo ataques individuais por parte de Eva, a partir dos teoremas de Csiszár e Körner (1978) e de Hall (1995), como nas eq. 3.19. O primeiro diz que a informação mútua de Alice e Bob deve ser maior que a informação mútua de Alice e Eva. O segundo pode ser considerado como uma formulação alternativa do princípio da incerteza, de forma que a soma dessas informações mútuas deve ser no máximo unitária, ou seja, a informação que Eva adquire não é obtida por Bob [13].

$$\begin{cases} I(A;B) > I(A;E) \\ I(A;B) + I(A;E) \leq 1 \end{cases} \tag{3.19}$$

Combinando as eq. 3.19 e 3.18, obtém-se o limite superior da QBER como 15% [6,13]. Assumindo que Eva pode proceder com quaisquer tipos de ataque (coerente ou incoerente) e para sistemas baseados em partículas simples ou emaranhadas, este valor reduz-se a 11% [6,13].

Porém, este limite inferior pode ser aumentado, caso Alice efetue um pré-processamento em seus bits. Ao trocar o valor de alguns bits enviados a Bob, erros são introduzidos na chave, induzindo ruído. Porém, este ruído se diferencia do induzido pelo canal. Apesar de reduzir sua informação mútua em relação a Bob, este valor reduz drasticamente a informação mútua em relação a Eva [41]. O limite superior da QBER passa a ser, no caso do protocolo BB84 por exemplo, igual a 12,4%.

Caso a estimativa da taxa de erro seja maior que o limite estabelecido, o protocolo deve ser finalizado, pois pode ter havido vazamento excessivo de informação para Eva, não redutível com a amplificação de privacidade. Caso seja aceitável, os bits revelados são descartados e é iniciada a fase de correção de erro.

3.4.6. Correção de erro

O sucesso da utilização da chave criptográfica requer que Alice e Bob tenham cópias idênticas. A correção de erro, próxima etapa de reconciliação, utiliza o canal público, e também deve ser o mais sigilosa possível.

Segundo o teorema da codificação de Shannon, o número mínimo de bits (r) que Alice e Bob devem compartilhar publicamente para corrigir os erros da

chave (de comprimento n), sendo ε a probabilidade de erro de transmissão de um bit, será dado pela eq. 3.20 [9].

$$r = n\left[-\varepsilon \log_2 \varepsilon - (1-\varepsilon)\log_2 (1-\varepsilon)\right] \tag{3.20}$$

É possível aproximar-se deste limite utilizando o esquema de correção de erro proposto por Brassard e Salvail [6]. Nele, Alice e Bob agrupam seus bits em blocos de um determinado tamanho, otimizado em função da taxa de erro de bits estimada, e trocam informações a respeito da paridade de cada bloco pelo canal público. Se suas paridades estiverem de acordo, seguem para o próximo bloco, senão, eles sabem que há um número ímpar de erros no bloco e o dividem em dois sub-blocos menores. É feita a comparação da paridade para os sub-blocos e, se o valor divergir, seguem dividindo e comparando os sub-blocos com paridade ímpar recursivamente.

Quando todos os blocos possuírem paridade par, eles trocam a posição de alguns bits e efetuam a comparação das paridades de blocos maiores (também otimizados). Um determinado número de passos segue até que se atinja o nível de correção adequado.

3.4.7. Amplificação de privacidade

Uma vez detentores de chaves iguais, Alice e Bob podem, se necessário, reduzir a informação possivelmente obtida por Eva a um valor arbitrariamente baixo, à custa do sacrifício de bits, através da assim chamada amplificação de privacidade.

Alice escolhe aleatoriamente um par de bits e informa a Bob suas posições. Ambos efetuam a soma módulo 2 (ou OU-exclusivo) destes bits, substituindo-os pelo resultado. Caso Eva conheça apenas um dos bits, perderá esta informação, pois não será capaz de determinar o resultado da operação. Além disso, se Eva tiver informação parcial dos bits, ou seja, se houver determinada probabilidade de conhecimento dos bits, ainda assim esta informação reduzir-se-á.

3.4.8. Espionagem

Os ataques de um espião, comumente referidos como *eavesdropping*, podem ser agrupados em três classes distintas, segundo a forma como os qubits são acessados e medidos [6]: os ataques incoerentes, os ataques coerentes coletivos e os ataques coerentes conjuntos.

Nos ataques incoerentes ou individuais, Eva acopla sondas independentes a cada qubit e os mede individualmente após a reconciliação de bases entre Alice e Bob. Este tipo de ataque pode ser tratado de forma clássica, assumindo que Alice, Bob e Eva possuem uma distribuição de probabilidade conjunta, com restrições impostas pelas leis da física quântica [6].

O tipo mais simples de ataque individual, conhecido como interceptação-reenvio, consiste em Eva medir os fótons transmitidos por Alice e reenviar novas partículas para Bob de acordo com seus resultados. Entretanto, o aumento da QBER poderia revelá-la no momento da reconciliação. Neste caso Alice e Bob podem tomar uma decisão crítica e interromper o protocolo, caso a QBER exceda 15% (limite de Csiszár-Körner), ou prosseguir e reduzir a informação de Eva com a amplificação de privacidade até um valor aceitável.

Caso os pulsos contenham mais de um fóton, o espião pode medir um deles enquanto o outro segue para Bob. Neste caso, chamado divisão do número de fótons (PNS – *Photon number splitting*), o ganho de informação de Eva pode ser alto, dependendo da estratégia por ela adotada e da tecnologia que tenha disponível. Caso opte por não bloquear os pulsos que contenham apenas um fóton, deixando-os seguir intactos, não haverá aumento da taxa de erro quântica e as partes comunicantes não serão capazes de perceber a espionagem. Entretanto, o espião pode escolher interceptar estes pulsos, o que resultaria em um aumento da QBER. A redução no número de pulsos com fótons que Bob recebe poderia ser mascarada por Eva caso ela fosse capaz de substituir o canal quântico por um canal com perdas reduzidas.

Atualmente, o espião encontra-se tecnologicamente limitado, não sendo ainda possível proceder a medição do número de fótons de um pulso sem alterar seus estados quânticos (*quantum nondemolition photon-number measurement*), além da dificuldade de se reduzir as perdas do canal quântico. Para isso, seria necessário superar os limitantes físicos da atenuação das fibras ópticas, já no limite de transparência nos comprimentos de onda de telecomunicações (0,2dB/km em 1550nm), ou encurtar o enlace, algo provavelmente inviável.

Outras opções, também de complexidade impeditiva, seriam a conversão de comprimento de onda dos fótons sem alterar seus estados ou a teleportação quântica[1] com alta fidelidade [6]. Por fim, até que sejam plenamente desenvolvidas as memórias quânticas, Eva teria de medir logo seus qubits, antes do anúncio de bases na reconciliação, momento ideal para extrair o máximo de informação.

Nos ataques coerentes coletivos, Eva acopla sondas independentes a cada qubit, como no caso anterior, medindo-os, entretanto, coletivamente ao fim de todo o protocolo.

Já nos ataques coerentes conjuntos, Eva processa várias sondas de forma coerente após a última etapa do protocolo, a amplificação de privacidade.

Nestas duas últimas formas de ataque, o espião possui tecnologia superior, incluindo talvez um computador quântico. A QBER limite, que indica que Alice e Bob possuem quantidade de informação mútua superior à de Eva suficiente para que possam assegurar a confidenciabilidade da chave após o processo de amplificação de privacidade, pode cair para 11%. Entretanto, o limite de 15% continua sendo válido se for assumido que Eva não pode medir coerentemente todos os qubits que comporão a chave.

Para se provar a total segurança de um sistema pode-se considerar apenas os ataques coletivos, pois são equivalentes aos ataques coerentes, caso seja feito um pré-processamento por parte de Alice e se o sistema de comunicação for assumido como de apenas uma via (*one-way*). Neste caso, o limite de segurança passa a ser de 12,4% na taxa de erro de qubits.

[1] A teleportação quântica, proposta em 1993 por Bennett, Brassard, Crépeau, Jozsa, Peres e Wootters, permite a transmissão de um estado quântico entre dois pontos sem o envio direto da partícula. Atuando em um par emaranhado, uma das partes comunicantes é capaz de transmitir, através de um canal clássico, informações suficientes para que a outra parte possa reconstruí-lo, destruindo-se o estado original [9].