Revista Brasileira de Ensino de Física, v. 27, n. 4, p. 517 - 526, (2005)
www.sbfisica.org.br

Introdução à criptografia quântica

(Introduction to quantum cryptography)

Gustavo Rigolin[1] e Andrés Anibal Rieznik

Instituto de Física Gleb Wataghin, Universidade Estadual de Campinas, Campinas, SP, Brasil
Recebido em 16/6/2005; Aceito em 6/10/2005

Apresentamos de maneira detalhada os quatro protocolos de distribuição de chaves que fundaram a importante área da criptografia quântica, numa linguagem acessível a alunos de graduação em Física. Começamos pelo protocolo BB84, o qual se utiliza de estados de polarização de fótons para transmitir chaves criptográficas. Em seguida, apresentamos o protocolo E91, que faz uso de singletos para gerar uma seqüência de números aleatórios. Finalizamos este artigo apresentando o protocolo BBM92 e o B92, os quais podem ser vistos como simplificações dos dois primeiros protocolos.
Palavras-chave: criptografia quântica, teoria quântica da informação, emaranhamento.

We show in details the four quantum key distribution protocols which initiated the important field of quantum cryptography, using an accessible language for undergraduate students. We begin presenting the BB84 protocol, which uses polarization states of photons in order to transmit cryptographic keys. Thereupon we show the E91 protocol, whose security is based on the use of singlet states to generate a random sequence of bits. We end the paper with the BBM92 and the B92 protocol. These last two protocols can be seen as simplified versions of the first two.
Keywords: quantum cryptography, quantum information theory, entanglement.

1. Introdução

Desde os primórdios da civilização o homem sempre se deparou com o problema de transmitir secretamente informações importantes. A ciência que estuda essa arte de se comunicar confidencialmente, tendo a certeza de que somente as partes interessadas terão acesso à informação, recebe o nome de criptografia.

Muitos dos modernos protocolos de criptografia anunciam publicamente o algoritmo utilizado para encriptar e decriptar a mensagem. Ao anunciar publicamente este procedimento, permitimos a todos, inclusive quem desejamos que não tenha acesso à mensagem, conhecer o modo de deixá-la secreta. A segurança desses protocolos se baseia apenas em uma longa seqüência de números aleatórios que o emissor (Alice) e o receptor (Bob) da mensagem devem compartilhar em segredo. Ninguém mais pode conhecer esses números. Ou seja, o sucesso desses protocolos depende exclusivamente da capacidade de os envolvidos na comunicação serem capazes de compartilhar essa seqüência de números aleatórios, também conhecida como chave criptográfica, certificando-se de que ninguém mais consiga ter acesso a ela.

Para compartilhar essa chave, Alice e Bob usam um canal clássico de comunicação. Por mais seguro que ele seja, em princípio ele pode ser monitorado por algum agente externo (Eva) sem que Alice e Bob percebam. Eva pode obter a chave, sem Alice e Bob notarem, pois qualquer informação clássica pode ser clonada. Eva pode, por exemplo, interceptar a chave enviada por Alice a Bob e, em seguida, reenviá-la a ele. Hoje em dia, no entanto, para contornar este problema utilizamos os, assim chamados, protocolos de chave pública (amplamente utilizados nas transações financeiras via internet). Sua segurança, porém, não é matematicamente provada e desabaria perante o aparecimento de computadores quânticos. Na seção seguinte nos detemos um pouco mais neste aspecto.

Agora, se Alice e Bob usarem um canal quântico de comunicação, eles terão certeza de que a transmissão da chave foi realizada com segurança total, ou de que ela foi interceptada por Eva. Essa segurança é baseada nas leis da mecânica quântica e, desde que aceitemos que ela é uma teoria completa no sentido de Bohr [1, 2], não há meio de se burlar essa segurança.

O primeiro protocolo de criptografia quântica, ou mais corretamente, protocolo de distribuição de chaves quânticas, foi proposto por Bennett e Brassard, no ano de 1984 [3]. Ele também é conhecido como protocolo

[1]E-mail: rigolin@ifi.unicamp.br.

BB84. É usual, entre os criptólogos, nomear um protocolo de criptografia usando-se as iniciais dos nomes dos autores que o criaram mais o ano de sua invenção. A transmissão da chave é feita enviando-se fótons que podem ser preparados em quatro estados de polarização. Os fótons, neste protocolo, não estão emaranhados. Entretanto, Artur K. Ekert criou um protocolo (E91) [4] que faz uso do estado de Bell $|\Psi^-\rangle = (1/\sqrt{2})(|01\rangle - |10\rangle)$ para transmitir chaves quânticas. Sua segurança está baseada na impossibilidade de violação da desigualdade de Clauser-Horne-Shimony-Holt (CHSH) [5]. Em 1992, Bennett, Brassard e Mermin [6] simplificaram o protocolo E91 criando o protocolo BBM92 e provaram de um modo muito simples e profundo a impossibilidade de as chaves serem conhecidas por outra pessoa sem Alice e Bob perceberem. Também em 1992, Bennett [7] criou o protocolo B92, no qual apenas dois estados de polarização de fótons são utilizados para se transmitir seguramente uma chave criptográfica.

Neste artigo discutimos em detalhes os quatro protocolos de transmissão de chaves quânticas acima mencionados. Pretendemos apresentá-los do modo mais simples e intuitivo possível, pois acreditamos que alguns deles já podem e devem ser ensinados durante um curso de graduação em Física. Alunos que já tenham ou estejam estudando mecânica quântica (MQ) conseguem, sem muito esforço, entendê-los. Acreditamos também que estes protocolos possam vir a ser ferramentas muito úteis até para se ensinar MQ, pois eles representam aplicações práticas e importantes de conceitos inerentes ao mundo quântico.

2. BB84

Uma das particularidades da criptografia quântica (CQ) está no fato de que a melhor forma de se começar a entendê-la e estudá-la consiste na leitura do primeiro artigo dedicado a esse assunto [3]. Em ciência isto é um fato raro. Não é comum recomendar a um aluno iniciando-se em alguma área do conhecimento a leitura dos artigos que a fundaram. Geralmente, após a aparição desses artigos, outros mais simples e pedagógicos são publicados, os quais são mais adequados para um aprendiz. Felizmente isso não ocorre com a CQ. De fato, a simplicidade da Ref. [3] a torna não somente ampla e unanimente reconhecida como a fundadora da CQ, como também, a nosso ver, a melhor introdução a essa área. Ela tem quatro páginas e está escrita numa linguagem tão clara, precisa e direta que qualquer aluno que tenha feito um curso introdutório de mecânica quântica pode entendê-la sem muito esforço. A Ref. [3] se enquadra na honrosa categoria de trabalhos científicos que podem ser lidos ao sofá, em 15 min, desfrutando-se de um bom café. No restante desta seção vamos fazer um resumo deste artigo, enfatizando aspectos que serão fundamentais para o entendimento dos outros protocolos de CQ apresentados nas seções seguintes. Para os leitores mais interessados, recomendamos com entusiasmo a leitura do trabalho original de Bennett e Brassard, o qual pode ser gratuitamente copiado a partir da página pessoal de Charles H. Bennett: www.research.ibm.com/people/b/bennetc/chbbib.htm.

Antes de iniciar a exposição do protocolo BB84, vale a pena dizer que este protocolo é usado em todos os sistemas bem-sucedidos de CQ instalados até hoje e, mais ainda, ele é o único oferecido por duas companhias especializadas em segurança de transmissão de dados. Assim, mesmo sendo o primeiro protocolo proposto na literatura, ele ainda é, apesar das muitas alternativas de CQ apresentadas *a posteriori*, aquele de maior importância prática e comercial.

A Ref. [3] apresenta, pela primeira vez, a idéia de que a mecânica quântica (MQ) pode ser utilizada para alcançar uma das principais metas da criptografia, *i.e.*, a distribuição segura de uma chave criptográfica (seqüência de números aleatórios) entre duas partes (Alice e Bob) que inicialmente não compartilham nenhuma informação secreta. Para isso, Alice e Bob devem dispor não só de um canal quântico, mas também de algum canal clássico de comunicação. Este último pode ser monitorado passiva mas não ativamente por um agente externo (Eva). Por meio dessa chave, Alice e Bob podem com absoluta certeza se comunicar com segurança. A garantia da distribuição segura de chaves por meio da CQ se sustenta na validade da MQ tal qual a conhecemos. Em contraste, a criptografia de chave pública é considerada segura devido a um suposto grau de complexidade matemática inerente ao algoritmo de decodificação necessário para recuperar a mensagem criptografada se não conhecemos a chave privada. No entanto, esse resultado nunca foi matematicamente provado e não há nada que impeça a criação de um algoritmo (quem sabe ele já não esteja nas mãos de alguma agência de inteligência governamental) que possa facilmente decodificar, por meio de computadores convencionais, mensagens secretas oriundas de protocolos de chaves públicas. Pior ainda, a segurança da criptografia de chave pública tradicional desabaria perante o aparecimento de computadores quânticos, o que não aconteceria com sistemas de distribuição de chaves por CQ.

Na Introdução da Ref. [3], após uma breve digressão sobre sistemas criptográficos tradicionais, os autores explicitam claramente as novidades que serão apresentadas no artigo: como utilizar a MQ para (1) criar protocolos de transmissão segura de chaves criptográficas e (2) "jogar cara-ou-coroa"sem possibilidade de enganar o oponente. Após a seção 2, onde os autores apresentam o formalismo a ser utilizado, na seção 3 discute-se o protocolo para distribuição de chaves e na seção 4 o protocolo para jogar cara-ou-coroa sem trapacear. Aqui expomos apenas o protocolo de transmissão de chave criptográfica, *i.e.*, o famoso protocolo BB84.

Este protocolo utiliza-se de sistemas quânticos de

dois níveis. Assim, os estados $|0\rangle$ e $|1\rangle$ representam fótons linearmente polarizados em direções ortogonais. Por exemplo, os estados $|0\rangle$ e $|1\rangle$ podem representar fótons que se propagam na direção z com campos elétricos oscilando no plano xy. As direções de polarização são representadas por vetores unitários. Usando coordenadas esféricas, de acordo com a notação definida na Fig. 1, precisamos de dois parâmetros (ângulos) para especificar uma direção de polarização.

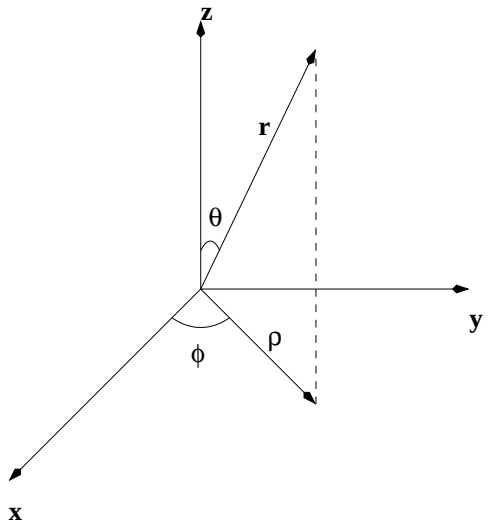

Figura 1 - Coordenadas esféricas. O ângulo polar θ varia de 0 a π e o ângulo azimutal ϕ de 0 a 2π. Aqui, o vetor $\mathbf{r}$, de módulo r, tem projeção no plano xy dada por $\rho = r\sin\theta$. As coordenadas cartesianas se relacionam com as coordenadas esféricas pela seguinte equação: $\mathbf{r} = x\,\hat{\mathbf{x}} + y\,\hat{\mathbf{y}} + z\,\hat{\mathbf{z}} = r\sin\theta\cos\phi\,\hat{\mathbf{x}} + r\sin\theta\sin\phi\,\hat{\mathbf{y}} + r\cos\theta\,\hat{\mathbf{z}}$.

Alice e Bob devem primeiramente escolher duas bases que serão utilizadas para a transmissão e recepção dos fótons. Cada base é composta por dois estados ortogonais de polarização. Eles podem escolher, por exemplo, polarizações contidas no plano xy ($\theta = \pi/2$). Tomando $\phi = 0$ e $\phi = \pi/2$ definimos as direções de polarização de uma das bases (base A). Usando $\phi = \pi/4$ e $\phi = 3\pi/4$ obtemos a outra (base B). Veja Fig. 2.

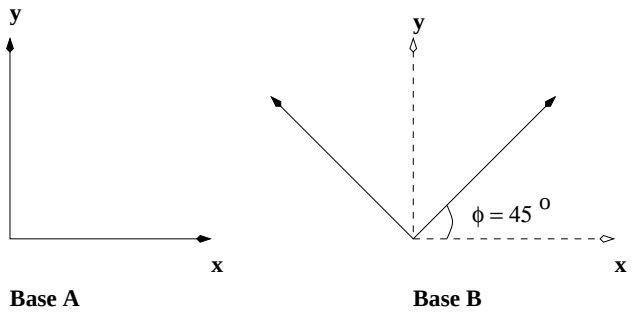

Figura 2 - Representação das bases A e B. O eixo z não está desenhado pois temos polarizações pertencentes ao plano xy.

O estado de polarização de qualquer fóton pode ser representado como uma combinação linear de dois estados ortogonais de polarização. Dessa forma, por meio dos estados que formam a base A ou a base B, podemos representar qualquer estado de polarização de um fóton.

Alice e Bob também devem combinar previamente quais estados ortogonais de cada uma das bases representam o bit 0 e o bit 1. Isso pode ser feito via um canal tradicional (clássico) de comunicação. No nosso exemplo, utilizamos os fótons polarizados na direção $\phi = 0$ ou $\phi = \pi/4$ para representar o bit 0 ($|0\rangle_A$ e $|0\rangle_B$) e aqueles com polarização na direção $\phi = \pi/2$ ou $\phi = 3\pi/4$ representando o bit 1 ($|1\rangle_A$ e $|1\rangle_B$). Nesta notação, o subíndice em cada ket indica se temos fótons polarizados nos autoestados da base A ou B. Note que $|0\rangle_B = (1/\sqrt{2})(|0\rangle_A + |1\rangle_A)$ e $|1\rangle_B = (1/\sqrt{2})(|0\rangle_A - |1\rangle_A)$.

Alice, para transmitir a chave, procede da seguinte forma. Primeiro ela escolhe qual seqüência aleatória de bits enviará a Bob (vamos usar, por exemplo, 001111...). Depois, qual a base utilizada para transmitir cada bit. Ela pode transmitir os dois primeiros bits utilizando-se da Base A, os três bits seguintes utilizando-se da Base B, o bit seguinte utilizando-se novamente da Base A, e assim por diante. Dessa forma, ela estaria enviando a Bob uma seqüência de fótons representados pelos seguintes kets: $|0\rangle_A, |0\rangle_A, |1\rangle_B, |1\rangle_B, |1\rangle_B, |1\rangle_A$, etc. Bob, por sua vez, deve escolher apenas qual base ele irá utilizar para detectar cada fóton. Ele oscila entre as bases A e B aleatoriamente.

Após a transmissão e detecção dos fótons, Alice e Bob revelam publicamente quais bases utilizaram para enviar e detectar cada fóton, respectivamente. Mas Alice não revela se enviou 0s ou 1s e Bob não revela o resultado de suas medidas. Apenas as bases utilizadas (base A ou base B) são publicamente reveladas. A seguir, eles consideram apenas os resultados nos quais ambos utilizaram a mesma base, descartando todos os demais. Agora eles revelam publicamente uma parte destes resultados (metade, ou um terço, por exemplo). Se Eva não monitorou a transmissão, os resultados revelados por Bob e Alice devem coincidir; mas se ela a monitorou, a probabilidade de que todos os dados públicos coincidam é praticamente nula (provamos isso um pouco mais à frente). Se os dados revelados publicamente coincidirem, isso será uma prova de que Eva não monitorou a transmissão e eles podem usar o restante dos dados como a chave. (Por restante dos dados entendemos aqueles nos quais ambos usaram a mesma base para enviar e medir os fótons.) E aqui termina o protocolo.

Se Eva monitorou os dados, a parte da informação revelada publicamente por Alice e Bob não irá coincidir ou, mais rigorosamente, a probabilidade de que elas coincidam é praticamente nula. A prova deste fato é como segue. Para simplificar a demonstração e sem perda de generalidade, supomos que Alice, Bob e Eva utilizam metade das vezes a Base A e metade das vezes a Base B, Alice para transmitir e Eva e Bob para detectar os

fótons. Se Alice e Bob utilizam a mesma base, a probabilidade de Eva usar a mesma base vale 0.5 (se Alice e Bob utilizaram a Base A, por exemplo, a probabilidade de Eva também ter utilizado essa base é 0.5). Agora, se Eva utiliza para monitorar os fótons a outra base, a probabilidade de Bob medir corretamente o valor do bit transmitido é de apenas 0.5 e não 1, como deveria ser se não tivéssemos um espião ou se Eva tivesse optado pela base correta. Formalmente, suponhamos que Alice enviou o fóton representando o bit 1, na Base A ($|1\rangle_A$) e Bob corretamente mediu na base A, porém Eva mediu o fóton, antes de ele chegar a Bob, na base B. Procedendo dessa forma, Eva terá colapsado o estado de polarização dos fótons em um dos autovetores da base por ela utilizada, *i.e.*, $|0\rangle_B = (1/\sqrt{2})(|0\rangle_A + |1\rangle_A)$ ou $|1\rangle_B = (1/\sqrt{2})(|0\rangle_A - |1\rangle_A)$. Assim, quando Bob realizar sua medida, a chance de ele medir, $|1\rangle_A$ é de apenas $(1/\sqrt{2})^2 = 0.5$, independente do resultado obtido por Eva. O fato de Eva escolher a base errada implica, para um evento, uma probabilidade igual a 0.5 de Bob detectar o valor correto para o bit transmitido por Alice. Para uma chave muito grande, a probabilidade de Bob detectar todos os bits corretamente, com Eva interferindo, tende a zero ou, mais rigorosamente, a $(0.5)^N$, onde N é o número de vezes que Eva usou a base errada.

Vale a pena lembrar que estados quânticos arbitrários não podem ser clonados. Isso foi demonstrado independentemente por Wootters e Zureck [8] e por Dieks [9]. Isso garante que Eva não pode simplesmente duplicar o estado quântico dos fótons enviados por Alice, medir um deles e enviar a Bob o outro. Isso possibilitaria a Eva detectar a polarização correta dos fótons transmitidos por Alice sem ser descoberta, tornando o protocolo BB84 inseguro.

Para melhor entender todas as etapas do protocolo, a Tab. 1 simula um exemplo de transmissão de chave quântica. Consideramos uma situação bem geral, na qual alguns fótons podem se perder durante a transmissão, de forma que Bob não os recebe.

Finalizamos esta seção contando dois fatos relacionados ao nascimento desta primeira proposta de CQ. Acreditamos que estas duas histórias são de interesse para estudantes de graduação em Física. Ambas foram extraídas do livro *The Code Book*, de Simon Singh [10]. Elas revelam bastante bem as angústias e momentos de tensão pelas quais muitos Físicos passam durante alguns (para não dizer vários) momentos de suas vidas profissionais.

Tabela 1 - As cinco primeiras linhas correspondem à transmissão quântica. As outras cinco, à discussão pública entre Alice e Bob. A última representa a chave compartilhada por eles.

Seqüência de bits de Alice	0	1	1	0	1	1	0	0	1	0	1	1
Bases escolhidas por Alice	B	A	B	A	A	A	A	A	B	B	A	B
Fótons enviados por Alice	$\|0\rangle_B$	$\|1\rangle_A$	$\|1\rangle_B$	$\|0\rangle_A$	$\|1\rangle_A$	$\|1\rangle_A$	$\|0\rangle_A$	$\|0\rangle_A$	$\|1\rangle_B$	$\|0\rangle_B$	$\|1\rangle_A$	$\|1\rangle_B$
Bases escolhidas por Bob	A	B	B	A	A	B	B	A	B	A	B	B
Bits recebidos por Bob	1		1		1	0	0	0		1	1	1
Bob informa fótons detectados	A		B		A	B	B	A		A	B	B
Alice informa bases corretas			OK		OK			OK				OK
Informação compartilhada			1		1			0				1
Bob revela alguns bits da chave					1							
Alice confirma estes bits					OK							
Restante de bits é a chave			1					0				1

A primeira delas trata-se de uma pessoa que estava à frente de seu tempo: Stephen Wiesner, quem, em 1960, teve a idéia de utilizar a MQ de forma parecida a utilizada hoje em CQ. Ele demonstrou a possibilidade teórica de se fazer "dinheiro quântico", impossível de ser falsificado graças a um sistema de armazenamento quântico de bits. Longe de prática, a idéia era, porém, revolucionária. Anos mais tarde Bennett e Brassard inspiraram-se nessa idéia de "dinheiro quântico"para criar o protocolo BB84. Contudo, o mais interessante dessa história consiste em a idéia de Wiesner ter sido absolutamente ignorada no seu tempo. O seu orientador pediu-lhe que abandonasse a idéia e voltasse ao "trabalho", mostrando total desinteresse por ela. Conta Wiesner: "Não obtive nenhum apoio do meu orientador de tese - ele não mostrou o mínimo interesse pela minha idéia. Mostrei-a para outras várias pessoas e todas fizeram uma cara de estranheza e voltaram ao que já estavam fazendo naquela hora". Apesar disso, Wiesner submeteu a sua idéia para ser publicada numa revista científica. O artigo foi recusado. Submeteu-o a outras três revistas, e outras três vezes ele foi recusado. Desiludido, e consciente do grande interesse de Bennett por assuntos mais amplos, Wiesner enviou o seu rejeitado artigo a ele. Bennett ficou imediatamente fascinado pela idéia, mostrando-a para Brassard. Alguns anos depois, os dois juntos, inspirados na idéia de utilizar a MQ como proposto por Wiesner, inventaram o hoje em dia reconhecido e aclamado campo da CQ.

A segunda história pitoresca refere-se ao exato mo-

mento no qual Bennett e Brassard inventaram o protocolo BB84. Em 1984 fazia já algum tempo que ambos vinham tentando achar uma solução para o problema da distribuição de chaves, num cenário futurístico onde a computação quântica inviabilizara os atuais métodos de criptografia de chave pública. Um dia, quando estavam esperando o trem que levaria Brassard a seu lar, em Montreal, desde os laboratórios Thomas. J. Watson, da IBM, onde Bennett trabalhava, a solução para o problema surgiu. Esperando o trem na estação Croton-Harmon, conversando descontraída e informalmente, num momento de *eureka*, eles tiveram a brilhante idéia que levou ao protocolo BB84. Como afirma Simon Singh em *The Code Book*, se o trem tivesse chegado apenas alguns minutos antes eles teriam se despedido sem fazer nenhum progresso no problema da distribuição de chaves.

3. E91

Alice e Bob dispõem, agora, de um canal quântico que emite singletos: $|\Psi^-\rangle = (1/\sqrt{2})(|01\rangle - |10\rangle)^2$. Alice recebe um dos constituintes do singleto enquanto Bob recebe o outro. Vamos supor, sem perder em generalidade, que as partículas viajam até Alice e Bob ao longo da direção z. Ao receberem-nas, Alice e Bob medem o spin de suas partículas ao longo da direção $\mathbf{a}_i$ e $\mathbf{b}_j$, respectivamente. O vetor $\mathbf{a}_i$ ($\mathbf{b}_j$) é unitário e caracterizado pelos ângulos polar θ_i^a (θ_j^b) e azimutal φ_i^a (φ_j^b). Veja a Fig. 1. Tanto Alice quanto Bob orientam, aleatoriamente para cada medida de spin, seus detectores ao longo de três vetores contidos no plano xy, *i.e.* $\theta_i^a = \theta_j^b = \pi/2$. Os ângulos azimutais que caracterizam estes vetores são: $\varphi_1^a = 0$, $\varphi_2^a = \pi/4$ e $\varphi_3^a = \pi/2$ para Alice, e $\varphi_1^b = \pi/4$, $\varphi_2^b = \pi/2$ e $\varphi_3^b = 3\pi/4$ para Bob.

A partir destes vetores, podemos definir o coeficiente de correlação de medidas de spin (polarização) ao longo das direções $\mathbf{a}_i$ e $\mathbf{b}_j$ como sendo

$$\begin{aligned} E(\mathbf{a}_i,\mathbf{b}_j) &= P_{00}(\mathbf{a}_i,\mathbf{b}_j) + P_{11}(\mathbf{a}_i,\mathbf{b}_j) \\ &\quad -P_{01}(\mathbf{a}_i,\mathbf{b}_j) - P_{10}(\mathbf{a}_i,\mathbf{b}_j). \end{aligned} \quad (1)$$

Aqui $P_{00}(\mathbf{a}_i,\mathbf{b}_j), P_{11}(\mathbf{a}_i,\mathbf{b}_j), P_{01}(\mathbf{a}_i,\mathbf{b}_j)$ e $P_{10}(\mathbf{a}_i,\mathbf{b}_j)$ representam a probabilidade de obtermos os resultados $(+1,+1)$, $(-1,-1)$, $(+1,-1)$ e $(-1,+1)$ ao longo das direções $\mathbf{a}_i$ e $\mathbf{b}_j$, respectivamente. Atribuímos o valor 1 para uma medida do estado $|0\rangle$ e valor -1 para uma medida do estado $|1\rangle$. Assim, o coeficiente de correlação nada mais é do que a probabilidade de Alice e Bob medirem o mesmo valor de spin menos a probabilidade de obterem valores diferentes.

Para um estado puro, a Eq. (1) pode ser escrita da seguinte forma,

$$E(\mathbf{a}_i,\mathbf{b}_j) = \langle\Psi^-|\sigma^A_{\mathbf{a}_i}\otimes\sigma^B_{\mathbf{b}_j}|\Psi^-\rangle, \quad (2)$$

onde $\sigma^A_{\mathbf{a}_i} = \mathbf{a}_i\cdot\sigma^A$ e $\sigma^B_{\mathbf{b}_j} = \mathbf{b}_j\cdot\sigma^B$, $\sigma^A = (\sigma^A_x,\sigma^A_y,\sigma^A_z)$ e $\sigma^B = (\sigma^B_x,\sigma^B_y,\sigma^B_z)$ e o ponto representa o produto escalar. Para vermos isso basta lembrar que qualquer estado puro de dois qbits pode ser escrito como $|\Psi^-\rangle = a|0\rangle_{\mathbf{a}_i}|0\rangle_{\mathbf{b}_j} + b|0\rangle_{\mathbf{a}_i}|1\rangle_{\mathbf{b}_j} + c|1\rangle_{\mathbf{a}_i}|0\rangle_{\mathbf{b}_j} + d|1\rangle_{\mathbf{a}_i}|1\rangle_{\mathbf{b}_j}$, com a, b, c e d complexos, $|0(1)\rangle_{\mathbf{a}_i}$ autovetor de $\sigma^A_{\mathbf{a}_i}$ e $|0(1)\rangle_{\mathbf{b}_j}$ autovetor de $\sigma^B_{\mathbf{b}_j}$. Substituindo essa expansão de $|\Psi^-\rangle$ na Eq. (2) obtemos

$$E(\mathbf{a}_i,\mathbf{b}_j) = |a|^2 + |d|^2 - |b|^2 - |c|^2. \quad (3)$$

Agora, como $|a|^2 = P_{00}(\mathbf{a}_i,\mathbf{b}_j)$, $|d|^2 = P_{11}(\mathbf{a}_i,\mathbf{b}_j)$, $|b|^2 = P_{01}(\mathbf{a}_i,\mathbf{b}_j)$ e $|c|^2 = P_{10}(\mathbf{a}_i,\mathbf{b}_j)$, recuperamos a Eq. (1) a partir de (2).

Sendo as componentes cartesianas dos vetores $\mathbf{a}_i = (a_x,a_y,a_z)$ e $\mathbf{b}_j = (b_x,b_y,b_z)$ temos que

$$\begin{aligned} \sigma^A_{\mathbf{a}_i}\otimes\sigma^B_{\mathbf{b}_j} &= a_xb_x\sigma^A_x\sigma^B_x + a_xb_y\sigma^A_x\sigma^B_y \\ &\quad + a_xb_z\sigma^A_x\sigma^B_z + a_yb_x\sigma^A_y\sigma^B_x \\ &\quad + a_yb_y\sigma^A_y\sigma^B_y + a_yb_z\sigma^A_y\sigma^B_z \\ &\quad + a_zb_x\sigma^A_z\sigma^B_x + a_zb_y\sigma^A_z\sigma^B_y \\ &\quad + a_zb_z\sigma^A_z\sigma^B_z. \end{aligned} \quad (4)$$

Já que $\sigma^A_{\mathbf{a}_i}\otimes\sigma^B_{\mathbf{b}_j}$ é um observável (sua média tem que ser real) e $\sigma_y|0\rangle = \mathrm{i}|0\rangle$ e $\sigma_y|1\rangle = -\mathrm{i}|1\rangle$, somente termos com um número par de σ_y's na Eq. (4) são relevantes no cálculo de $E(\mathbf{a}_i,\mathbf{b}_j)$. Além disso, como as aplicações de σ_x e σ_y em $|0(1)\rangle$ produzem estados ortogonais e a aplicação de σ_z produz apenas uma fase global no estado em que ele atua, termos que possuem um número ímpar de σ_z's se anulam. Dessa forma, os únicos termos da Eq. (4) contribuindo no cálculo de $E(\mathbf{a}_i,\mathbf{b}_j)$ são:

$$\begin{aligned} E(\mathbf{a}_i,\mathbf{b}_j) &= \langle\Psi^-|a_xb_x\sigma^A_x\sigma^B_x + a_yb_y\sigma^A_y\sigma^B_y|\Psi^-\rangle \\ &\quad + \langle\Psi^-|a_zb_z\sigma^A_z\sigma^B_z|\Psi^-\rangle \\ &= -\frac{a_xb_x}{2}\left(\langle01|\sigma^A_x\sigma^B_x|10\rangle + \langle10|\sigma^A_x\sigma^B_x|01\rangle\right) \\ &\quad -\frac{a_yb_y}{2}\left(\langle01|\sigma^A_y\sigma^B_y|10\rangle + \langle10|\sigma^A_y\sigma^B_y|01\rangle\right) \\ &\quad +\frac{a_zb_z}{2}\left(\langle01|\sigma^A_z\sigma^B_z|01\rangle + \langle10|\sigma^A_z\sigma^B_z|10\rangle\right) \\ &= -(a_xb_x + a_yb_y + a_zb_z) \\ &= -\mathbf{a}_i\cdot\mathbf{b}_j. \end{aligned} \quad (5)$$

Como era de se esperar, se Alice e Bob medem seus qbits na mesma direção, $\mathbf{a}_i = \mathbf{b}_j$, obtemos $E(\mathbf{a}_i,\mathbf{a}_i) = -1$. Isto expressa, para este caso em particular, o fato de que o novo estado descrevendo o par de qbits sempre será $|01\rangle$ ou $|10\rangle$, não importando a orientação do vetor $\mathbf{a}_i$.

Precisamos definir só mais uma quantidade [5] antes de apresentarmos o protocolo de transmissão de chave quântica [4]:

$$S \equiv E(\mathbf{a}_1,\mathbf{b}_1) - E(\mathbf{a}_1,\mathbf{b}_3) + E(\mathbf{a}_3,\mathbf{b}_1) + E(\mathbf{a}_3,\mathbf{b}_3). \quad (6)$$

[2] Vale a pena observar que o estado $|\Psi^-\rangle$ é um estado emaranhado e não-local. Ele não pode ser escrito como um produto tensorial de um único estado pertencente a Alice e de um outro pertencente a Bob.

Como o ângulo formado por todos os pares de vetores que aparecem acima vale $\pi/4$, exceto para o par $\mathbf{a}_1$ e $\mathbf{b}_3$, o qual é de $3\pi/4$, temos que $E(\mathbf{a}_1,\mathbf{b}_1) = -E(\mathbf{a}_1,\mathbf{b}_3) = E(\mathbf{a}_3,\mathbf{b}_1) = E(\mathbf{a}_3,\mathbf{b}_3) = -\sqrt{2}/2$. Portanto,

$$S = -2\sqrt{2}. \tag{7}$$

Voltando ao protocolo, após Alice e Bob finalizarem as medidas nos vários pares de qbits oriundos de singletos, eles anunciam publicamente as orientações escolhidas para cada medida e se detectaram ou não seus qbits. Eles descartam todas as medidas em que pelo menos um deles não detectou nenhum qbit. Isso ocorre pois o detector não tem eficiência um. Em seguida eles separam todas as suas medidas em dois grupos: 1) grupo de todas as medidas nas quais Alice e Bob usaram orientações diferentes em seus detectores; 2) grupo onde ambos usaram a mesma orientação ($\{\mathbf{a}_2,\mathbf{b}_1\}$ e $\{\mathbf{a}_3,\mathbf{b}_2\}$). Feita essa triagem, Alice e Bob anunciam publicamente os resultados obtidos para todas as medidas do grupo 1. A partir destes dados eles calculam S, cujo resultado deve ser igual ao fornecido pela Eq. (7). Se esse resultado se verificar, eles podem utilizar os dados do grupo 2, os quais estão anticorrelacionados, como chave criptográfica. Caso o valor de S não seja aquele dado pela Eq. (7), Alice e Bob descartam todos os seus dados e recomeçam o protocolo.

A fim de provar a segurança desse protocolo, devemos calcular o valor de S supondo que um terceiro sujeito, diga-se Eva, interfira na transmissão dos qbits. Suponhamos que Eva meça os qbits de Alice e Bob numa direção $\mathbf{n}_a$ e $\mathbf{n}_b$, respectivamente. Dessa forma, ao medir o singleto Eva obtém uma das quatro possibilidades abaixo representadas:

$$\begin{aligned}
|\Psi^-\rangle &\overset{\text{medida}}{\longrightarrow} |0\rangle_{\mathbf{n}_a}|0\rangle_{\mathbf{n}_b},\\
|\Psi^-\rangle &\overset{\text{medida}}{\longrightarrow} |0\rangle_{\mathbf{n}_a}|1\rangle_{\mathbf{n}_b},\\
|\Psi^-\rangle &\overset{\text{medida}}{\longrightarrow} |1\rangle_{\mathbf{n}_a}|0\rangle_{\mathbf{n}_b},\\
|\Psi^-\rangle &\overset{\text{medida}}{\longrightarrow} |1\rangle_{\mathbf{n}_a}|1\rangle_{\mathbf{n}_b},
\end{aligned} \tag{8}$$

onde $|\cdot\rangle_{\mathbf{n}_a}$ e $|\cdot\rangle_{\mathbf{n}_b}$ são os autoestados dos operadores $\sigma^A_{\mathbf{n}_a}$ e $\sigma^B_{\mathbf{n}_b}$.

Vamos definir as funções $|\alpha(\mathbf{n}_a,\mathbf{n}_b)|^2$, $|\beta(\mathbf{n}_a,\mathbf{n}_b)|^2$, $|\gamma(\mathbf{n}_a,\mathbf{n}_b)|^2$ e $|\delta(\mathbf{n}_a,\mathbf{n}_b)|^2$ para representar as probabilidades de detecção de cada uma das respectivas quatro possibilidades acima expostas. Explicitamos a dependência das probabilidades em termos das orientações $\mathbf{n}_a$ e $\mathbf{n}_b$ para realçar que elas dependem da estratégia de medida utilizada por Eva. Sendo assim, o estado misto que chega a Alice e Bob após Eva realizar suas medidas é:

$$\begin{aligned}
\zeta \;=\; & |\alpha(\mathbf{n}_a,\mathbf{n}_b)|^2 |0\rangle_{\mathbf{n}_a}|0\rangle_{\mathbf{n}_b}\,{}_{\mathbf{n}_a}\langle 0|\,{}_{\mathbf{n}_b}\langle 0|\\
&+|\beta(\mathbf{n}_a,\mathbf{n}_b)|^2 |0\rangle_{\mathbf{n}_a}|1\rangle_{\mathbf{n}_b}\,{}_{\mathbf{n}_a}\langle 0|\,{}_{\mathbf{n}_b}\langle 1|\\
&+|\gamma(\mathbf{n}_a,\mathbf{n}_b)|^2 |1\rangle_{\mathbf{n}_a}|0\rangle_{\mathbf{n}_b}\,{}_{\mathbf{n}_a}\langle 1|\,{}_{\mathbf{n}_b}\langle 0|\\
&+|\delta(\mathbf{n}_a,\mathbf{n}_b)|^2 |1\rangle_{\mathbf{n}_a}|1\rangle_{\mathbf{n}_b}\,{}_{\mathbf{n}_a}\langle 1|\,{}_{\mathbf{n}_b}\langle 1|.
\end{aligned} \tag{9}$$

Para um estado misto qualquer, a Eq. (1) pode ser escrita como:

$$E(\mathbf{a}_i,\mathbf{b}_j) = \text{Tr}\left[\zeta\left(\sigma^A_{\mathbf{a}_i}\otimes\sigma^B_{\mathbf{b}_j}\right)\right]. \tag{10}$$

Novamente podemos ver isso expandindo ζ na base $\{|n\rangle_{\mathbf{a}_i}|m\rangle_{\mathbf{b}_j}\,{}_{\mathbf{a}_i}\langle k|\,{}_{\mathbf{b}_j}\langle l|\}$, no qual $n,m,k,l = 0,1$. Temos no total 16 vetores. No entanto, ao tomarmos o traço, apenas os elementos da diagonal serão diferentes de zero. Estes, por sua vez, são dados por $P_{00}(\mathbf{a}_i,\mathbf{b}_j), P_{11}(\mathbf{a}_i,\mathbf{b}_j), -P_{01}(\mathbf{a}_i,\mathbf{b}_j)$ e $-P_{10}(\mathbf{a}_i,\mathbf{b}_j)$, mostrando que a Eq. (10) é equivalente a Eq. (1).

Para simplificar as contas, e sem perder em generalidade, podemos expandir o vetor $\mathbf{a}_i$ num sistema de referência $x'y'z'$, onde z' é paralelo a $\mathbf{n}_a$ e o vetor $\mathbf{b}_j$ num sistema $x''y''z''$ onde z'' é paralelo a $\mathbf{n}_b$. Fizemos esta escolha de tal forma que as relações abaixo sejam satisfeitas:

$$\begin{aligned}
\sigma^A_{x'}|0(1)\rangle_{\mathbf{n}_a} &= |1(0)\rangle_{\mathbf{n}_a}, && (11)\\
\sigma^B_{x''}|0(1)\rangle_{\mathbf{n}_b} &= |1(0)\rangle_{\mathbf{n}_b}, && (12)\\
\sigma^A_{y'}|0(1)\rangle_{\mathbf{n}_a} &= \text{i}(-\text{i})|1(0)\rangle_{\mathbf{n}_a}, && (13)\\
\sigma^B_{y''}|0(1)\rangle_{\mathbf{n}_b} &= \text{i}(-\text{i})|1(0)\rangle_{\mathbf{n}_b}, && (14)\\
\sigma^A_{z'}|0(1)\rangle_{\mathbf{n}_a} &= +(-)|0(1)\rangle_{\mathbf{n}_a}, && (15)\\
\sigma^B_{z''}|0(1)\rangle_{\mathbf{n}_b} &= +(-)|0(1)\rangle_{\mathbf{n}_b}. && (16)
\end{aligned}$$

Nestes sistemas de coordenadas,

$$\begin{aligned}
\sigma^A &= \sigma^A_{x'}\mathbf{x}' + \sigma^A_{y'}\mathbf{y}' + \sigma^A_{z'}\mathbf{z}', && (17)\\
\sigma^B &= \sigma^B_{x''}\mathbf{x}'' + \sigma^B_{y''}\mathbf{y}'' + \sigma^B_{z''}\mathbf{z}'', && (18)\\
\mathbf{a}_i &= a'_x\mathbf{x}' + a'_y\mathbf{y}' + a'_z\mathbf{z}', && (19)\\
\mathbf{b}_j &= b''_x\mathbf{x}'' + b''_y\mathbf{y}'' + b''_z\mathbf{z}'', && (20)\\
\mathbf{n}_a &= \mathbf{z}', && (21)\\
\mathbf{n}_b &= \mathbf{z}'', && (22)
\end{aligned}$$

onde $\mathbf{x}',\mathbf{y}',\mathbf{z}'$ e $\mathbf{x}'',\mathbf{y}'',\mathbf{z}''$ são os versores que expandem, respectivamente, os sistemas de referência $x'y'z'$ e $x''y''z''$.

Usando as expansões anteriores podemos escrever os operadores $\sigma^A_{\mathbf{a}_i}$ e $\sigma^B_{\mathbf{b}_j}$ da seguinte forma:

$$\sigma^A_{\mathbf{a}_i} = \mathbf{a}_i\cdot\sigma^A = a'_x\sigma^A_{x'} + a'_y\sigma^A_{y'} + a'_z\sigma^A_{z'}, \tag{23}$$

$$\sigma^B_{\mathbf{b}_j} = \mathbf{b}_i\cdot\sigma^A = b''_x\sigma^B_{x''} + b''_y\sigma^B_{y''} + b''_z\sigma^B_{z''}. \tag{24}$$

Por meio das Eqs. (23) e (24) vemos que:

$$\begin{aligned}
\sigma^A_{\mathbf{a}_i}\otimes\sigma^B_{\mathbf{b}_j} \;=\; & a'_xb''_x\sigma^A_{x'}\sigma^B_{x''} + a'_xb''_y\sigma^A_{x'}\sigma^B_{y''}\\
&+a'_xb''_z\sigma^A_{x'}\sigma^B_{z''} + a'_yb''_x\sigma^A_{y'}\sigma^B_{x''}\\
&+a'_yb''_y\sigma^A_{y'}\sigma^B_{y''} + a'_yb''_z\sigma^A_{y'}\sigma^B_{z''}\\
&+a'_zb''_x\sigma^A_{z'}\sigma^B_{x''} + a'_zb''_y\sigma^A_{z'}\sigma^B_{y''}\\
&+a'_zb''_z\sigma^A_{z'}\sigma^B_{z''}.
\end{aligned}$$

Retornando ao cálculo do coeficiente de correlação, vemos que substituindo a Eq. (9) em (10) temos:

$$
\begin{aligned}
E(\mathbf{a}_i,\mathbf{b}_j) = {} & |\alpha(\mathbf{n}_a,\mathbf{n}_b)|^2\, {}_{\mathbf{n}_a}\langle 0|\,{}_{\mathbf{n}_b}\langle 0|\Sigma|0\rangle_{\mathbf{n}_a}|0\rangle_{\mathbf{n}_b} \\
& +|\beta(\mathbf{n}_a,\mathbf{n}_b)|^2\, {}_{\mathbf{n}_a}\langle 0|\,{}_{\mathbf{n}_b}\langle 1|\Sigma|0\rangle_{\mathbf{n}_a}|1\rangle_{\mathbf{n}_b} \\
& +|\gamma(\mathbf{n}_a,\mathbf{n}_b)|^2\, {}_{\mathbf{n}_a}\langle 1|\,{}_{\mathbf{n}_b}\langle 0|\Sigma|1\rangle_{\mathbf{n}_a}|0\rangle_{\mathbf{n}_b} \\
& +|\delta(\mathbf{n}_a,\mathbf{n}_b)|^2\, {}_{\mathbf{n}_a}\langle 1|\,{}_{\mathbf{n}_b}\langle 1|\Sigma|1\rangle_{\mathbf{n}_a}|1\rangle_{\mathbf{n}_b},
\end{aligned}
$$

onde $\Sigma = \sigma^A_{\mathbf{a}_i} \otimes \sigma^B_{\mathbf{b}_j}$.

Observando as Eqs. (11-16), os únicos termos de $\sigma^A_{\mathbf{a}_i} \otimes \sigma^B_{\mathbf{b}_j}$ que contribuem no cálculo de $E(\mathbf{a}_i,\mathbf{b}_j)$ são:

$$
\begin{aligned}
\frac{E(\mathbf{a}_i,\mathbf{b}_j)}{a'_z b''_z} &= |\alpha(\mathbf{n}_a,\mathbf{n}_b)|^2\, {}_{\mathbf{n}_a}\langle 0|\,{}_{\mathbf{n}_b}\langle 0|\Sigma_z|0\rangle_{\mathbf{n}_a}|0\rangle_{\mathbf{n}_b} \\
&\quad +|\beta(\mathbf{n}_a,\mathbf{n}_b)|^2\, {}_{\mathbf{n}_a}\langle 0|\,{}_{\mathbf{n}_b}\langle 1|\Sigma_z|0\rangle_{\mathbf{n}_a}|1\rangle_{\mathbf{n}_b} \\
&\quad +|\gamma(\mathbf{n}_a,\mathbf{n}_b)|^2\, {}_{\mathbf{n}_a}\langle 1|\,{}_{\mathbf{n}_b}\langle 0|\Sigma_z|1\rangle_{\mathbf{n}_a}|0\rangle_{\mathbf{n}_b} \\
&\quad +|\delta(\mathbf{n}_a,\mathbf{n}_b)|^2\, {}_{\mathbf{n}_a}\langle 1|\,{}_{\mathbf{n}_b}\langle 1|\Sigma_z|1\rangle_{\mathbf{n}_a}|1\rangle_{\mathbf{n}_b} \\
E(\mathbf{a}_i,\mathbf{b}_j) &= f(\mathbf{n}_a,\mathbf{n}_b) a'_z b''_z. \qquad (25)
\end{aligned}
$$

Na expressão anterior $\Sigma_z = \sigma^A_{z'}\sigma^B_{z''}$ e $f(\mathbf{n}_a,\mathbf{n}_b) = |\alpha(\mathbf{n}_a,\mathbf{n}_b)|^2 - |\beta(\mathbf{n}_a,\mathbf{n}_b)|^2 - |\gamma(\mathbf{n}_a,\mathbf{n}_b)|^2 + |\delta(\mathbf{n}_a,\mathbf{n}_b)|^2$. Como a soma do módulo quadrado dos coeficientes da expansão de ζ vale 1, então $|f(\mathbf{n}_a,\mathbf{n}_b)| \leq 1$.

Por meio das Eqs. (19-22) obtemos

$$
\begin{aligned}
a'_z &= \mathbf{a}_i \cdot \mathbf{n}_a, \qquad (26) \\
b''_z &= \mathbf{b}_j \cdot \mathbf{n}_b. \qquad (27)
\end{aligned}
$$

Assim, a Eq. (25) é reescrita como:

$$
E(\mathbf{a}_i,\mathbf{b}_j) = |f(\mathbf{n}_a,\mathbf{n}_b)|(\mathbf{a}_i\cdot\mathbf{n}_a)(\mathbf{b}_j\cdot\mathbf{n}_b), \qquad (28)
$$

onde tomamos o módulo de $f(\mathbf{n}_a,\mathbf{n}_b)$ para enfatizar que sempre podemos tê-lo positivo, simplesmente redefinindo os eixos $\mathbf{n}_a$ e $\mathbf{n}_b$.

Além disso, Eva pode mudar sua estratégia de medida para cada par interceptado, bastando para isso alterar a orientação de $\mathbf{n}_a$ e $\mathbf{n}_b$. A função de correlação final se torna, pois,

$$
E(\mathbf{a}_i,\mathbf{b}_j) = \int \mathrm{d}\mathbf{n}_a \mathrm{d}\mathbf{n}_b \varrho(\mathbf{n}_a,\mathbf{n}_b)(\mathbf{a}_i\cdot\mathbf{n}_a)(\mathbf{b}_j\cdot\mathbf{n}_b), \qquad (29)
$$

onde $\varrho(\mathbf{n}_a,\mathbf{n}_b)$ é probabilidade de cada estratégia[3] utilizada por Eva, *i.e.*, $\int \mathrm{d}\mathbf{n}_a \mathrm{d}\mathbf{n}_b\ \varrho(\mathbf{n}_a,\mathbf{n}_b) = 1$.

Finalmente, usando a Eq. (29) a função S pode ser assim escrita:

$$
\begin{aligned}
S &= \int \mathrm{d}\mathbf{n}_a \mathrm{d}\mathbf{n}_b \varrho(\mathbf{n}_a,\mathbf{n}_b)[\\
&\quad (\mathbf{a}_1\cdot\mathbf{n}_a)(\mathbf{b}_1\cdot\mathbf{n}_b) - (\mathbf{a}_1\cdot\mathbf{n}_a)(\mathbf{b}_3\cdot\mathbf{n}_b) \\
&\quad +(\mathbf{a}_3\cdot\mathbf{n}_a)(\mathbf{b}_1\cdot\mathbf{n}_b) + (\mathbf{a}_3\cdot\mathbf{n}_a)(\mathbf{b}_3\cdot\mathbf{n}_b)] \\
&= \int \mathrm{d}\mathbf{n}_a \mathrm{d}\mathbf{n}_b \varrho(\mathbf{n}_a,\mathbf{n}_b)\{ \\
&\quad (\mathbf{a}_1\cdot\mathbf{n}_a)[\mathbf{b}_1\cdot\mathbf{n}_b - \mathbf{b}_3\cdot\mathbf{n}_b] \\
&\quad +(\mathbf{a}_3\cdot\mathbf{n}_a)[\mathbf{b}_1\cdot\mathbf{n}_b + \mathbf{b}_3\cdot\mathbf{n}_b]\}. \qquad (30)
\end{aligned}
$$

Agora, como todos os vetores que aparecem na Eq. (30) são unitários, todos os produtos escalares têm módulo menor ou igual a 1. Assim,

$$
\begin{aligned}
|S| &\leq \int \mathrm{d}\mathbf{n}_a \mathrm{d}\mathbf{n}_b \varrho(\mathbf{n}_a,\mathbf{n}_b)\{ \\
&\quad |\mathbf{a}_1\cdot\mathbf{n}_a||\mathbf{b}_1\cdot\mathbf{n}_b - \mathbf{b}_3\cdot\mathbf{n}_b| \\
&\quad +|\mathbf{a}_3\cdot\mathbf{n}_a||\mathbf{b}_1\cdot\mathbf{n}_b + \mathbf{b}_3\cdot\mathbf{n}_b|\}. \\
&\leq \int \mathrm{d}\mathbf{n}_a \mathrm{d}\mathbf{n}_b \varrho(\mathbf{n}_a,\mathbf{n}_b)\{|\mathbf{b}_1\cdot\mathbf{n}_b - \mathbf{b}_3\cdot\mathbf{n}_b| \\
&\quad +|\mathbf{b}_1\cdot\mathbf{n}_b + \mathbf{b}_3\cdot\mathbf{n}_b|\}. \qquad (31)
\end{aligned}
$$

Analisando o termo entre chaves na Eq. (31) vemos que ele é da forma $|x-y|+|x+y|$, onde $x = \mathbf{b}_1\cdot\mathbf{n}_b$ e $y = \mathbf{b}_3\cdot\mathbf{n}_b$. Mas $|x-y|+|x+y| \leq |x|-|y|+|x|+|y| = 2|x|$, se $|x| > |y|$ ou $|x-y|+|x+y| \leq |y|-|x|+|x|+|y| = 2|y|$, se $|x| < |y|$. Portanto, $|x-y|+|x+y| \leq \max\{2|x|, 2|y|\}$. E como $|x| \leq 1$ e $|y| \leq 1$ então $|x-y|+|x+y| \leq 2$. Usando este último resultado na Eq. (31) e lembrando que $\varrho(\mathbf{n}_a,\mathbf{n}_b)$ está normalizada,

$$
|S| \leq 2. \qquad (32)
$$

A Eq. (32) claramente mostra que qualquer interferência feita por Eva nos pares de qbits que se dirigem até Alice e Bob pode ser detectada por eles, pois nunca Eva conseguirá ao mesmo tempo extrair alguma informação e reproduzir o valor $S = -2\sqrt{2}$. Eva, no máximo[4], fará com que os estados que cheguem a Alice e Bob alcancem $S = -2$, não importando a engenhosidade de sua estratégia. É neste sentido que devemos considerar como garantido pelas leis da física o segredo da chave criptográfica transmitida.

4. BBM92

Podemos simplificar ainda mais o protocolo anterior [6]. Agora, ao invés de Alice e Bob orientarem seus detectores aleatoriamente em três direções, eles necessitam apenas de duas direções. Eles orientam seus polarizadores ou na direção x ou na direção y. Note que ambas as direções formam um ângulo de 90°.

Novamente, Alice e Bob anunciam publicamente a orientação de cada polarizador em cada medida. No entanto, eles não informam os resultados. Em seguida, eles descartam todas as medidas nas quais foram utilizadas orientações diferentes. São mantidos apenas os eventos cujos polarizadores foram orientados numa mesma direção. Se Eva não interferiu, toda medida onde ambos utilizaram uma mesma direção para seus polarizadores deve estar anticorrelacionada. Dessa forma, a grandeza

$$
S = E(\mathbf{x},\mathbf{x}) + E(\mathbf{y},\mathbf{y}) = -2, \qquad (33)
$$

[3] Se $\varrho(\mathbf{n}_a,\mathbf{n}_b) = |f(\mathbf{n}_a,\mathbf{n}_b)|\delta(\mathbf{n}_a - \mathbf{n'}_a)\delta(\mathbf{n}_b - \mathbf{n'}_b)$ recuperamos a Eq. (28). Ou seja, Eva fixou uma estratégia e a manteve para todas as medidas.

[4] Se tivéssemos utilizado explicitamente as orientações de $\mathbf{a}_1, \mathbf{a}_3, \mathbf{b}_1$ e $\mathbf{b}_3$, teríamos obtido um limite superior ainda menor: $|S| \leq \sqrt{2}$.

se Eva não interfere. Isso ocorre pois para o singleto $E(\mathbf{x},\mathbf{x}) = E(\mathbf{y},\mathbf{y}) = -1$. Agora, se Eva interfere, mostramos na seção anterior que:

$$E(\mathbf{a}_i,\mathbf{b}_j) = \int \mathrm{d}\mathbf{n}_a \mathrm{d}\mathbf{n}_b \varrho(\mathbf{n}_a,\mathbf{n}_b)(\mathbf{a}_i\cdot\mathbf{n}_a)(\mathbf{b}_j\cdot\mathbf{n}_b). \quad (34)$$

Portanto,

$$\begin{aligned} |S| &= \Big| \int \mathrm{d}\mathbf{n}_a \mathrm{d}\mathbf{n}_b \rho(\mathbf{n}_a,\mathbf{n}_b)\left[(\mathbf{x}\cdot\mathbf{n}_a)(\mathbf{x}\cdot\mathbf{n}_b)\right. \\ &\quad \left. +(\mathbf{y}\cdot\mathbf{n}_a)(\mathbf{y}\cdot\mathbf{n}_b)\right]\Big| \\ &= \left| \int \mathrm{d}\mathbf{n}_a \mathrm{d}\mathbf{n}_b \rho(\mathbf{n}_a,\mathbf{n}_b)\left[\mathbf{n}_{a_x}\mathbf{n}_{b_x} + \mathbf{n}_{a_y}\mathbf{n}_{b_y}\right]\right| \\ &\leq \int \mathrm{d}\mathbf{n}_a \mathrm{d}\mathbf{n}_b \rho(\mathbf{n}_a,\mathbf{n}_b)\left|\mathbf{n}_{a_x}\mathbf{n}_{b_x} + \mathbf{n}_{a_y}\mathbf{n}_{b_y}\right| \\ &\leq \int \mathrm{d}\mathbf{n}_a \mathrm{d}\mathbf{n}_b \rho(\mathbf{n}_a,\mathbf{n}_b)\left|\mathbf{n}_a\cdot\mathbf{n}_b\right| \\ &\leq \int \mathrm{d}\mathbf{n}_a \mathrm{d}\mathbf{n}_b \rho(\mathbf{n}_a,\mathbf{n}_b) = 1. \end{aligned} \quad (35)$$

A última desigualdade vem do fato de que $\mathbf{n}_a$ e $\mathbf{n}_b$ são unitários. Observando a Eq. (35) vemos que não há meios de Eva atingir o valor de S dado pela Eq. (33). Assim, usando uma parte dos resultados válidos, Alice e Bob podem calcular S. Se seu valor for dado pela Eq. (33), eles utilizam a outra parte dos resultados como chave. Caso o valor de S seja diferente, eles descartam todas as medidas e recomeçam o protocolo.

Na verdade, este protocolo é equivalente ao BB84. Para ver isso, basta notar que as medidas de fótons com os polarizadores orientados na direção x (y) são equivalentes, no protocolo BB84, aos fótons preparados por Alice na base A (B) e medidos por Bob também nessa mesma base. A única diferença entre os dois protocolos está na escolha dos números aleatórios a serem transmitidos. No BB84 essa escolha é feita por Alice ao escolher em qual base ela prepara seu fóton. Por outro lado, no BBM92 Alice não tem mais essa liberdade. Nesse protocolo a seqüência é gerada no momento em que Alice mede os seus fótons de cada singleto.

Para mostrar a segurança destes protocolos, precisamos provar que toda medida que não perturbe estados não-ortogonais não fornece nenhuma informação sobre eles. Sejam $|u\rangle$ e $|v\rangle$ estes estados, *i.e.*, $\langle u|v\rangle \neq 0$. Vamos representar pela transformação unitária U a interação entre os estados de Eva, nossa espiã, com os estados transmitidos por Alice. O estado inicial de Eva é $|a\rangle$. Este estado é bem geral. Eva pode usar quantos fótons julgar necessário. Assim, para que Alice e Bob não percebam que Eva interferiu na transmissão,

$$U\left(|u\rangle|a\rangle\right) = |u\rangle|a'\rangle, \quad (36)$$

$$U\left(|v\rangle|a\rangle\right) = |v\rangle|a''\rangle. \quad (37)$$

Aqui, $|a'\rangle$ e $|a''\rangle$ são outros dois estados possíveis de Eva. Usando o fato de que U é uma transformação unitária,

$$\begin{aligned} \langle a|\langle u|U^\dagger U|v\rangle|a\rangle &= \langle a'|\langle u|v\rangle|a''\rangle \\ \langle a|a\rangle\langle u|v\rangle &= \langle u|v\rangle\langle a'|a''\rangle \\ \langle u|v\rangle &= \langle u|v\rangle\langle a'|a''\rangle \\ 1 &= \langle a'|a''\rangle. \end{aligned} \quad (38)$$

A última igualdade decorre de $|u\rangle$ e $|v\rangle$ não serem ortogonais. Mas a Eq. (38) nos diz que $|a'\rangle$ e $|a''\rangle$ são idênticos (estamos assumindo sempre estados normalizados). Dessa forma, qualquer medida que não perturbe os estados não-ortogonais não fornece nenhuma informação que permita a Eva distinguir entre eles. Provamos, assim, e de maneira bem geral, a segurança de qualquer protocolo que se utilize de estados não-ortogonais.

5. B92

Neste artigo [7] é demonstrada a possibilidade de se realizar CQ utilizando apenas dois estado quânticos não-ortogonais (no protocolo BB84 [3] tínhamos quatro estados). Sua importância é mais conceitual do que prática, pois esta proposta é difícil de ser implementada com as tecnologias atuais. A motivação que levou Bennett a propor este protocolo é declarada no início de seu artigo: "Na Ref. [6] a segurança dos sistemas de distribuição de chaves que não se utilizam de emaranhamento (*BB84 é um exemplo*) advém do fato de que qualquer medida que não perturbe nenhum dos dois estados não-ortogonais também não fornece nenhuma informação que permita distinguir entre esses dois estados. Isto naturalmente sugere a possibilidade de que a distribuição de chaves possa ser realizada utilizando apenas *dois* estados não-ortogonais..." (tradução e ênfase nossas).

A demonstração de que apenas dois estados não-ortogonais são suficientes é como se segue. Sejam $|A\rangle$ e $|B\rangle$ dois estados não-ortogonais ($\langle A|B\rangle \neq 0$) e sejam $P_A = \mathcal{I} - |B\rangle\langle B|$ e $P_B = \mathcal{I} - |A\rangle\langle A|$, onde $\mathcal{I}$ é o operador identidade. P_A e P_B são operadores de projeção em espaços ortogonais a $|B\rangle$ e a $|A\rangle$, respectivamente (note os índices trocados). Dessa forma, P_A aniquila $|B\rangle$ ($P_A|B\rangle = 0$), mas fornece um resultado positivo com probabilidade $Tr[P_A|A\rangle\langle A|] = 1-|\langle A|B\rangle|^2$ quando é aplicado em $|A\rangle$. Resultado semelhante obtemos para P_B. Alice e Bob devem combinar de antemão quais serão os estados $|A\rangle$ e $|B\rangle$ utilizados e qual corresponderá ao bit 0 e qual ao bit 1. $|A\rangle$ pode representar um fóton com polarização linear na direção dada por $\theta = \pi/2$ e $\phi = 0$ e $|B\rangle$ um fóton com orientação de polarização dada por $\theta = \pi/2$ e $\phi = \pi/4$. Veja Figs. 1 e 2. Para começar a distribuição de chaves, Alice deve primeiramente escolher uma seqüência de bits e enviá-la

a Bob codificando-a usando os estados $|A\rangle$ (bit 0) e $|B\rangle$ (bit 1). Bob, por sua vez, escolhe aleatoriamente para cada estado recebido de Alice qual medida realizará: P_A ou P_B. Terminada a transmissão, Bob anuncia publicamente para quais bits ele obteve resultados positivos sem, no entanto, informar o tipo de medida feita (se P_A ou P_B). São estes bits que serão utilizados por Alice e Bob para obter a chave criptográfica. Como nos outros esquemas de CQ, alguns destes bits devem ser sacrificados para checar se Eva monitorou a comunicação. Assim, Bob publicamente informa que base utilizou para medir alguns de seus fótons. Se Eva não interferiu, todas as medidas nas quais Bob obteve um resultado positivo devem corresponder a duas únicas possíveis situações: 1) Alice enviou um estado $|A\rangle$ e Bob mediu P_A ou 2) Alice enviou $|B\rangle$ e Bob mediu P_B. Caso ocorra um evento positivo para uma outra situação, Alice e Bob descartam seus bits pois Eva interferiu na transmissão. Se apenas estes dois eventos positivos ocorreram, eles têm certeza da segurança da chave, a qual é constituída pelos bits restantes.

Mostramos, agora, uma maneira de se implementar o protocolo B92. Como dito no parágrafo anterior, supomos que $|A\rangle$ e $|B\rangle$ representam estados de polarização linear de fótons. As direções de polarização de ambos os fótons diferem de 45°. Em coordenadas esféricas, para $|A\rangle$ temos $\phi = 0$ e para $|B\rangle$ temos $\phi = \pi/4$. Assim, a medida P_A pode ser feita utilizando um polarizador orientado na direção dada por $\phi = 3\pi/4$ (um polarizador transmite fótons com probabilidade $\cos^2\alpha$, onde α é o ângulo entre as direções de polarização do fóton e do polarizador). A medida de P_B é realizada por um polarizador orientado na direção $\phi = \pi/2$. Veja Figs. 1 e 2. Dessa forma, quando Alice enviar um fóton representado pelo estado $|A\rangle$ ($|B\rangle$) ele não será detectado por Bob quando ele fizer uma medida P_B (P_A), pois $P_B|A\rangle = 0$ ($P_A|B\rangle = 0$). Este resultado já era esperado pois temos, para estes casos, direções de polarização dos fótons ortogonais às direções dos polarizadores. No entanto, quando Alice enviar o estado $|A\rangle$ ($|B\rangle$) e Bob medir P_A (P_B), ele terá 50% de chance de detectar um fóton (resultado positivo). Isso ocorre pois o ângulo entre as direções de polarização dos fótons e dos polarizadores é de 45°. Neste esquema, se Alice enviou metade das vezes fótons descritos por $|A\rangle$ e metade das vezes fótons descritos por $|B\rangle$ e supondo que Bob mediu metade das vezes P_A e metade das vezes P_B, em apenas 25% das vezes Bob obterá um resultado positivo. Em outras palavras, metade das vezes ele não detectará nada porque o eixo do seu polarizador será colocado numa direção perpendicular à direção de oscilação dos fótons e, para a outra metade, somente a metade fornecerá um resultado positivo, devido ao eixo do polarizador estar a 45° em relação ao eixo de polarização dos fótons. E mais, se eles ainda sacrificarem metade dos bits para testar a não interferência de Eva, eles obterão, no final, como chave, uma seqüência aleatória de bits de tamanho igual a 1/8 do tamanho da seqüência original enviada por Alice.

Reiteramos que o protocolo B92 é conceitualmente importante pois mostra a possibilidade de se fazer CQ utilizando apenas dois estados não-ortogonais. Isso pode ajudar numa compreensão mais intuitiva da CQ. Além disso, a nosso ver, é fácil imaginar uma montagem experimental utilizando apenas polarizadores para detectar os fótons, como feito no parágrafo anterior. Essa simplicidade da montagem via polarizadores, o uso de apenas dois estados e mais o fato de que a maioria dos estudantes tem uma boa intuição física do que acontece quando um fóton passa por um polarizador fazem do B92 um protocolo muito útil para se apresentar a iniciantes no assunto.

6. Discussão e Conclusão

Neste artigo apresentamos de maneira acessível a estudantes de graduação em Física os quatro protocolos de distribuição de chaves quânticas que fundaram a área da criptografia quântica (CQ).

O primeiro deles, o protocolo BB84, é recomendado também como texto introdutório a esse assunto. Devido a sua clareza e concisão, ainda hoje consideramos a Ref. [3] uma ótima opção para se introduzir CQ a estudantes de Física.

O protocolo E91 requer um pouco mais de conhecimento do estudante. Contudo, com um pouco de esforço e uma introdução às desigualdades de Clauser, Horne, Shimony e Holt [5] ele também pode ser ensinado durante um curso de graduação em Física.

Os outros dois protocolos, por se tratarem de extensões e simplificações dos protocolos anteriores, são facilmente entendidos por estudantes que já dominaram o assunto dos primeiros dois protocolos.

Enfim, acreditamos na viabilidade de se ensinar CQ durante um curso de graduação em Física. E mais, ensinar CQ pode ser também extremamente vantajoso para convencer um público mais amplo da importância da mecânica quântica.

Referências

[1] N. Bohr, Phys. Rev. **48**, 696 (1935).

[2] A. Einstein, B. Podolsky and N. Rosen, Phys. Rev. **47**, 777 (1935).

[3] C.H. Bennett and G. Brassard, in *Proceedings of IEEE*

International Conference on Computers Systems and Signal Processing (Bangalore, Índia, 1984), p. 175.

[4] A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[5] J.F. Clauser, M.A. Horne, A. Shimony and R.A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[6] C.H. Bennett, G. Brassard and N.D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[7] C.H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[8] W.K. Wootters and W.H. Zurek, Nature **299**, 802 (1982).

[9] D. Dieks, Phys. Lett. A **92**, 271 (1982).

[10] S. Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (First Anchor Books Edition, New York, 2000).