Rodrigo Otávio Gonçalves Chaves

Táticas de ataque a protocolos quânticos de distribuição de chaves criptográficas utilizando estratégias de discriminação de estados

Dissertação apresentada ao Programa de Pós-Graduação em Física do Instituto de Ciências Exatas da Universidade Federal de Minas Gerais como requisito para obtenção do título de Mestre em Ciências.

Orientador: Leonardo Teixeira Neves

Belo Horizonte
2018

Dados Internacionais de Catalogação na Publicação (CIP)

Chaves, Rodrigo Otávio Gonçalves.

C375t Táticas de ataque a protocolos quânticos de distribuição de Chaves criptográficas utilizando estratégias de discriminação de estados / Rodrigo Otávio Gonçalves Chaves. – 2018.
76 f. il.

Orientador: Leonardo Teixeira Neves.
Dissertação (mestrado) – Universidade Federal de Minas Gerais – Departamento de Física.
Bibliografia: f.73 - 76.

1. Informação quântica. 2. Criptografia quântica. 3. Mecânica quântica. I.Título. II. Leonardo Teixeira Neves.

CDU – 519.67 (043)

Elaborada pela Biblioteca Professor Manoel Lopes de Siqueira da UFMG.

Agradecimentos

À minha família, pelo apoio, amor e carinho; à minha companheira, pelo amor e amizade; aos meus amigos pela alegria e oportunidade de carregá-los no Dota e CS:GO; ao meu orientador, pela oportunidade e ensinamento; à instituição de fomento FAPEMIG.

Resumo

Os postulados da mecânica quântica geram condições que garantem a segurança dos protocolos quânticos de distribuição de chaves criptográficas (QKD), essenciais à criptografia quântica. Uma espiã que deseje interceptar a construção da chave em um protocolo de QKD não poderá discriminar entre dois ou mais estados quânticos com certeza absoluta caso os mesmos sejam não-ortogonais e, além disso, ela não poderá clonar este estado. Essas limitações físicas fazem com que a espiã busque por outras formas de ataque aos protocolos. Diferentes estratégias de discriminação de estados foram criadas e elas podem ser aplicadas para a espionagem em QKD. Tais estratégias atendem aos objetivos de quem as utiliza, como minimizar a probabilidade média de erro ou obter a maior confiança possível na identificação de um estado. Todas elas, porém, não são capazes de identificar um estado perfeitamente e isso fará com que, quando utilizadas com o intuito de espionar, surjam incompatibilidades nas chaves criadas. Os propósitos desse trabalho são dois: primeiramente, estudar a aplicação da discriminação de estados quânticos em ataques a dois protocolos de QKD, sendo eles o B92 e o PBC00; em segundo lugar, analisar a taxa de erro que as diferentes estratégias introduzem nas chaves criptográficas. Considerando ataques de interceptação-reenvio, mostra-se quais estratégias são mais vantajosas para a espiã permanecer indetectável e quais medidas os comunicadores podem utilizar para se defenderem.

Palavras-chave: Mecânica quântica, informação quântica, discriminação de estados, criptografia quântica, distribuição quântica de chaves criptográficas.

Abstract

The postulates of quantum mechanics generates conditions that garantee the security of quantum key distribution (QKD) protocols, essencials to quantum cryptography. A spy that wishes to intercept the construction of a key in a QKD protocol will not be able to discriminate between two or more quantum states with certainty if they are non-orthogonal and, besides that, she will not be able to clone the states. These physical limitations compel the spy to search for different ways of attacking the protocols. Several state-discrimination strategies were created and they can be applied in the spying of QKD. Each strategy has its own purpose that fits the necessity of whom is using them, like the minimzation of the average probability of error or to attain the the maximum confidence possible in the identification of a state. All of them, however, are not capable of perfectly identifying a state and, accordingly, when they are used as tools for spying, they will create mismatches between the keys created by the protocols. The goals of this work are twofold: firstly, study the attack of QKD protocols, as the B92 and the PBC00, using discrimination of quantum states; secondly, analyze the error rate that different strategies introduce to the keys. Considering intercept-resend attacks, one shows which strategies are more advantageous to the spy so she can remain undetected and how the users of the protocol can defend themselves.

Keywords: Quantum mechanics, quantum information, quantum-key distribution, quantum cryptography.

Sumário

1 Introdução

Os avanços tecnológicos atuais nos permitiram obter diversas facilidades na comunicação entre as pessoas, empresas e governos. A cada dia se torna mais corriqueiro o acesso a uma conta bancária, o envio de uma foto para um parente ou a comunicação entre pessoas pela internet. A possibilidade de poder se conectar facilmente traz ao centro do palco a discussão de como garantir a segurança desses processos, e a criptografia tem papel central nessa discussão. Originalmente, a criptografia se limitava à confidencialidade da comunicação, ou seja, à transformação de uma mensagem em algo incompreensível que poderia ser retransformado em algo compreensível. Nesse sentido, foi bastante difundida nos meios militares para garantir que, caso um mensageiro fosse interceptado, o conteúdo da mensagem seria ininteligível para os inimigos. A área se tornou mais abrangente após o trabalho fundamental de Shannon [1] que quantificou a noção de informação e construiu os alicerces para que ela pudesse se expandir para análise de segurança, autenticação de mensagens [2–4], assinaturas digitais [5–7] e compressão de dados [8, 9].

A mecânica quântica trouxe revoluções na física, química, filosofia e recentemente reflexos tanto na teoria de informação quanto na criptografia. A possibilidade de armazenar informação em estados quânticos possibilitou o surgimento de novos recursos computacionais, circuitos lógicos, definições do conceito de informação [10, 11], e o computador quântico, que antes era apenas uma ideia, se tornou real[1] [12, 13]. O novo ramo foi batizado de computação quântica e, ao mesmo tempo em que trouxe júbilo com a possibilidade de novos algoritmos que possibilitam menor complexidade na resolução de problemas, ocasionou também a preocupação com a segurança dos protocolos de criptografia difundidos em todos os processos modernos de troca de mensagens. O receio teve seu início com um trabalho mostrando que, com a existência de um computador quântico, um dos protocolos de criptografia mais utilizados teria sua segurança comprometida devido ao algoritmo de Schror [14] e, consequentemente, se iniciou uma busca por soluções clássicas [15] ou por alternativas utilizando a própria mecânica quântica [16].

A era da criptografia quântica teve o seu início com o artigo de 1984 de Bennett e Brassard [17]: usando os postulados da mecânica quântica, eles propuseram uma maneira segura de distribuir uma chave criptográfica entre dois comunicadores, na qual seria possível inclusive detectar a presença de um espião no canal de comunicação. A chave criptográfica é o elemento que permite a codificação e decodificação das mensagens, sendo assim, a distribuição quântica de chaves criptográficas (QKD[2]) não é a criptografia em si, mas é um componente essencial para estes protocolos. A possibilidade da detecção do espião, como

[1] Na realidade, esses computadores quânticos ainda se limitam a poucos qubits. A escalabilidade para um que possua maior capacidade de processamento ainda é um desafio a ser superado.

[2] Do inglês *Quantum Key Distribution*.

será descrito futuramente, advém da impossibilidade de discriminar perfeitamente estados não-ortogonais, e ao tentá-lo, erros são introduzidos nos bits da chave construída por um dos comunicadores. Como todo protocolo criptográfico, sua segurança deve ser testada, pois existem várias possibilidades de ataques de espionagem [16]. Porém essa dissertação se limitará a ataques simples denominados interceptação-reenvio e supressão. No primeiro deles, o espião intercepta a transmissão do qubit no canal, realiza a discriminação de estados e o resultado corresponderá ao qubit que será reenviado para o destinatário. O segundo caso se assemelha ao primeiro, mas a diferença surge no fato que as falhas de algumas estratégias serão mascaradas dentro do próprio QKD.

No primeiro capítulo, o leitor será apresentado a alguns protocolos clássicos de criptografia como a cifra de César, a cifra de Vigenère, a cifra de uso único (OTP[3]) e o RSA. No segundo capítulo, ferramentes básicas de mecânica quântica serão introduzidas, entre elas a noção de um qubit, a esfera de Bloch, medições generalizadas, o teorema de não clonagem e as estratégias de discriminação de estados que serão necessárias para compreender os capítulos posteriores. O terceiro capítulo tratará da apresentação de alguns protocolos de QKD como o BB84 [17], B92 [18] e o PBC00 [19].[4] O capítulo seguinte tratará da espionagem ao B92 e ao PBC00 utilizando dois ataques distintos: interceptação-reenvio e supressão. O capítulo final se destina à conclusão onde é feito um resumo do que foi apresentado e dos resultados dos ataques. Os cálculos da taxa de erro estão presentes no apêndice.

[3] Do inglês *One-Time Pad*.

[4] Os protocolos são batizados utilizando as iniciais dos criadores e o ano no qual o artigo foi publicado.

2 Criptografia Clássica

Atualmente, a criptografia está presente em diferentes aplicações e não se limita somente à encriptação. Aqui, porém, apenas esta será estudada junto com a contextualização da QKD dentro dela. O leitor interessado poderá encontrar mais detalhes sobre o que será discutido aqui e outras aplicações modernas da criptografia na obra de Katz e Lindel [20] que serviu de base para esse capítulo. A encriptação consiste em esquemas no qual o signatário de uma mensagem encripta um texto puro (mensagem) obtendo um texto cifrado através de um algoritmo (cifra). Essa cifra impossibilita a determinação do texto puro, a menos que o receptor possua a chave para decifrar a mensagem cifrada. Um esquema de criptografia, em geral, deve ser estruturado utilizando três algoritmos:

1. O algoritmo Ger irá gerar probabilisticamente duas chaves que serão utilizadas para encriptar e decriptar a mensagem;

2. O algoritmo Enc será utilizado para encriptar a mensagem de modo aleatório. A aleatoriedade é necessária para garantir que o mesmo texto puro não resulte sempre no mesmo texto cifrado;

3. O algoritmo Dec será utilizado para decifrar o texto cifrado. Porém, não existe a probabilidade da decifração resultar em um texto que seja diferente do enviado.

É possível separar os esquemas de criptografia em duas classes: a criptografia de chave simétrica (ou de chave privada) e a criptografia de chave assimétrica (ou de chave pública).

A ideia de que a chave deve permanecer secreta é algo comum de se imaginar, mas outra pergunta que pode ser levantada é: o método utilizado para decifrar uma mensagem também deve ser mantido em segredo? Em um artigo de 1883, Auguste Kerckhoffs [21] argumentou o que ficou conhecido como princípio de Kerckhoffs:

> *O método de ciframento não deve ser um segredo e*
> *deve ser possível cair nas mãos do inimigo sem incovenientes.*

Em outras palavras, a segurança de um protocolo de criptografia deve ser assegurada pela manutenção do segredo da chave criptográfica e não pelo método como o algoritmo funciona. Argumentos a favor desse princípio são fáceis de serem pensados, como por exemplo, há maior facilidade em se manter o segredo da chave do que de todo um protocolo de criptografia. Caso haja uma brecha na segurança da comunicação, será mais fácil trocar a chave do que o protocolo em si. Outro exemplo é a atuação de um servidor que receberá mensagens de diferentes usuários. O mais simples nessa situação seria cada usuário possuir sua própria chave ao invés de criar um algoritmo para cada um deles.

O princípio também tem como consequência a publicidade dos protocolos para que seja possível um estudo extensivo da sua segurança. O risco de se manter um esquema de encriptação seguro devido a sua obscuridade é muito alto e isso faz com que esquemas públicos se tornem mais fortes, graças aos testes a que eles são constantemente submetidos.

2.1 Criptografia de chave simétrica (ou de chave privada)

Existem diversos protocolos de chave simétrica, mas todos possuem um mesmo formato geral. Eles são definidos implementando os seguintes algoritmos:

1. O algoritmo de geração da chave Ger recebe o parâmetro de segurança n através de uma sequência de bits 1 com tamanho n, ou seja 1^n, e tem como saída uma chave k. Assumimos que Ger pode ser probabilístico e, sem perda de generalidade, $\text{Gen}(1^n)$ gerará uma chave k de mesmo tamanho ou até maior que o parâmetro de segurança n;

2. O algoritmo de encriptação Enc recebe uma entrada de uma chave k e uma mensagem m. O algoritmo tem como saída um texto cifrado c. Nesse caso, Enc deve ser probabilístico;

3. O algoritmo de decifração Dec recebe uma entrada k e um texto cifrado c, e tem na saída uma mensagem m ou um erro; Dec é determinístico.

É necessário que para todo n, toda chave k e toda mensagem m, a igualdade $\text{Dec}_k(\text{Enc}_k(m)) = m$ seja satisfeita. Isso é, a decifração do texto cifrado c resultará sempre na mensagem m que foi encriptada. A figura 1 apresenta uma visualização do protocolo onde Alice e Bob utilizam um esquema de criptografia de chave simétrica para se comunicarem.

Os protocolos que serão mostrados a seguir são simples e por esse motivo não utilizaremos parâmetros de segurança ao descrevê-los.

2.1.1 A cifra de César

A cifra de César é uma das cifras mais antigas existentes e tem sua origem nas mensagens privadas do imperador romano Júlio César. O protocolo consiste na rotação das letras do alfabeto por um parâmetro determinado pela chave k, que é um número de 0 a 25. Isto é:

1. O algoritmo Ger tem na saída um $k \in \{0, ..., 25\}$;

2. O algoritmo Enc recebe a chave k e uma mensagem $m = m_1...m_l$ onde $m_i \in \{0, ..., 25\}$ e l é o tamanho da mensagem. Ele tem como saída um texto cifrado $c = c_1...c_l$ tal que $c_i = [(m_i + k) \text{mod } 26]$;

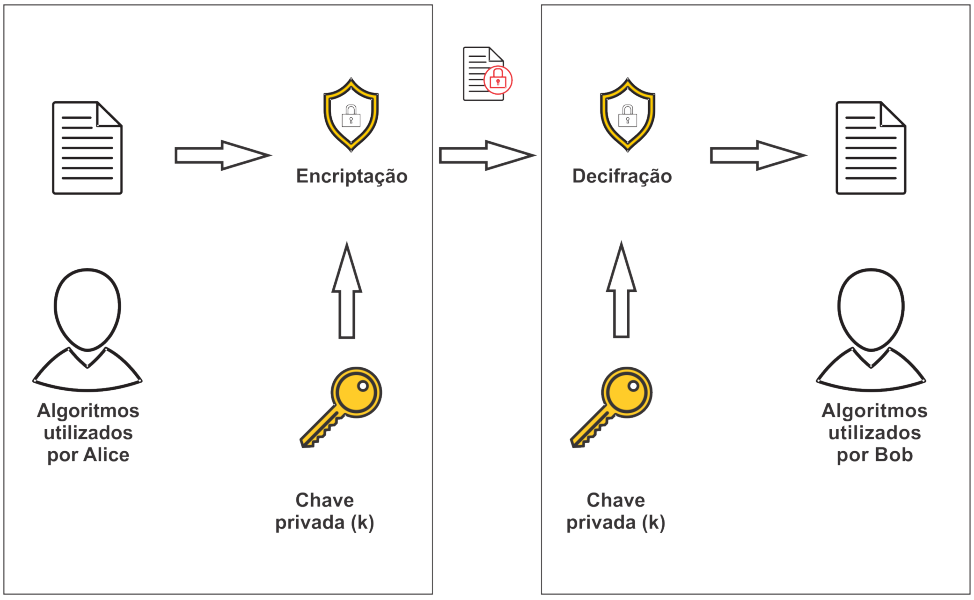

Figura 1 – Digrama descrevendo de maneira geral um protocolo de chave privada. Alice deseja enviar uma mensagem pra Bob e, para garantir a segurança, ela encripta sua mensagem utilizando uma chave k. A mensagem é enviada a Bob que, ao recebê-la, faz a decriptação utilizando a mesma chave k.

3. O algoritmo Dec recebe a chave k e o texto cifrado $c = c_1...c_l$ e tem como saída a mensagem $m = m_1...m_l$ tal que $m_i = [(c_i - k) \text{mod } 26]$.

Um exemplo elementar é aquele que utiliza a chave $k = 1$ para cifrar um texto simples. Aqui, as letras minúsculas serão usadas para o texto puro e as maiúsculas para o texto cifrado:

a	t	a	q	u	e	a	g	o	r	a
B	U	B	R	V	F	B	H	P	S	B

É possível perceber que esse protocolo não é seguro, pois a espiã poderá utilizar todas as chaves possíveis ao interceptar um texto cifrado. Esse ataque simples, nos dias atuais, é muito trivial para se automatizar. Porém, existe uma maneira diferente de atacá-lo que utiliza as frequências médias das letras em um texto.

A figura 2 mostra estas frequências em um texto em inglês. A partir delas é possível obter um valor para a soma quadrática das frequências médias (p_i):

$$\sum_{i=0}^{25} p_i^2 \approx 0.065. \tag{2.1}$$

O ataque agora consiste em calcular as frequências médias q_i das letras no texto cifrado. Isso é feito somando todas as ocorrências de cada letra no texto para, em seguida, dividir o resultado pela quantidade total de letras no texto cifrado. Se q_i for aproximadamente igual a p_i, a soma das frequências médias ao quadrado será aproximadamente igual a (2.1). Dessa forma, utilizando todas as chaves possíveis k, mapeia-se a frequência q_i para q_{i+k} utilizando $[(i + k) \text{ mod } 26]$ e computa-se

$$I_j = \sum_{i=0}^{25} p_i q_{i+j}, \tag{2.2}$$

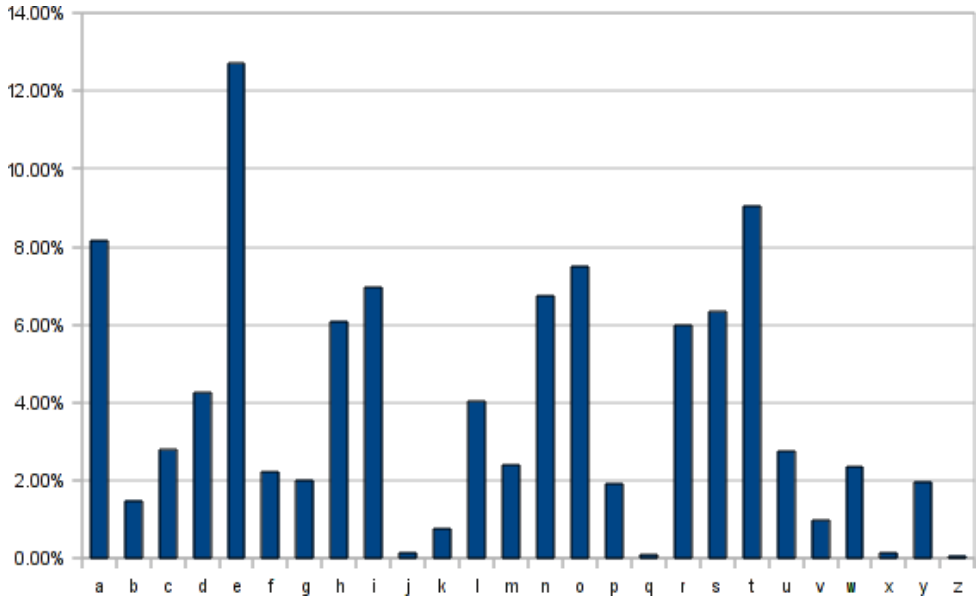

Figura 2 – Frequência média das letras em um texto de língua inglesa.

para cada valor de $j \in \{0, ..., 25\}$. Caso $j = k$, o valor de I_j será aproximadamente 0.065 e se $j \neq k$, I_j não estará próximo desse valor.

2.1.2 A cifra de Vigenère

A cifra de Vigenère [22, 23] consiste na utilização de uma chave diferente na cifra de César para cada letra do texto puro. A chave é formada por uma sequência de letras e a letra "b", por exemplo, corresponderia a um bit da chave com valor de $k = 1$ enquanto a letra "c" seria um bit da chave com valor de $k = 2$. A tabela abaixo exemplifica o protocolo:

Purotexto	a	t	a	q	u	e	a	g	o	r	a
Chave	a	b	d	a	b	d	a	b	d	a	b
Texto cifrado	A	U	D	Q	V	H	A	H	R	R	B

Uma maneira de ataque ao protocolo é parecida com o ataque à cifra de César, pois utiliza as frequências médias das letras em um texto. Supõe-se que uma chave terá um determinado período t, ou seja, a mesma troca será usada na primeira letra do texto cifrado c_1 e na letra c_{1+t}. No exemplo apresentado acima, pode-se ver um período de $t = 3$ e tanto a letra t quanto a letra u são trocadas utilizando um mesmo deslocamento. Uma sequência é escolhida começando da primeira letra do texto cifrado tal que:

$$c_1, c_{1+t}, c_{1+2t} \cdots, \tag{2.3}$$

onde todos os caracteres dessa sequência serão trocados pela mesma chave k_1. A frequência média da letra j do texto cifrado (q_j) terá que ser aproximadamente igual a frequência média da letra i para um texto puro em inglês (p_i). Por exemplo, supondo uma chave

que possua no primeiro bit $k_1 = 1$, ela deslocaria a letra do texto puro original pela letra seguinte a cada salto t. A frequência média da mensagem para a letra p_4 (que corresponde à frequência do "e") seria aproximadamente 13%. Após a encriptação, a frequência da letra q_5 terá que corresponder a 13% das ocorrências. É possível perceber que a frequência média para cada letra só foi deslocada, então se pode utilizar novamente a soma quadrática das frequências médias e obter:

$$\sum_{i=0}^{25} q_i^2 \approx \sum_{i=0}^{25} p_i^2 \approx 0.065. \tag{2.4}$$

Caso um período incorreto seja usado, a probabilidade de uma letra aparecer é a mesma para qualquer que seja letra, pois ela não seguirá nenhum padrão de escrita. Isso faz com que, no caso de erro:

$$\sum_{i=0}^{25} q_i^2 \approx \sum_{i=0}^{25} \left(\frac{1}{26}\right)^2 \approx 0.038. \tag{2.5}$$

Isso será necessário como ferramenta para descobrir o período t. O próximo passo será determinar um parâmetro $\tau = 1, 2, 3..$, que terá valores diferentes em cada passo do algoritmo e calculará várias somas quadráticas para diferentes períodos τ:

$$S_\tau = \sum_{i=0}^{25} q_i^2. \tag{2.6}$$

Se $\tau = t$, $S_\tau \approx 0.065$ e caso $\tau \neq t$, $S_\tau \approx 0.038$. Quando o período é encontrado, basta determinar, em seguida, o valor de cada caractere da chave fazendo uma permutação de 0 a 25. É possível melhorar o valor de τ utilizando uma segunda sequência $c_2, c_{2+\tau}, c_{2+2\tau}, ...$, uma terceira sequência e assim por diante.

O ataque apresentado é baseado no fato de que a chave terá um tamanho menor que o texto enviado e apresentará um período, mas caso a chave seja tão grande quanto o texto, o ataque a esse protocolo não será bem sucedido.

2.1.3 A cifra de uso único (*One-Time Pad*)

A cifra de uso único foi descrita em 1882 por Miller [24] e reinventada em 1917 por Vernam e Mauborgne [25]. Esta cifra é iniciada fixando-se um inteiro $l > 0$. O espaço de mensagens $\mathcal{M}$, o espaço de chaves $\mathcal{K}$ e o espaço de texto cifrados $\mathcal{C}$ possuem o mesmo tamanho $\{0,1\}^l$. Em seguida, os seguintes passos são executados:

1. O algoritmo Ger sorteia uma chave $k = \{0,1\}^l$ de uma distribuição uniforme, isto é, cada uma das 2^l chaves podem ser escolhidas com a mesma probabilidade 2^{-l};

2. O algoritmo Enc utiliza a chave k e uma mensagem $m \in \{0,1\}^l$, e envia um texto cifrado $c = k \oplus m$;

3. O algoritmo Dec recebe a chave $k \in \{0,1\}^l$ e o texto cifrado $c \in \{0,1\}^l$ e tem na saída uma mensagem $m = k \oplus c$;

onde $a \oplus b$ significa uma adição de módulo 2. Um exemplo do uso da cifra única seria:

Purotexto	0	1	1	1	0	1	1	0	0	1	1
Chave	1	1	0	0	0	1	0	1	0	0	1
Texto cifrado	1	0	1	1	0	0	1	1	0	1	0
Chave	1	1	0	0	0	1	0	1	0	0	1
Texto decifrado	0	1	1	1	0	1	1	0	0	1	1

É possível provar que a cifra de uso único é perfeitamente segura [20]. Isso significa que uma espiã, ao interceptar um texto cifrado, possui a mesma probabilidade de associá-lo a qualquer mensagem que poderia ser enviada. Essa segurança implica em algumas limitações do esquema. Uma delas está relacionada ao tamanho da chave utilizada que deve ser igual ao da mensagem. Outra limitação está no fato que a mesma chave não pode ser usada para duas mensagens diferentes, e agora fica evidente a razão do nome. Pois, suponha que um adversário intercepte duas mensagens $c = m \oplus k$ e $c' = m' \oplus k$, encriptadas com a mesma chave. Ele poderia realizar a seguinte operação:

$$c \oplus c' = (m \oplus k) \oplus (m' \oplus k) = m \oplus m',$$

e assim obter alguma informação das mensagens enviadas.

A cifra de uso único era o método principal de encriptação durante a Guerra Fria e um exemplo interessante dessa limitação do protocolo está em um projeto do governo norte-americano chamado *VENONA project*. O projeto era capaz de decifrar mensagens interceptadas da União Soviética devido a erros nos sorteios realizados pela URSS ao construir suas chaves. Partes de diferentes chaves se repetiam e permitiam que o governo americano utilizasse dessa falha para conseguir decifrar outras mensagens que utilizavam as mesmas partes repetidas. Esse erro na construção da chave soviética foi explorado por muitas décadas e um número grande de mensagens foram decifradas e elas podem ser encontradas no site do projeto [20, 26].

Como última curiosidade, provavelmente a utilização mais famosa dessa cifra, foi na comunicação entre o Kremlin e a Casa Branca através do famoso "telefone vermelho". Toda a comunicação que ocorria nesse canal era protegida pela cifra de uso único e era necessário que ambos os governos trocassem chaves extremamente longas através de mensageiros carregando maletas contendo as chaves.

2.2 Criptografia de chave assimétrica (ou de chave pública)

Na seção anterior, a criptografia de chave simétrica foi apresentada e, apesar de útil para certas aplicações, existem três situações que dificultam o uso desses protocolos. A primeira delas é na troca da chave entre os comunicadores. Como a chave é a mesma para encriptação e a decriptação, o sigilo dela será sempre um problema a ser considerado.

O método mais fácil seria trocar as chaves pessoalmente e isso é simples quando se trata de uma organização militar, mas qual a solução se dois comunicadores não possuírem tais recursos? O que levará direto ao segundo problema: a comunicação entre dois desconhecidos. Caso os comunicadores nem se conheçam e desejem realizar uma comunicação à distância pela primeira vez, como essa troca ocorreria se eles não puderem se encontrar pessoalmente? A garantia de um canal seguro ou um mensageiro confiável sairia caro para ambas as partes. O último empecilho surge quando se imagina a comunicação entre diversas pessoas. Imagine um servidor de uma empresa que estabelece um canal de comunicação entre N funcionários da empresa. Cada par de funcionários terão que ter sua própria chave e será necessário o segredo de um grande número chaves, pois cada um deles terá que manter o segredo de $N - 1$ chaves.

As respostas para essas limitações da criptografia surgiram com o trabalho de Diffie e Hellman [5]. A base da ideia parte do fato de que existem problemas chamados de assimétricos na computação. Eles são fáceis de serem computados em uma determinada direção, mas difíceis de serem invertidos. Isso faz com que dois comunicadores possam combinar uma chave em um canal público sem fazer com que o sigilo da mensagem seja perdido, pois uma chave diferente seria usada para a decifração. A praticidade desse novo método fica evidente ao aplicá-lo aos problemas anteriores. A comunicação entre partes desconhecidas e a necessidade de um canal privado ficarão facilitados já que uma das chaves poderá ser comunicada publicamente. No caso em que o protocolo é utilizado entre várias pessoas, o uso de uma chave pública facilitará a comunicação, já que só há a necessidade de se manter sigilo de uma chave privada para cada par de indivíduos.

Um protocolo de criptografia de chave pública é definido como uma sequência de algoritmos Ger, Enc, Dec tais que:

1. O algoritmo de geração de chave, Ger, recebe na entrada o parâmetro de segurança 1^n e tem na saída duas chaves: sk e pk. A primeira é chamada de chave privada e a segunda de chave pública. Ambas as chaves possuem tamanho n;

2. O algoritmo de encriptação, Enc, tem como entrada a chave pública pk e uma mensagem m. Como saída, ele escolherá probabilisticamente um determinado texto cifrado c entre todos os possíveis;

3. O algoritmo de decriptação, Dec, recebe como entrada um texto cifrado c e uma chave privada sk e tem na saída uma mensagem m ou um erro.

Como sempre, é requerido que $\text{Dec}_{sk}(\text{Enc}_{pk}(m)) = m$, a não ser que haja um erro com probabilidade negligenciável. A figura 3 apresenta uma visualização de um esquema de criptografia de chave pública sendo utilizado por Alice e Bob. Existem diversos protocolos de chave pública que estão disponíveis ao leitor no livro de Katz e Lindell [20].

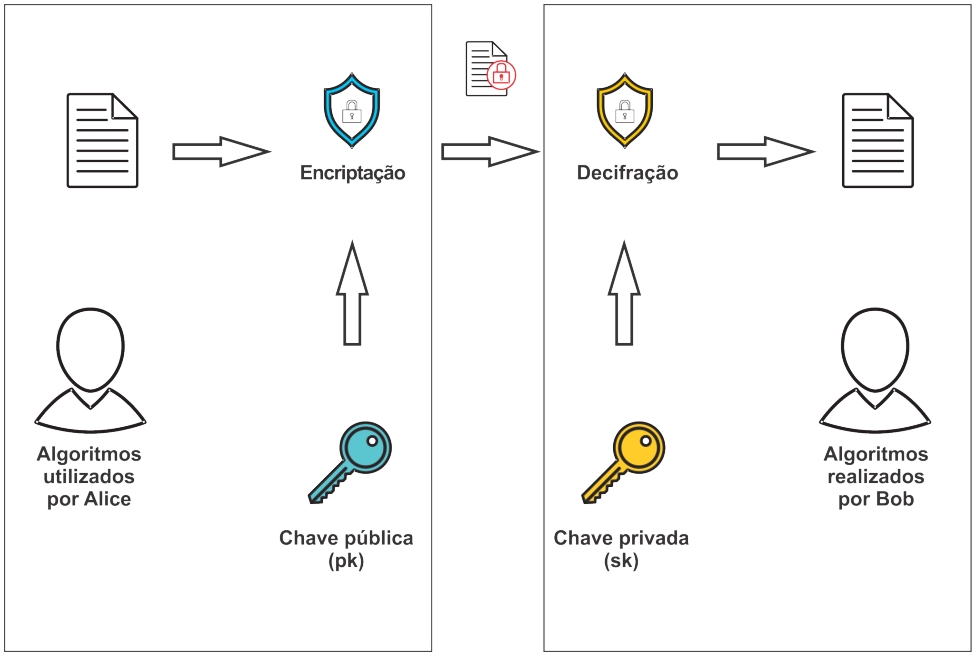

Figura 3 – Diagrama representando um esquema geral de criptografia de chave pública. Alice deseja enviar uma mensagem para Bob e, para garantir sua segurança, ela utiliza uma chave pública *pk* criada por Bob. A mensagem é enviada a Bob que, ao recebê-la, utiliza uma chave privada *sk* para decriptar a mensagem.

2.2.1 O algoritmo RSA

O protocolo RSA foi desenvolvido por Rivest, Shamir e Adleman em 1978 [6]. Ele se baseia na dificuldade computacional em fatorar um número primo N. No protocolo se assume que $N = pq$, onde p e q são dois números primos. Então, o protocolo RSA é definido como:

1. O algoritmo Ger recebe como entrada o parâmetro de segurança n no formato 1^n e tem como saída (N, e, d), onde (e, d) são dois inteiros. A chave pública será (N, e) e a chave privada (N, d);

2. O algoritmo Enc recebe a chave pública e uma mensagem m e obtém o texto cifrado c tal que $c = [m^e \bmod N]$;

3. O algoritmo Dec utilizará a chave privada e o texto cifrado c e obtém a mensagem m tal que $m = [c^d \bmod N]$.

É possível perceber um problema evidente no protocolo apresentado. No início do capítulo foi enfatizada a necessidade do algoritmo Enc ser probabilístico para impedir que o protocolo envie sempre o mesmo texto cifrado para a mesma mensagem. O RSA apresentado acima não cumpre essa regra e, consequentemente, possui uma brecha na segurança. O estudo do RSA foi realizado por muito tempo e variações foram criadas para atender essa e outras brechas de segurança. Ao leitor interessado novamente é indicado o livro de Katz e Lindell [20].

É possível que exista uma maneira de resolver o problema RSA que o torne fácil, apesar da fatoração continuar difícil. Classicamente, acredita-se que isso seja improvável, porém, com a existência de um computador quântico, a fatoração se torna facilmente resolvível com o algoritmo de Shor [14]. O computador quântico, então, tornaria todos os protocolos RSA inseguros.

2.3 QKD e a criptografia clássica

Após essa breve apresentação, já é possível responder a uma pergunta importante: onde se encaixa a QKD dentro da criptografia clássica? Como será apresentado mais a frente, ela só é capaz de gerar chaves iguais para os dois usuários do protocolo. Logo, a QKD só poderia ser aplicada dentro de um esquema de criptografia de chave privada. Os algoritmos utilizados nesse esquema se tornariam então:

1. Ger irá gerar uma chave k utilizando a QKD;
2. Enc utiliza k para encriptar;
3. Dec utiliza k para decifrar.

A figura 4 apresenta um diagrama resumindo os algoritmos utilizados no esquema.

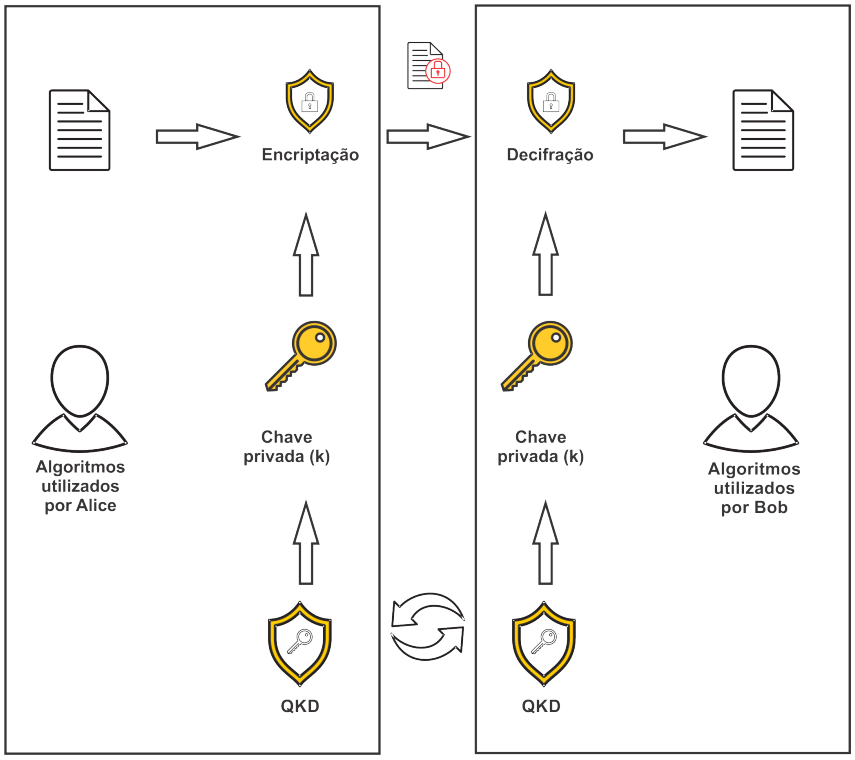

Figura 4 – Diagrama representando um esquema geral de criptografia de chave privada utilizando a QKD. Alice deseja enviar uma mensagem para Bob e, para garantir sua segurança, ela utiliza uma chave k criada em conjunto com Bob através da QKD. A mensagem é enviada a Bob que, ao recebê-la, utiliza a mesma chave k para decifrar a mensagem.

Os protocolos de QKD utilizam os próprios postulados da mecânica quântica para garantir que as chaves permaneçam secretas e eles podem ser implementados a distância pelos usuários. Então, fica evidente o interesse neles, pois são uma possível solução ao problema de comunicação a longas distâncias dos esquemas de chave privada. Além disso, os protocolos quânticos tem uma vantagem adicional que é a possibilidade de detecção de uma espiã no processo de geração de chaves. Esses conceitos serão revisitados mais a frente com mais detalhes.

3 Conceitos básicos de mecânica quântica

Até agora, apenas protocolos criptográficos clássicos foram discutidos e, consequentemente, somente noções clássicas eram requeridas. Porém, ao introduzir protocolos quânticos, algumas noções de mecânica quântica serão necessárias para entender tanto a razão de sua segurança quanto as estratégias de ataque. Portanto, esse é o intuito desse capítulo onde será discutido o qubit, as medições generalizadas, o teorema da não-clonagem e as estratégias de discriminação de estados quânticos.

3.1 O qubit

O bit clássico pode ser relacionado a duas coisas distintas. Ele corresponde à unidade de informação e a uma abstração de todo sistema clássico de dois estados. A conexão vem do fato que um sistema clássico de dois estados pode carregar no máximo um bit de informação. Um exemplo seria o apertar de um botão: quando o botão é acionado o sistema recebe o bit 1 e, no caso contrário, o bit 0.

O qubit representa qualquer sistema quântico de dois níveis, como a polarização de um fóton ou o spin de um elétron. Os estados são subespaços de um espaço de Hilbert bidimensional. Nesse espaço, pode-se utilizar dois estados ortogonais, $|0\rangle$ e $|1\rangle$, para construir todos os outros estados possíveis para o sistema. Desse fato, surge a diferença entre o clássico e o quântico: enquanto $bit = \{0, 1\}$, estados quânticos podem ser descritos por uma combinação linear de $|0\rangle$ e $|1\rangle$. Apesar dessa diversidade na representação, a informação contida no qubit será sempre obtida através de uma medição e resultará em 0 ou 1 com uma determinada probabilidade [27].

O estado puro mais geral de um qubit pode ser escrito como:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\,, \tag{3.1}$$

onde $0 \leq \phi \leq 2\pi$ e $0 \leq \theta \leq \pi$. As constantes ϕ e θ representarão os ângulos azimutal e polar, respectivamente, de um vetor com módulo 1 em uma esfera. Os pontos na casca da esfera serão estados puros e os pontos antipodais representam estados ortogonais. A figura 5 ilustra esta esfera conhecida como esfera de Bloch. Uma consequência dessa representação na esfera de Bloch é o fato que toda unitária aplicada a um estado puro $|\psi\rangle$ tem como resultado uma rotação e/ou reflexão na esfera para um estado $|\psi'\rangle$. Essa visualização se torna útil para a interpretação de algumas transformações unitárias que serão apresentadas mais a frente.

A matriz densidade representa uma mistura estatística dos estados para um determinado sistema quântico. No espaço de Hilbert bidimensional, ela também pode ser

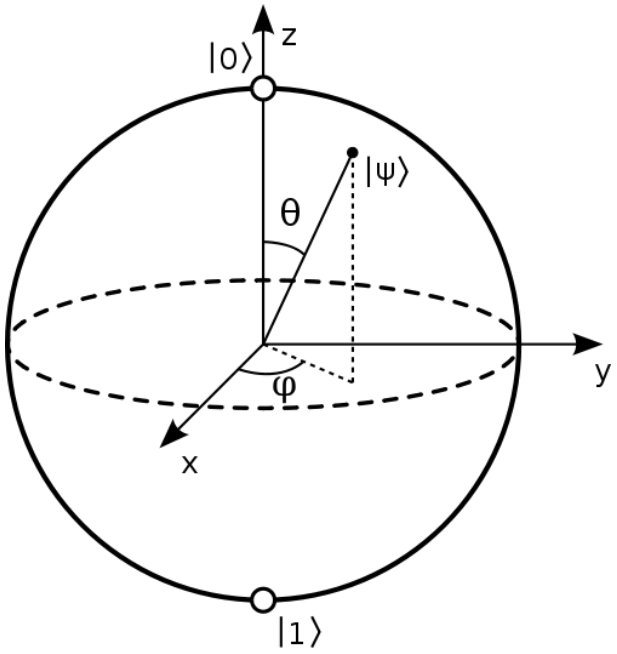

Figura 5 – Representação de um estado puro ψ na esfera de Bloch.

descrita em termos dos ângulos na esfera de Bloch e será dada por:

$$\hat{\rho} = \frac{1}{2}(\hat{I} + \vec{r}.\vec{\hat{\sigma}}), \tag{3.2}$$

onde $\vec{r}$ representa um vetor na esfera de Bloch, $\hat{I}$ é a matriz identidade e $\vec{\hat{\sigma}}$ é o vetor das matrizes de Pauli $\hat{\sigma}_x, \hat{\sigma}_y$ e $\hat{\sigma}_z$ que são definidas como:

$$\hat{\sigma}_x = |0\rangle\langle 1| + |1\rangle\langle 0|\,, \tag{3.3}$$

$$\hat{\sigma}_y = i\,|1\rangle\langle 0| - i\,|0\rangle\langle 1|\,, \tag{3.4}$$

$$\hat{\sigma}_z = |0\rangle\langle 0| - |1\rangle\langle 1|\,. \tag{3.5}$$

A utilização das matrizes de Pauli surge naturalmente, pois qualquer matriz quadrada com quatro elementos pode ser escrita como uma combinação linear das matrizes de Pauli e da identidade.

3.2 Teorema da não-clonagem

Classicamente, não há limite quando se trata de clonar um sinal e isto é, inclusive, parte de vários processos de comunicação. O uso de repetidoras para transmissões de rádio e TV é uma parte fundamental para o funcionamento das telecomunicações. Uma espiã quando está interrompendo uma comunicação que utiliza meios clássicos pode interceptar um sinal, cloná-lo e reenviá-lo sem ser notada. A mesma pergunta pode ser levantada quando se trata um sistema quântico: é possível clonar qualquer estado quântico?

O teorema da não-clonagem [28, 29] surgiu como uma resposta a essa pergunta. Suponha que existam dois sistemas A e B que realizam o processo de clonagem. No

primeiro, um estado $|\psi\rangle$ será enviado e, no segundo, a cópia será realizada utilizando uma unitária U. Assim:

$$\hat{U}\Big(\,|\psi\rangle \otimes |s\rangle\,\Big) = |\psi\rangle \otimes |\psi\rangle\,, \tag{3.6}$$

onde $|s\rangle$ o estado inicial do sistema B. O objetivo dessa máquina seria clonar qualquer estado quântico que ela recebesse. Então caso $|\phi\rangle$ seja enviado ao invés de $|\psi\rangle$, ela também deveria ser capaz de copiá-lo. Colocando isso em linguagem matemática:

$$\hat{U}\Big(\,|\psi\rangle \otimes |s\rangle\,\Big) = |\psi\rangle \otimes |\psi\rangle\,, \tag{3.7}$$

$$\hat{U}\Big(\,|\phi\rangle \otimes |s\rangle\,\Big) = |\phi\rangle \otimes |\phi\rangle\,. \tag{3.8}$$

O problema dessa operação surge ao se realizar o produto interno das duas equações acima. Ele será dado por:

$$\begin{aligned} \langle\phi| \otimes \langle s|\, \hat{U}^\dagger \hat{U}\, |\psi\rangle \otimes |s\rangle &= \langle\phi| \otimes \langle\phi|\psi\rangle \otimes |\psi\rangle \\ \langle\phi|\psi\rangle\, \langle s|s\rangle &= \langle\phi|\psi\rangle\, \langle\phi|\psi\rangle \\ \langle\phi|\psi\rangle &= (\langle\phi|\psi\rangle)^2, \end{aligned} \tag{3.9}$$

As únicas soluções possíveis para a equação (3.9) são $\langle\phi|\psi\rangle = 0$ ou $\langle\phi|\psi\rangle = 1$. Ou seja, a clonagem só seria possível para um sistema quântico se os estados enviados fossem sempre iguais ou ortogonais. Isso faz com que a clonagem perfeita de estados não-ortogonais seja impossível.

O leitor pode se perguntar: e se estados mistos ou transformações não-unitárias fossem utilizadas? Em [30], Barnum *et al.* provaram que mesmo alterando essas condições, o teorema da não-clonagem ainda é válido e a clonagem perfeita não pode ser realizada. O tema ainda é bastante estudado e apesar da clonagem perfeita ser impossível, pesquisadores conseguiram obter clonagens com fidelidades ótimas [31–33] ou clonagem perfeita com uma determinada probabilidade de sucesso [34].

3.3 Medições quânticas

A informação é extraída de um sistema quântico através de medições. Quando são fisicamente realizáveis, elas podem ser tratadas dentro do formalismo de medida com valores em operadores positivos (POVM[1]). O POVM é um conjunto de operadores $\hat{\Pi}_m$, chamados elementos do POVM, que devem satisfazer as seguintes condições:

$$\forall m, \qquad \hat{\Pi}_m^\dagger = \hat{\Pi}_n; \tag{3.10}$$

$$\hat{\Pi}_m \geq 0; \tag{3.11}$$

$$\sum_m \hat{\Pi}_m = \hat{I}. \tag{3.12}$$

[1] Do inglês *Positive-Operator Valued Measure*.

Os operadores podem ou não serem formados por estados ortonormais. O primeiro caso é uma particularidade do segundo e é denominado medição projetiva enquanto o caso geral é chamado de medição generalizada [10, 11].

A probabilidade P_m de se obter um resultado m na medição, dado um estado qualquer $\hat{\rho}$, será:

$$P_m = \mathrm{Tr}(\hat{\rho}\hat{\Pi}_m). \tag{3.13}$$

Os elementos do POVM podem ser representados por operadores de detecção da seguinte maneira:

$$\hat{\Pi}_m = \hat{A}_m^\dagger \hat{A}_m. \tag{3.14}$$

Como todo estado quântico se transforma após uma medição, essa representação dos operadores será importante para definir como isso ocorre. Caso o resultado da medição seja conhecido, a transformação será da seguinte maneira:

$$\hat{\rho} \to \hat{\rho}'_m = \frac{\hat{A}_m \hat{\rho} \hat{A}_m^\dagger}{P_m}, \tag{3.15}$$

e no caso contrário, a transformação será:

$$\hat{\rho}' = \sum_m P_m \hat{\rho}'_m = \sum_m \hat{A}_m \hat{\rho} \hat{A}_m^\dagger. \tag{3.16}$$

3.4 Estratégias de discriminação de estados não-ortogonais

No contexto de criptografia quântica, a seguinte situação ocorrerá: Alice preparará de modo aleatório um entre dois estados não-ortogonais $|\psi_0\rangle$ e $|\psi_1\rangle$ que serão enviados para Bob. Eva espionará o canal e será bem sucedida quando ela conseguir determinar qual estado foi enviado por Alice. Suponha que ela tente adotar uma estratégia que distingue com certeza absoluta entre esses dois estados. Caso ela exista, haverá dois operadores $\hat{\Pi}_0$ e $\hat{\Pi}_1$, de tal forma que:

$$\hat{\Pi}_0 |\psi_1\rangle = 0, \tag{3.17}$$

$$\hat{\Pi}_1 |\psi_0\rangle = 0. \tag{3.18}$$

Esses operadores devem atender aos critérios de uma medição generalizada, então:

$$\hat{\Pi}_0 + \hat{\Pi}_1 = \hat{I}. \tag{3.19}$$

Se a equação (3.19) for multiplicada à esquerda por $\langle\psi_0|$ e à direita por $|\psi_1\rangle$:

$$\begin{aligned} \langle\psi_0| \hat{I} |\psi_1\rangle &= \langle\psi_0| \hat{\Pi}_0 |\psi_1\rangle + \langle\psi_0| \hat{\Pi}_1 |\psi_1\rangle \\ \langle\psi_0|\psi_1\rangle &= 0, \end{aligned} \tag{3.20}$$

onde as equações (3.17) e (3.18) foram utilizadas. Assim, a estratégia só será possível para estados ortogonais, mas isso é impossível já que, por definição, eles são não-ortogonais.

Consequentemente, outras estratégias de discriminação foram pensadas, mas todas elas possuem uma probabilidade de erro ou falha. A literatura sobre esse tema é extensa [11, 35–38]. Nessa obra, quatro estratégias serão abordadas: a discriminação com erro mínimo [39], a discriminação sem ambiguidade [40–44], a discriminação com confiança máxima [45] e a separação de estados [46–48].

3.4.1 Discriminação com erro mínimo

Na seção passada, a impossibilidade da discriminação sem erro entre dois estados puros não-ortogonais, $|\psi_0\rangle$ e $|\psi_1\rangle$, foi mostrada. O caminho seguinte, mais natural a ser tomado, é desenvolver um método que minimize a probabilidade média de erro da medição. Essa estratégia é chamada de discriminação com erro mínimo e dois exemplos serão apresentados: para dois e três estados não-ortogonais de um qubit.

Discriminação com erro mínimo para dois estados não-ortogonais

Alice enviará para Bob um entre dois estados não-ortogonais, $|\psi_0\rangle$ e $|\psi_1\rangle$, o primeiro com probabilidade p_0 e o segundo com probabilidade p_1. A partir de agora, e para todas as seções seguintes, as probabilidades de envio serão consideradas iguais, ou seja, $p_0 = p_1 = \frac{1}{2}$. Bob utilizará um POVM com dois elementos dados por $\hat{\Pi}_0$ e $\hat{\Pi}_1$, sendo que o primeiro terá ω_0 como resultado se o estado enviado for $|\psi_0\rangle$ e o segundo ω_1 caso o estado enviado seja $|\psi_1\rangle$. Existe a possibilidade de Bob errar e obter ω_0 (ω_1) na sua medição, mas o estado enviado ter sido $|\psi_1\rangle$ ($|\psi_0\rangle$). A probabilidade média de que um erro ocorra será:

$$\begin{aligned} P_{\text{err}} &= P(\psi_0)P(\omega_1|\psi_0) + P(\psi_1)P(\omega_0|\psi_1) \\ &= \frac{1}{2}\langle\psi_0|\hat{\Pi}_1|\psi_0\rangle + \frac{1}{2}\langle\psi_1|\hat{\Pi}_0|\psi_1\rangle \\ &= \frac{1}{2} - \text{Tr}\left[\left(\frac{1}{2}|\psi_0\rangle\langle\psi_0| - \frac{1}{2}|\psi_1\rangle\langle\psi_1|\right)\hat{\Pi}_0\right], \end{aligned} \tag{3.21}$$

onde foi usada a equação (3.12). O objetivo é minimizar P_{err}, então quanto maior o valor do traço na equação (3.21), menor será o erro médio. Esse valor máximo será obtido quando $\hat{\Pi}_0$ for composto por autoestados com maior autovalor do operador $\frac{1}{2}|\psi_0\rangle\langle\psi_0| - \frac{1}{2}|\psi_1\rangle\langle\psi_1|$.

Os estados $|\psi_0\rangle$ e $|\psi_1\rangle$ serão escritos como:

$$|\psi_0\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle, \tag{3.22}$$

$$|\psi_1\rangle = \cos\theta|0\rangle - \sin\theta|1\rangle, \tag{3.23}$$

onde $0 \leq \theta \leq \frac{\pi}{4}$. Os autovalores do operador $\frac{1}{2}|\psi_0\rangle\langle\psi_0| - \frac{1}{2}|\psi_1\rangle\langle\psi_1|$ para esse caso serão:

$$\lambda_\pm = \pm\frac{1}{2}\sin 2\theta. \tag{3.24}$$

A probabilidade média de erro, utilizando λ_+ da equação (3.24) na equação (3.21), será o denominado limite de Helstrom [39]:

$$P_{\text{err}} = \frac{1}{2}(1 - \sin 2\theta). \tag{3.25}$$

A figura 6 apresenta o gráfico para essa probabilidade média de erro em função de θ.

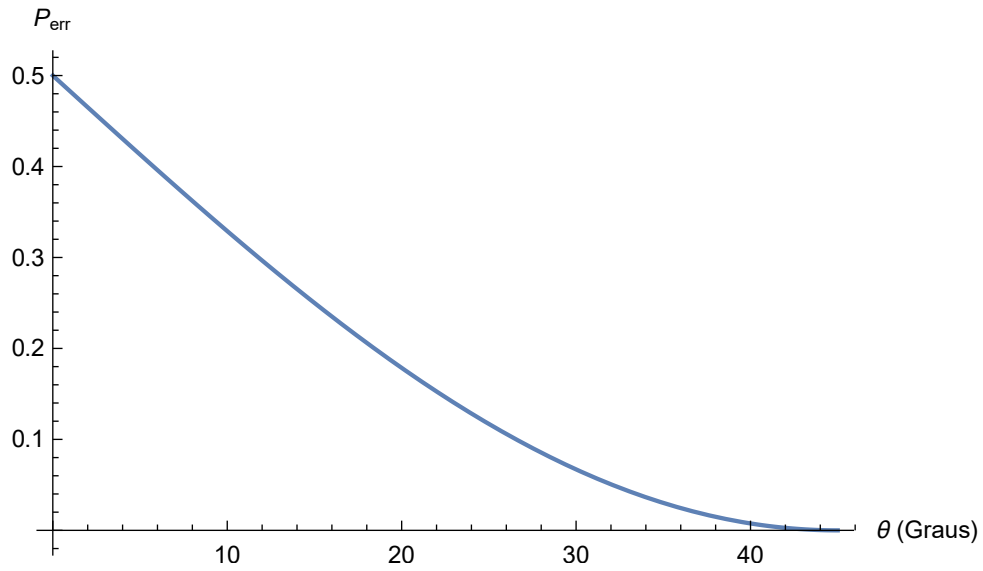

Figura 6 – Gráfico da probabilidade de erro para a discriminação com erro mínimo entre dois estados não-ortogonais.

Nesse caso, a medição será projetiva e os elementos do POVM serão projetores nos seguintes estados:

$$\hat{\Pi}_0^{\text{EM}} = |+\rangle\langle+|\,, \tag{3.26}$$

$$\hat{\Pi}_1^{\text{EM}} = |-\rangle\langle-|\,, \tag{3.27}$$

onde $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ e $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. O superíndice EM do operador tem sua origem no nome da estratégia. A figura 7 ilustra os estados enviados por Alice e os estados que serão utilizados como projetores para a medição.

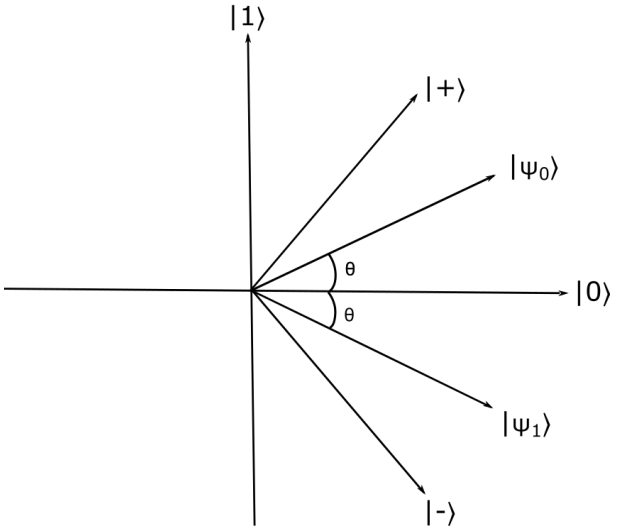

Figura 7 – A medição ótima para distinguir entre os dois estados $|\psi_0\rangle$ e $|\psi_1\rangle$ é uma medição projetiva. No caso em que as probabilidades de envio são iguais, as projeções serão dadas pelos estados $|+\rangle$ e $|-\rangle$.

Discriminação com erro mínimo para três estados não-ortogonais

Considere um conjunto de três estados não ortogonais igualmente prováveis dados por:

$$|\psi_0\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle\,, \tag{3.28}$$

$$|\psi_1\rangle = \cos\theta\,|0\rangle + e^{\frac{2\pi i}{3}}\sin\theta\,|1\rangle\,, \tag{3.29}$$

$$|\psi_2\rangle = \cos\theta\,|0\rangle + e^{\frac{-2\pi i}{3}}\sin\theta\,|1\rangle\,, \tag{3.30}$$

onde $0 \leq \theta \leq \frac{\pi}{4}$. A obtenção da probabilidade de discriminação com erro mínimo e do POVM ótimo correspondente, para esses estados, não é tão trivial como no caso anterior. Os elementos do POVM foram obtidos por Ban *et al.* [49] e são:

$$\hat{\Pi}_j^{\mathrm{EM}} = \frac{2}{3}\,|\phi_j\rangle\langle\phi_j|\,, \tag{3.31}$$

onde os estados $|\phi_j\rangle$ são:

$$|\phi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tag{3.32}$$

$$|\phi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{\frac{2\pi i}{3}}\,|1\rangle), \tag{3.33}$$

$$|\phi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{\frac{-2\pi i}{3}}\,|1\rangle). \tag{3.34}$$

Os estados $|\psi_j\rangle$ enviados por Alice (vermelho) e os $|\phi_j\rangle$ que são utilizados na medição (azuis) estão representados na figura 8. A probabilidade média de erro será:

$$P_{\mathrm{err}} = \frac{2}{3}\left(1 - \frac{\sin 2\theta}{2}\right); \tag{3.35}$$

e ela é apresentada na figura 9 em função de θ.

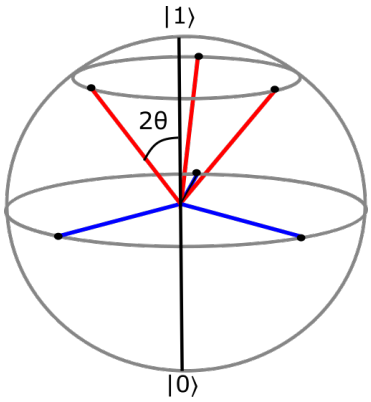

Figura 8 – A medição ótima para distinguir entre os três estados $|\psi_0\rangle$, $|\psi_1\rangle$ e $|\psi_2\rangle$ é uma medição generalizada proporcional aos projetores dos estados $|\phi_0\rangle$, $|\phi_1\rangle$ e $|\phi_2\rangle$. Nessa figura, os estados azuis são os estados da medição e os estados vermelhos são os estados enviados por Alice.

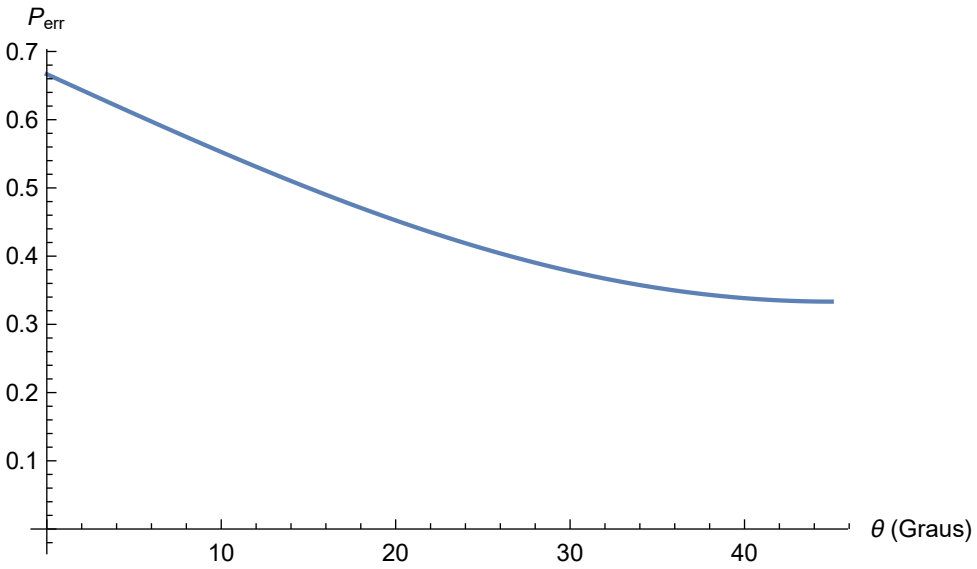

Figura 9 – Gráfico da probabilidade de erro para a discriminação com erro mínimo entre três estados não-ortogonais e igualmente prováveis.

3.4.2 Discriminação sem ambiguidade

Na discriminação sem ambiguidade, Bob não poderá cometer um erro na identificação dos estados enviados por Alice. Como foi visto no início dessa seção, essa tarefa é impossível para estados não-ortogonais. Porém, suponha que um dos possíveis resultados da medição de Bob possa ser uma falha (também chamado de resultado inconclusivo). Quando ela ocorrer, ele não poderá inferir qual estado foi enviado. Generalizando os resultados da equação (3.19), os seguintes elementos de POVM serão dados:

$$\hat{\Pi}_0^{\mathrm{SA}} + \hat{\Pi}_1^{\mathrm{SA}} + \hat{\Pi}_F^{\mathrm{SA}} = \hat{I}, \tag{3.36}$$

onde o superíndice SA indica a estratégia de discriminação sem ambiguidade. Os dois primeiros distinguirão entre os dois estados, mas o terceiro elemento ($\hat{\Pi}_F^{\mathrm{SA}}$) está relacionado a uma medição inconclusiva. Esse resultado não é considerado um erro quando se trata de discriminação, pois não é possível inferir nada sobre os estados enviados. Porém, quando

Eva aplicar essa estratégia em QKD, não existirá a possibilidade de interceptação de um estado sem reenviá-lo para Bob. Consequentemente, a falha forçará um sorteio entre os possíveis estados e ocasionará uma chance de erro na espionagem.

Chefles mostrou em [44] que a discriminação sem ambiguidade só é possível para estados linearmente independentes. Portanto, os três estados apresentados nas equações (3.28-3.30) não podem ser utilizados na estratégia dessa subseção.

Discriminação sem ambuiguidade para dois estados não-ortogonais

Suponha que Alice envie para Bob um entre os seguintes estados:

$$|\psi_0\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle\,, \tag{3.37}$$

$$|\psi_1\rangle = \cos\theta\,|0\rangle - \sin\theta\,|1\rangle\,. \tag{3.38}$$

Necessita-se que os elementos de POVM satisfaçam $\langle\psi_0|\,\hat{\Pi}_1\,|\psi_0\rangle = \langle\psi_1|\,\hat{\Pi}_0\,|\psi_1\rangle = 0$. A representação na esfera de Bloch se torna conveniente, pois estados antipodais serão sempre ortogonais. Aplicando uma rotação nas equações (3.37) e (3.38), é possível obter os operadores que serão projeções nos estados ortogonais aos enviados por Alice:

$$\hat{\Pi}_0^{\mathrm{SA}} = a_0(\sin\theta\,|0\rangle + \cos\theta\,|1\rangle)(\sin\theta\,\langle 0| + \cos\theta\,\langle 1|), \tag{3.39}$$

$$\hat{\Pi}_1^{\mathrm{SA}} = a_1(\sin\theta\,|0\rangle - \cos\theta\,|1\rangle)(\sin\theta\,\langle 0| - \cos\theta\,\langle 1|), \tag{3.40}$$

onde $0 \leq a_0, a_1 \leq 1$. Esses operadores não formam um conjunto completo para nenhuma escolha de a_0 e a_1. Logo, surgirá a necessidade do operador de medição inconclusiva que será dado por:

$$\hat{\Pi}_F^{\mathrm{SA}} = \hat{I} - \hat{\Pi}_0^{\mathrm{SA}} - \hat{\Pi}_1^{\mathrm{SA}}. \tag{3.41}$$

A probabilidade média de se obter um resultado inconclusivo será:

$$P_F = \frac{1}{2}\langle\psi_0|\,\Pi_F^{\mathrm{SA}}\,|\psi_0\rangle + \frac{1}{2}\langle\psi_1|\,\Pi_F^{\mathrm{SA}}\,|\psi_1\rangle = 1 - \frac{\sin 2\theta}{2}(a_0 + a_1). \tag{3.42}$$

O resultado ótimo será obtido através de uma minimização da equação (3.42) submetido aos vínculos $a_0, a_1 \geq 0$ e $\hat{\Pi}_F^{\mathrm{SA}} \geq 0$. No caso em questão, a probabilidade mínima de falha é o limite de Ivanovic-Dieks-Peres (IDP) [40–42] dado por:

$$P_F = |\langle\psi_0|\psi_1\rangle| = \cos 2\theta. \tag{3.43}$$

Após descoberto os valores ótimos de a_0 e a_1, os operadores se tornam:

$$\hat{\Pi}_0^{\mathrm{SA}} = \frac{1}{2\cos^2\theta}(\sin\theta\,|0\rangle + \cos\theta\,|1\rangle)(\sin\theta\,\langle 0| + \cos\theta\,\langle 1|), \tag{3.44}$$

$$\hat{\Pi}_1^{\mathrm{SA}} = \frac{1}{2\cos^2\theta}(\sin\theta\,|0\rangle - \cos\theta\,|1\rangle)(\sin\theta\,\langle 0| - \cos\theta\,\langle 1|), \tag{3.45}$$

$$\hat{\Pi}_F^{\mathrm{SA}} = (1 - \tan^2\theta)\,|0\rangle\langle 0|\,. \tag{3.46}$$

A figura 10 apresenta a probabilidade de resultado inconclusivo em função de θ.

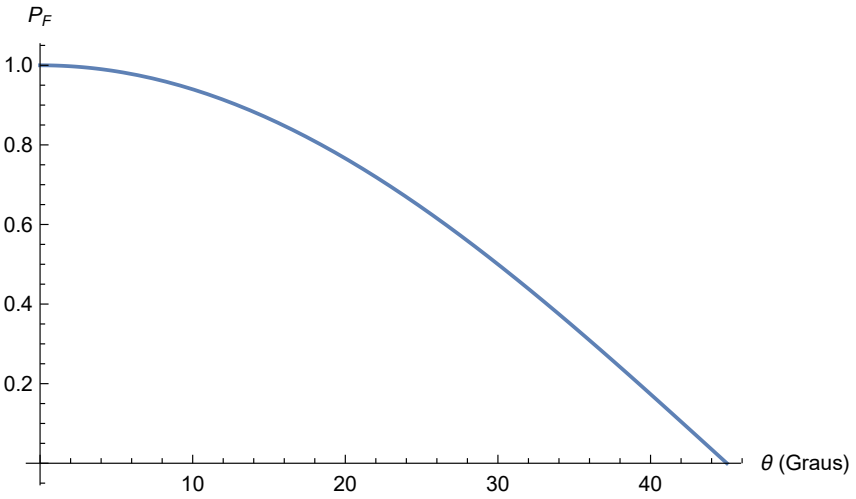

Figura 10 – Gráfico da probabilidade de falha para a discriminação sem ambiguidade entre dois estados não-ortogonais.

3.4.3 Discriminação com confiança máxima

A discriminação sem ambiguidade, apresentada na seção anterior, é um caso particular de uma estratégia mais geral denominada discriminação com confiança máxima [45, 50]. Ela se aplica a estados linearmente dependentes e o seu objetivo é maximizar a confiança de que o estado $\hat{\rho}_i$ foi identificado, dado que ω_i foi observado como resultado da medição. Matematicamente, a confiança será dada por:

$$\begin{aligned} P(\hat{\rho}_i|\omega_i) &= \frac{P(\hat{\rho}_i)P(\omega_i|\hat{\rho}_i)}{P(\hat{\rho}_i)} \\ &= \frac{p_i \mathrm{Tr}(\hat{\rho}_i \hat{\Pi}_i^{\mathrm{CM}})}{\mathrm{Tr}(\hat{\rho}\hat{\Pi}_i^{\mathrm{CM}})}, \end{aligned} \tag{3.47}$$

onde p_i é a probabilidade de preparação e $\hat{\Pi}_i^{CM}$ é o elemento do POVM associado ao resultado ω_i. No caso de estados puros, esses operadores são dados por [45]:

$$\hat{\Pi}_i^{\mathrm{CM}} \propto \hat{\rho}^{-1}\hat{\rho}_i\hat{\rho}^{-1}. \tag{3.48}$$

A proporcionalidade presente na equação (3.48) é devido ao fato que os operadores podem possuir uma constante multiplicativa. Isso é uma consequência direta da equação (3.47), pois o elemento do POVM está presente tanto no denominador quanto no numerador.

A estratégia dessa subseção, quando utilizada para identificar entre estados linearmente independentes, se assemelhará a discriminação sem ambiguidade. Para evitar redundâncias, a discriminação com confiança máxima será aplicada somente para três estados linearmente dependentes.

Discriminação com confiança máxima para três estados não-ortogonais

A discriminação com confiança máxima será ilustrada utilizando o conjunto de três estados igualmente prováveis das equações (3.28-3.30) . Os elementos do POVM podem

ser encontrados a partir da equação (3.48) e eles são dados por:

$$\hat{\Pi}_i^{\mathrm{CM}} = a_i \left|\mu_i\right\rangle\!\left\langle\mu_i\right|, \tag{3.49}$$

onde a_i é uma constante a ser determinada e os estados $\{|\mu_i\rangle\}$ são dados por:

$$|\mu_0\rangle = \sin\theta\,|0\rangle + \cos\theta\,|1\rangle\,, \tag{3.50}$$

$$|\mu_1\rangle = \sin\theta\,|0\rangle + e^{\frac{2\pi i}{3}}\cos\theta\,|1\rangle\,, \tag{3.51}$$

$$|\mu_2\rangle = \sin\theta\,|0\rangle + e^{-\frac{2\pi i}{3}}\cos\theta\,|1\rangle\,. \tag{3.52}$$

Utilizando os operadores da equação (3.49), a confiança máxima se torna:

$$P_{\max}(\hat{\rho}_i|\omega_i) = \frac{2}{3}, \tag{3.53}$$

para qualquer estado $|\psi_i\rangle$. A figura 11 apresenta a visualização na esfera de Bloch dos três estados usados (verde) para se obter a medição com confiança máxima. Na figura é possível ver também os estados utilizados na estratégia com erro mínimo (azul) e os estados enviados por Alice (vermelho).

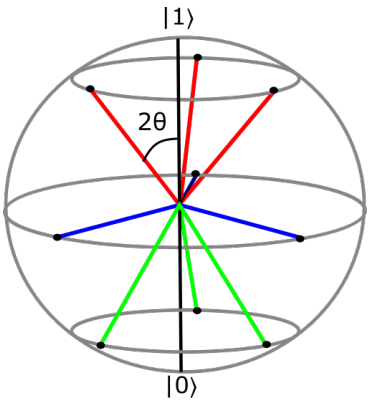

Figura 11 – A medição com erro mínimo para distinguir entre os três estados $|\psi_i\rangle$, $|\psi_1\rangle$ e $|\psi_2\rangle$ (vermelho) é uma medição generalizada proporcional aos projetores dos estados $|\phi_0\rangle$, $|\phi_1\rangle$ e $|\phi_2\rangle$ (azul). Quando a estratégia utilizada é a com confiança máxima, a medição generalizada se torna proporcional aos projetores dos estados $|\mu_0\rangle$, $|\mu_1\rangle$ e $|\mu_2\rangle$ (verde).

Os operadores $\hat{\Pi}_i^{\mathrm{CM}}$ não formam um conjunto completo para nenhum valor de a_i e uma medição inconclusiva será necessária. A maneira usual de se obter o operador de falha é:

$$\hat{\Pi}_F^{\mathrm{CM}} = \hat{I} - \sum_i \hat{\Pi}_i^{\mathrm{CM}}, \tag{3.54}$$

e a probabilidade de uma falha será dada por:

$$P_F = \mathrm{Tr}(\hat{\rho}\hat{\Pi}_F^{\mathrm{CM}}) = 1 - 2(a_0 + a_1 + a_2)\cos^2\theta\sin^2\theta, \tag{3.55}$$

onde $\hat{\rho} = \sum_i \hat{\rho}_i$. Como pode ser visto, a probabilidade de falha depende das constantes a_i e uma otimização é realizada para minimizá-la. Isso é feito utilizando o vínculo $\hat{\Pi}_F^{\mathrm{CM}} \geq 0$ e

notando que a probabilidade é uma função monotonicamente decrescente, ou seja, quanto maior o valor dos a_i, menor ela será. É possível mostrar que:

$$a_0 = a_1 = a_2 = \frac{1}{3\cos^2\theta}, \tag{3.56}$$

e a probabilidade de falha se torna:

$$P_F = \cos 2\theta. \tag{3.57}$$

Os operadores $\hat{\Pi}_i^{\mathrm{CM}}$ e $\hat{\Pi}_F^{\mathrm{CM}}$ serão, respectivamente:

$$\hat{\Pi}_i^{\mathrm{CM}} = \frac{1}{3\cos^2\theta}\,|\mu_i\rangle\langle\mu_i|\,, \tag{3.58}$$

$$\hat{\Pi}_F^{\mathrm{CM}} = (1-\tan^2\theta)\,|0\rangle\langle 0|\,. \tag{3.59}$$

É interessante comparar a estratégia com confiança máxima e a discriminação com erro mínimo. Bob, ao receber um estado de Alice, deverá escolher entre uma delas. Caso escolha a primeira, dado um resultado conclusivo, ele terá a maior confiança possível na identificação do estado enviado por Alice. Já com o erro mínimo, a confiança dele será menor, entretanto, a média do erro será menor. Isso se deve ao fato que a discriminação com confiança máxima possui uma probabilidade de falhar e quando Bob obtiver resultados inconclusivos, ele não saberá dizer qual o estado foi enviado por Alice. A figura 12 ilustra esses fatos através dos gráficos com a confiança (esquerda) e a probabilidade média de erro (direita). A linha contínua azul corresponde à estratégia com erro mínimo e a linha tracejada vermelha corresponde à estratégia com confiança máxima.

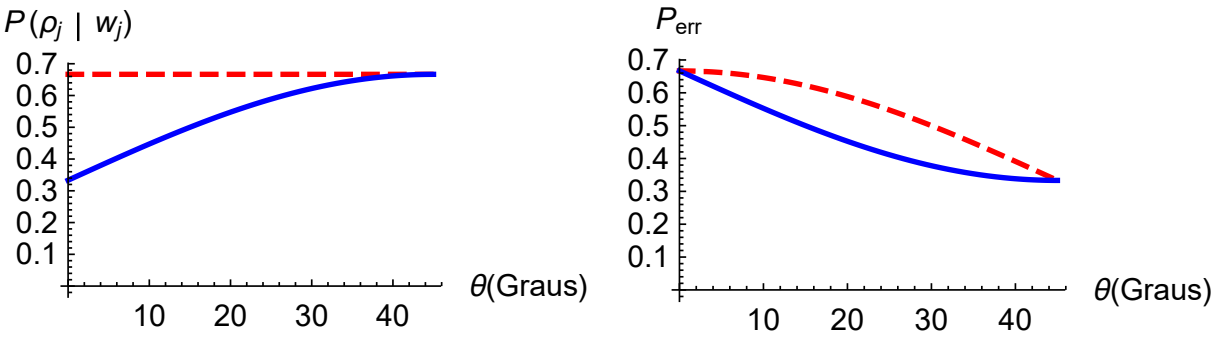

Figura 12 – Comparação entre a discriminação com erro mínimo (linha contínua azul) e a discriminação com confiança máxima (linha tracejada vermelha). O gráfico da esquerda mostra a confiança para cada estratégia e o gráfico da direita representa a probabilidade média de erro.

3.4.4 A separação de estados

As estratégias de discriminação sem ambiguidade ou com confiança máxima podem ser descritas como um processo de duas etapas. A primeira etapa consiste em tornar os estados mais distinguíveis para, logo em seguida, realizar uma medição com erro mínimo.

A transformação que aumenta a distinguibilidade dos estados terá certa probabilidade de sucesso. Consequentemente, também haverá um resultado inconclusivo nesse processo. É possível implementar uma estratégia que engloba e interpola entre todas as outras anteriores. Ela foi denominada separação de estados [46] e o seu objetivo é fazer com que o conjunto formado por $\{|\psi_j\rangle\}$, se transforme nos estados mais distinguíveis $\{|\beta_j\rangle\}$, ou seja:

$$|\langle\beta_0|\beta_1\rangle|^2 \leq |\langle\psi_0|\psi_1\rangle|^2. \tag{3.60}$$

A figura 13 apresenta como seria essa separação para dois estados não-ortogonais.

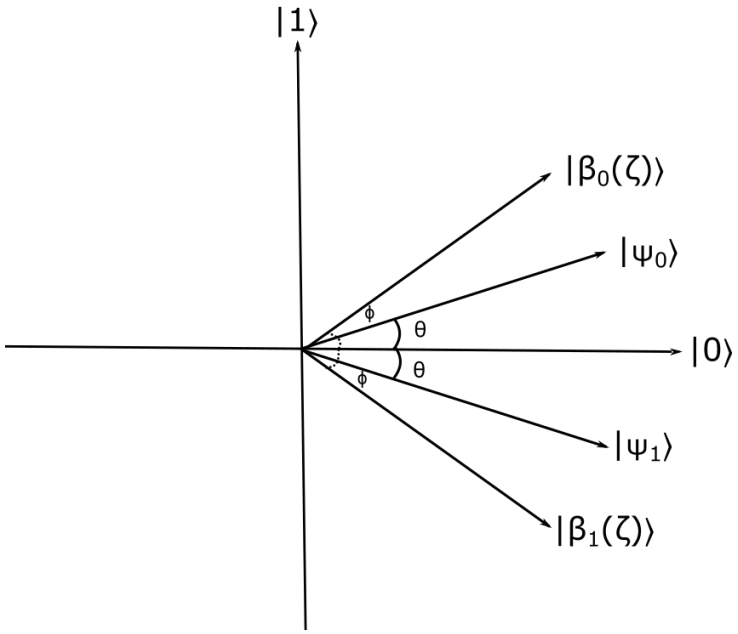

Figura 13 – Figura representando como seria a transformação dos estados para o caso de dois estados não-ortogonais.

A transformação será implementada por dois operadores: $\hat{A}_S$ e $\hat{A}_F$, associados a um processo bem sucedido ou a uma falha, respectivamente. A atuação desses operadores é a seguinte:

$$\hat{A}_S\,|\psi_j\rangle = \sqrt{P_S}\,|\beta_j\rangle\,, \tag{3.61}$$

$$\hat{A}_F\,|\psi_j\rangle = \sqrt{1-P_S}\,|\gamma_j\rangle\,, \tag{3.62}$$

onde P_S é a probabilidade de sucesso e $|\gamma_j\rangle$ é o estado inconclusivo.

Chefles e Barnett em [46] apresentaram originalmente uma determinada maneira de se realizar a separação de estados. Porém, o método que será utilizado nessa seção é baseado no artigo de Prosser *et al.* [47]. Os estados utilizados nas seções anteriores serão maximamente distinguíveis quando eles se tornarem uniformes. Os estados uniformes, $|\alpha_j\rangle$, são definidos como:

$$|\alpha_j\rangle = \frac{1}{\sqrt{2}}\Big(\,|0\rangle + e^{\frac{2\pi j i}{N}}\,|1\rangle\,\Big), \tag{3.63}$$

onde N é o número de estados sendo utilizado. Em geral, os estados pós-separação podem ser parametrizados da seguinte maneira:

$$|\beta_j(\zeta)\rangle = b_0(\zeta)\,|0\rangle + b_1(\zeta)e^{\frac{i\pi j}{N}}\,|1\rangle\,. \tag{3.64}$$

Os coeficientes $b_k(\zeta)$ serão dados por:

$$b_k(\zeta) = \sqrt{(1-\zeta)c_k^2 + \frac{\zeta}{2}}, \tag{3.65}$$

onde $c_0 = \cos\theta$ e $c_1 = \sin\theta$. Utilizando essa parametrização, é possível perceber que com $\zeta = 0$ os estados serão iguais aos iniciais e não haverá separação. A distinguibilidade entre os estados cresce linearmente no intervalo de $0 < \zeta < 1$, até atingir o máximo com $\zeta = 1$.

Os operadores que realizam essa transformação serão dados por:

$$\hat{A}_S = \sqrt{P_S(\zeta)}\left(\frac{b_0(\zeta)}{c_0}\,|0\rangle\langle 0| + \frac{b_1(\zeta)}{c_1}\,|1\rangle\langle 1|\right), \tag{3.66}$$

$$\hat{A}_F = \frac{\sqrt{1-P_S(\zeta)}}{\cos\theta}\,|0\rangle\langle 0|\,. \tag{3.67}$$

O valo máximo da probabilidade de sucesso, após a otimização, é:

$$P_S(\zeta) = \frac{1}{(1-\zeta) + \frac{\zeta}{2\sin^2\theta}}. \tag{3.68}$$

Separação de estados para dois estados não-ortogonais

A atuação desses operadores nos dois estados, $|\psi_j\rangle$, das equações (3.22) e (3.23) resultarão em:

$$\hat{A}_S\,|\psi_j\rangle = \sqrt{P_S(\zeta)}\Big(b_1(\zeta)\,|0\rangle + e^{i\pi j}b_2(\zeta)\,|1\rangle\Big) = \sqrt{P_S(\zeta)}\,|\beta_j(\zeta)\rangle\,, \tag{3.69}$$

$$\hat{A}_F\,|\psi_j\rangle = \sqrt{1-P_S(\zeta)}\,|0\rangle\,. \tag{3.70}$$

Quando $\zeta = 0$, os estados não serão modificados, pois $|\beta_j(0)\rangle = |\psi_j\rangle$, e as probabilidades de falha e sucesso serão 0 e 1, respectivamente. Para $\zeta = 1$, os estados se tornam ortogonais e a probabilidade de falha atinge o limite IDP da discriminação sem ambiguidade, dado na equação (3.43).

A segunda etapa da estratégia consiste em utilizar os operadores definidos em (3.26) e (3.27). Eles serão implementados em uma medição com erro mínimo após a transformação que separa os estados. Sendo assim, a probabilidade de erro será:

$$P_{\text{err}}(\zeta) = \sum_{k=0}^{1}\sum_{j\neq k}\text{Tr}(\hat{\Pi}_k^{ME}\hat{A}_S\,|\psi_j\rangle\langle\psi_j|\,\hat{A}_S^\dagger) = \frac{1}{2}\left(1 - \sqrt{1-(1-\zeta)^2\cos^2 2\theta}\right). \tag{3.71}$$

Os limites de ζ para essa probabilidade são os que possibilitam encontrar os limites das seções anteriores. É possível perceber que, quando $\zeta = 0$, o limite de Helstrom é obtido,

dado na equação (3.25). Quando $\zeta = 1$, $P_{\text{err}} = 0$ o que corresponde à discriminação sem ambiguidade. Isso confirma que essa parametrização define uma estratégia de discriminação capaz de interpolar entre o erro mínimo e a sem ambiguidade.

A probabilidade média de um acerto (P_{acer}) utilizando esse protocolo será definida como:

$$P_{\text{acer}}(\zeta) = \frac{1}{2}P_F(\zeta) + P_S(\zeta)[1 - P_{\text{err}}(\zeta)]. \tag{3.72}$$

O primeiro termo corresponde à adivinhação aleatória de um estado em caso de uma falha. O segundo equivale à probabilidade da separação ser bem sucedida e não ocorrer um erro na discriminação com erro mínimo.

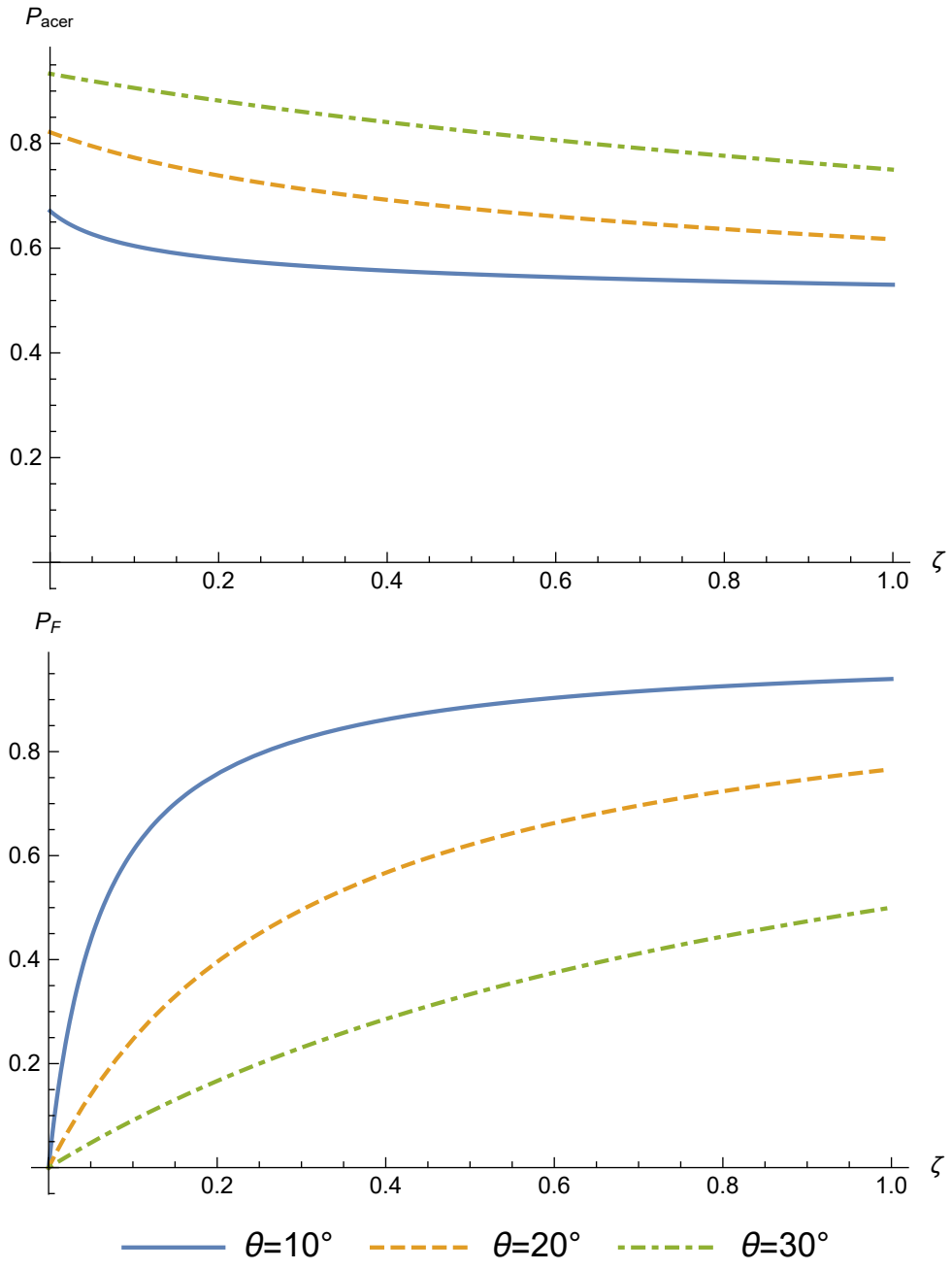

Figura 14 – A figura apresenta a probabilidade média de acerto (P_{acer}) e a probabilidade de falha da separação de estados (P_F). Os gráficos estão em função de ζ para três valores de θ: 10°, 20°, 30°.

A figura 14 apresenta acima a probabilidade média de acerto (P_{acer}) e abaixo a probabilidade de falha da separação de estados (P_F), em função do parâmetro ζ, para três valores de θ: 10°, 20° e 30°. O gráfico mostra que os valores de P_{acer} diminuem quando θ é pequeno e isso é devido ao fato que P_F cresce para esses valores de θ. Quanto menor θ, mais improvável vai se tornando para a estratégia conseguir separar os estados, pois eles vão se aproximando do autovetor de $\hat{A}_F$, $|0\rangle$. Outra observação importante é que P_{acer} decresce com o aumento de ζ e isso está de acordo com o desejado, pois definimos a discriminação com erro mínimo como a estratégia com o menor valor possível para a probabilidade média de erro.

Separação de estados para três estados não-ortogonais

A aplicação dos operadores (3.66) e (3.67) nos estados $\{|\psi_j\rangle\}$, dados nas equações (3.28-3.30), resultará em:

$$\hat{A}_S |\psi_j\rangle = \sqrt{P_S(\zeta)}\Big(b_1(\zeta)|0\rangle + e^{\frac{i2\pi j}{3}} b_2(\zeta)|1\rangle\Big), = \sqrt{P_S(\zeta)}\,|\beta_j(\zeta)\rangle \tag{3.73}$$

$$\hat{A}_F |\psi_j\rangle = \sqrt{1 - P_S(\zeta)}\,|0\rangle\,. \tag{3.74}$$

A equação (3.73) possui o resultado desejado e é possível ver que com $\zeta = 0$, os estados não são modificado; para $\zeta = 1$, os estados se tornam maximamente distinguíveis. Caso ocorra uma falha, os estados se tornarão indistinguíveis. Como pode ser visto, essa parametrização atende todos os requisitos e, como no exemplo para dois estados, existe a possibilidade de aplicar a estratégia de erro mínimo ao final do processo de separação. Utilizando os operadores definidos em (3.31), a probabilidade de erro será parametrizada da mesma maneira e será dada por:

$$P_{\text{err}}(\zeta) = \frac{2}{3}\left(1 - \frac{1}{2}\sqrt{1 - (1-\zeta)^2\cos^2 2\theta}\right). \tag{3.75}$$

Aqui, novamente, o parâmetro ζ relacionará duas estratégias: o erro mínimo e a discriminação com confiança máxima. Quando $\zeta = 0$, é possível ver que a probabilidade de erro se torna a mesma que foi encontrada na equação (3.35). Já para $\zeta = 1$, será correspondente ao que se obteria na estratégia com confiança máxima.

A probabilidade média de acerto (P_{acer}) será definida como:

$$P_{\text{acer}}(\zeta) = \frac{1}{3}P_F(\zeta) + P_S(\zeta)[1 - P_{\text{err}}(\zeta)], \tag{3.76}$$

onde o primeiro termo após a igualdade é uma adivinhação aleatória dos estados quando ocorre uma falha. O segundo termo é a probabilidade de não ocorrer um erro dado que a separação de estados foi bem sucedida.

A figura 15 apresenta acima a probabilidade média de acerto (P_{acer}) e abaixo a probabilidade de falha da separação de estados (P_F), em função do parâmetro ζ, para três θ selecionados: 10°, 20°, 30°. Igualmente ao caso para dois estados, o parâmetro ζ

definirá se a estratégia utilizada é o mínimo erro, confiança máxima ou alguma estratégia intermediária. Como o caso para três e dois estados se assemelham, todas as discussões realizadas anteriormente também se aplicam aqui.

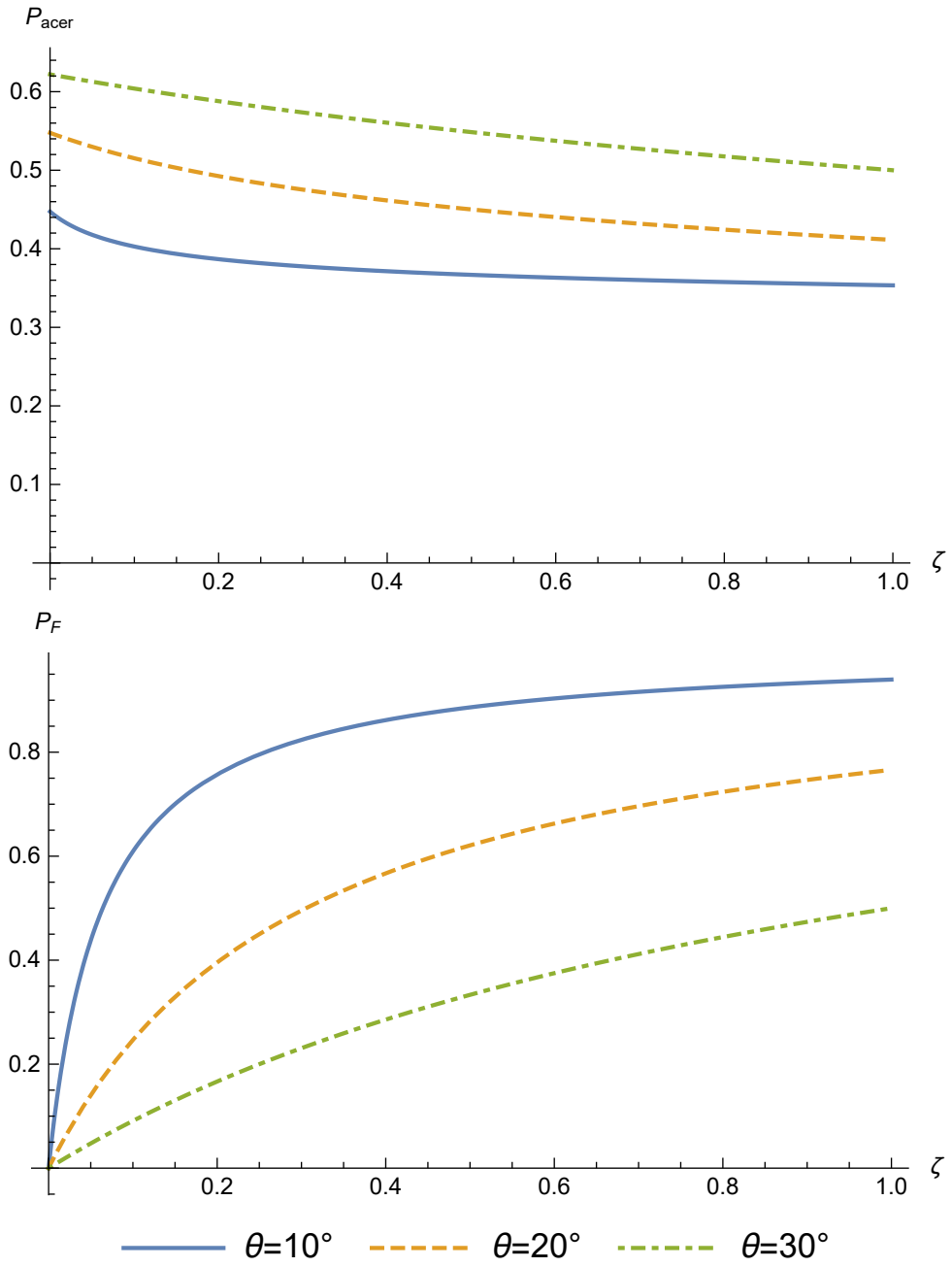

Figura 15 – A figura apresenta a probabilidade média de acerto da estratégia (P_{acer}) e a probabilidade de falha da separação de estados dado que $0 \leq \zeta \leq 1$ e $\theta = 10°, 20°, 30°$. O gráfico acima apresenta a probabilidade média de acerto e o gráficos abaixo é para a probabilidade de falha (ou medição inconclusiva) para a separação de estados sendo os dois com $0 \leq \zeta \leq 1$.

4 Distribuição quântica de chaves criptográficas

Quando a criptografia de chave privada foi descrita na seção 2.1, os problemas dessa classe de protocolos foram apresentados e o principal deles era a necessidade de um método seguro para compartilhar a chave secreta. Alice e Bob, antes de se comunicarem utilizando essa chave, precisariam se encontrar em algum lugar ou garantir que a chave chegasse em segurança para ambas as partes. Com isso em mente, a distribuição quântica de chaves (QKD) foi criada e baseia-se nos próprios postulados da mecânica quântica para garantir o sigilo da chave.

Todo protocolo de criptografia consiste de algoritmos para gerar a chave, encriptar e decriptar a mensagem, como foi visto no capítulo 2. A QKD, por oferecer somente uma maneira de construção da chave, não pode ser considerada um protocolo de criptografia; e sim, um algoritmo de geração. Como a chave gerada por Bob será igual à chave obtida por Alice, os protocolos quânticos só podem ser utilizados na criptografia de chave privada. A figura 16 apresenta um diagrama mostrando de forma geral como um protocolo quântico de distribuição de chaves criptográficas se encaixaria dentro de um processo de criptografia.

Na seção 3.4, mostrou-se que é impossível na mecânica quântica discriminar com certeza absoluta entre dois ou mais estados não-ortogonais. Logo, essa é a base para a eficácia de diversos protocolos de QKD. Se Alice e Bob implementarem um esquema no qual eles consigam construir uma chave utilizando estados não-ortogonais, Eva introduzirá incompatibilidades caso decida identificar os estados. Isso faz com que os comunicadores sempre tenham maneiras de detectar se há espiões no canal de comunicação. Costuma-se relacionar a QKD com esquemas de cifra de uso único (OTP), pois algum vazamento da informação das mensagens estaria estritamente ligado ao protocolo de construção da chave. Isso se deve ao fato da OTP ser perfeitamente segura. Essa união entre os dois esquemas, faz com que a análise de segurança se restrinja ao estudo do algoritmo de geração. Caso este não ofereça alguma brecha de segurança, toda a comunicação se torna inviolável.

Nesse capítulo, três protocolos de QKD serão apresentados: o BB84 [17], o B92 [18] e o PBC00 [19].

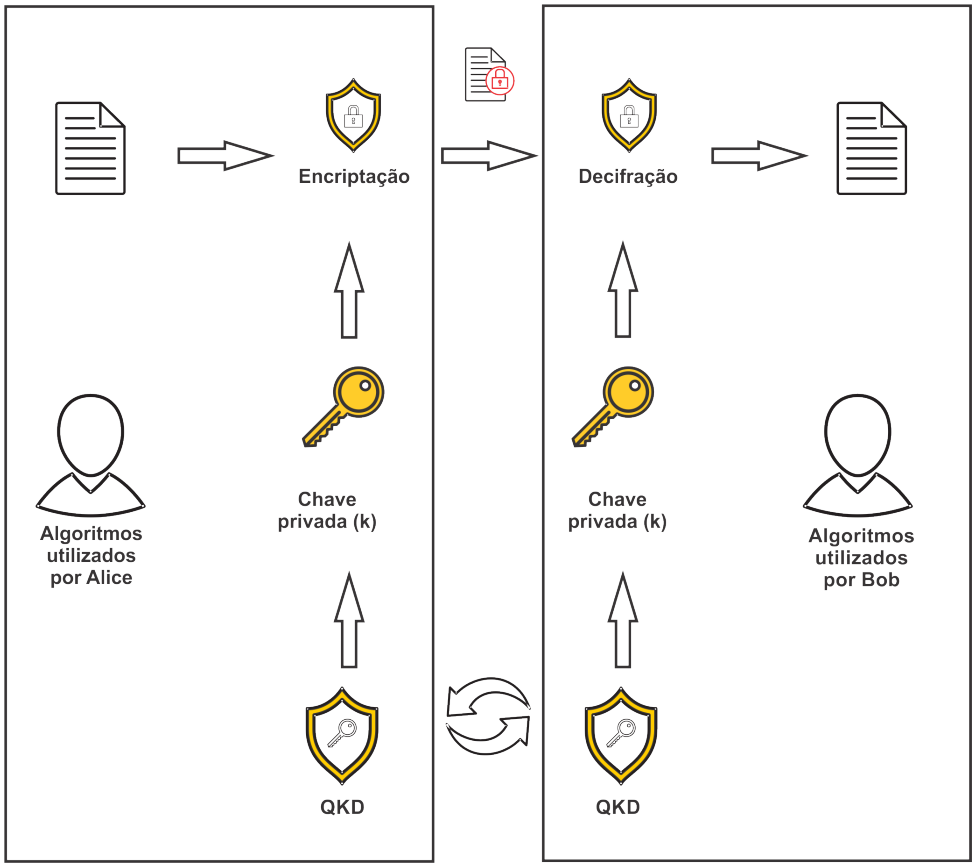

Figura 16 – Digrama descrevendo de maneira geral a criptografia de chave privada utilizando um protocolo quântico de distribuição de chaves criptográficas. Alice deseja enviar uma mensagem para Bob e, para garantir a segurança, ela encripta sua mensagem utilizando uma chave k que foi gerada através de um protocolo QKD. A mensagem é enviada a Bob que, ao recebê-la, faz a decriptação utilizando a mesma chave k.

4.1 O protocolo BB84

Bennett e Brassard criaram o primeiro protocolo de QKD, hoje conhecido como BB84 [17]. O protocolo se inicia com Alice e Bob definindo os quatro possíveis estados para os qubits, nos quais os bits da chave serão codificados:

$$|\psi_0\rangle = |0\rangle\,, \tag{4.1}$$

$$|\psi_1\rangle = |1\rangle\,, \tag{4.2}$$

$$|\psi_0'\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tag{4.3}$$

$$|\psi_1'\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \tag{4.4}$$

onde $B = \{|\psi_0\rangle\,, |\psi_1\rangle\}$ e $B' = \{|\psi_0'\rangle\,, |\psi_1'\rangle\}$ formam bases. Os bits 0 da chave corresponderão aos estados $|\psi_0\rangle$ e $|\psi_0'\rangle$, enquanto os bits 1 aos estados $|\psi_1\rangle$ e $|\psi_1'\rangle$. Em seguida, Alice escolherá aleatoriamente um entre os quatro estados e o enviará para Bob. Ao recebê-lo, ele implementará, aleatoriamente, uma medição projetiva na base B ou B'. Através de um canal público, Bob comunicará a Alice qual a medição projetiva implementada. Caso ele escolha uma composta por estados que são ortogonais ao estado enviado, Alice anunciará

a aceitação do estado como um bit da chave. No caso contrário, ele será descartado. O processo se repetirá até que a chave construída seja do tamanho desejado.

Como exemplo, suponha que Alice envie o estado $|\psi_0\rangle$. Bob escolherá, aleatoriamente, medir na base B ou B'. Caso ele escolha B e comunique isso a Alice, ela saberá que a identificação de $|\psi_0\rangle$ ocorrerá sem erros. Então, Bob será informado que a base foi correta, e o bit aceito. Caso ele escolha B', Alice perceberá que existe uma possibilidade de erro, pois tanto o estado $|\psi_1'\rangle$ quanto o estado $|\psi_0'\rangle$ poderão ser obtidos com a mesma probabilidade. Logo, ela dirá ao Bob que as bases são incompatíveis, e o resultado será descartado. Teoricamente, todo o erro que houvesse na chave seria oriundo exclusivamente de uma espionagem na comunicação. O passo final do protocolo consiste na verificação de incompatibilidades na chave de Bob quando comparada com a de Alice. Eles poderão selecionar alguns bits das suas chaves e compará-los em um canal público. Caso exista algum erro, eles terão certeza que estão sendo espionados e irão descartar a chave gerada.

A tabela 1 ilustra a construção de uma chave com 4 bits. Nela, Alice envia nove estados, mas somente quatro são aceitos. O algoritmo gerou a chave: 0010.

Tabela 1 – Exemplo de construção de uma chave utilizando o BB84.

Estado enviado por Alice	$\|\psi_0\rangle$	$\|\psi_1\rangle$	$\|\psi_0'\rangle$	$\|\psi_0'\rangle$	$\|\psi_1'\rangle$	$\|\psi_1'\rangle$	$\|\psi_0'\rangle$	$\|\psi_0\rangle$	$\|\psi_1\rangle$
Base usada por Bob	B	B'	B'	B	B	B'	B	B	B'
Compatibilidade entre as base	✓	✗	✓	✗	✗	✓	✗	✓	✗
Chave	0		0			1		0	

4.2 O protocolo B92

O protocolo B92 criado por Bennett em 1992 [18] emprega explicitamente, como base para a QKD, a impossibilidade de discriminar entre dois estados não-ortogonais. Ao contrário do BB84, esse protocolo utiliza somente dois estados dados por:

$$|\psi_0\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle\,, \tag{4.5}$$

$$|\psi_1\rangle = \cos\theta\,|0\rangle - \sin\theta\,|1\rangle\,, \tag{4.6}$$

os quais são não-ortogonais, com $|\psi_0\rangle$ correspondendo ao bit 0 e $|\psi_1\rangle$ ao bit 1. Alice prepara, aleatoriamente, um qubit em um desses estados e o envia ao Bob. Ao recebê-lo, ele aplica a estratégia de discriminação sem ambiguidade descrita na seção 3.4.2. Em um canal público, ele comunica à Alice apenas se a estratégia foi bem sucedida (resultado conclusivo) ou não (resultado inconclusivo), sem comunicar qual estado foi obtido. No primeiro caso, o bit é aceito na chave e, no segundo, ele é descartado. O processo se repete até que a chave construída tenha o tamanho desejado. Ao final, eles compartilharão uma chave idêntica, pois Alice conhece o estado enviado nas ocasiões em que Bob obteve um resultado conclusivo e Bob, ao aplicar a discriminação sem ambiguidade, não comete erros.

Assim como no BB84, a teoria não prevê qualquer erro na chave gerada pelo B92. Caso ocorra, é devido exclusivamente à implementação experimental ou espionagem. Novamente, na etapa final, eles comparam alguns bits das suas chaves para verificar se existe algum tipo de espionagem.

A tabela 2 apresenta um exemplo da geração de chave utilizando o B92. Nele, Alice envia uma sequência de oito estados, mas Bob consegue identificá-los somente em quatro ocasiões. A falha da estratégia faz com que os outros quatro resultados sejam descartados, e a chave final é: 0110.

Tabela 2 – Exemplo de construção de uma chave utilizando o B92.

Estado enviado por Alice	$\|\psi_0\rangle$	$\|\psi_1\rangle$	$\|\psi_0\rangle$	$\|\psi_1\rangle$	$\|\psi_1\rangle$	$\|\psi_0\rangle$	$\|\psi_0\rangle$	$\|\psi_1\rangle$
Resultado da medição de Bob	Conc	Conc	Inc	Inc	Conc	Inc	Conc	Inc
Compatibilidade dos resultados	✓	✓	✗	✗	✓	✗	✓	✗
Chave	0	1			1		0	

4.3 O protocolo PBC00

O protocolo PBC00 foi criado por Phoenix, Barnett e Chefles em 2000 [19]. Diferentemente dos protocolos anteriores, ele utiliza três estados para implementar a QKD, os quais devem ser não-ortogonais entre si e podem ser escrito como[1]:

$$|A\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle\,, \tag{4.7}$$

$$|B\rangle = \cos\theta\,|0\rangle + e^{\frac{2\pi i}{3}}\sin\theta\,|1\rangle\,, \tag{4.8}$$

$$|C\rangle = \cos\theta\,|0\rangle + e^{-\frac{2\pi i}{3}}\sin\theta\,|1\rangle\,. \tag{4.9}$$

Uma unitária dada por $\hat{U} = |0\rangle\langle 0| + e^{\frac{2\pi ji}{3}}\,|1\rangle\langle 1|$ com $\hat{U}^3 = \hat{I}$, quando aplicada uma ou duas vezes, ela transformará um estado em outro. A figura 17 ilustra a situação que será usada mais a frente no protocolo.

Com essas definições, o PBC00 funciona da seguinte maneira. Alice prepara cada qubit que enviará para Bob em um dos estados. Isso é feito de forma aleatória e com a mesma probabilidade $\frac{1}{3}$. Ao receber um qubit, Bob implementa aleatoriamente, um entre os três projetores $\hat{P}_{\bar{A}}, \hat{P}_{\bar{B}}, \hat{P}_{\bar{C}}$ definidos pelos seguintes estados:

$$\left|\bar{A}\right\rangle = \sin\theta\,|0\rangle - \cos\theta\,|1\rangle\,, \tag{4.10}$$

$$\left|\bar{B}\right\rangle = \sin\theta\,|0\rangle - e^{\frac{2\pi i}{3}}\cos\theta\,|1\rangle\,, \tag{4.11}$$

$$\left|\bar{C}\right\rangle = \sin\theta\,|0\rangle - e^{-\frac{2\pi i}{3}}\cos\theta\,|1\rangle\,, \tag{4.12}$$

[1] O artigo original utiliza estados diferentes, mas o protocolo pode ser realizado com qualquer conjunto de três estados não-ortogonais. Os estados apresentados aqui constituem uma família mais geral (devido a dependência em θ) e, assim como em [19], possuem estratégias de discriminação bem definidas como foi visto na seção 3.4.

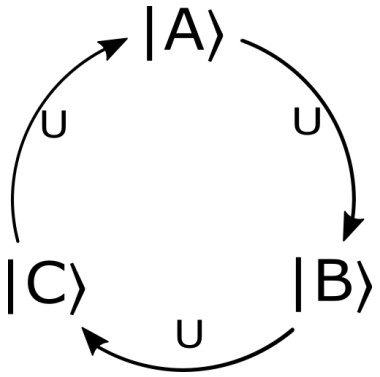

Figura 17 – Uma transformação unitária relaciona os estados enviados por Alice. A aplicação de $\hat{U}$ produz transformações $|A\rangle \to |B\rangle$, $|B\rangle \to |C\rangle$ ou $|C\rangle \to |A\rangle$. A aplicação de $\hat{U}^2$ produz $|A\rangle \to |C\rangle$, $|B\rangle \to |A\rangle$ ou $|C\rangle \to |B\rangle$

que são ortogonais a $|A\rangle$, $|B\rangle$ e $|C\rangle$, respectivamente, ou seja, $\left\langle A\middle|\bar{A}\right\rangle = \left\langle B\middle|\bar{B}\right\rangle = \left\langle C\middle|\bar{C}\right\rangle = 0$. A medição terá dois resultados possíveis, 1 ou 0, que corresponderão a Bob obter um sinal ou não no seu detector, respectivamente. Ele anunciará, em um canal público, todos os casos em que os qubits enviados produziram resultado 0, e essas tentativas serão descartadas, uma vez que não geram ganho de informação. Para os casos em que o resultado for 1, ele terá certeza do envio de um dos dois estados não-ortogonais ao projetor utilizado. Por sua vez, Alice escolherá aleatoriamente um dos dois estados que ela *não enviou* e o anunciará no canal público. De posse da informação de estados não enviados, Bob os comparará com os projetores utilizados em cada tentativa com resultado 1. Quando ambos tiverem a mesma letra, ou seja, quando forem ortogonais, não há ganho de informação e Bob comunicará à Alice o descarte dessa tentativa. Em caso de letras diferentes, Bob saberá imediatamente qual estado foi enviado por Alice e o resultado é mantido para a construção da chave. Resta definir como obter o bit 0 ou 1 na chave e isso será feito utilizando a figura 17. Os usuários do protocolo irão contar quantas unitárias são necessárias para, a partir do estado enviado, chegar ao que foi anunciado como "não enviado" por Alice. No caso de uma única transformação ser exigida, o bit será 0 e, no caso de duas, o bit será 1.

Como exemplo, suponha que Alice envie o estado $|A\rangle$ para Bob. Se ele sortear $\hat{P}_{\bar{A}}$, essa tentativa será descartada, pois o resultado será 0. Porém, se sortear $\hat{P}_{\bar{B}}$, ele terá uma probabilidade de obter um entre dois resultados: 0 ou 1. Isso se deve ao fato que o estado $|A\rangle$ pode ser reescrito como uma combinação linear de $|B\rangle$ e $\left|\bar{B}\right\rangle$. Caso o resultado da medição seja 0, ele descartará a tentativa. Caso seja 1, Bob terá certeza que Alice não enviou o estado $|B\rangle$. Em seguida, se Alice anunciar $|B\rangle$ a tentativa será descartada, pois Bob ganhará nenhuma informação adicional. A tentativa será aceita como um bit da chave somente quando ela anunciar $|C\rangle$. Já que ambos sabem qual estado foi enviado, só restará definir se o bit da chave será 0 ou 1. A transformação do estado $|A\rangle$ para o estado $|C\rangle$ é feita atuando duas vezes a unitária e isso faz com o que bit da chave seja 1. Igualmente aos dois protocolos anteriores, uma parte da chave poderá ser selecionada pelos dois para

verificar a presença de uma espiã.

A tabela 3 apresenta a construção de uma chave utilizando o PBC00. Dez estados são enviados e a chave 0111 é gerada. Assim como nos protocolos anteriores, não é possível, teoricamente, ocorrer incompatibilidades na chave gerada entre Alice e Bob. Como se vê pela tabela, o processo pode ser resumido da seguinte maneira: um bit será gerado sempre que o resultado da medição de Bob for 1 e as três letras das etapas "estado enviado", "projetor utilizado" e "anúncio de Alice" sejam diferentes. Para as sequências ABC, BCA e CAB, o bit é 1 e para as sequências ACB, BAC e CBA, o bit é 0.

Tabela 3 – Exemplo de construção de uma chave utilizando o PBC00.

Estado enviado por Alice	$\|A\rangle$	$\|B\rangle$	$\|A\rangle$	$\|C\rangle$	$\|C\rangle$	$\|A\rangle$	$\|B\rangle$	$\|C\rangle$	$\|C\rangle$	$\|B\rangle$
Projetor utilizado por Bob	$\hat{P}_{\bar{A}}$	$\hat{P}_{\bar{C}}$	$\hat{P}_{\bar{C}}$	$\hat{P}_{\bar{C}}$	$\hat{P}_{\bar{A}}$	$\hat{P}_{\bar{B}}$	$\hat{P}_{\bar{C}}$	$\hat{P}_{\bar{A}}$	$\hat{P}_{\bar{A}}$	$\hat{P}_{\bar{C}}$
Resultado	0	0	1	0	1	1	1	0	1	1
Anuncio de Alice (não enviado)			$\|B\rangle$		$\|B\rangle$	$\|C\rangle$	$\|A\rangle$		$\|A\rangle$	$\|C\rangle$
Confirmação de Bob			✓		✓	✓	✓		✗	✗
Sequências das transformações			AB		CB	AC	BA			
Chave			0		1	1	1			

5 Ataque a protocolos quânticos de distribuição de chaves criptográficas

Na seção 3.2 mostrou-se que não existe uma máquina de clonagem perfeita para estados quânticos e isso será um fator importante para garantir a segurança dos protocolos quânticos de distribuição de chaves criptográficas (QKD). Devido ao teorema da não-clonagem, a espiã, Eva, deve escolher uma estratégia de discriminação para identificar qual o estado enviado por Alice. Como visto na seção 3.4, isso não pode ser implementado sem erros ou falhas. No capítulo anterior mostrou-se que, teoricamente, é impossível para Alice e Bob obterem discrepâncias em suas chaves. Então, se eles mantiverem seu erro experimental abaixo do erro introduzido por Eva, a espionagem sempre será detectável. Os usuários da QKD podem selecionar alguns bits da chave construída e comparar entre eles para checar a quantidade de incompatibilidades. Os esquemas quânticos, além de serem uma maneira segura de realizar criptografia de chave privada a distância, são também protocolos que permitem a detecção de espiões sem utilizar recursos externos. Isso torna evidente a razão de tanto estudo em torno desses algoritmos.

Os tipos de ataque a protocolos quânticos são diversos [16], mas o objetivo dessa obra é utilizar as estratégias de discriminação de estados como base para eles. Dessa forma, os ataques realizados por Eva se restringirão a uma atuação passiva da espiã, pois ela não interferirá no aparato utilizado por Alice e Bob [51,52] (chamado de ataque cavalo de Troia), nem diretamente no canal de comunicação [53–55] (chamado de *photon number splitting attack*) ou em grupos de qubits [56,57] (chamado de ataque coerente). Esse capítulo tratará dos chamados ataques individuais, pois Eva atua em cada qubit separadamente. Eles serão: interceptação-reenvio e supressão. No primeiro, como o nome sugere, Eva interceptará o qubit enviado pela Alice, aplicará uma estratégia de discriminação para, logo em seguida, preparar um qubit no estado correspondente ao resultado da sua medição e reenviá-lo ao Bob. O segundo se assemelha ao primeiro, sendo que a única diferença é a tentativa de mascarar as falhas que podem ocorrer quando Eva aplicar estratégias probabilísticas, como discriminação sem ambiguidade, confiança máxima ou intermediária (seção 3.4).

As estratégias de discriminação são várias, como foi visto na seção 3.4. Porém, todas elas podem ser descritas utilizando a separação de estados (demonstrado na seção 3.4.4) com o valor adequado do parâmetro ζ, o qual define a distinguibilidade entre os estados de um conjuntos após uma dada transformação. Para $\zeta = 0$, a distinguibilidade não é alterada e a estratégia correspondente é o erro mínimo; para $\zeta = 1$, a distinguibilidade é máxima e as estratégias correspondentes são sem ambiguidade ou confiança máxima; para 0
correspondentes são intermediárias às das extremidades. Logo, toda a análise será feita

com essa estratégia e, ao final, escolhe-se o valor conveniente de ζ.

O objetivo final será obter as taxas de erro do B92 e PBC00 devido à espionagem. Isso permitirá que Alice e Bob estabeleçam uma tolerância máxima de erro experimental para que a espiã seja sempre detectável. Os detalhes das contas não serão mostrados nesse capítulo, mas podem ser encontrados no Apêndice A.

5.1 Ataque ao B92: interceptação-reenvio

A taxa de erro para o ataque de interceptação-reenvio já é conhecido [58] tanto para a discriminação com erro mínimo quanto para a discriminação sem ambiguidade quando $\theta = 22,5°$. Porém, aqui será apresentado esse valor para estratégias intermediárias e diferentes ângulos θ. O primeiro passo consiste em calcular o erro na identificação do estado. Alice escolherá aleatoriamente, como visto na seção 4.2, um entre os seguintes estados:

$$|\psi_0\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle\,, \tag{5.1}$$

$$|\psi_1\rangle = \cos\theta\,|0\rangle - \sin\theta\,|1\rangle\,, \tag{5.2}$$

com $0 \leq \theta \leq \frac{\pi}{4}$. Supondo que ela envie $|\psi_0\rangle$, Eva terá uma probabilidade P_0 de identificar o estado corretamente e P_1 de fazê-lo erroneamente. Essas probabilidades serão dadas por:

$$P_0 = P_S(1 - P_{\text{err}}), \tag{5.3}$$

$$P_1 = P_S P_{\text{err}}, \tag{5.4}$$

onde P_S é a probabilidade de sucesso na separação de estados e P_{err} é a probabilidade média de identificação incorreta do estado.[1] De acordo com o resultado da seção 3.4.4:

$$P_S = \frac{1}{(1-\zeta) + \frac{\zeta}{2\sin^2\theta}}, \tag{5.5}$$

$$P_{\text{err}} = \frac{1}{2}\left(1 - \sqrt{1 - (1-\zeta)^2\cos^2 2\theta}\right). \tag{5.6}$$

Há também a possibilidade da separação de estados falhar com uma probabilidade de $1 - P_S$ e, como a espiã não pode deixar de reenviar um estado, isso a forçará a sortear entre $|\psi_0\rangle$ e $|\psi_1\rangle$. Nesse caso, Eva cometerá um erro metade das vezes. Considerando todas essas possibilidades, o estado que Bob receberá de Eva, dado que Alice enviou $|\psi_0\rangle$, será:

$$\hat{\rho}' = \frac{1}{2}\Big[1 + P_S(1 - 2P_{\text{err}})\Big]\,|\psi_0\rangle\langle\psi_0| + \frac{1}{2}\Big[1 - P_S(1 - 2P_{\text{err}})\Big]\,|\psi_1\rangle\langle\psi_1|\,. \tag{5.7}$$

Viu-se, na seção 4.2, que o B92 utiliza a discriminação sem ambiguidade. Uma incompatibilidade surgirá na chave quando Bob identificar que o estado enviado foi $|\psi_1\rangle$.

[1] Ao longo do capítulo, as dependências das probabilidades, estados e taxas de erro com ζ será omitida para se manter a clareza das equações.

Isso ocorrerá com uma determinada probabilidade (P_M) quando ele receber o estado da equação (5.7). Utilizando o operador da equação (3.45), P_M será dado por:

$$P_M = \mathrm{Tr}[\hat{\Pi}_1^{\mathrm{SA}}\hat{\rho}'] = \frac{1}{2}\Big[1 - P_S(1 - 2P_{\mathrm{err}})\Big]\sin^2\theta. \tag{5.8}$$

O bit da chave de Bob será compatível com o da Alice quando ele identificar $|\psi_0\rangle$ em sua medição. Utilizando o operador da equação (3.44), isso ocorrerá com uma probabilidade P_C dada por:

$$P_C = \mathrm{Tr}[\hat{\Pi}_0^{\mathrm{SA}}\hat{\rho}'] = \frac{1}{2}\Big[1 + P_S(1 - 2P_{\mathrm{err}})\Big]\sin^2\theta. \tag{5.9}$$

As probabilidades da equação (5.8) e (5.9) serão iguais caso Alice envie $|\psi_1\rangle$. A fração de bits incompatíveis na chave de Bob é a denominada taxa de erro Q que será dada por:

$$Q = \frac{P_M}{P_M + P_C} = \frac{1}{2}\Big[1 - P_S(1 - 2P_{\mathrm{err}})\Big]. \tag{5.10}$$

A figura 18 apresenta a taxa de erro em função de θ para três estratégias diferentes: erro mínimo ($\zeta = 0$), discriminação sem ambiguidade ($\zeta = 1$) e uma estratégia intermediária com $\zeta = 0.5$. O gráfico mostra que a taxa de erro introduzida na chave sempre será maior

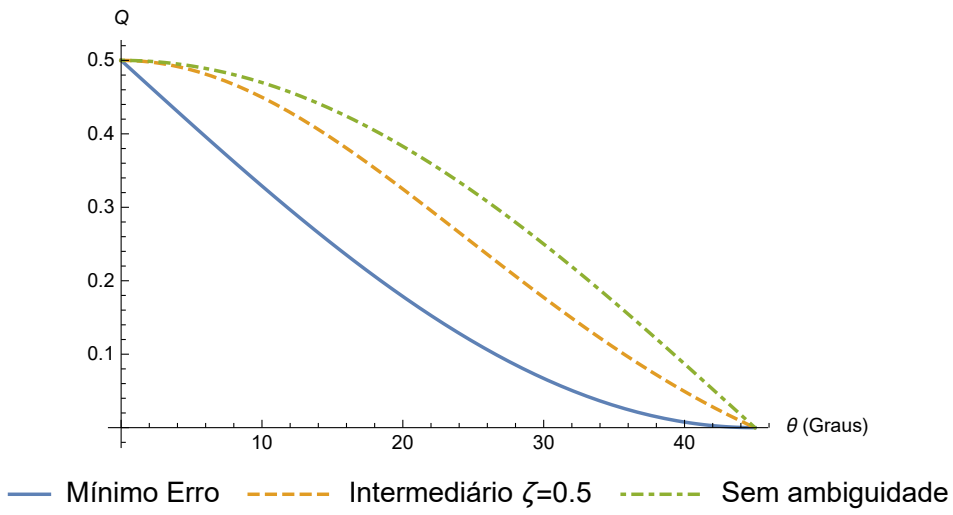

Figura 18 – Taxa de erro (Q) em função de θ no protocolo B92 devido ao ataque de interceptação-reenvio. O gráfico utiliza três valores de ζ diferentes: 0 (linha contínua azul), 0.5 (linha tracejada laranja) e 1 (linha pontilhada-tracejada verde).

que zero, desde que θ não seja 45°. Então, Bob sempre poderá verificar se está sendo espionado desde que o seu erro experimental seja menor. Como exemplo, suponha que Bob e Alice combinem de utilizar estados com $\theta = 20°$. Eva terá que escolher uma estratégia de discriminação e todas as três introduzem taxas de erro diferentes. A espiã, ao utilizar ζ igual a 0, 0.5 ou 1, fará com que Q seja aproximadamente 18%, 32% ou 38%, respectivamente. Se Bob garantir que seu erro experimental seja menor que 18%, ele poderá escolher alguns bits da chave para verificar se estão sendo espionados. No momento que Bob observar um erro na faixa de 18%, ele terá certeza da presença de Eva.

A comparação entre as estratégias leva a crer que o mínimo erro é a estratégia que introduzirá a menor quantidade de erro e, portanto, seria a melhor para manter o anonimato da espionagem. Porém, e se Eva conseguir, de alguma forma, mascarar suas falhas? Esse é o objetivo do próximo ataque.

5.2 Ataque ao B92: supressão

O ataque de supressão já é conhecido na literatura e no próprio artigo do B92 existe uma longa discussão de como Alice e Bob se preveniriam desse ataque. Aqui, porém, será apresentada uma maneira nova de realizar esse ataque que foi desenvolvida pelo autor e o seu orientador. Na seção anterior, o gráfico da figura 18 mostrou que a discriminação sem ambiguidade introduz a maior quantidade de erros na chave de Bob. Como apresentado na seção 4.2, Bob utilizará uma discriminação sem ambiguidade para selecionar os bits de sua chave e os resultados inconclusivos serão descartados.

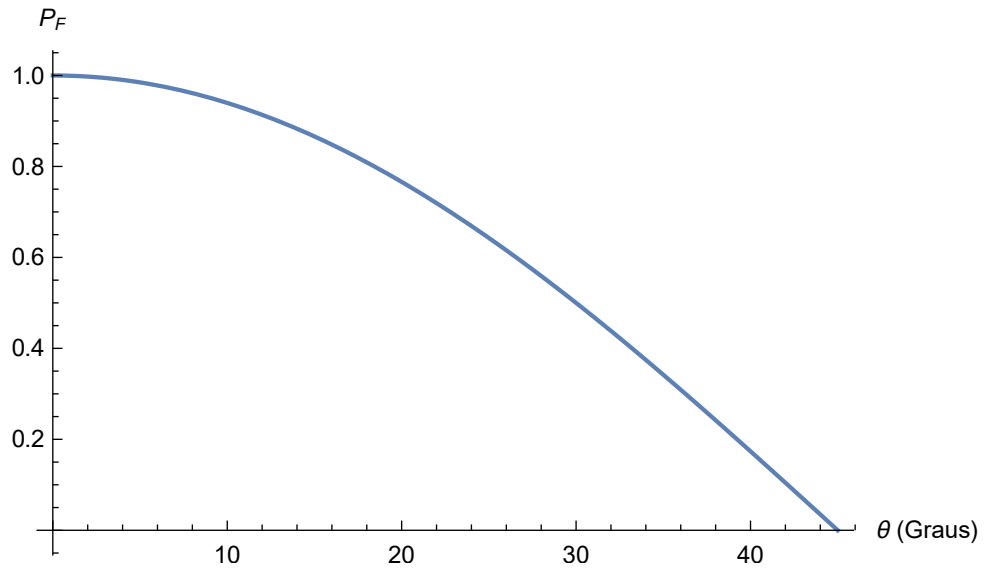

Figura 19 – Gráfico da probabilidade de medida inconclusiva para a discriminação sem ambiguidade para dois estados não-ortogonais.

A figura 19 mostra a probabilidade de se obter uma falha em função de θ. É possível ver que quando $\theta = 0$, a discriminação sem ambiguidade sempre falhará. Isso se deve ao fato que o estado $|0\rangle$ é um autovetor do operador $\hat{A}_F$, definido na equação (3.67). Eva poderá utilizar isso para esconder os próprios resultados inconclusivos. Quando ela obtiver uma falha, poderá simplesmente enviar $|0\rangle$ para Bob e forçar um descarte no protocolo. Ela construirá uma chave igual a de Bob, mas qual será o custo dessa estratégia? Caso esse ataque não tenha um ônus, a segurança do protocolo estaria comprometida. A interferência dela surgirá exatamente nos bits descartados pelo protocolo. Nesse ataque, um descarte ocorrerá com uma probabilidade (P_F) dada por:

$$P_F = (1 - \cos 2\theta)\cos 2\theta + \cos 2\theta, \tag{5.11}$$

onde o primeiro termo é a probabilidade de falha de Bob, dado que Eva teve um resultado conclusivo, e o segundo é a probabilidade da espiã falhar.

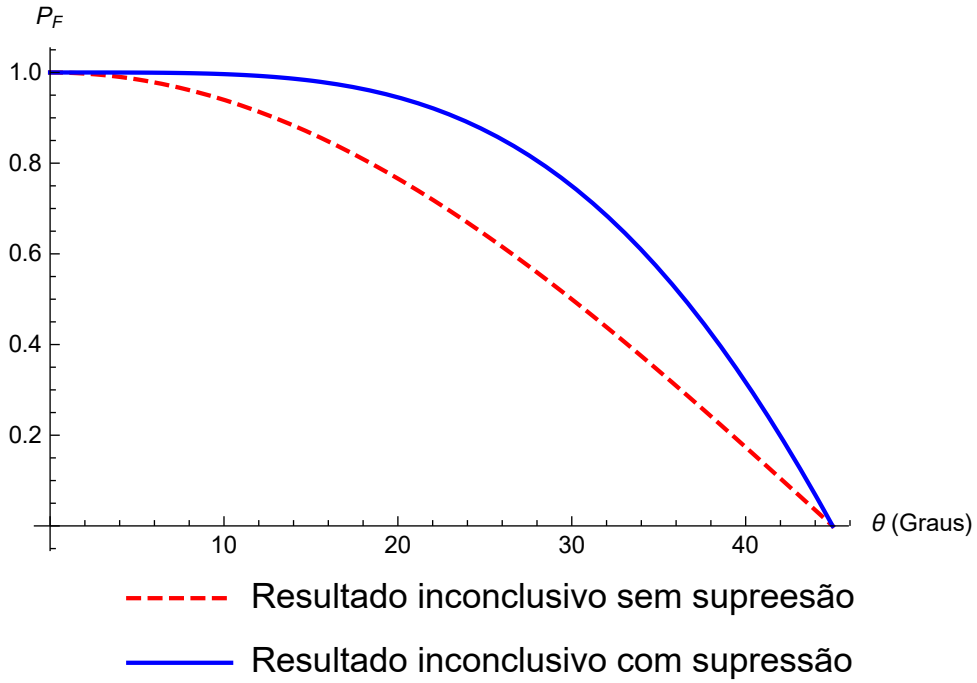

Figura 20 – Gráfico da probabilidade de resultado inconclusivo para Bob, caso Eva suprima ou não suas falhas no ataque ao B92.

A figura 20 compara a probabilidade de resultado inconclusivo de Bob caso Eva decida suprimir ou não suas falhas. É possível perceber que a presença de Eva não sai despercebida, mesmo ela não introduzindo nenhum tipo de erro na chave. Porém, surge a necessidade da implementação de um algoritmo extra no protocolo, pois a verificação da quantidade de bits descartados seria indispensável. Suponha, novamente, que Alice e Bob utilizem estados com $\theta = 20°$. Eva, ao atacar o protocolo, optará por utilizar ou não a supressão e a probabilidade de um resultado inconclusivo será de aproximadamente 0.94 e 0.77, respectivamente.

A discriminação sem ambiguidade pode ser tratada como um caso limite da separação de estados, então é possível implementar este último no ataque de supressão. Como a separação de estados permite estratégias intermediárias, o objetivo é verificar se ela oferece alguma vantagem quando comparada com os outros ataques.

Caso Alice envie $|\psi_0\rangle$, Eva interceptará o qubit e, após a medição, enviará ao Bob o seguinte:

$$\hat{\rho}' = P_S(1 - P_{\text{err}})\,|\psi_0\rangle\langle\psi_0| + P_S P_{\text{err}}\,|\psi_1\rangle\langle\psi_1|\,, \tag{5.12}$$

onde as probabilidades P_S e P_{err} foram definidas em (5.5) e (5.6), respectivamente. É possível perceber, comparando as equações (5.12) e (5.7), que não há o termo referente à falha. A probabilidade de surgir ou não uma incompatibilidade na chave será obtida

seguindo o mesmo raciocínio das equações (5.8) e (5.9). Logo,

$$P_M = \mathrm{Tr}(\hat{\Pi}_1^{\mathrm{SA}}\hat{\rho}') = P_S P_{\mathrm{err}} \sin^2\theta, \tag{5.13}$$

$$P_C = \mathrm{Tr}(\hat{\Pi}_0^{\mathrm{SA}}\hat{\rho}') = P_S(1 - P_{\mathrm{err}}) \sin^2\theta. \tag{5.14}$$

A taxa de erro(Q) introduzida por Eva devido a sua espionagem será:

$$Q = \frac{P_M}{P_M + P_C} = P_{\mathrm{err}}. \tag{5.15}$$

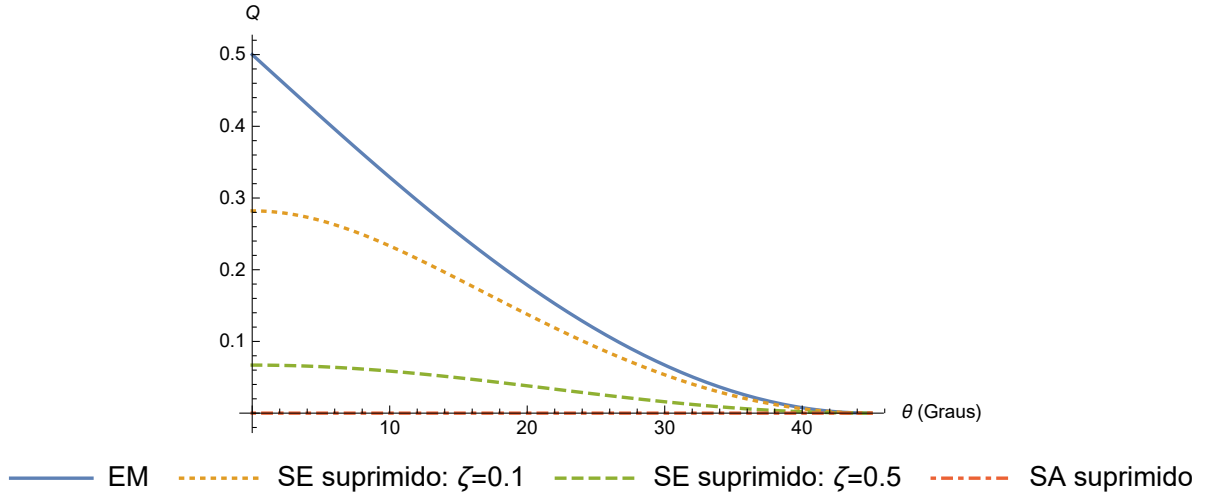

Figura 21 – Gráfico da taxa de erro para Bob caso Eva suprima ou não seus resultados inconclusivos no ataque ao B92. Quatro estratégias foram analisadas: discriminação com erro mínimo (EM), sem ambiguidade com supressão (SA), separação de estados suprimida (SE) com ζ igual a 0.1 e 0.5.

A figura 21 apresenta a taxa de erro para a discriminação com erro mínimo (EM), sem ambiguidade suprimido (SA), a separação de estado suprimida (SE) com ζ igual a 0.1 e 0.5. Suponha que Alice e Bob decidam realizar o protocolo com $\theta = 20°$; Eva introduzirá diferentes taxas de erro que dependerão da escolha de ζ. Para ζ igual a 0, 0.1, 0.5 ou 1, a taxa de erro será de aproximadamente 18%, 14%, 4% ou 0%, respectivamente.

Esse tipo de ataque fará com que a probabilidade de descarte aumente e seja dada por:

$$P_F = P_S \cos 2\theta + (1 - P_S). \tag{5.16}$$

A figura 22 ilustra a alteração dessa probabilidade em função de θ para a discriminação sem ambiguidade com e sem supressão, a separação de estados suprimida com ζ igual a 0.1 e 0.5. Se Alice e Bob escolhessem $\theta = 20°$, a probabilidade de um bit ser descartado se alterará de acordo com a estratégia. Caso a discriminação sem ambiguidade seja usada com ou sem supressão, essa probabilidade será de aproximadamente 0.94 e 0.77, respectivamente. Quando a separação de estados é utilizada com ζ igual a 0.1 ou 0.5, a probabilidade será de aproximadamente 0.82 e 0.91, respectivamente. Novamente, a supressão faz com que Bob consiga identificar a presença de Eva através dos bits descartados no algoritmo.

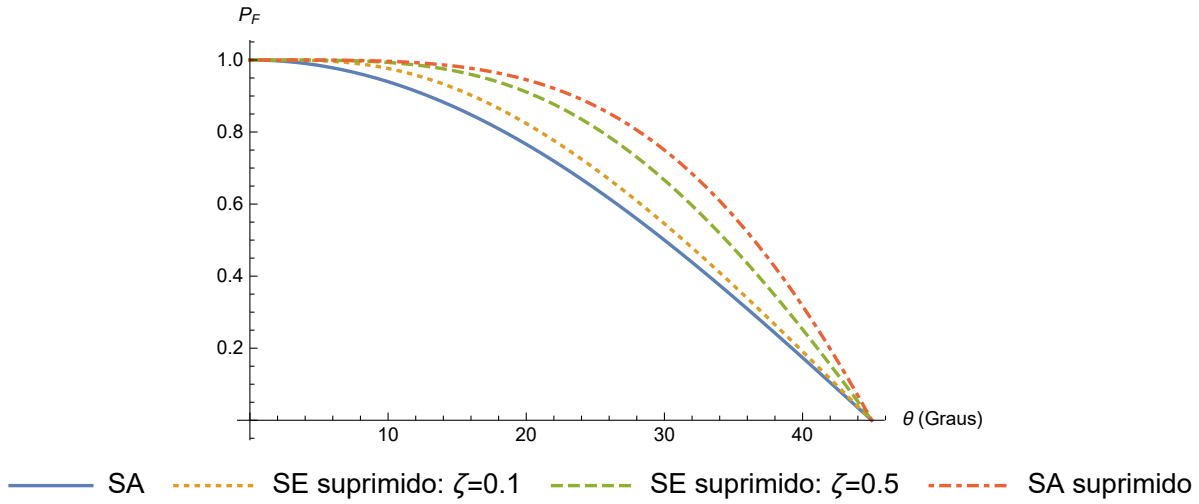

Figura 22 – Gráfico da probilidade de que Bob falhe caso Eva suprima ou não seus resultados inconclusivos no ataque ao B92. Quatro estratégias foram analisadas: discriminação sem ambiguidade (SA) com e sem supressão, separação de estados (SE) suprimidos com ζ igual a 0.1 e 0.5.

O ataque de interceptação-reenvio permite que Eva espione a construção da chave criptográfica entre Alice e Bob, ao custo de introduzir erros detectáveis na chave de Bob. Em contrapartida, o ataque de supressão permite que a espiã controle tanto a taxa de erro quanto a quantidade de bits descartados no protocolo. Como foi visto, Eva poderá selecionar um valor de ζ e, consequentemente, uma taxa de erro de 0% a 18% conjuntamente com uma probabilidade de um descarte de 0.77 a 0.94. Esse ataque possibilita que Eva escolha quais probabilidades se adequam melhor à sua necessidade de permanecer indetectável, dado que ela tenha ciência da taxa de erro experimental de Bob. Isso cria uma possível brecha, caso os usuários do esquema não se previnam.

5.3 Ataque ao PBC00: interceptação-reenvio

A tática de interceptação-reenvio para esse protocolo será igual à apresentada anteriormente para o B92. Os autores originais do protocolo fizeram a análise da taxa de erro para esse ataque utilizando a discriminação com erro mínimo para $\theta = 45°$ [19]. Como no caso para o B92, a análise em função do ângulo e para estratégias intermediárias é uma novidade. Com a estratégia de ataque definida, o próximo passo é calcular a probabilidade de erro ou acerto na chave de Bob. Como foi visto na seção 4.3, Alice escolherá aleatoriamente um entre os três estados dados por:

$$
\begin{aligned}
|A\rangle &= \cos\theta\,|0\rangle + \sin\theta\,|1\rangle\,, \\
|B\rangle &= \cos\theta\,|0\rangle + e^{\frac{2\pi i}{3}}\sin\theta\,|1\rangle\,, \\
|C\rangle &= \cos\theta\,|0\rangle + e^{\frac{-2\pi i}{3}}\sin\theta\,|1\rangle\,.
\end{aligned}
$$

Supondo que Alice envie o estado $|A\rangle$, Eva terá uma probabilidade de identificar corretamente (P_A) ou de errar. Em caso de erro, a espiã assumirá, aleatoriamente, que interceptou

$|B\rangle$ ou $|C\rangle$ com probabilidades P'_B e P'_C, respectivamente. De acordo com o resultado da seção 3.4.4:

$$P_A = \frac{P_S}{3}\Big[1+\sqrt{1-(1-\zeta)^2\cos^2 2\theta}\Big], \tag{5.17}$$

$$P'_B = P'_C = \frac{P_S}{3}\Big[1-\frac{1}{2}\sqrt{1-(1-\zeta)^2\cos^2 2\theta}\Big], \tag{5.18}$$

$$\tag{5.19}$$

onde P_S é a probabilidade de sucesso da separação de estados dada por:

$$P_S = \frac{1}{(1-\zeta)+\frac{\zeta}{2\sin^2\theta}}. \tag{5.20}$$

Em sua medição, Eva poderá ter um resultado inconclusivo com uma probabilidade $1-P_S$. Quando isso ocorrer, ela terá que sortear um entre os três estados para enviar ao Bob. Após esse processo, o estado enviado por Eva, caso Alice envie $|A\rangle$ será:

$$\hat{\rho}' = \frac{P_S}{3}\Big(P_A\,|A\rangle\langle A| + P'_B\,|B\rangle\langle B| + P'_C\,|C\rangle\langle C|\Big) + \frac{1-P_S}{3}\Big(\,|A\rangle\langle A| + |B\rangle\langle B| + |C\rangle\langle C|\,\Big). \tag{5.21}$$

Bob terá um erro em sua chave quando ele sortear um projetor ortogonal a $|A\rangle$ e obtiver 1 como resultado. Isso o levará a assumir que Alice enviou $|B\rangle$ ou $|C\rangle$ e não será possível o descarte dessa tentativa quando ocorrer o anúncio de Alice. Logo, a probabilidade de uma incompatibilidade (P_M) será:

$$P_M = \frac{1}{3}\mathrm{Tr}\Big(\,\big|\bar{A}\big\rangle\big\langle\bar{A}\big|\,\hat{\rho}'\Big) = \frac{2}{3}\left[\Big(1-\frac{P_S}{2}\sqrt{1-(1-\zeta)^2\cos^2 2\theta}\Big)\sin^2\theta\cos^2\theta\right], \tag{5.22}$$

onde o termo $\frac{1}{3}$ é devido à probabilidade que $\hat{P}_{\bar{A}}$ seja implementado. A chave de Bob não terá um bit incorreto quando ela sortear o projetor $\hat{P}_{\bar{B}}$ ou $\hat{P}_{\bar{C}}$ e Alice anunciar que não enviou $|C\rangle$ ou $|B\rangle$, respectivamente. Isso se deve ao fato que, caso Bob implemente um projetor ortogonal a $|B\rangle$ e Alice anuncie que não enviou $|B\rangle$, a tentativa será descartada. A probabilidade do bit da chave estar correto (P_C) será:

$$\begin{aligned} P_C &= \frac{1}{3}\frac{1}{2}\mathrm{Tr}\Big(\,\big|\bar{B}\big\rangle\big\langle\bar{B}\big|\,\rho' + \big|\bar{C}\big\rangle\big\langle\bar{C}\big|\,\hat{\rho}'\Big) \\ &= \frac{1}{3}\left[\Big(2+\frac{P_S}{2}\sqrt{1-(1-\zeta)^2\cos^2 2\theta}\Big)\sin^2\theta\cos^2\theta\right], \end{aligned} \tag{5.23}$$

onde os termos $\frac{1}{3}$ e $\frac{1}{2}$ são devidos à escolha do projetor e estado anunciado, respectivamente. A taxa de erro (Q) será dada por:

$$Q = \frac{P_M}{P_M+P_C} = \frac{2-P_S\sqrt{1-(1-\zeta)^2\cos^2 2\theta}}{4-\frac{P_S}{2}\sqrt{1-(1-\zeta)^2\cos^2 2\theta}}. \tag{5.24}$$

A figura 23 mostra o gráfico de Q em função do ângulo θ e de três valores para ζ. Os ζ selecionados foram: 0, 0.5, 1. Deve ser lembrado que os valores 0 e 1 do parâmetro equivalem ao mínimo erro e a discriminação com confiança máxima, respectivamente.

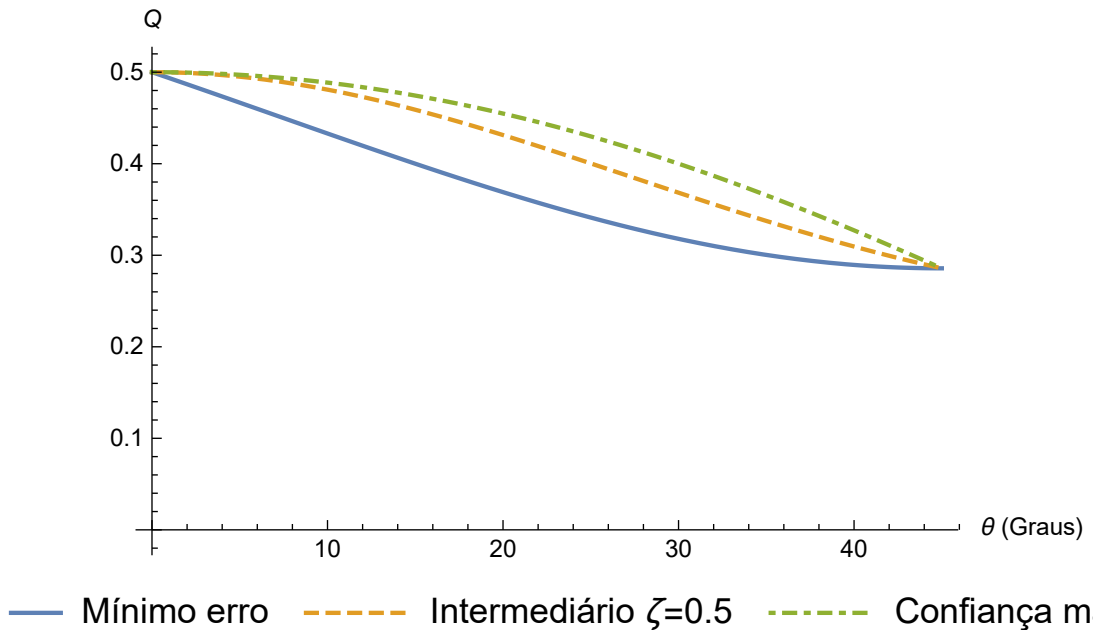

Figura 23 – Taxa de erro (Q) em função de θ no protocolo PBC00 devido ao ataque de interceptação-reenvio. O gráfico utiliza três valores de ζ selecionados: 0 (linha contínua azul), 0.5 (linha tracejada laranja) e 1 (linha pontilhada-tracejada verde).

Ao atacar o protocolo da forma descrita acima, Eva introduzirá, assim como no ataque ao B92, erros na chave construída por Bob. Isso fará com que seu ataque seja desmascarado desde que o erro experimental do equipamento de Bob seja menor. Supondo que Bob e Alice utilizem estados com $\theta = 20°$, a espiã introduzirá uma taxa de erro de aproximadamente 37%, 43% e 45% para ζ igual a 0, 0.5 e 1, respectivamente. Percebe-se que, nesse tipo de protocolo, existe um piso para a taxa de erro obtido com $\theta = 45°$. Nesse caso, essa taxa será de aproximadamente 29% para as três estratégias de discriminação. Isso advém do fato que, quando $\theta = 45°$, os estados serão maximamente distinguíveis, porém ainda não-ortogonais. Nesse caso, as estratégias se tornam equivalentes e o ataque se resumiria à utilização da discriminação com erro mínimo. Pode-se concluir que, se Bob possuir um erro experimental menor que 29%, Eva será perceptível independente de qual valor de θ seja utilizado.

5.4 Ataque ao PBC00: supressão

Uma das motivações para se criar o protocolo PBC00, segundo os autores [19], foi para minimizar a eficácia do ataque de supressão. Na época de criação do protocolo não existia ainda a discriminação com confiança máxima, já que ela foi criada em 2006. Então, se acreditava na época que o protocolo estaria protegido desse ataque devido a simples utilização de estados linearmente dependentes. Nessa seção, todos os cálculos e estratégias de como aplicar esse ataque foram desenvolvidas pelo autor e seu orientador. Similarmente ao ataque de supressão realizado para o B92, aqui Eva utilizará a separação de estados e

mascarará as falhas nas suas tentativas de identificar o estado enviado por Alice. A maneira como ocorrerá a ocultação dos resultados inconclusivos será diferente daquela apresentada anteriormente. No B92, Bob utilizava a discriminação sem ambiguidade como parte do algoritmo e isso permitia com que Eva utilizasse o estado $|0\rangle$ para forçar um descarte no protocolo. Essa possibilidade não é mais possível para o PBC00, pois a discriminação sem ambiguidade não é utilizada por Bob. Logo, deve-se pensar uma maneira diferente de realizar esse tipo de ataque contra o PBC00.

No PBC00, Bob utilizará sempre algum projetor ortogonal aos estados enviados e, experimentalmente, isso corresponde a obter ou não algum sinal no detector. Suponha que Alice envie um qubit no estado $|A\rangle$. Bob o receberá e, em seguida, terá que escolher um projetor que seja ortogonal a $|A\rangle$, $|B\rangle$ ou $|C\rangle$. Caso o projetor sorteado produza um resultado 0, não haverá ganho de informação e a tentativa será descartada. Nesse caso, uma estratégia possível para Eva conseguir mascarar seus resultados inconclusivos seria se ela interceptasse o qubit de Alice e, em caso de falha, enviaria nenhum qubit. Bob, então, não veria um sinal em seu detector e interpretaria que obteve o resultado 0. Logo, assume-se que Bob não implementará nada além dos projetores apresentados para que não interfira na realização do ataque.

Supondo que Alice envie $|A\rangle$, o estado que Eva enviará ao Bob será:

$$\hat{\rho}' = \frac{P_S}{3}\Big(P_A\,|A\rangle\langle A| + P_B\,|B\rangle\langle B| + P_C\,|C\rangle\langle C|\Big), \tag{5.25}$$

onde P_A, P_B, P_C e P_S foram definidos em (5.17), (5.18), (**??**) e (5.20) respectivamente. Se compararmos $\hat{\rho}'$ com a matriz densidade da equação (5.21), nota-se que o termo referente à falha não está presente. O erro e acerto que Bob obterá na sua chave seguirão os mesmos raciocínios apresentados na seção anterior. Sendo assim, a probabilidade de um erro na sua chave (P_M) será:

$$P_M = \frac{2P_S}{3}\left[1 - \frac{1}{2}\sqrt{1-(1-\zeta)^2\cos^2 2\theta}\right]\sin^2\theta\cos^2\theta. \tag{5.26}$$

A probabilidade de não ocorrer uma incompatibilidade será dada por:

$$P_C = \frac{P_S}{3}\left(2 + \frac{1}{2}\sqrt{1-(1-\zeta)^2\cos^2 2\theta}\right)\sin^2\theta\cos^2\theta. \tag{5.27}$$

A taxa de erro (Q) será:

$$Q = \frac{P_M}{P_M + P_C} = \frac{2 - \sqrt{1-(1-\zeta)^2\cos^2 2\theta}}{4 - \frac{1}{2}\sqrt{1-(1-\zeta)^2\cos^2 2\theta}}. \tag{5.28}$$

O gráfico da figura 24 mostra a taxa de erro da chave de Bob em função de θ e três valores selecionados de ζ. Caso Alice e Bob utilizem estados com $\theta = 20°$, as estratégias com ζ igual a 0, 0.5 e 1 introduzirão um erro de 37%, 30% e 29% na chave de Bob, respectivamente.

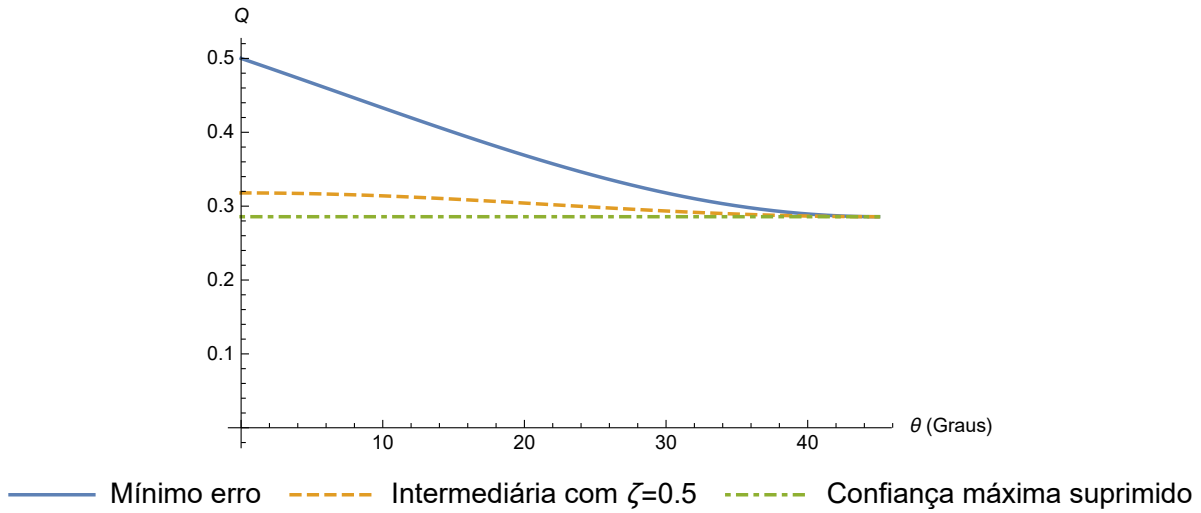

Figura 24 – Taxa de erro (Q) em função de θ no protocolo PBC00 devido ao ataque de supressão. A separação de estados suprimida foi utilizada com três valores distintos: $\zeta = 0$ (linha contínua azul), $\zeta = 0.5$ (linha tracejada laranja) e $\zeta = 1$ (linha tracejada-pontilhada verde).

Antes de verificar como a probabilidade de Bob descartar um resultado se modificará com o ataque de supressão, é preciso obtê-la sem a presença da espiã. Supondo que Alice envie o estado $|A\rangle$, o algoritmo de Bob terá duas maneiras distintas de resultar em um descarte. A primeira delas ocorrerá quando Bob sortear o projetor $\left|\bar{A}\right\rangle\!\left\langle\bar{A}\right|$ que é formado pelo estado ortogonal a $|A\rangle$. A segunda maneira resultará da utilização de um projetor que não seja ortogonal ao estado enviado por Alice, como por exemplo $\left|\bar{B}\right\rangle\!\left\langle\bar{B}\right|$, e a medição poderá resultar em zero com uma determinada probabilidade. Isso é devido ao fato que os estados são não-ortogonais, logo $|A\rangle$ pode ser reescrito utilizando $|B\rangle$ e $\left|\bar{B}\right\rangle$ como base. Apesar de um estado ter sido escolhido como exemplo, o mesmo raciocínio será válido para qualquer outro. Então, a probabilidade de descarte (P_D) será:

$$\begin{aligned} P_D &= \frac{1}{3} + \frac{1}{9}\Big(|\langle A|B\rangle|^2 + |\langle A|C\rangle|^2 + |\langle B|A\rangle|^2 + |\langle B|C\rangle|^2 + |\langle C|A\rangle|^2 + |\langle C|B\rangle|^2\Big) \\ &= \frac{1}{3} + \frac{2}{3}\Big(\cos^4\theta + \sin^4\theta - \cos^2\theta\sin^2\theta\Big). \end{aligned} \tag{5.29}$$

O ataque de supressão alterará a probabilidade de Bob obter um zero da seguinte forma:

$$P_{\text{zero}} = P_S P_D + (1 - P_S), \tag{5.30}$$

onde P_S é a probabilidade de sucesso da separação de estados definida na equação (5.20). O gráfico da figura 25 apresenta P_{zero} para caso com e sem supressão. Nota-se que o fato de Eva utilizar a supressão, faz com que a probabilidade seja alterada de acordo com a estratégia utilizada. Suponha que Alice e Bob implementem estados com $\theta = 20°$, Eva poderá não suprimir ou utilizar a separação de estados suprimida com ζ igual a 0.5 e 1. Nesses casos, as probabilidades de descarte serão de 0.79, 0.92 e 0.95, respectivamente.

Uma diferença essencial desse tipo de ataque, quando comparado ao realizado no B92, pode ser notada na figura 24. No caso do B92, a separação de estados com a supressão

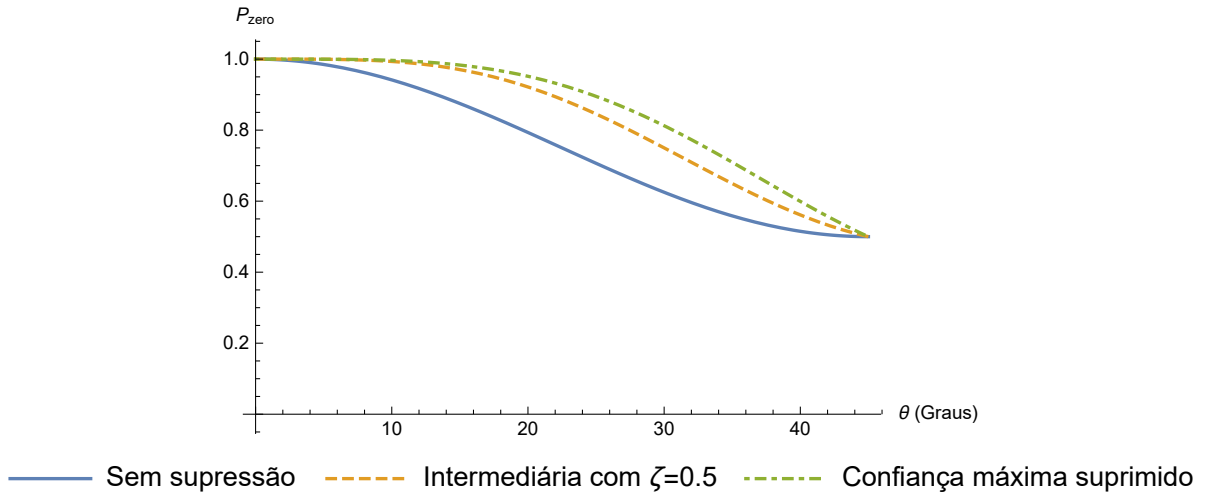

Figura 25 – Gráfico da probabilidade de Bob obter um zero (P_{zero}) em função de θ, caso Eva suprima ou não seus resultados inconclusivos em um ataque ao PBC00.

permitiria que a espiã escolhesse uma taxa de erro entre 0% e 18% para ζ entre 0 e 1. Já para o PBC00, nota-se que, mesmo utilizando a estratégia com $\zeta = 1$, sempre existirá um piso de aproximadamente 29%. Consequentemente, Eva nunca poderá passar despercebida e a análise dos bits descartados se torna desnecessária para Bob. Desde que ele mantenha seu erro experimental abaixo de 29%, haverá sempre a garantia que Eva seja detectável tanto na interceptação-reenvio quanto na supressão.

A utilização de três estados linearmente dependentes nesse protocolo é a razão da segurança contra ataques de supressão. O B92, ao empregar estados linearmente independentes, permite com que Eva utilize a discriminação sem ambiguidade. Essa estratégia sempre distinguirá entre os estados com certeza absoluta quando uma falha não ocorre. Já a estratégia com confiança máxima, usada para atacar o PBC00, não identificará o estado sem erro. Isso faz com que sempre exista um piso para a taxa de erro no ataque. Fica evidente a vantagem de se utilizar mais de dois estados em protocolos quânticos de distribuição de chaves quando analisados dessa perspectiva.

6 Conclusão

O leitor foi apresentado a diversos conceitos que permitiram uma maior compreensão tanto da QKD quanto da discriminação de estados quânticos. Ela se iniciou com uma breve introdução à criptografia clássica no capítulo 2. Nele, mostrou-se como a noção de segurança, dentro do contexto da criptografia, é descrita. A segurança perfeita e a computacional foram descritas com o intuito de entender como quantificar e testar a segurança de um protocolo. Em seguida, uma descrição foi dada de como os esquemas criptográficos, em geral, podem ser descritos e o porquê de dividi-los em duas classes: a criptografia de chave privada e pública. Protocolos dos dois tipos foram exibidos com esta sendo exemplificada pelo algoritmo RSA e aquela pela cifra de César, cifra de Vigenère e a perfeitamente segura OTP. Esse capítulo pavimentou o caminho para o entendimento de como a QKD se encaixa dentro de um esquema criptográfico clássico.

O capítulo 3 foi a pedra de Roseta do restante da obra. Ele se iniciou com a descrição do qubit e como seus estados podem ser representados na esfera de Bloch. Logo após, foi demonstrado uma das peças fundamentais para a segurança da QKD: o teorema da não-clonagem. Esse teorema implica na impossibilidade de clonar estados quânticos com perfeição e, portanto, limita Eva nos possíveis ataques aos protocolos quânticos. A incapacidade de espionagem com clonagem, obriga Eva a escolher estratégias para discriminar estados não-ortogonais. Isso levou diretamente à discussão de medições quânticas e estratégias de discriminação de estados. Demonstrou-se que é impossível discriminar perfeitamente entre dois ou mais estados não-ortogonais. A segurança da QKD se torna evidente, pois Eva estará sempre sujeita a ser detectada durante a espionagem.

Três protocolos QKD foram exibidos no capítulo 4: o BB84, o B92 e o PBC00. Nesse capítulo, os três esquemas foram apresentados e exemplificados com detalhes. Ficou evidente que, apesar da QKD utilizar probabilidade em seu algoritmo, a chave gerada sempre coincidirá, teoricamente, entre os dois usuários dos protocolos. O BB84, precursor da QKD, é escolhido por razões históricas e os outros dois foram os alvos dos ataques.

No capítulo 5 se aplicou todo o conhecimento adquirido no capítulo 3 e 4 para atacar tanto o B92 quanto o PBC00. Os ataques individuais escolhidos foram a interceptação-reenvio e a supressão. Apesar de serem simples, eles são uma aplicação direta das estratégias de discriminação discutidas. Nesses ataques, Eva intercepta o estado enviado por Alice, realiza uma medição para identificá-lo e, logo em seguida, o reenvia para Bob. A diferença entre os dois está no fato de Eva realizar, no segundo, uma tentativa de ocultação das suas falhas. O ataque de interceptação-reenvio mostrou que Eva sempre introduzirá certa quantidade de incompatibilidade na chave de Bob nos dois protocolos. No B92 essa taxa foi de aproximadamente 18%, 32% e 38% para ζ igual a 0, 0.5 e 1, respectivamente, e $\theta = 20°$. No PBC00, foi de aproximadamente 37%, 43% e 45% para os mesmos parâmetros.

Há uma diferença evidente entre os dois protocolos: enquanto no B92 a taxa de erro decai com o aumento de θ, no PBC00 ela atingirá um piso de aproximadamente 29%. Isso é devido à utilização de três estados linearmente dependentes pelo protocolo PBC00. No ataque de supressão, Eva também introduzirá uma taxa de erro na chave de Bob e, além disso, aumentará a probabilidade de descarte de um resultado pelo protocolo. Quando utilizado contra o B92, ele mostrou uma eficácia marcante por possibilitar que a espiã escolha qual taxa de erro ela introduzirá independente do ângulo θ. Caso $\theta = 20°$, ela poderia escolher uma taxa de erro entre 0% a 18% ao custo da alteração da probabilidade de descarte de 0.94 a 0.77, respectivamente. Bob, nesse caso, se vê obrigado a sempre verificar a quantidade de bits que está sendo descartado pelo protocolo ou ele estará sempre vulnerável. O mesmo ataque contra o PBC00 não se mostrou tão eficaz. Apesar de Eva conseguir controlar sua taxa de erro, ela sempre terá um piso de aproximadamente 29%. Devido a isso, ela será sempre detectável sem a necessidade de verificação da quantidade de tentativas descartadas. Novamente, a vantagem de utilizar estados linearmente dependentes é incontestável nesse contexto.

Apêndices

APÊNDICE A – Cálculo das taxas de erro

Esse apêndice será dedicado ao cálculo das taxas de erros para as diferentes estratégias de ataques à QKD apresentadas no capítulo 5. Nele será mostrado, também, que essa taxa utilizando a separação de estados se equivale ao erro mínimo e a discriminação sem ambiguidade nos limites de $\zeta = 0$ e $\zeta = 1$, respectivamente. O cálculo será feito para o B92 e o PBC00 tanto para o ataque de interceptação-reenvio quanto para a supressão.

A.1 Taxas de erro para os ataques ao B92

A.1.1 Interceptação-reenvio

Discriminação com erro mínimo

Supondo que Alice envie o estado $|\psi_0\rangle$, Eva poderá ter um resultado errado com uma determinada probabilidade (P_1) ou um resultado correto com outra determinada probabilidade (P_0) que serão dadas por:

$$P_0 = \mathrm{Tr}\Big(\hat{\Pi}_0^{\mathrm{EM}} |\psi_0\rangle\langle\psi_0|\Big) = \frac{1}{2}(1 + \sin 2\theta), \tag{A.1}$$

$$P_1 = \mathrm{Tr}\Big(\hat{\Pi}_1^{\mathrm{EM}} |\psi_0\rangle\langle\psi_0|\Big) = \frac{1}{2}(1 - \sin 2\theta), \tag{A.2}$$

onde $\hat{\Pi}_j^{\mathrm{EM}}$ são os elementos do POVM definidos em (3.26) e (3.27) para a discriminação com erro mínimo. A matriz densidade resultante do processo será:

$$\hat{\rho}' = \frac{1}{2}\Big[(1 + \sin 2\theta)\,|\psi_0\rangle\langle\psi_0| + (1 - \sin 2\theta)\,|\psi_1\rangle\langle\psi_1|\Big]. \tag{A.3}$$

Um erro na chave de Bob ocorrerá quando ele receber $\hat{\rho}'$ e identificar $|\psi_1\rangle$ em suas medições. Logo, a probabilidade de erro na chave (P_M) será:

$$\begin{aligned} P_M = \mathrm{Tr}(\hat{\Pi}_1^{\mathrm{SA}}\hat{\rho}') &= \frac{1}{2}\mathrm{Tr}\left[\frac{1 + \sin 2\theta}{2\cos^2\theta}\left|\bar{\psi}_0\right\rangle\left\langle\bar{\psi}_0\middle|\psi_0\right\rangle\langle\psi_0| + \frac{1 - \sin 2\theta}{2\cos^2\theta}\left|\bar{\psi}_0\right\rangle\left\langle\bar{\psi}_0\middle|\psi_1\right\rangle\langle\psi_1|\right] \\ &= (1 - \sin 2\theta)\sin^2\theta, \end{aligned} \tag{A.4}$$

onde $\left|\bar{\psi}_0\right\rangle$ é o estado ortogonal a $|\psi_0\rangle$. A intervenção de Eva será bem sucedida quando Bob atribuir o mesmo valor que Alice para o bit de sua chave. Isso acontecerá com uma probabilidade (P_C) dada por:

$$\begin{aligned} P_C = \mathrm{Tr}(\hat{\Pi}_0^{\mathrm{SA}}\hat{\rho}') &= \frac{1}{2}\mathrm{Tr}\left[\frac{1 + \sin 2\theta}{2\cos^2\theta}\left|\bar{\psi}_1\right\rangle\left\langle\bar{\psi}_1\middle|\psi_0\right\rangle\langle\psi_0| + \frac{1 - \sin 2\theta}{2\cos^2\theta}\left|\bar{\psi}_1\right\rangle\left\langle\bar{\psi}_1\middle|\psi_1\right\rangle\langle\psi_1|\right] \\ &= (1 + \sin 2\theta)\sin^2\theta, \end{aligned} \tag{A.5}$$

onde $\left|\bar{\psi}_1\right\rangle$ é o estado ortogonal a $|\psi_1\rangle$.

A taxa de erro (Q) será então:

$$Q = \frac{P_M}{P_M + P_C} = \frac{1}{2}(1 - \sin 2\theta). \tag{A.6}$$

Discriminação sem ambiguidade

Novamente, suponha que Alice envie $|\psi_0\rangle$. Com a discriminação sem ambiguidade, Eva terá uma probabilidade de acerto (P_0), erro (P_1) ou falha (P_F) que serão dadas por:

$$P_0 = \mathrm{Tr}\Big(\hat{\Pi}_0^{\mathrm{SA}} |\psi_0\rangle\langle\psi_0|\Big) = 2\sin^2\theta, \tag{A.7}$$

$$P_1 = \mathrm{Tr}\Big(\hat{\Pi}_1^{\mathrm{SA}} |\psi_0\rangle\langle\psi_0|\Big) = 0, \tag{A.8}$$

$$P_F = \mathrm{Tr}\Big(\hat{\Pi}_F^{\mathrm{SA}} |\psi_0\rangle\langle\psi_0|\Big) = \cos 2\theta. \tag{A.9}$$

A matriz densidade resultante do processo será:

$$\begin{aligned}\hat{\rho}' &= 2\sin^2\theta\,|\psi_0\rangle\langle\psi_0| + \frac{\cos 2\theta}{2}\Big(\,|\psi_0\rangle\langle\psi_0| + |\psi_1\rangle\langle\psi_1|\,\Big) \\ &= \frac{1}{2}\Big[(\cos^2\theta + 3\sin^2\theta)\,|\psi_0\rangle\langle\psi_0| + \cos 2\theta\,|\psi_0\rangle\langle\psi_0|\Big].\end{aligned} \tag{A.10}$$

Similarmente ao caso anterior, a probabilidade P_M será:

$$\begin{aligned}P_M &= \mathrm{Tr}(\hat{\Pi}_1^{\mathrm{SA}}\hat{\rho}') = \frac{1}{2}\mathrm{Tr}\left[\frac{\cos^2\theta + 3\sin^2\theta}{2\cos^2\theta}\left|\bar{\psi}_0\right\rangle\left\langle\bar{\psi}_0\middle|\psi_0\right\rangle\langle\psi_0| + \frac{\cos 2\theta}{2\cos^2\theta}\left|\bar{\psi}_0\right\rangle\left\langle\bar{\psi}_0\middle|\psi_1\right\rangle\langle\psi_1|\right] \\ &= \cos 2\theta \sin^2\theta.\end{aligned} \tag{A.11}$$

A probabilidade P_C será:

$$\begin{aligned}P_C &= \mathrm{Tr}(\hat{\Pi}_0^{\mathrm{SA}}\hat{\rho}') = \frac{1}{2}\mathrm{Tr}\left[\frac{\cos^2\theta + 3\sin^2\theta}{2\cos^2\theta}\left|\bar{\psi}_1\right\rangle\left\langle\bar{\psi}_1\middle|\psi_0\right\rangle\langle\psi_0| + \frac{\cos 2\theta}{2\cos^2\theta}\left|\bar{\psi}_1\right\rangle\left\langle\bar{\psi}_1\middle|\psi_1\right\rangle\langle\psi_1|\right] \\ &= (\cos^2\theta + 3\sin^2\theta)\sin^2\theta.\end{aligned} \tag{A.12}$$

A taxa de erro (Q) será dada por:

$$Q = \frac{P_M}{P_M + P_C} = \frac{\cos 2\theta}{2}. \tag{A.13}$$

Separação de estados

O cálculo da taxa de erro para a separação de estados é similar ao que foi realizado anteriormente. Inicia-se supondo que Alice enviou $|\psi_0\rangle$. A probabilidade que Eva obtenha um erro (P_1), um certo (P_0) ou uma falha (P_F) serão dadas por:

$$P_0 = \mathrm{Tr}\Big(\hat{\Pi}_0^{\mathrm{EM}}\hat{A}_S |\psi_0\rangle\langle\psi_0| \hat{A}_S^\dagger\Big) = P_S(1 - P_{\mathrm{err}}), \tag{A.14}$$

$$P_1 = \mathrm{Tr}\Big(\hat{\Pi}_1^{\mathrm{EM}}\hat{A}_S |\psi_0\rangle\langle\psi_0| \hat{A}_S^\dagger\Big) = P_S P_{\mathrm{err}}, \tag{A.15}$$

$$P_F = \mathrm{Tr}\Big(\hat{A}_F |\psi_0\rangle\langle\psi_0| \hat{A}_F^\dagger\Big) = 1 - P_S, \tag{A.16}$$

onde P_S e P_{err} são definidos como:

$$P_S = \frac{1}{(1-\zeta) + \frac{\zeta}{2\sin^2\theta}}, \tag{A.17}$$

$$P_{\text{err}} = \frac{1}{2}\left[1 - \sqrt{1-(1-\zeta)^2\cos^2 2\theta}\right]. \tag{A.18}$$

A matriz densidade resultante do processo será:

$$\begin{aligned}\hat{\rho}' &= P_S(1-P_{\text{err}})\,|\psi_0\rangle\langle\psi_0| + P_S P_{\text{err}}\,|\psi_1\rangle\langle\psi_1| + \frac{1-P_S}{2}\Big(\,|\psi_0\rangle\langle\psi_0| + |\psi_1\rangle\langle\psi_1|\,\Big) \\ &= \frac{1}{2}\Big[1 - P_S(1-2P_{\text{err}})\,|\psi_0\rangle\langle\psi_0| + 1 - P_S(1+2P_{\text{err}})\,|\psi_1\rangle\langle\psi_1|\,\Big].\end{aligned} \tag{A.19}$$

Novamente, a probabilidade P_M será:

$$P_M = \text{Tr}\big(\hat{\Pi}_1^{\text{SA}}\rho'\big) = \Big[1 - P_S(1+2P_{\text{err}})\Big]\sin^2\theta. \tag{A.20}$$

A probabilidade P_C será dada por:

$$P_C = \text{Tr}\big(\hat{\Pi}_0^{\text{SA}}\rho'\big) = \Big[1 - P_S(1-2P_{\text{err}})\Big]\sin^2\theta. \tag{A.21}$$

A taxa de erro (Q) será dada, então, por:

$$Q = \frac{P_M}{P_M + P_C} = \frac{1}{2}\left[1 - P_S\sqrt{1-(1-\zeta)^2\cos^2 2\theta}\right]. \tag{A.22}$$

Os valores de ζ são definidos entre em 0 e 1, sendo que, nessa estratégia, os limites correspondem ao erro mínimo e a discriminação sem ambiguidade respectivamente. Ao substituir $\zeta = 0$ na equação (A.22), o valor de Q será igual ao obtido na equação (A.6) e, quando $\zeta = 1$, ele será igual ao da equação (A.13).

A.1.2 Supressão

A interceptação-reenvio com supressão se assemelha ao caso da separação de estados na interceptação-reenvio, porém Eva mascara suas falhas. Consequentemente, as probabilidades de erro e acerto (P_0 e P_1) de Eva serão as mesmas, logo a matriz densidade que ela enviará será:

$$\hat{\rho}' = P_S(1-P_{\text{err}})\,|\psi_0\rangle\langle\psi_0| + P_S P_{\text{err}}\,|\psi_1\rangle\langle\psi_1|\,. \tag{A.23}$$

A probabilidade P_M será:

$$P_M = \text{Tr}(\hat{\Pi}_1^{\text{SA}}\hat{\rho}') = P_S P_{\text{err}}. \tag{A.24}$$

A probabilidade P_C será dada por:

$$P_C = \text{Tr}(\hat{\Pi}_0^{\text{SA}}\hat{\rho}') = P_S(1-P_{\text{err}}). \tag{A.25}$$

A taxa de erro (Q) será, então:

$$Q = \frac{P_M}{P_M + P_C} = \frac{1}{2}P_{\text{err}} = \frac{1}{2}\left[1 - \sqrt{1-(1-\zeta)^2\cos^2 2\theta}\right]. \tag{A.26}$$

A.2 Taxas de erro para os ataques ao PBC00

A.2.1 Interceptação-reenvio

Discriminação com erro mínimo

Supondo que Alice envie $|A\rangle$, Eva aplicará a discriminação com erro mínimo e identificará, com determinada probabilidade, erroneamente (P'_B, P'_C) ou corretamente (P_A). Essas probabilidades serão:

$$P_A = \mathrm{Tr}\Big(\hat{\Pi}_0^{\mathrm{EM}} |A\rangle\langle A|\Big) = \frac{1}{3}(1+\sin 2\theta), \tag{A.27}$$

$$P'_B = \mathrm{Tr}\Big(\hat{\Pi}_1^{\mathrm{EM}} |A\rangle\langle A|\Big) = \frac{1}{3}\left(1-\frac{1}{2}\sin 2\theta\right), \tag{A.28}$$

$$P'_C = \mathrm{Tr}\Big(\hat{\Pi}_2^{\mathrm{EM}} |A\rangle\langle A|\Big) = \frac{1}{3}\left(1-\frac{1}{2}\sin 2\theta\right), \tag{A.29}$$

onde $\hat{\Pi}_j^{\mathrm{EM}}$ são os elementos do POVM definidos em (3.31) para a discriminação com erro mínimo de três estados não-ortogonais. A matriz densidade, após a medição de Eva, se torna então:

$$\hat{\rho}' = \frac{1}{3}\left[\left(1+\sin 2\theta\right)|A\rangle\langle A| + \left(1-\frac{1}{2}\sin 2\theta\right)\Big(|B\rangle\langle B| + |C\rangle\langle C|\Big)\right]. \tag{A.30}$$

Eva introduzirá um erro na chave construída por Bob quando ele ao utilizar o operador ortogonal a $|A\rangle$ e obtiver 1 como resultado. Sendo assim, a probabilidade (P_M) que isso aconteça será:

$$P_M = \frac{1}{3}\mathrm{Tr}\Big(|\bar{A}\rangle\langle\bar{A}|\,\rho'\Big) = \frac{2}{3}\left(1-\frac{1}{2}\sin 2\theta\right)\sin^2\theta\cos^2\theta. \tag{A.31}$$

Eva será bem sucedida quando Bob utilizar operadores ortogonais a $|B\rangle$ ou $|C\rangle$ e Alice anunciar que não enviou $|C\rangle$ ou $|B\rangle$, respectivamente. A probabilidade (P_C) que isso aconteça será:

$$P_C = \frac{1}{3}\frac{1}{2}\mathrm{Tr}\left[\Big(|\bar{B}\rangle\langle\bar{B}| + |\bar{C}\rangle\langle\bar{C}|\Big)\rho'\right] = \frac{1}{3}\left[\left(2+\frac{1}{2}\sin 2\theta\right)\sin^2\theta\cos^2\theta\right]. \tag{A.32}$$

A taxa de erro (Q) será então:

$$Q = \frac{P_M}{P_M + P_C} = \frac{2-\sin 2\theta}{4-\frac{1}{2}\sin 2\theta}. \tag{A.33}$$

Discriminação com confiança máxima

A discriminação com confiança máxima, terá uma probabilidade de erro (P'_B e P'_C), acerto (P_A) ou falha (P_F), para o caso em que Alice envie $|A\rangle$. Seguindo os cálculos feitos

anteriormente:

$$P_A = \mathrm{Tr}\Big(\hat{\Pi}_0^{\mathrm{CM}} \left|A\right\rangle\!\left\langle A\right| \Big) = \frac{4}{3}\sin^2\theta, \tag{A.34}$$

$$P'_B = \mathrm{Tr}\Big(\hat{\Pi}_1^{\mathrm{CM}} \left|A\right\rangle\!\left\langle A\right| \Big) = \frac{1}{3}\sin^2\theta, \tag{A.35}$$

$$P'_C = \mathrm{Tr}\Big(\hat{\Pi}_2^{\mathrm{CM}} \left|A\right\rangle\!\left\langle A\right| \Big) = \frac{1}{3}\sin^2\theta, \tag{A.36}$$

$$P_F = \mathrm{Tr}\Big(\hat{\Pi}_F^{\mathrm{CM}} \left|A\right\rangle\!\left\langle A\right| \Big) = \cos 2\theta, \tag{A.37}$$

sendo que os operadores $\hat{\Pi}_j^{\mathrm{CM}}$ foram definidos em (3.58) e (3.59). A matriz densidade após a medição de Eva será então:

$$\begin{aligned}\hat{\rho}' &= \frac{1}{3}\Bigg[4\sin^2\theta \left|A\right\rangle\!\left\langle A\right| + \sin^2\theta \left|B\right\rangle\!\left\langle B\right| + \sin^2\theta \left|C\right\rangle\!\left\langle C\right| + \cos 2\theta\Big(\left|A\right\rangle\!\left\langle A\right| + \left|B\right\rangle\!\left\langle B\right| + \left|C\right\rangle\!\left\langle C\right| \Big)\Bigg] \\ &= \frac{1}{3}\Bigg[(\cos^\theta + 3\sin^2\theta) \left|A\right\rangle\!\left\langle A\right| + \cos^2\theta \left|B\right\rangle\!\left\langle B\right| + \cos^2\theta \left|C\right\rangle\!\left\langle C\right| \Bigg].\end{aligned} \tag{A.38}$$

A probabilidade P_M será:

$$P_M = \frac{1}{3}\mathrm{Tr}\Big(\left|\bar{A}\right\rangle\!\left\langle \bar{A}\right| \rho' \Big) = \frac{2}{3}\sin^2\theta\cos^4\theta. \tag{A.39}$$

A probabilidade P_C será dada por:

$$P_C = \frac{1}{2}\frac{1}{3}\mathrm{Tr}\Bigg[\Big(\left|\bar{B}\right\rangle\!\left\langle \bar{B}\right| + \left|\bar{C}\right\rangle\!\left\langle \bar{C}\right| \Big)\hat{\rho}'\Bigg] = \frac{1}{3}\Big[(2+\sin^2\theta)\sin^2\theta\cos^2\theta\Big]. \tag{A.40}$$

A taxa de erro (Q) será, então:

$$Q = \frac{P_M}{P_M + P_C} = \frac{2 - 2\sin^2\theta}{4 - \sin^2\theta}. \tag{A.41}$$

Separação de estados

Seguindo o raciocínio apresentado para as estratégias anteriores:

$$P_A = \mathrm{Tr}\Big(\hat{\Pi}_0^{\mathrm{EM}} \hat{A}_S \left|A\right\rangle\!\left\langle A\right| \hat{A}_S^\dagger\Big) = P_S(1 - P_{\mathrm{err}}), \tag{A.42}$$

$$P_B = \mathrm{Tr}\Big(\hat{\Pi}_1^{\mathrm{EM}} \hat{A}_S \left|A\right\rangle\!\left\langle A\right| \hat{A}_S^\dagger\Big) = \frac{1}{2}P_S P_{\mathrm{err}}, \tag{A.43}$$

$$P_C = \mathrm{Tr}\Big(\hat{\Pi}_2^{\mathrm{EM}} \hat{A}_S \left|A\right\rangle\!\left\langle A\right| \hat{A}_S^\dagger\Big) = \frac{1}{2}P_S P_{\mathrm{err}}, \tag{A.44}$$

$$P_F = 1 - P_S, \tag{A.45}$$

sendo P_S e P_{err}:

$$P_S = \frac{1}{(1-\zeta) + \frac{\zeta}{2\sin^2\theta}}, \tag{A.46}$$

$$P_{\mathrm{err}} = \frac{2}{3}\Bigg[1 - \frac{1}{2}\sqrt{1 - (1-\zeta)^2\cos^2 2\theta}\Bigg]. \tag{A.47}$$

A matriz densidade após a medição de Eva será:

$$\begin{aligned}\hat{\rho}' &= \frac{1-P_S}{3}\Big(|A\rangle\langle A| + |B\rangle\langle B| + |C\rangle\langle C| \Big) + \frac{P_S}{3}\left[1 - P_{\text{err}}\,|A\rangle\langle A| + \frac{P_{\text{err}}}{2}\,|B\rangle\langle B| + \frac{P_{\text{err}}}{2}\,|C\rangle\langle C|\right] \\ &= \frac{1}{3}\left[1 - P_S P_{\text{err}}\,|A\rangle\langle A| + 1 - P_S\left(1 - \frac{P_{\text{err}}}{2}\right)|B\rangle\langle B| + 1 - P_S\left(1 - \frac{P_{\text{err}}}{2}\right)|C\rangle\langle C|\right].\end{aligned} \tag{A.48}$$

A probabilidade P_M será:

$$P_M = \frac{1}{3}\text{Tr}\Big(\big|\bar{A}\big\rangle\big\langle\bar{A}\big|\,\rho'\Big) = \frac{2}{3}\left[1 - P_S\left(1 - \frac{P_{\text{err}}}{2}\right)\right]\sin^2\theta\cos^2\theta. \tag{A.49}$$

A probabilidade P_C será:

$$P_C = \frac{1}{2}\frac{1}{3}\text{Tr}\left(\big|\bar{B}\big\rangle\big\langle\bar{B}\big|\,\rho' + \big|\bar{C}\big\rangle\big\langle\bar{C}\big|\,\rho'\right) = \frac{1}{3}\left[2 - P_S\left(1 + \frac{P_{\text{err}}}{2}\right)\right]\sin^2\theta\cos^2\theta. \tag{A.50}$$

A taxa de erro (Q) se torna, então:

$$Q = \frac{P_M}{P_M + P_C} = \frac{2 - P_S\sqrt{1-(1-\zeta)^2\cos^2 2\theta}}{4 - \frac{P_S}{2}\sqrt{1-(1-\zeta)^2\cos^2 2\theta}}. \tag{A.51}$$

A verificação que o resultado corresponde ao esperado é feita utilizando ζ igual a 0 e 1. Quando $\zeta = 0$, o resultado encontrado é igual ao obtido na equação (A.33). Quando $\zeta = 1$, o resultado será igual ao encontrado em (A.41).

A.2.2 Supressão

A análise da taxa de erro da supressão é a mesma que foi realizada para a separação de estados, mas agora Eva irá mascarar suas falhas. As probabilidades de erro e acerto de Eva serão iguais às obtidas anteriormente, sendo assim:

$$P_A = P_S(1 - P_{\text{err}}), \tag{A.52}$$

$$P'_B = \frac{1}{2}P_S P_{\text{err}}, \tag{A.53}$$

$$P'_C = \frac{1}{2}P_S P_{\text{err}}, \tag{A.54}$$

A matriz densidade, após a medição, será:

$$\hat{\rho}' = \frac{P_S}{2}\left[(2 - 2P_{\text{err}})\,|A\rangle\langle A| + P_{\text{err}}\Big(|B\rangle\langle B| + |C\rangle\langle C| \Big)\right]. \tag{A.55}$$

A probabilidade P_M será:

$$P_M = \frac{1}{3}\text{Tr}\Big(\big|\bar{A}\big\rangle\big\langle\bar{A}\big|\,\hat{\rho}'\Big) = P_S P_{\text{err}}\sin^2\theta\cos^2\theta. \tag{A.56}$$

A probabilidade P_C será:

$$P_C = \frac{1}{2}\frac{1}{3}\mathrm{Tr}\left[\left(\left|\bar{B}\right\rangle\!\left\langle\bar{B}\right| + \left|\bar{C}\right\rangle\!\left\langle\bar{C}\right|\right)\hat{\rho}'\right] = \frac{P_S}{2}\left[2 - P_{\mathrm{err}}\right]\sin^2\theta\cos^2\theta. \tag{A.57}$$

A taxa de erro (Q) será, então:

$$Q = \frac{P_M}{P_M + P_C} = \frac{2 - \sqrt{1-(1-\zeta)^2\cos 2\theta}}{4 - \frac{1}{2}\sqrt{1-(1-\zeta)^2\cos 2\theta}}. \tag{A.58}$$

Referências

[1] C. E. Shannon: *Communication Theory of Secrecy Systems.* Bell Labs Technical Journal **28**, 656-715 (1949).

[2] M. Bellare, O. Goldreich, A. Mityagin: *The Power of Verification Queries in Message Authentication and Authenticated Encryption.* IACR Cryptology ePrint Archive (2004).

[3] M. Bellare, J. Kilian, P. Rogaway: *The security of the cipher block chaining message authentication code.* Journal of Computer and System Sciences **61**, 362-399 (2000).

[4] D. J. Bernstein: *How to stretch random functions: the security of protected counter sums.* Journal of Cryptology **12**, 185–192 (1999).

[5] W. Diffie, M. Hellman: *New directions in cryptography.* IEEE transactions on Information Theory **22**, 644 - 654 (1976).

[6] R. L. Rivest, A. Shamir, L. Adleman: *A method for obtaining digital signatures and public-key cryptosystems.* Communications of the ACM **21**, 120-126 (1978).

[7] M. O. Rabin: *Digitalized signatures and public-key functions as intractable as factorization.* Tehcnical Report TR-212, MIT/LCS (1979).

[8] M. Bellare, R. Canetti, H. Krawczyk: *Keying hash functions for message authentication.* Advances in Cryptology — CRYPTO '96, 1-15 (1996).

[9] I. B. Damgård: *A design principle for hash functions.* Advances in Cryptology — CRYPTO' 89 Proceedings, 416-427 (1989).

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

[11] S. M. Barnett: *Quantum Information.* Oxford University Press (2009).

[12] M. Giles, W. Knight: *Google thinks it's close to "quantum supremacy". Here's what that really means.* MIT Technology Review (2018).

[13] D. Alsina, J. I. Latorre: *Experimental test of Mermin inequalities on a five-qubit quantum computer.* Physical Review A **94**, 012314 (2016).

[14] P. W. Shor: *Algorithms for quantum computation: discrete logarithms and factoring.* Proceedings 35th Annual Symposium on Foundations of Computer Science, 124-134 (1994).

[15] D. J. Bernstein, T. Lange: *Post-quantum cryptography.* Nature **549**, 188–194 (2017).

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

[17] C. H. Bennett, G. Brassard: *Quantum cryptography: public key distribution and coin tossing.* Proceedings of IEEE International Conference on Computers, Systems and Signal Processing 175, 9-12 (1984); republicado em Theoretical Compututer Science **560**, 7-11 (2014).

[18] C. H. Bennett: *Quantum cryptography using any two nonorthogonal states.* Physical Review Letters **68**, 3121-3124 (1992).

[19] S. J. D. Phoenix, S. M. Barnett, A. Chefles: *Three-state quantum cryptography.* Journal of Modern Optics **47-2**, 507-516 (2000).

[20] J. Katz, Y. Lindel: *Introduction to Modern Cryptography.* Chapman & Hall/CRC (2008).

[21] A. Kerckhoffs: *La cryptographie militaire.* Journal des sciences militaires **IX**, 5-38 (1883).

[22] G. B. Bellaso: *La Cifra del Sig. Giovan Battista Belaso.* Veneza (1553).

[23] B. de Vigenère: *Traicté des Chiffres, ou Secretes Manieres d'Escrire.* Paris (1586).

[24] S. M. Bellovin: *Frank Miller: Inventor of the One-Time Pad.* Cryptologia **35**, 203–222.

[25] G. S. Vernam: *Secret Signaling system.* Patente US1310719A arquivada do original por *google.com* (2016).

[26] National security agency-USA: *Venona.* site criado em 2016 e último acesso em 2018.

[27] A. S. Holevo: *The Capacity of Quantum Channel with General Signal States.* IEEE Transactions on Information Theory **44**, 269-273 (1973).

[28] D. Dieks: *Communication by EPR devices.* Physics Letters A **92**, 271-272 (1982).

[29] W. K. Wootters, W. H. Zurek: *A single quantum cannot be cloned.* Nature **299**, 802–803 (1982).

[30] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, B. Schumacher: *Noncommuting Mixed States Cannot Be Broadcast.* Physical Review Letters **76**, 2818-2821 (1996).

[31] N. Gisin, S. Massar: *Optimal Quantum Cloning Machines.* Physical Review Letters **79**, 2153-2156 (1997).

[32] D. Bruß, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, J. A. Smolin: *Optimal universal and state-dependent quantum cloning.* Physical Reviews A **57**, 2368-2378 (1998).

[33] V. Bužek, M. Hillery: *Quantum copying: Beyond the no-cloning theorem.* Physical Review A **54**, 1844 - 1852 (1996).

[34] L. M. Duan, G. C. Guo: *Probabilistic cloning and identification of linearly independent quantum states.* Physical Review Letters **80**, 4999-5002 (1998).

[35] J. A. Bergou, M. Hillery: *Introduction to the Theory of Quantum Information Processing.* Springer (2013).

[36] J. A. Bergou: *Discrimination of quantum states.* Journal of Modern Optics **57**, 160-180 (2010).

[37] A. Chefles: *Quantum state discrimination.* Contemporary Physics **41**, 401-424 (2000).

[38] S. M. Barnett, S. Croke: *Quantum state discrimination.* Advances in Optics and Photonics **1**, 238-278 (2009).

[39] C. W. Helstrom: *Quantum Detection and Estimation Theory.* Springer (1976).

[40] I. D. Invnovic: *How to differentiate between non-orthogonal states.* Physics Letters A **123**, 257-259 (1987).

[41] A. Peres: *How to differentiate between non-orthogonal states.* Physics Letters A **128**, 19 (1988).

[42] D. Dieks: *Overlap and distinguishability of quantum states.* Physics Letters A **126**, 303-306 (1988).

[43] G. Jaeger, A. Shimony: *Optimal distinction between two non-orthogonal quantum states.* Physics Letters A **197**, 83-87 (1995).

[44] A. Chefles: *Unambiguous Discrimination Between Linearly-Independent Quantum States.* Physics Letters A **239**, 339-347 (1998).

[45] S. Croke, E. Andersson, S. M. Barnett, C. R. Gilson, J. Jeffers: *Maximum confidence quantum measurements.* Physical Review Letters **96**, 070401 (2006).

[46] A. Chefles, S. M. Barnett: *Quantum state separation, unambiguous discrimination and exact cloning.* Journal of Physics A: Mathematical and General **31**, 10097–10103 (1998).

[47] M.A. Solís-Prosser, A. Delgado, O. Jiménez, L. Neves: *Parametric separation of symmetric pure quantum states.* Physical Review A **93**, 012337 (2016.

[48] A. Chefles, S.M. Barnett: *Strategies for discriminating between non-orthogonal quantum states*. Journal of Modern Optics **45**, 1295-1302 (1998).

[49] M. Ban, K. Kurokawa, R. Momose, O. Hirota: *Optimum measurements for discrimination among symmetric quantum states and parameter estimation*. International Journal of Theoretical Physics **36**, 1269–1288 (1997).

[50] S. Crooke, P. J. Mosley, S. M. Barnett, I. A. Walmsley: *Maximum confidence measurements and their optical implementation*. European Physical Journal D **41**, 589–598 (2007).

[51] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, G. Ribordy: *Trojan-horse attacks on quantum-key-distribution systems*, Physical Review A **73**, 022320 (2006).

[52] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, G. Leuchs: *Risk analysis of Trojan-horse attacks on practical quantum key distribution systems*, IEEE Journal of Selected Topics in Quantum Electronics **21**, 6600710 (2015).

[53] S. Félix, N. Gisin, A. Stefanov, H. Zbinden: *Faint laser quantum key distribution: Eavesdropping exploiting multiphoton pulses*, Journal of Modern Optics **48**, 2009-2021 (2001).

[54] G. Brassard, N. Lütkenhaus, T. Mor, B. C. Sanders: *Limitations on Practical Quantum Cryptography*, Physical Review Letters **85**, 1330-1333 (2000).

[55] N. Lütkenhaus, M. Jahma: *Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack*, New Journal of Physics **4**, 1-9 (2002).

[56] E. Biham, T. Mor: *Security of Quantum Cryptography against Collective Attacks*, Physical Review Letters **78**, 2256-2259 (1997).

[57] E. Biham, T. Mor: *Bounds on Information and the Security of Quantum Cryptography*, Physical Review Letters **79**, 4034-4037 (1997).

[58] J. A. Bergou: *Quantum state discrimination and selected applications*. Journal of Physics: Conference Series **84**, 012001 (2007).