Universidade Federal do Ceará
Centro de Tecnologia
Departamento de Engenharia de Teleinformática

Protocolos quânticos para sistemas de prova de conhecimento nulo

José Cláudio do Nascimento

Fortaleza, CE
3 de março de 2010

José Cláudio do Nascimento

Protocolos quânticos para sistemas de prova de conhecimento nulo

Universidade Federal do Ceará

Centro de Tecnologia

Departamento de Engenharia de Teleinformática

Tese submetida a Coordenação do Programa de Pós-Graduação em Engenharia de Teleinformática da Universidade Federal do Ceará, como parte dos pré-requisitos para a obtenção do grau de Doutor em Engenharia de Teleinformática.

Orientador: Rubens Viana Ramos

Fortaleza, CE
3 de março de 2010

Título em Inglês:	Quantum protocols for zero knowledge systems
Palavras-chave em Inglês:	Quantum protocols, zero knowledge, cryptograpy, security Communication, one-way functions, Complexity Theory,
Área de concentração:	Engenharia de Computação
Titulação:	Doutor em Engenharia de Teleinformática
Banca Examinadora:	Dr. Carlile Campos Lavor, Dr. Francisco Marcos de Assis, Dra. Hilma Helena Macedo de Vasconcelos, Dr. João Batista Rosa Silva e Dr. Paulo Benício Melo de Sousa
Data da defesa:	11/12/2009

X***x

Nascimento, José Cláudio do
Protocolos quântico para sistemas de prova de conhecimento nulo
José Cláudio do Nascimento. – Fortaleza, CE: [s.n.], 2009.

Orientador: Rubens Viana Ramos.
Tese (doutorado) - Universidade Federal do Ceará, Departamento de Engenharia de Teleinformática.

1. Sistemas de comunicações. 2. Teoria da Computação. 3. Criptografia. 4. Teoria da informação quântica. 5. Teoria da computação quântica.

José Cláudio do Nascimento

Protocolos quânticos para sistemas de prova de conhecimento nulo

Tese submetida a Coordenação do Programa de Pós-Graduação em Engenharia de Teleinformática da Universidade Federal do Ceará, como parte dos pré-requisitos para a obtenção do grau de Doutor em Engenharia de Teleinformática.

Aprovada em 11 de dezembro de 2009.

Banca Examinadora:

_____

Prof. Dr. Rubens Viana Ramos - UFC

_____

Prof. Dr. Carlile Campos Lavor - UNICAMP

_____

Prof. Dr. Francisco Marcos de Assis - UFCG

_____

Prof. Dr. Hilma Helena Macedo de Vasconcelos - UFC

_____

Prof. Dr. João Batista Rosa Silva - UFC

_____

Prof. Dr. Paulo Benício Melo de Sousa - UNIFOR

Fortaleza, CE
2009

Aos meus pais, José Manuel do Nascimento e Cícera Maria Conceição do Nascimento.

Agradecimentos

A Deus por provar a sua graça e ser misericordioso para comigo.

Ao meu orientador, Prof. Dr. Rubens Viana Ramos, pelo esforço em me orientar neste tema.

Pelos momentos de trabalho juntos, eu faço meus agradecimentos aos meus colegas de pós-graduação: Paulo Vinícios, Fátima Regina, Daniel Barbosa, Daniela, Fernando, Werther Xisto, Fábio Alencar e Glaucionor. .

À minha família, pelo apoio durante esta jornada.

À CAPES, pelo apoio financeiro.

*Ora, a fé é o firme fundamento das coisas que se esperam, e a **prova** das coisas que se não vêem.*

Hebreus 11:1

Resumo

A presente tese propõe protocolos quânticos aplicados a sistemas interativos de conhecimento nulo. Primeiramente, o uso de estados coerente para construir o compromisso necessário para os sistemas de prova de conhecimento nulo para toda linguagem $\mathcal{NP}$ é proposta. Em seguida, dois protocolos quânticos, com e sem entrelaçamento, são construídos para impedir a simulação da interação entre provador e verificador em protocolos de conhecimento nulo. Depois, é mostrado um protocolo quântico para resgatar a autoria de uma assinatura anônima em um esquema de assinatura em anel usando estados de Bell. Por fim, é proposto um esquema quântico de denúncia anônima em que o delator pode optar por revelar sua identidade após a assinatura.

Abstract

The present thesis proposes quantum protocols applied to interactive zero-knowledge systems. Firstly, the use of coherent states for construction of the commitment needed for implementation of zero-knowledge systems, based on $\mathcal{NP}$ language, is proposed. Following it, two quantum protocols, with and without entanglement, were proposed in order to prevent the classical simulation of the interaction between prover and verifier in zero-knowledge systems. After that, it is shown a quantum protocol which uses Bell states to recover the anonymous copyright signature in a scheme for signatures in a ring topology. Finally, it is proposed a quantum scheme for anonymous delation in which the delator can decide whether to reveal or not their identity afterwards.

Sumário

Lista de Figuras

Lista de Tabelas

Introdução

Criptografia é uma área de estudo, dentro da teoria da informação, voltada às técnicas de comunicação com mensagens secretas. Essas técnicas sempre existiram em situações de conflito em que a comunicação secreta era necessária. Um exemplo é o código de César usado pelas tropas romanas. No entanto, a era da criptografia moderna começa realmente com Claude Shannon. Em 1949, ele publicou com Warren Weaver um artigo intitulado *Communication Theory of Secrecy Systems* [1]. Esse artigo, junto com outros de seus trabalhos que criaram a área da teoria da informação, estabeleceram uma base teórica sólida para a criptografia e para a criptoanálise. Falando de forma intuitiva, nesta formalização, um criptossistema tem sigilo ideal quando, independente de quantos textos em claro um criptoanalista obtenha, para ele nunca haverá uma solução única para os textos cifrados, mas várias soluções com a mesma probabilidade. Em outras palavras, a entropia que o criptoanalista tem a respeito da mensagem, dado qualquer texto cifrado, é igual a entropia da própria mensagem.

Uma mudança de paradigma na definição de segurança em criptografia ocorreu com a publicação do artigo *New Directions in Cryptography* por Whitfield Diffie e Martin Hellman. Esse trabalho iniciou a pesquisa em sistemas de criptografia de chave pública [2]. O algoritmo proposto ficou conhecido como "algoritmo Diffie-Hellman para troca de chaves" e levou ao imediato surgimento de pesquisas nesse campo, que culminou com a criação do algoritmo RSA, por Ronald Rivest, Adi Shamir e Leonard Adleman [3]. Nesse novo paradigma de criptografia as teorias de Shannon, como previamente mencionadas, eram de pouca valia: a noção importante agora não era mais a de um sigilo perfeito, impossível de ser atingido na criptografia assimétrica, mas de um sigilo computacional, que indicasse que o custo envolvido em quebrar um criptossistema seria de tempo não polinomial.

Os anos 80 do século XX trouxeram uma necessidade de reavaliação do conceito de segurança segundo o novo paradigma proposto por Diffie e Hellman. As ferramentas utilizadas até então para a avaliação de segurança de criptossistemas não se adequavam bem ao novo cenário, uma vez que a segurança não estava mais baseada na existência de informação relativa a textos em claro nos respectivos textos cifrados, mas em quão difícil é calcular (ou utilizar) tal infor-

mação. Um profundo estudo da formalização da criptografia demonstrável, fortemente baseado na teoria da complexidade, marcou aquela década, impulsionado por trabalhos como o de Goldwasser e Micali em 1982 [4], Yao em 1982 [5], Blum e Goldwasser em 1985 [6], e Micali at al em 1988 [7].

Dentro desse novo conceito de segurança, uma classe de protocolos começou a mostrar sua importância na década de 80. Sistemas de provas de conhecimentos nulo foram inicialmente concebidas em 1985 por Goldwasser, Micali e Rackoff em um artigo sobre prova de conhecimento em sistemas interativos [8]. Nesse artigo, eles implantaram a idéia de prova interativa e complexidade de conhecimento, como uma medida de conhecimento computacional na transferência de uma prova de um provador para um verificador. As pesquisas a cerca desse conceito avançaram até que, Oded Goldreich e outros em [9], deram um passo adiante, mostrando que, assumindo a existência de encriptação inquebrável, pode-se criar um sistema de prova de conhecimento nulo $\mathcal{NP}$-completo (problema de coloração de grafos em três cores). Então, desde que cada problema em $\mathcal{NP}$ possa ser reduzido de forma eficiente a um problema dessa classe, isso significa que, nessa hipótese, todos os problemas em $\mathcal{NP}$ têm um sistema de prova de conhecimento nulo, desde que exista um esquema de criptografia que permita a construção do esquema de compromisso de informação. Em criptografia clássica foi discutida a existência de encriptação inquebrável que cria funções de sentido único, mas é possível que alguns meios físicos também possam consegui-lo. A partir dessa suposição, usam-se os sistemas de cifra quântica com estados coerentes para construir esse algoritmo [10]. Os detalhes dessa proposta são apresentados no Capítulo 3.

Ainda na década de 80, um novo paradigma de segurança começou a surgir. Em 1983, em [11], Wiesner explicou como a teoria quântica pode ser usada para unir duas mensagens em uma única transmissão quântica na qual o receptor poderia decodificar cada uma das mensagens, porém, nunca as duas simultaneamente, pela impossibilidade de violar uma lei da natureza (o princípio de incerteza de Heisenberg). Desse momento em diante, protocolos foram propostos com essa idéia. A distribuição quântica de chaves assumiu um papel de destaque como uma viabilidade de implementação dos sistemas criptográficos de sigilo perfeito (one-time-pad) com segurança incondicional provada [12]. Os protocolos como BB84 e B92 são os mais famosos protocolos dessa classe de criptografia [13, 14].

Peter Shor, em 1997, descobriu um algoritmo quântico para a fatoração [15]. Ele permite um computador quântico fatorar grandes inteiros rapidamente (tempo polinomial). Ele resolve tanto o problema da fatoração quanto o problema do logaritmo discreto. O Algoritmo de Shor poderia, em teoria, quebrar muitos dos sistemas criptográficos em uso atualmente. Essa descoberta criou um enorme interesse nos computadores quânticos, principalmente na busca dos limites do

paradigma da segurança demonstrável, avaliando o poder computacional dessas máquinas.

Em 2006, Watrous mostrou que sistemas de prova de conhecimento nulo são inquebráveis contra ataques de máquinas quânticas, pelo menos nos algoritmos quânticos de redução de complexidade já existente [16]. Neste trabalho, verificadores com poder de simulação em computadores quânticos em tempo polinomial não conseguem bons resultados após interagirem com o provador. Além disso, alguns protocolos de prova de conhecimento nulo executados por máquinas quânticas interativas foram propostos [17, 18]. Mas um fato que se quer destacar nesta tese é o efeito de sistemas quânticos em sistemas de segurança demonstrável para a construção de argumentos que quebram o paradigma da simulação. Os protocolos baseados em segurança demonstrável são fortemente construídos no paradigma da simulação. Muitas demonstrações de segurança de propriedades desses protocolos são construídas sobre a afirmativa de que uma máquina de poder computacional em tempo polinomial pode simular o conhecimento de um procedimento com uma comparação computacional indistinguível. Assim, foi percebido em [19, 20] que dispositivos quânticos podem quebrar essas propriedades e construir outras em sistemas de segurança demonstrável. Esta tese discute melhor esse assunto no Capítulo 4. Nesse capítulo, alguns resultados são apresentados sobre a impossibilidade de transferência de prova em sistemas de prova de conhecimento nulo [10,21,22]. Também é mostrado como uma delator, num esquemas de assinaturas em anel, pode assumir a autoria da assinatura apenas provando que a assinatura é única e não pode ser simulada.

Nessa direção, a presente tese discute sistemas de prova de conhecimento nulo com a aplicação de propriedades quânticas. Novos protocolos foram propostos e análises de segurança foram realizadas. Por fim, o trabalho está organizado da seguinte forma: o Capítulo 1 apresenta os conceitos necessários ao entendimento da tese e os dois principais protocolos de prova de conhecimento nulo baseados na dificuldade de problemas de grafos; o Capítulo 2 apresenta uma básica introdução à teoria da informação quântica para a compreensão dos cálculos feitos nos capítulos seguintes; o Capítulo 3 apresenta a construção do protocolo de prova de conhecimento nulo para toda linguagem em $\mathcal{NP}$ quando a fase de compromisso desse protocolo é feita com o envio de estados quânticos coerentes; o Capítulo 4 trata da construção de argumentos que se valem da impossibilidade de simulação quando sistemas quânticos são inseridos como parte da execução de protocolos clássicos. Esse capítulo mostra como uma simples memória quântica traça a interação entre o provador e verificador em sistema de prova de conhecimento nulo. Depois, apresenta-se como um delator, usando estados de Bell, pode resgatar a sua identidade como autor de assinatura em anel. Por fim, no Capítulo 5 as conclusões e perspectivas são apresentadas.

Capítulo 1

Sistema de transferência de prova com conhecimento nulo

Este capítulo tem como objetivo introduzir alguns conceitos importantes sobre prova de conhecimento nulo seguindo o seguinte roteiro: na seção 1.2, são discutidas as classificações de algoritmos quanto à sua complexidade; na seção 1.3, é apresentado o conceito de prova em sistemas interativos; na seção 1.4, é apresentado o conceito de indistinguibilidade computacional para sistemas que possuem algoritmos indistinguíveis por máquinas de tempo polinomial; por fim, na seção 1.5, são apresentados dois protocolos de prova de conhecimento nulo que serão alvo dos resultados apresentados nesta tese. O primeiro é construído sobre a dificuldade de encontrar um isomorfismo entre grafos, e o segundo protocolo é construído sobre o problema da coloração de grafos (grafos tricoloríveis).

1.1 Introdução

Antes de apresentar a definição de prova de conhecimento nulo, é necessário voltar no tempo para observar um conflito que iniciou a motivação para o desenvolvimento da álgebra moderna. Em meados do século XVI, um debate com objetivo de descobrir o autor do método de solução de equações cúbicas foi promovido devido ao seguinte episódio [23]: Scipione del Ferro (1465-1526), professor de Matemática em Bologna, descobriu uma equação que daria as raízes de equações de terceiro grau. Não publicou a solução, mas antes de sua morte a revelou a um estudante, Antônio Maria Fior. De qualquer maneira os boatos correram. A idéia da existência da solução algébrica para uma equação cúbica se propagou e Tartaglia foi inspirado a dedicar-se a achar o método por conta própria. De forma independente, ou baseado numa sugestão, Tartaglia de fato aprendeu, por volta de 1541, a resolver equações cúbicas. Quando essa notícia

se espalhou foi organizada uma competição matemática entre Tartaglia e Fior. Assim, cada um dos concorrentes propôs trinta questões para que o adversário resolvesse num intervalo de tempo fixado. Chegado o dia da decisão, Tartaglia havia resolvido todas as questões propostas por Fior, enquanto que o seu oponente não tinha resolvido nenhuma das questões.

Esse cenário ilustra muito bem o conceito de prova de conhecimento nulo. Tartaglia e Fior afirmam conhecer um método para encontrar raízes de equações cúbicas. Ambos querem provar isso através de um duelo de questões sem que ambos revelem o método de solução que possuem. Agora, distorcendo um pouco os fatos históricos, será elaborado um algoritmo interativo em que ambos propõem um desafio de uma questão por vez. Suponha que a comissão julgadora do duelo estabeleça como regulamento do desafio o seguinte procedimento:

- Fior desafia Tartaglia elaborando um polinômio de grau 3, $p_{F_1}(x)$, com as suas raízes, x_1, x_2, x_3. Como desafio, Fior envia $p_{F_1}(x) = 0$ a Tartaglia;
- Passado o tempo estabelecido pela comissão, simultaneamente, Fior revela à comissão a resposta de $p_{F_1}(x) = 0$ e Tartaglia revela a solução encontrada por ele.

Os passos são repetidos 30 vezes para que Fior não argumente que Tartaglia teve sorte com a questão. No primeiro momento, Tartaglia é o provador e Fior junto com a comissão julgadora assumem o papel de verificadores do conhecimento de Tartaglia. Terminada a execução, é a vez de Fior ser o provador e Tartaglia e a comissão julgadora fazerem o papel de verificadores. Ao final, quem resolver todas as questões terá provado conhecer o método sem que o adversário e a comissão aprendam o mesmo. Então, a comissão poderá julgar quem é o verdadeiro conhecedor do método de solução de equações cúbicas.

O método que se descreve tem a mesma validade do método real usado pela comissão julgadora para decidir o debate real. Tartaglia provou ter conhecimento para solucionar equações cúbicas sem revelar o método para outros matemáticos, que continuou em oculto até a sua publicação em 1545, [24]. Pode-se dizer que ele transferiu uma prova de conhecimento sem revelar o conhecimento que ele tinha.

Neste trabalho, essa ação é chamada de prova de conhecimento nulo. Naquela época, qualquer outro que tentasse encontrar uma solução levaria bastante tempo ou talvez nunca a encontrasse. As soluções que Tartaglia apresentou no debate em nada caracterizava o método usado por ele para encontrar as raízes da equação. Era dada a ele uma equação cúbica $p_{F_1}(x) = 0$, ele a resolvia e apresentava suas raízes, x_1, x_2, x_3. Para examinar se a solução estava correta, bastava substituir as raízes na equação dada e verificar o resultado, $p_{F_1}(x_1) = p_{F_1}(x_2) = p_{F_1}(x_3) = 0$, algo que podia ser feito em tempo eficiente naquela época. Os verificadores nada aprendiam sobre o método de Tartaglia, uma vez que com a verificação eles não podiam fazer nada melhor

do que simular o conhecimento das raízes de uma equação cúbica. Isso se deve ao fato de que escolhendo-se três números reais, a_1, a_2, a_3, têm-se uma equação cúbica com raízes conhecidas, $p(x) = (x - a_1)(x - a_2)(x - a_3) = 0$.

Usando a teoria da complexidade para a solução de problemas computacionais, Rackoff, Micali e Goldwasser construíram em 1985 o primeiro sistema de prova de conhecimento nulo [8]. Depois disso, muitas aplicações em segurança foram encontradas para tais sistemas. Por exemplo, sistema para votação eletrônica [25,26], sistemas de identificação [27], e dinheiro eletrônico [28]. Em essência, esses protocolos são construídos a partir de problemas computacionais que são lançados a outros usuários da rede como um desafio. Junto dos desafios está uma aplicação que pode ser uma votação, um pagamento em dinheiro eletrônico ou uma simples prova de identidade. Aquele que sabe resolver o desafio é o único capaz de completar as tarefas. A seguir, os conceitos necessários ao entendimento desses protocolos serão apresentados.

1.2 Preliminares sobre complexidade de problemas

Pode-se dizer que linguagens formais são mecanismos formais para a representação e especificação de linguagens. Elas podem ser representadas de maneira finita e precisa através de sistemas com sustentação matemática. Assim, um alfabeto é um conjunto finito e não vazio de símbolos. Aqui, nós consideramos $\Sigma = \{0, 1\}$ como sendo o alfabeto binário. Uma palavra sobre o alfabeto Σ é uma sequência finita de símbolos de Σ. O comprimento de uma palavra w sobre Σ, descrito por $|w|$, é o número de símbolos presentes em w. Em particular, a palavra vazia, denotada por ϵ, é a palavra com zero ocorrência de símbolos. Além disso, quando o comprimento de uma palavra w é indefinido, dizemos que $w \in \Sigma^*$. Um subconjunto $L \subseteq \Sigma^*$ é dito uma linguagem de Σ^* por possuir um conjunto de palavras de Σ^* que podem ser reconhecidas por uma dado problema computacional.

Alan Turing (1912-1954) propôs um modelo de máquina conhecida como Máquina Universal ou Máquina de Turing, considerando apenas os aspectos lógicos para a solução de problemas (memória, estados e transições). Turing construiu esse modelo para provar que não existe um algoritmo universal capaz de detectar proposições indecidíveis em um sistema axiomático [29]. Assim, uma máquina de Turing pode ser pensada como um matemático trabalhando com uma fita infinita de papel, dividida em pequenas casas, e um lápis-borracha que segue suas instruções. Essas instruções são bastante simples: a máquina pode ler um símbolo na fita e, analisando-o, pode apagá-lo e escrever por cima do símbolo lido. A cada mudança de estado, pode mover-se para a direita ou para a esquerda para analisar um novo símbolo, ou simplesmente parar. O modelo de Turing foi proposto em 1936, anos antes dos modernos computadores digitais, e at-

ualmente serve para modelar o funcionamento das máquinas simples de cálculo até as mais complexas. Formalmente, uma máquina de Turing determinística é definida da seguinte maneira:

Definição 1. (*Máquina de Turing determinística*) - *Uma máquina de Turing determinística (com uma fita) é usualmente definida como uma 7-upla* $M = (Q, \Sigma, \Gamma, q_0, \epsilon, F, \delta)$*, onde:*

- Q *é um conjunto finito de estados;*
- Σ *é um alfabeto finito de símbolos;*
- Γ *é o alfabeto da fita (conjunto finito de símbolos);*
- q_0 *é o estado inicial*
- ϵ *é o símbolo branco (o único símbolo que se permite ocorrer na fita infinitamente em qualquer passo durante a computação);*
- F *é o conjunto dos estados finais;*
- $\delta : Q \times \Gamma \rightarrow Q \times \Gamma \times \{\leftarrow, \rightarrow, STAY\}$ *é uma função parcial chamada função de transição, onde* $\leftarrow$ *é o movimento para a esquerda,* $\rightarrow$ *é o movimento para a direita e* $STAY$ *representa o não deslocamento na fita.*

A máquina de Turing determinística funciona da seguinte maneira. A entrada da máquina é escrita numa fita onde ela pode ler e escrever. A máquina começa no estado inicial q_0 com o ponteiro apontando para o primeiro símbolo x_1 da entrada x. O resto da entrada é uma sequência finita de símbolos $x_2x_3 \cdots x_n$. A função de transição δ pode ser vista como o programa da máquina. Em cada passo, a máquina lê o símbolo da entrada. Baseado no símbolo e no estado corrente, a máquina escolhe o próximo estado e define o seu próximo movimento, $\leftarrow$, $STAY$, ou $\rightarrow$. A função de transição δ é projetada para garantir que o ponteiro nunca saia do fim da fita. Se o estado final pertence ao conjunto de estados finais, então diz-se que a máquina aceitou a entrada x. Caso contrário, que ela rejeitou a entrada x. Um *algoritmo* corresponde a uma máquina de Turing que sempre pára.

Para medir a eficiência de um algoritmo é necessário usar o tempo teórico que o programa leva para encontrar uma resposta em função dos dados de entrada. Esse cálculo é feito associando-se uma unidade de tempo para cada transição que o algoritmo executa. Se a dependência do tempo com relação aos dados de entrada for polinomial com o comprimento da entrada $p(|x|)$, o programa é considerado rápido. Se, entretanto, a dependência do tempo for

exponencial com o comprimento da entrada ($a^{|x|}$ para $a > 0$), então o programa é considerado lento. Verifica-se que:

$$\lim_{|x|\to\infty} \frac{a^{|x|}}{|p(|x|)|} = \infty \tag{1.1}$$

A noção de computação em tempo polinomial foi introduzida pro Cobham [30] e Edmonds [31] como parte do desenvolvimento da teoria da complexidade computacional na década de 60 (embora em 1953, von Neumann tenha distinguido entre algoritmos de tempo polinomial e algoritmos de tempo exponencial [32]). Nessa época, foram encontrados muitos algoritmos que resistiam a uma simplificação polinomial. Então, Stephen Cook [33] observou um fato simples: se um problema pode ser resolvido em tempo polinomial, então pode-se também verificar se uma possível solução é correta em tempo polinomial (diz-se que o algoritmo pode ser certificado em tempo polinomial). Uma maneira mais formal de expressar essa idéia, é através da descrição do problema de decisão. Um problema de decisão pode ser visto como um problema de reconhecimento de linguagem. Considere Σ^* como sendo o conjunto de todas as possíveis entradas para um problema de decisão. Considere $L \subseteq \Sigma^*$ como sendo o conjunto de todas as entradas cuja a resposta é sim. Esse conjunto é chamado de linguagem correspondente ao problema. Em [33], Cook definiu duas classes de problemas quanto à complexidade deles.

Definição 2. ($\mathcal{P}$ *- Dizemos que uma linguagem* L *está na classe de complexidade* $\mathcal{P}$*, se* L *é reconhecível em tempo polinomial determinístico, e se existe uma máquina de Turing* M *e um polinômio* $p(\cdot)$ *tal que:*

- *Tendo uma string* x *como entrada, a máquina tem parada após* $p(|x|)$ *passos;*
- $M(x) = 1$*, se somente se,* $x \in L$*.*

Entretanto, existiam problemas que insistiam em não admitir uma simplificação polinomial no seu tempo de execução, mas podiam ser certificados em tempo polinomial. Assim, Cook ainda introduziu a definição de algoritmos *não determinísticos em tempo polinomial*. A classe dos problemas $\mathcal{NP}$ é aquela para a qual apenas pode-se verificar, em tempo polinomial, se uma possível solução é correta. Formalmente, a classe $\mathcal{NP}$ é definida da seguinte maneira:

Definição 3. ($\mathcal{NP}$) *- Uma linguagem* L *está em* $\mathcal{NP}$ *se existe uma relação Booleana* $R_L \subseteq \Sigma^* \times \Sigma^*$ *que pode ser reorganizada em tempo polinomial determinístico e um polinômio* $p(\cdot)$ *de forma que:*

- $x \in L$*, se somente se, existe um* $y \in \Sigma^*$ *tal que* $(x, y) \in R_L$ *e* $|y| \leq p(|x|)$*;*
- $x \notin L$*, se somente se,* $(x, y) \notin R_L$ *para todo* $y \in \Sigma^*$*.*

Olhando para uma máquina de Turing, pode-se entender como os problemas $\mathcal{NP}$ existem. Primeiramente, uma *máquina de Turing não determinística* difere um pouco da Definição 1, pois um estado e um símbolo da fita não mais definem de forma única um novo símbolo a ser escrito, a direção de movimento e o novo estado. Nessa máquina, mais de uma ação pode ser aplicável, dados um novo estado e um novo símbolo. Enquanto uma máquina de Turing determinística possui um único "caminho de computação" a ser seguido, uma máquina de Turing não determinística possui uma "árvore de computação" com diferentes caminhos como opções de computação. Se qualquer ramo da árvore termina em uma condição de aceitação, diz-se que a máquina de Turing não determinística aceita a entrada. Uma indagação sobre o cálculo de tais máquinas é: como uma máquina não determinística sabe qual dessas ações ela deve tomar? Há duas maneiras de olhar essa questão. Uma é supor que a máquina sempre escolherá uma transição que eventualmente leve a um estado de aceitação. Esse caso pode ser calculado deterministicamente por máquinas de Turing determinísticas, no entanto, ela precisa de uma entrada auxiliar que lhe indique o caminho. Por isso, a verificação de um problema pode ser feito em tempo polinomial determinístico. A outra maneira é imaginar que a máquina se ramifica em muitas cópias, cada qual leva a diferentes possíveis transições.

Obviamente $\mathcal{P} \subseteq \mathcal{NP}$, pois a classe $\mathcal{P}$ representa um caso particular de $\mathcal{NP}$. Mas o contrário, $\mathcal{NP} \subseteq \mathcal{P}$, no que implica que $\mathcal{P} = \mathcal{NP}$, não tem sua validade provada. O protocolos apresentados neste capítulo são construídos sobre a conjectura de que $\mathcal{P} \neq \mathcal{NP}$.

Outras definições em complexidade computacional são possíveis. A quantidade de espaço de memória é outro fator considerado na classificação de problemas de acordo com a sua dificuldade de computação. Modificando as Definições 2 e 3 de modo a usar espaço polinomial de memória ao invés de tempo polinomial, têm-se as definições das classes $\mathcal{P}$-space e $\mathcal{NP}$-space.

Algoritmos para transportar de uma linguagem L a outra linguagem L' podem ser criados. Por isso, se existe uma função $f(x)$ computável em tempo polinomial no comprimento da entrada, $p(|x|)$, tal que $x \in L$ se somente se $f(x) \in L'$, então diz-se que L é *polinomialmente redutível* para uma linguagem L'. Nesse caso, simplesmente expressamos por $L \geq_p L'$ (lê-se L é p-redutível a L'). Leonid Levin [34] e Stephen Cook [33] observaram que dentre os problemas $\mathcal{NP}$ existem alguns que são mais difíceis do que outros, no sentido de que, resolvendo um desses problemas em tempo polinomial, então todos os problemas em $\mathcal{NP}$ também podem ser resolvidos em tempo polinomial. Assim, a classe dos problemas $\mathcal{NP}$-completos é o subconjunto dos mais difíceis problemas não-determinísticos polinomiais.

Definição 4. ($\mathcal{NP}$*-completo*) *- Uma linguagem L é $\mathcal{NP}$-completo se:*

- *L está em $\mathcal{NP}$, e*

- *cada linguagem* $L' \in \mathcal{NP}$ *é* $L' \geq_p L$.

Uma questão fundamental em teoria da complexidade é se uma fonte de bits aleatórios pode ser usada para acelerar o reconhecimento de algumas linguagens, aceitando uma afirmativa com baixa probabilidade de erro. A classe de linguagens $\mathcal{BPP}$ consiste de todas as linguagens L que podem ser reconhecidas por algoritmo aleatório de tempo polinomial, com no máximo uma pequena probabilidade de erro para toda entrada. Uma *máquina de Turing probabilística* M é um tipo de Máquina de Turing não determinística que possui passos de transição chamados de lançamento-de-moeda, dando à máquina duas possibilidades a cada transição. As escolhas aleatórias de transição são independentes da entrada. A saída de uma máquina M numa entrada x não é uma string, mas uma variável aleatória que assume possíveis valores de string. Por $\Pr[M(x) = y]$, denota-se a probabilidade de M ter gerado a saída y na entrada x. Usualmente, denota-se por $\Pr[M(x) = 1]$ como a probabilidade de M aceitar x.

Definição 5. $(\mathcal{BPP})$ *- A classe de complexidade* $\mathcal{BPP}$ *é a classe de toda linguagem* L *para a qual existe uma máquina de Turing probabilística de tempo polinomial de maneira que:*

1. *Se* $x \in L$ *então* $\Pr[M(x) = 1] \geq \frac{2}{3}$*;*
2. *Se* $x \notin L$ *então* $\Pr[M(x) = 1] \geq \frac{1}{3}$.

Se um problema está em $\mathcal{BPP}$, então existe um algoritmo que pára em tempo polinomial permitindo lançamentos de moedas e tomadas de decisões aleatórias. Uma execução deste algoritmo para qualquer entrada oferece uma probabilidade de erro de no máximo $1/3$. A escolha de $1/3$ na definição é arbitrária. Pode ser qualquer constante entre 0 e $1/2$. Mesmo existindo uma probabilidade de erro na classe $\mathcal{BPP}$, se o algoritmo é executado muitas vezes, então o erro cai exponencialmente como consequência do limite de Chernoff [35]. Isto torna possível a criação de um algoritmo probabilístico de alta precisão apenas executando-o várias vezes (uma quantidade polinomial de execuções no tamanho da entrada, $p(|x|)$).

1.3 Sistema de prova interativa

A assimetria entre a complexidade da tarefa de verificação e a complexidade da tarefa do ato de provar faz com que a classe $\mathcal{NP}$ seja vista como um sistema de prova. Em cada linguagem $L \in \mathcal{NP}$ tem um procedimento eficiente de verificação para provas de sentenças da forma "$x \in$

L". Por definição toda linguagem $L \in \mathcal{NP}$ é caracterizada pela relação R_L de reconhecimento em tempo polinomial

$$x \in L \text{ se somente se } \exists\, y \in \Sigma^* \text{ tal que } (x, y) \in R_L \text{ e } |y| \leq p(|x|).$$

Assim, o procedimento de membros para declarações da forma "$x \in L$" consiste em aplicar o algoritmo para reconhecer a relação booleana R_L, quando um membro afirma x e sua respectiva prova, denotada por y. Qualquer y satisfazendo $(x, y) \in R_L$ é considerada uma prova da linguagem $x \in L$. Note que o procedimento de verificação é fácil, enquanto que chegar até prova é uma tarefa difícil (se de fato $\mathcal{NP}$ não está contida em $\mathcal{BPP}$, [36]).

Duas propriedades de um sistema de prova são a sua validade e completude. A propriedade de *validade diz que o procedimento de verificação não pode ser trapaceado em aceitar sentenças falsas*. Em outras palavras, o verificador deve ter habilidade de se proteger contra argumentos falsos para não ser convencido por eles. Por outro lado, a propriedade de *completude afirma a capacidade de um provador convencer sempre com sentenças verdadeiras*.

Uma interação entre duas partes é definida de maneira natural. No contexto de sistemas de prova interativa, uma entrada comum para as duas máquinas representa a sentença a ser provada. Seja A e B um par de máquinas interativas, supondo que todas as interações entre A e B têm uma entrada comum e que as interações terminam num número finito de passos. Denota-se por $(A, B)(x)$ a variável aleatória representando a saída local de B quando interage com a máquina A numa entrada comum x. Nesse caso, a entrada aleatória para cada máquina é uniforme e independentemente escolhida. A eficiência das máquinas também deve ser mencionada. Diz-se que uma máquina interativa A tem *complexidade de tempo* $t : \mathbb{N} \to \mathbb{N}$ ($\mathbb{N}$ é o conjunto dos números naturais) se para toda máquina interativa B e para toda entrada x, quando A interage com B, a máquina A sempre termina dentro de $t(|x|)$ passos. Em particular, dizemos que A tem *tempo polinomial* se existe um polinômio $p(\cdot)$ tal que A tem complexidade de tempo p.

Definição 6. ($\mathit{Sistema\ de\ Prova\ Interativo}$) *- Um par de máquinas interativas* $(\boldsymbol{P}, \boldsymbol{V})$ *é chamado um sistema de prova interativo para uma linguagem* L*, se a máquina* $\boldsymbol{V}$ *tem eficiência de tempo polinomial e satisfaz as seguinte condições*

1. ($\mathit{Completude}$) *Para todo* $x \in L$*,*

$$\Pr[(\boldsymbol{P}, \boldsymbol{V})(x) = 1] \geq \frac{2}{3};$$

2. (*Validade*) *Para todo* $x \notin L$ *e um provador interativo* $\boldsymbol{P}'$*, então*

$$\Pr[(\boldsymbol{P}', \boldsymbol{V})(x) = 1] \geq \frac{1}{3}.$$

É evidente que a definição dos limites para a satisfação das propriedades de completude e validade podem ser modificados. Havendo assim, definições mais gerais que dizem que um sistema de prova interativo tem completude limitada por probabilidade p_c e tem validade limitada por p_v. Mas deve-se avaliar o bom senso de que sempre a probabilidade que limita a completude deve estar mais próxima de 1, enquanto que a probabilidade que limita a validade deve estar próxima de 0.

1.4 Indistinguibilidade computacional

Uma noção central em criptografia é a de "similaridade efetiva"(introduzida por Goldwasser, Micali e Yao [5, 37]). A idéia é descrever a capacidade de discernimento entre dois objetos, ou seja, verificar se dois objetos são ou não iguais, ou se dois objetos são ou não diferentes. O conceito de computação eficiente conduz naturalmente a um novo tipo de equivalência de objetos. *Objetos são considerados computacionalmente equivalentes se eles não podem ser diferenciados por qualquer procedimento eficiente*. Assim, as famílias de processos estatísticos $\{A_2(x)\}_{x\in L}$ e $\{A_2(x)\}_{x\in L}$ que representam algoritmos para uma dada entrada x são ditos computacionalmente indistinguíveis se nenhum procedimento eficiente, ou seja, todo algoritmo probabilístico T de tempo polinomial, pode distingui-los um do outro.

Definição 7. (*Algoritmo computacionalmente indistinguível, [9]*) - *Sejam* A_1 *e* A_2 *dois algoritmos probabilísticos com entrada* $x \in \{0,1\}^*$*. Os algoritmos* A_1 *e* A_2 *são computacionalmente indistinguíveis se para qualquer algoritmo de decisão em tempo polinomial,* T*, o polinômio* $p(\cdot)$ *e a entrada* x *suficientemente grande, então a condição abaixo é satisfeita:*

$$|\Pr[T(A_1(x)) = 1] - \Pr[T(A_2(x)) = 1]| \leq \frac{1}{p(|x|)} \tag{1.2}$$

A probabilidade de o algoritmo de tempo polinomial T aceitar o algoritmo A_1, com entrada x, menos a probabilidade do mesmo algoritmo T aceitar o algoritmo A_2, com entrada x, é menor ou igual ao inverso de um polinômio cujo argumento é o comprimento da string x, denotada por $|x|$. Ainda. quando esta diferença é nula, isto acontece por exemplo quando os dois algoritmos têm distribuições de probabilidade independentes uma da outra e uniforme, diz-se que os algoritmos têm perfeita indistinguibilidade computacional.

1.5 Sistema de prova de conhecimento nulo

Deve ser enfatizado que o conceito de *conhecimento* discutido neste trabalho tem um significado diferente de *informação* como apresentado na teoria da informação. Enquanto o conceito de informação está vinculado à incerteza sobre um evento, conhecimento está associado a dificuldade computacional de se chegar a solução de um problema. Por exemplo, existe uma diferença de conhecimento revelado, no caso de Alice responder uma questão de baixa complexidade para a resposta de uma questão de alta complexidade, enquanto que para a teoria da informação não há diferença. Conhecimento relata principalmente a complexidade do procedimento que encontra uma resposta satisfatória para uma dada entrada x.

É dito que um sistema de prova interativo $(\boldsymbol{P}, \boldsymbol{V})$ para uma linguagem L tem conhecimento nulo se tudo o que pode ser eficientemente computado com a entrada x, após interagir com $\boldsymbol{P}$, pode ser eficientemente calculado de x sem qualquer interação. Ou seja, não se tem mais conhecimento (ou habilidade computacional) do que havia antes da interação. De fato, conhecimento nulo é uma propriedade prescrita para manter a completude do provador após uma interação. Ela captura a robustez do provador contra tentativas de verificadores em ganhar conhecimento sobre as habilidades computacionais do provador após interagir com ele.

Definição 8. $(\textit{Perfeito conhecimento nulo})$ *- Seja* $(\boldsymbol{P}, \boldsymbol{V})$ *um sistema de prova interativa para alguma linguagem* L*. Diz-se que* $(\boldsymbol{P}, \boldsymbol{V})$*, ou de fato a máquina do provador* $\boldsymbol{P}$*, tem perfeito conhecimento nulo se para toda máquina interativa probabilística de tempo polinomial* $\boldsymbol{V}$*, existe um algoritmo* S*, tal que para toda entrada* $x \in L$*, as seguintes duas variáveis aleatórias são identicamente distribuídas:*

- $(\boldsymbol{P}, \boldsymbol{V})(x)$*, ou seja, a saída da máquina interativa* $\boldsymbol{V}$ *após interagir com a máquina* $\boldsymbol{P}$ *na entrada* x*;*
- $S(x)$*, ou seja, a saída da máquina* S *na entrada* x*. A máquina* S *é chamado de simulador da interação de* $\boldsymbol{V}$ *com* $\boldsymbol{P}$*.*

Assumindo a existência de um simulador perfeito S, esse simulador é perfeitamente capaz de simular a interação entre o verificador $\boldsymbol{V}$ e o provador, embora ele não tenha acesso à máquina do provador. O fato de tais simuladores existirem não garante que $\boldsymbol{V}$ ganhe qualquer conhecimento de $\boldsymbol{P}$ dado que a mesma entrada poderia ser gerada sem qualquer acesso a $\boldsymbol{P}$. O *paradigma da simulação* postula que após a interação entre as máquinas $\boldsymbol{V}$ e $\boldsymbol{P}$, a máquina $\boldsymbol{V}$ não é capaz de fazer computações além do que ela era capaz de fazer sozinha antes da interação. O real ganho de conhecimento de habilidade computacional é caracterizado quando uma máquina, após interagir

com outra parte, é capaz de computar algo que antes ela não era capaz. Isto fica bem ilustrado na definição de perfeito conhecimento nulo.

A definição de conhecimento nulo não precisa ter um limite tão rigoroso quanto as chances de ganho de conhecimento, ou seja, as variáveis aleatórias não precisam ser identicamente distribuídas, mas próximas o suficiente por algum limite polinomial do comprimento da string de entrada.

Definição 9. $(\textit{Conhecimento nulo})$ *- Um sistema de prova interativa* $(\boldsymbol{P}, \boldsymbol{V})$ *para uma linguagem* L *tem conhecimento nulo se para toda máquina interativa* $\boldsymbol{V}$ *existe um perfeito simulado* S *tal que a distribuição de probabilidade entre* $(\boldsymbol{P}, \boldsymbol{V})_{x \in L}$ *e* $S_{x \in L}$ *é computacionalmente indistinguível.*

1.5.1 Sistema interativo de prova de conhecimento nulo para grafos isomorfos

Para ilustrar um sistema interativo de prova de conhecimento nulo para grafos isomorfos, Goldreich usa a seguinte história [36]:

> Paula afirma que existe um caminho entre o portão sul e o portão norte do labirinto dela (um caminho por dentro do labirinto). Victor não crê nela. Paula está solidária para provar a sua afirmativa para Victor, mas não quer provê-lo de qualquer conhecimento adicional. Para provar a afirmativa de Paula, ela e Victor repetem o seguinte procedimento um número de vezes suficiente para convencer Victor.
>
> Paula miraculosamente transporta Victor para um local aleatório no labirinto dela. Então Victor pergunta se ela sabe mostrar o caminho para o portão sul ou para o portão norte. A escolha dele é suposta ser aleatória, mas na verdade, é dado todo o poder de decisão a ele para escolher o desafio. Então, Paula, por sua vez, escolhe um passeio aleatório suficientemente grande do local em que estão até o destino escolhido por Victor, e ele é guiado ao longo do caminho. Claramente, se o labirinto tem um caminho como afirmado por Paula, então Victor será sempre convencido da validade do argumento de Paula. Se por outro lado, o labirinto não possui tal caminho, então em cada iteração, com probabilidade 1/2, Victor perceberá a mentira de Paula.
>
> Finalmente, Victor não ganha nenhum conhecimento a cada visita guiada. A razão é que ele pode simular uma visita guiada pra si mesmo, como segue: Primeiro, ele seleciona norte ou sul (como ele faz na visita real guiada) e vai para o portão

escolhido. Depois ela pega um caminho aleatório do portão para dentro do labirinto enquanto desenrola um tubo de linha, e finalmente ele traça um caminho de volta para o portão. Um passeio aleatório suficientemente longo, cujo comprimento iguala o comprimento da visita guiada por Paula, garantirá que Victor visitará o local aleatório no labirinto, e o caminho de volta será visto como um passeio aleatório do local até o fim do fio para o portão escolhido.

Agora será apresentado um pouco sobre isomorfismo de grafos para montar o cenário do próximo protocolo. Um grafo $G = (V, A)$ consiste de um conjunto de elementos chamados vértices $V = \{v_1, v_2, \cdots, v_n\}$ e um conjunto de pares de vértices chamados arestas, $(v_i, v_j) \in A$ para $i, j = 1, 2, \cdots, n$. Diz-se que um par de grafos $G_0 = (V_0, A_0)$ e $G_1 = (V_1, A_1)$ é isomorfo quando existe um mapeamento dos vértices do grafo G_0 para os vértices do grafo G_1, $\sigma : V_0 \rightarrow V_1$, tal que $(v_i, v_j) \in A_0$ se somente se $(\sigma(v_i), \sigma(v_j)) \in A_1$. Na prática, a função que realiza tal mapeamento de forma que o isomorfismo é sempre preservado é função de permutação dos vértices. Portanto, dado um grafo G com n vértices é possível gerar $n!$ grafos isomorfos a G, pois sempre existirá uma permutação inversa dos vértices que retorna para o grafo G, já que a permutação é uma função bijetiva. Encontrar um isomorfismo entre dois grafos, G_0 e G_1, é um problema difícil, mas fornecida a permutação dos vértices de G_0 que o torna igual a G_1, fica fácil verificar o isomorfismo entre estes grafos. O isomorfismo entre grafos é um problema que acredita-se não está em $\mathcal{P}$ [36]. Aqui essa classe de problemas será chamada $\mathcal{IG}$.

Para a compreensão do uso de isomorfismos de grafos como um desafio computacional, supõe-se que Paula diz a Victor conhecer um isomorfismo entre dois grafos isomorfos de n vértices, G_0 e G_1. Em se tratando de grafos de n vértices de uma forma geral, ele poderia tentar encontrar a solução na força bruta testando todos os grafos isomorfos a G_0, mas isso daria um algoritmo de complexidade em $O(n!)$ (embora algoritmos heurísticos melhorem esse resultado [38]). Portanto, conhecendo G_0 e G_1, Victor não tem como descobrir em tempo polinomial o isomorfismo, tal que $\sigma : G_1 \rightarrow G_0$. Com isso, Paula pode pegar um grafo G_1 (com n suficientemente grande) e um isomorfismo $\sigma : G_1 \rightarrow G_0$, para então divulgar G_0 e G_1 e ter como segredo o isomorfismo σ. Dessa maneira, será um segredo difícil de ser descoberto. Paula também sabendo que a composição de duas transformações isomorfas é um isomorfismo, pode escolher aleatoriamente vários isomorfismos para formar as composições e gerar vários grafos aleatoriamente. Agora, sendo Paula uma provadora ***P*** e Victor um verificador ***V*** que conhecem dois grafos G_0 e G_1 com n vértices, em que ***P*** tem como segredo o isomorfismo $\sigma : G_1 \rightarrow G_0$. O seguinte protocolo implementa um sistema interativo de prova de conhecimento nulo:

Protocolo 1. (*Sistema de prova de conhecimento nulo para isomorfismos de grafos,* [9]) - *O seguintes passos são repetidos n vezes:*

1. ***P** gera um isomorfismo aleatório $\lambda : G_0 \rightarrow H$ e envia H para **V**;*

2. ***V** gera aleatoriamente um bit b e envia o bit a **P**;*

3. ***P** envia o isomorfismo $\xi = \sigma^b \circ \lambda$ para **V**;*

4. ***V** confere se $\xi(G_b) = H$. (Se $b = 0$ implicará em $\lambda H = G_0$ e se $b = 1$ implicará em $\sigma \circ \lambda\ H = \sigma\ G_0 = G_1$).*

Quando se olha o protocolo acima como um sistema de prova de interativo, percebe-se que a entrada desse sistema é o par de grafos isomorfos G_0 e G_1. Então, a sentença dessa linguagem é $(G_0, G_1) \in \mathcal{IG}$. No caso do provador, o programa dele é executado por uma máquina probabilística de tempo polinomial, ou seja, apenas uma permutação escolhida aleatoriamente é realizada no Passo 1. O programa do verificador pode ser executado em tempo polinomial determinístico no passo 4. A escolha do bit de desafio é uma simples computação probabilística no Passo 2. Em [9] é mostrado que esse par de máquinas interativas constitui um sistema de prova interativa com conhecimento nulo para a linguagem $\mathcal{IG}$ (Isomorfismo de Grafos).

Proposição 1. *A linguagem $\mathcal{IG}$ tem um perfeito sistema de prova interativa com conhecimento nulo. Para verificadores limitados por máquinas de tempo polinomial (determinística ou probabilística), o Protocolo 1 satisfaz as seguintes afirmativas* [36]*:*

1. *Se G_0 e G_1 são isomorfos, então o verificador sempre aceita quando interage com **P**;*

2. *Se G_0 e G_1 não são isomorfos, então a entrada será rejeitada com probabilidade menor do que $\frac{1}{2}$;*

3. ***P** realiza provas com perfeito conhecimento nulo.*

Quando n interações entre o verificador e o provador são realizadas a probabilidade de erro para a validade é limitada por $1/2^n$. Deve ser enfatizado que todas as computações probabilísticas são completamente independentes para cada iteração das máquinas probabilísticas, conseqüentemente, isto é válido para interações. Outro fato a ser destacado é que não se sabe se a linguagem $\mathcal{IG} \in \mathcal{BPP}$ ou $\mathcal{IG} \notin \mathcal{BPP}$ [36]. Portanto, segue a prova da Proposição 1:

1. **Prova**: Claramente, se os grafos G_0 e G_1 são isomorfos, então o grafo H construído por ***P*** no Passo 1 é isomorfo a eles dois. Conseqüentemente se cada parte segue o que está prescrito no protocolo então ***V*** sempre aceita os argumentos do provador.

2. **Prova**: Se os grafos G_0 e G_1 não são isomorfos, então nenhum grafo pode ser isomorfo a G_0 e G_1. Isto segue que nenhum provador trapaceiro constrói H isomorfo ao dois

simultaneamente, mas somente a um dos dois, ou seja, ele escolhe $b \in \{0,1\}$ de forma que H vai ser isomorfo a um dos dois. Conseqüentemente, o verificador segue o programa e rejeita o argumento do provador com probabilidade 1/2.

3. **Prova**: Seja ***V*** um verificador eventualmente desonesto, isto é, um verificador que não segue necessariamente os passos do Protocolo 1. O objetivo é mostrar que é possível simular a interação deste verificador com um provador honesto, sem uma real comunicação com este provador. Primeiro observa-se que o objetivo do simulador é produzir n tuplas (H, b, ξ) onde H é gerado uniformemente (pois o provador é honesto) e c é gerado de acordo com ***V***. Nota-se ainda que o simulador tem acesso ao código de ***V***. Nestas condições o verificador ***V*** é uma família de algoritmos probabilísticos em tempo polinomial $V_{k=1,2,\ldots,n}$ onde V_k corresponde ao algoritmos de escolha do bit de desafio na k-ésima iteração. O algoritmo V_k recebe o compromisso H e eventualmente poderá usar algum dado auxiliar $w_k \in \{0,1\}^*$ que calculou em iterações anteriores. No início ***V*** não tem nenhum dado auxiliar, ou seja, $w_k = \epsilon$ (sem símbolo). Então começa a simulação:

   (a) O simulador escolhe $b \in \{0,1\}$ de forma uniformemente aleatória;

   (b) O simulador gera o isomorfismo $\xi : G_b \rightarrow H$;

   (c) O simulador aplica $V_1(H, \epsilon)$ e verifica se o bit c calculado por V_1 é igual a b;

      i. Caso $c = b$, então a simulação foi feita com sucesso e a tupla nesta interação deve ser (H, c, ξ). A computação auxiliar feita por ***V*** com o fim de ser utilizada em interações futuras é gravada em w_1;

      ii. Se $c \neq b$, então o simulador volta para o Passo (a).

   Após a primeira iteração (k >1), no Passo (c), o simulador aplica $V_k(H, w_k)$ e verifica se o bit c calculado por V_k é igual a b;

      i. Caso $c = b$, então a simulação foi feita com sucesso e a tupla nesta iteração deve ser (H, c, ξ). A computação auxiliar feita por ***V***, com o fim de ser utilizada em iterações futuras, é gravada em w_{k+1};

      ii. Se $a \neq b$, então o simulador volta para o Passo (a).

   Observe que a probabilidade de $c = b$ é $1/2$, dado que b foi escolhido com distribuição de probabilidade uniforme. Assim, o simulador terá sucesso, em média, após duas tentativas. Para finalizar, basta verificar que a seqüência de tuplas (H, c, ξ) gerada pelo simulador tem exatamente a mesma distribuição que as tuplas produzidas por uma interação real com o provador. Por esta razão, estas seqüências são computacionalmente indistinguíveis. □

Uma outra propriedade de sistemas de interativos de conhecimento nulo é a *impossibilidade de transferência de prova*. Essa propriedade diz que após a interação entre o provador e o verificador, o anonimato do provador é preservado. Em outras palavras, um verificador com poder computacional de tempo polinomial não pode transferir uma prova da sua interação com o provador para uma terceira parte. O argumento para essa propriedade é bastante simples: Se o verificador consegue simular uma interação com o provador, então não conseguirá convencer com a sequência de tuplas $(H_i, c_i, \xi_i\}_{i=1}^{n}$ uma terceira, pois essa não saberá distinguir entre uma simulação e uma real interação a partir dessa seqüência.

1.5.2 Sistema interativo de prova de conhecimento nulo para grafos tricoloríveis

Um grafo $G(V, A)$ é dito ser tricolorível se existir um mapeamento $\Phi : V \rightarrow \{R, Y, B\}$ tal que sempre dois vértices adjacentes são marcados com cores diferentes, isto é, cada aresta $(u, v) \in A$ satisfaz $\Phi(u) \neq \Phi(v)$. A coloração de grafos é conhecida como um problema $\mathcal{NP}$-completo. É assumido, sem perda de generalidade, que se trata de um grafo simples e conectado. No seguinte protocolo [9], o provador necessita somente ser uma máquina probabilística de tempo polinomial que pega um grafo G colorível em 3 cores como uma entrada auxiliar. Dessa maneira, o cenário do protocolo é montado da seguinte forma:

1. É de conhecimento do provador e do verificador o grafo $G(V, A)$ simples e conectado ($n = |V|$ e $m = |A|$). Dessa maneira, n e m estão polinomialmente relacionados (i.e $n - 1 \leq m \leq n^2/2$). Por simplicidade, seja o conjunto dos vértices $V = \{1, 2, ..., n\}$.

2. O provador honesto possui um mapeamento tricolorível denotado por $(\Phi : V \rightarrow \{R, Y, B\})$ e um conjunto S_3 de todas as permutações dos n vértices em 3 cores.

3. O provador possui uma função de cifragem segura f. Neste momento, não se falará em detalhes sobre essa função, mas será dada uma descrição intuitiva de como ela deve funcionar. Imagine que Paula esconde uma mensagem em uma caixa fechada com uma chave e envia-a para Victor. A mensagem só poderá ser lida se a chave for entregue a Victor, porque a caixa é inviolável. Assim, Paula não pode mudar o segredo que ele fez compromisso de usar. A esses esquemas dá-se o nome de compromisso de informação. Em criptografia clássica, esquemas de compromisso de informação podem ser construídos com permutações de sentido único [39], ou com geradores pseudo-aleatório [40]. Um sistema físico também pode ser usado para a criação de tais sistemas. Na criptografia

quântica, sistemas de cifra são candidatas a compromisso de informação quântica. Esse assunto será discutido com mais detalhes no Capítulo 3.

Protocolo 2. (*Sistema interativo de prova de conhecimento nulo para grafos tricoloríveis*) - *Uma entrada comum aos agentes* ***P*** *e* ***V*** *é o grafo* $G(V, A)$. *Os passos seguintes são executados* m^2 *vezes, cada vez usando escolhas aleatórias independentes* [9].

1. *O provador escolhe aleatoriamente uma marcação tricolorível, cifra, e envia o resultado da cifra para o verificador. Mais especificamente, o provador escolhe uma permutação* $\pi \in S_3$, *cria aleatoriamente uma sequência de* n *bits,* r_v *(para todo* $v \in V$ *e* $r_v \in \{0,1\}^n$*). O provador calcula o resultado da cifra* $F_v = f\left(\pi(\Phi(v)), r_v\right)$ *e envia a sequência* $F_1, F_2, \ldots F_n$.

2. *O verificador escolhe aleatoriamente uma aresta* $\alpha \in A$ *e a envia para o provador. Desta maneira, o verificador pergunta se o provador é capaz de mostrar as cores dos extremos da aresta* α.

3. *Se* $\alpha = (u, v) \in A$ *então o provador é capaz de revelar as diferentes cores de* u *e* v, *e provar para o verificador que cifrou cores diferentes, enviando para ele a chave para decifrar as cores dos vértices* u *e* v. *Mais especificamente, o provador envia* $\left(\pi\left(\Phi(v)\right), r_v\right)$ *e* $\left(\pi\left(\Phi(u)\right), r_u\right)$ *para o verificador.*

4. *Agora, o verificador deve avaliar a prova revelada no Passo (3). Para isto ele decifra* $F_v = f\left(\pi(\Phi(v)), r_v\right)$ *e* $F_u = f\left(\pi(\Phi(u)), r_u\right)$, *verifica se os vértices têm cores diferentes, ou seja, se* $\pi\left(\Phi(v)\right) \neq \pi\left(\Phi(u)\right)$, *e se* $\pi\left(\Phi(v)\right)$ *e* $\pi\left(\Phi(u)\right)$ *estão em* $\{R, Y, B\}$. *Se estas condições são violadas o verificador rejeita a prova e para. Caso contrário, ele volta para o Passo (1). Se o verificador completou todas as* m^2 *interações com o provador, então a prova é aceita.*

É fácil verificar que o protocolo acima constitui um sistema de prova interativo para um grafo tricolorível. Se o grafo pode ser colorido em três cores e ambos, provador e verificador, seguem o protocolo corretamente, então o verificador aceita a prova do provador com probabilidade 1. Se o grafo não é colorível em 3 cores e o verificador segue o protocolo corretamente, então a cada rodada o verificador rejeitará a prova com probabilidade mínima de $1/m$ (isto significa que ao menos uma aresta possui dois vértices de mesma cor). Portanto, a probabilidade do verificador aceitar (isto é, completar todas as m^2 interações com o provador) a prova de um grafo que não é 3-colorível é no máximo igual a $(1 - \frac{1}{m})^{m^2} \approx \exp(-m)$.

O Protocolo 2 é de conhecimento nulo, dado que, a informação recebida pelo verificador a cada rodada é um par de elementos escolhidos aleatoriamente no conjunto $\{R, Y, B\}$ e nada é

aprendido sobre o mapeamento Φ. É crucial que o provador use a cada rodada uma permutação aleatoriamente selecionada. Assim, o nome das três cores dos vértices a cada rodada não estarão correlacionados aos nomes dos vértices das outras rodadas, não dando assim, chances ao verificador de inferir sobre o mapeamento Φ. Este simples protocolo é a base para provar que, se existe um esquema de compromisso de informação seguro, então este protocolo constitui um sistema de prova interativo de conhecimento nulo para toda linguagem $\mathcal{NP}$. A prova para esta afirmativa não será apresentada neste trabalho. Mas intuitivamente falando, o leitor deve pensar nas reduções polinomiais dentro de uma linguagem $\mathcal{NP}$. Se todo problema $\mathcal{NP}$ pode ser reduzido a este problema de coloração de grafos (que é um problema $\mathcal{NP}$-completo), então existe um sistema de prova interativa de conhecimento nulo para toda linguagem $\mathcal{NP}$ [9, 36].

Capítulo 2

Introdução à teoria da informação quântica

2.1 Estados quânticos e transformações unitárias

A informação quântica está construída sobre o conceito de bit quântico ou qubit. Da mesma forma que um bit clássico pode assumir os estados 0 ou 1, o qubit pode assumir os estados $|0\rangle$ ou $|1\rangle$. Porém, a diferença entre bit e qubit é que os qubits podem estar em estados diferentes de $|0\rangle$ e $|1\rangle$. O fato é que para eles, também são possíveis combinações lineares dos estados $|0\rangle$ e $|1\rangle$, chamadas de superposição:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle. \tag{2.1}$$

Os números α e β são números complexos que obedecem à relação $|\alpha|^2 + |\beta|^2 = 1$, o que mostra que na sua forma geral um qubit é um vetor unitário em um espaço vetorial complexo de duas dimensões. Os estados $|0\rangle$ e $|1\rangle$ formam a base canônica chamada de base retangular, representada por $B_0 = \{|0\rangle, |1\rangle\}$. A representação vetorial desses qubits é feita pelos seguintes vetores coluna:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}; \tag{2.2}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2.3}$$

Fisicamente, quando se mede o qubit em (2.1), encontra-se o estado $|0\rangle$ com probabilidade $|\alpha|^2$ e o estado $|1\rangle$ com probabilidade $|\beta|^2$. Note que os estados $|0\rangle$ e $|1\rangle$ representam apenas uma entre

muitas escolhas possíveis para a base de estados de um qubit. Outra escolha possível é a base $B_1 = \{|+\rangle, |-\rangle\}$, denominada base diagonal. Os estados quânticos $|+\rangle$ e $|-\rangle$ são superposições (ou combinações lineares) dos estados quânticos $|0\rangle$ e $|1\rangle$:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \text{ e } |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{2.4}$$

Expressando o estado de (2.1) na base diagonal, tem-se:

$$|\psi\rangle = \frac{\alpha + \beta}{\sqrt{2}}|+\rangle + \frac{\alpha - \beta}{\sqrt{2}}|-\rangle. \tag{2.5}$$

Naturalmente, uma medição de $|\psi\rangle$ na base diagonal resultará em $|+\rangle$ com probabilidade $|\alpha + \beta|^2/2$ e resultará em $|-\rangle$ com probabilidade $|\alpha - \beta|^2/2$.

Nos computadores clássicos existem portas lógicas que processam a informação alterando ou não os estados dos bits. Na computação quântica também existem portas que atuam sobre o qubit de forma a alterar o estado do mesmo. Um qubit é um vetor unitário num espaço vetorial de duas dimensões sobre o conjunto dos números complexos. Portanto, portas quânticas de um qubit podem ser descritas por matrizes 2×2, mas existem restrições para as matrizes que são usadas para representar uma porta quântica. Um qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ tem uma condição de normalização: $|\beta|^2 + |\alpha|^2 = 1$. Isso também deve ser verdade para o estado $|\psi'\rangle = \alpha'|0\rangle + \beta'|1\rangle$, após a atuação da porta. A condição para uma matriz representar uma porta em computação quântica é que a mesma seja uma matriz unitária, $U^\dagger U = UU^\dagger = I$, sendo $U^\dagger$ a matriz adjunta de U (transposta conjugada de U) e I, a matriz identidade.

Nos computadores clássicos, a porta NOT inverte o valor do bit de entrada, NOT$(0) = 1$ e NOT$(1) = 0$. Na computação quântica existem operações unitárias que realizam operações análogas. Para a base retangular, a operação unitária que realiza a inversão de qubit é definida por:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{2.6}$$

Os detalhes dos cálculos da operação X estão descritos abaixo:

$$\begin{aligned} X\left(\alpha|0\rangle + \beta|1\rangle\right) &= \alpha X|0\rangle + \beta X|1\rangle \\ &= \alpha \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ &= \alpha \begin{bmatrix} 0 \\ 1 \end{bmatrix} + \beta \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \alpha|1\rangle + \beta|0\rangle. \end{aligned} \tag{2.7}$$

Para a base diagonal, também existe uma transformação unitária que realiza a troca do qubit $|+\rangle$ para o qubit $|-\rangle$ e vice-versa. Essa transformação unitária é definida por:

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.8}$$

Os detalhes dos cálculos da operação Z estão descritos abaixo:

$$\begin{aligned} Z(\alpha|+\rangle + \beta|-\rangle) &= \alpha Z|+\rangle + \beta Z|-\rangle \\ &= \alpha \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} + \beta \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \\ &= \alpha \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} + \beta \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \alpha|-\rangle + \beta|+\rangle \end{aligned} \tag{2.9}$$

Por fim, existe uma transformação unitária que realiza a transformação de estados da base B_0 para estados da base B_1 e vice-versa. Essa transformação, chamada de porta Hadamard, é definida por:

$$H = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{2.10}$$

Os detalhes do cálculo dessa operação sobre os estados $|0\rangle$ e $|-\rangle$ estão descritos abaixo:

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = |+\rangle; \tag{2.11}$$

$$H|-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle. \tag{2.12}$$

A Tabela 2.1 mostra os resultados das operações realizadas pelas portas X, Z e H sobre os qubits de entradas $|0\rangle$, $|1\rangle$, $|+\rangle$ e $|-\rangle$.

2.1.1 Transformação unitária usada no protocolo 7

Neste trabalho a notação $|\psi_b^a\rangle$ é usada para representar o conjunto de quatro estados quânticos não ortogonais $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, de forma que a é o valor lógico de qubit e b indica uma das seguintes bases: $B_0 = \{|0\rangle, |1\rangle\}$ e $B_1 = \{|+\rangle, |-\rangle\}$. No dispositivo à prova de falsificação, a transformação unitária para provocar uma determinística transição no qubit é dada por $U_S = Z^z X^x H^h$. Agora, considera-se o seguinte problema: Eva envia para o verificador o estado

Operações unitárias	B_0		B_1	
	Entrada $\|0\rangle$	Entrada $\|1\rangle$	Entrada $\|+\rangle$	Entrada $\|-\rangle$
X	$\|1\rangle$	$\|0\rangle$	$\|+\rangle$	$-\|-\rangle$
Z	$\|0\rangle$	$-\|1\rangle$	$\|-\rangle$	$\|+\rangle$
H	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$

Tabela 2.1: Resultados das operações X, Z e H aplicada aos qubits de entrada $|0\rangle$ e $|1\rangle$ da base B_0, e aos qubits $|+\rangle$ e $|-\rangle$ da base B_1

$|\psi_a^b\rangle$ que para ele é desconhecido. O verificador realiza a transformação $U_S|\psi_b^a\rangle$, teleporta esse estado e envia o vetor $S' = (z', x', h')$. Se $S' = S$, então Eva pode recuperar o qubit que enviou para o verificador, pois $U_S^\dagger U_S|\psi_b^a\rangle = |\psi_b^a\rangle$. Caso contrário, isso não acontece. Ao realizar uma medição do estado $U_{S'}^\dagger U_S|\psi_b^a\rangle = |\psi_c^d\rangle$, na base B_b, com alguma probabilidade, Eva vai interpretar que $c = a$. Antes de analisar os casos é importante considerar os seguintes resultados sobre as transformações controladas classicamente:

$$H^h|\psi_b^a\rangle = |\psi_{h\oplus b}^a\rangle; \tag{2.13}$$

$$X^x|\psi_b^a\rangle = |\psi_b^{a\oplus(x\cdot\bar{b})}\rangle; \tag{2.14}$$

$$Z^z|\psi_b^a\rangle = |\psi_b^{a\oplus(z\cdot b)}\rangle. \tag{2.15}$$

O que implica em

$$\begin{aligned} |\psi_d^c\rangle &= U_{S'}^\dagger U_S|\psi_b^a\rangle \\ &= \mathrm{H}^{h'}\mathrm{X}^{x'}\mathrm{Z}^{z'}\mathrm{Z}^z\mathrm{X}^x\mathrm{H}^h|\psi_b^a\rangle \\ &= \left|\psi_{(h\oplus h')\oplus b}^{a\oplus[(z\oplus z')\cdot(h\oplus b)]\oplus\left[(x\oplus x')\cdot\overline{(h\oplus b)}\right]}\right\rangle. \end{aligned} \tag{2.16}$$

Os casos em que $S \neq S'$ são apresentados na Tabela 2.2. A última coluna da Tabela 2.2 é a probabilidade do verificador enganar Eva sem ser descoberto.

De acordo com a Tabela 2.2, o primeiro caso sempre indicará que $a = c$. Esse é o caso em que o verificador é honesto enviando $S = S'$. Agora, considera-se que o verificador é desonesto e deseja enviar $S \neq S'$ com objetivo de fazer com que Eva acredite que ele enviou $S = S'$. Desta maneira, o verificador descarta o Caso 3, pois sempre será flagrado trapaceando. No Caso 1, o verificador enganará Eva quando $b \oplus h = 0$, considerando que o verificador não conhece o estado $|\psi_b^a\rangle$, o sucesso dela terá probabilidade $\frac{1}{2}$. De forma análoga, no Caso 2, o verificador enganará Eva quando $b \oplus h = 0$, considerando que o verificador não conhece o estado $|\psi_b^a\rangle$, o sucesso dela terá probabilidade $\frac{1}{2}$. Os Casos de 4 até 7 oferecem probabilidade $\frac{1}{2}$ do verificador

	$h \oplus h'$	$x \oplus x'$	$z \oplus z'$	c	d	P
Caso 0	0	0	0	a	b	0
Caso 1	0	0	1	$a \oplus b \oplus \oplus h$	b	1/2
Caso 2	0	1	0	$a \oplus b \oplus h$	b	1/2
Caso 3	0	1	1	$a \oplus 1$	b	0
Caso 4	1	0	0	a	$b \oplus 1$	1/2
Caso 5	1	0	1	$a \oplus b \oplus h$	$b \oplus 1$	1/2
Caso 6	1	1	0	$a \oplus b \oplus h \oplus 1$	$b \oplus 1$	1/2
Caso 7	1	1	1	$a \oplus 1$	$b \oplus 1$	1/2

Tabela 2.2: Probabilidades do verificador enganar Eva com sucesso. No primeiro caso $S = S'$, os demais são os casos em que $S \neq S'$.

enganar Eva, pois nesses casos os resultados das medições são aleatórios pelo fato da base usada para realizar a medição do estado $|\psi_c^d\rangle$ ser $b \neq d = b \oplus 1$. Então, de acordo com a Tabela 2.2, percebe-se que a tentativa do verificador enganar Eva enviando $S \neq S'$ tem probabilidade total de sucesso $\frac{1}{2}$.

Agora, será generalizada a operação que deve ser usada pelo verificador para provocar a transição dos estados quânticos enviados por Eva. Seja $f : H \rightarrow S$, uma transformação bijetora que leva um grafo H a uma seqüência de bits S, U_f é uma transformação unitária de m qubits com controle clássico de $|S| = 3m$ bits, escrita da seguinte forma

$$U_{f(H)} = Z^{z_1} X^{x_1} H^{h_1} \otimes Z^{z_2} X^{x_2} H^{h_2} \otimes \cdots \otimes Z^{z_m} X^{x_m} H^{h_m}. \tag{2.17}$$

Em que o controle clássico é a seqüência $S = (x_1, z_1, h_1, \ldots, x_m, z_m, h_m)$. A transformação unitária $Z^{z_j} X^{x_j} H^{h_j}$, controlada pelo vetor (z_j, x_j, h_j), atua sobre o j-ésimo qubit para $j = 1, 2, \ldots, m$. Pode-se observar que $U_{f(H)}$ foi definida de forma que $U_{f(H)} \neq U_{f(H')}$ para $H \neq H'$. Desejando introduzir um grafo de n nós, diz-se que serão necessários $g(n)$ bits para representá-los, e a transformação $U_{f(H)}$ terá $m = g(n)/3$ entradas de qubits e um controle clássico de $|S| = g(n)$ bits.

2.2 Estados Coerentes

Qubits são estados quânticos que pertencem a um espaço de Hilbert de dimensão 2. Entretanto, existem outros estados quânticos definidos em espaços de Hilbert de dimensões maiores e até infinita, que é o caso do estado coerente, cuja representação é mais comum é $|\alpha\rangle$, sendo α um número complexo. Para esse espaço de dimensão infinita, uma base deve ter infinitos estados. A base aqui considerada é a base formada por estados de número, $|n\rangle$. Assim, nesse espaço de

Hilbert de dimensão infinita, qualquer estado pode ser escrito da forma:

$$|\psi\rangle = \sum_{n=0}^{\infty} c_n |n\rangle. \tag{2.18}$$

O estado coerente é o estado cuja decomposição na base de estados de número é

$$|\alpha\rangle = \exp\left(-\frac{1}{2}|\alpha|^2\right) \sum_n \frac{\alpha^n}{(n!)^{\frac{1}{2}}} |n\rangle. \tag{2.19}$$

Em uma medição de $|\alpha\rangle$ na base $\{|n\rangle\}_{n=0}^{\infty}$, a probabilidade do resultado $|n\rangle$ ser obtido é

$$p_n = \exp\left(-|\alpha|^2\right) \frac{|\alpha|^{2n}}{n!}. \tag{2.20}$$

A distribuição (A.14) é prontamente reconhecida como uma distribuição Poissoniana com média igual a $\langle n\rangle = |\alpha|^2$.

2.3 Estados Entrelaçados

O entrelaçamento quântico descreve a correlação não local entre sistemas quânticos que interagiram no passado. Estados entrelaçados podem ser criados interagindo dois ou mais sistemas individuais através de uma operação unitária. Propriedades como spin de elétrons ou polarização de fótons, por exemplo, podem ser entrelaçadas. O estado entrelaçado de dois qubits

$$|\Psi\rangle_{12} = \frac{|01\rangle_{12} - |10\rangle_{12}}{\sqrt{2}},$$

por exemplo, pode ser entendido da seguinte maneira: uma medição realizada na partícula 1 projeta-a em um estado que, dependendo do medidor usado, pode ser qualquer superposição linear dos estados $|0\rangle$ e $|1\rangle$ e, após conhecido o resultado da medição da partícula 1, a partícula 2 é projetada para o estado ortogonal.

A teleportação só é possível com a presença de entrelaçamento quântico, ou seja, é com base no princípio da não-localidade e do postulado da projeção da mecânica quântica em que a teleportação se fundamenta. O efeito prático da teleportação é a destruição do objeto original na fonte e a criação de uma réplica exata no local de destino. Na verdade, o objeto não atravessa a distância que separa o transmissor do receptor, apenas informações suficientes para criá-lo é transmitida.

O processo por trás da teleportação resume-se nos seguintes passos: inicialmente, Alice e Bob dividem um par EPR e Alice tem um qubit $|\Psi\rangle$ que deseja enviar para Bob; Alice interage

Medição de Alice	**Estado de Bell**	**Transformação Unitária σ**
00	$\|B_{00}\rangle \equiv (\|00\rangle + \|11\rangle)/\sqrt{2}$	$\sigma_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
01	$\|B_{01}\rangle \equiv (\|01\rangle + \|10\rangle)/\sqrt{2}$	$\sigma_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
10	$\|B_{10}\rangle \equiv (\|00\rangle - \|11\rangle)/\sqrt{2}$	$\sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
11	$\|B_{11}\rangle \equiv (\|01\rangle - \|10\rangle)/\sqrt{2}$	$\sigma_4 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$

Tabela 2.3: Mapeamento das quatro possíveis medições de Alice nos estados de Bell e as transformações unitárias correspondentes.

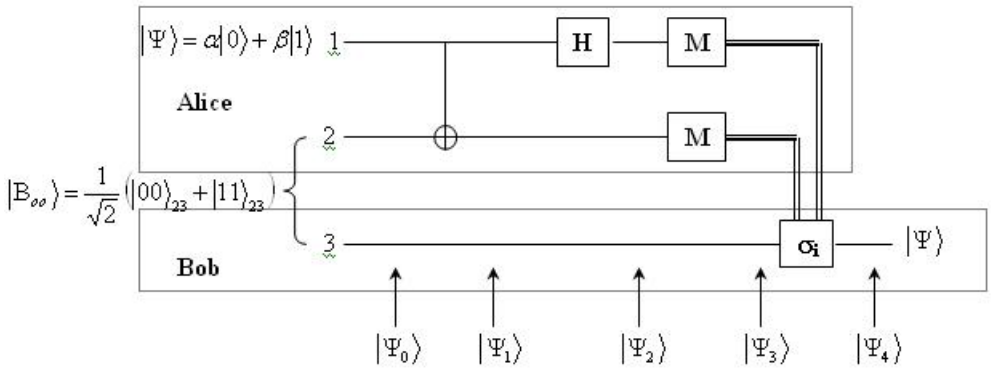

Figura 2.1: Circuito quântico para a teleportação de um qubit.

o qubit $|\Psi\rangle$ com sua metade do par EPR, e então realiza uma medição em ambos. Tal medição vai determinar em qual dos seguintes estados da base de Bell o conjunto fóton-qubit estará, conforme a Tabela 2.3. Esses estados são então codificados em quatro possíveis resultados (00, 01, 10 ou 11) e enviados a Bob, usando dois bits, por um canal clássico de comunicação. De acordo com a informação que recebeu de Alice, Bob executa uma das quatro transformações unitárias σ na sua metade do par EPR (terceira coluna da Tabela 2.3), recuperando o estado original $|\Psi\rangle$.

Na Figura 2.1, é apresentado o circuito quântico para a teleportação de um qubit, em que linha dupla significa um canal clássico de comunicação. O estado a ser teleportado e o par EPR são, respectivamente:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle; \tag{2.21}$$

$$|\mathrm{B}_{00}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}. \tag{2.22}$$

O estado na entrada do circuito é

$$|\Psi_0\rangle = |\Psi\rangle|B_{00}\rangle = \frac{1}{\sqrt{2}}\left[\alpha\left(|000\rangle + |011\rangle\right) + \beta\left(|100\rangle + |111\rangle\right)\right]_{123},$$

na qual os dois primeiros qubits pertencem à Alice (1 e 2), e o último (3), ao Bob, sendo que o segundo qubit de Alice e o qubit de Bob compõem o par EPR. Na seqüência, Alice envia sua segunda partícula através uma porta CNOT (*Controlled NOT*) e seu primeiro qubit por uma porta Hadamard (H), obtendo os seguintes estados, respectivos:

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}}\left[\alpha\left(|000\rangle + |011\rangle\right) + \beta\left(|110\rangle + |101\rangle\right)\right]_{123};$$

$$\begin{aligned} |\Psi_2\rangle &= \frac{1}{2}\left[|00\rangle_{12}\left(\alpha|0\rangle + \beta|1\rangle\right)_3 + |01\rangle_{12}\left(\beta|0\rangle + \alpha|1\rangle\right)_3\right] \\ &+ \frac{1}{2}\left[|10\rangle_{12}\left(\alpha|0\rangle - \beta|1\rangle\right)_3 + |11\rangle_{12}\left(\alpha|1\rangle - \beta|0\rangle\right)_3\right]. \end{aligned} \tag{2.23}$$

Alice, então, mede seus qubits e envia o resultado da medição para Bob que, com base na Tabela 2.3, executará a operação unitária correspondente para obter o estado $|\Psi\rangle$ em sua saída, conforme (2.24)

$$|\Psi_4\rangle = \sigma_i|\Psi_3\rangle = |\Psi\rangle. \tag{2.24}$$

Um importante fato observado na teleportação quântica é que todas as operações realizadas (medições de Alice e transformação unitária de Bob) são locais. Isso significa que não há necessidade de qualquer operação global que envolva os três qubits simultaneamente, caracterizando uma genuína teleportação.

2.3.1 Probabilidade do verificador quando ele mente a respeito de um bit de teleportação no protocolo 7

Seja $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ um qubit para ser teleportado, o estado quântico no estágio antes da medição realizada por ***V*** é:

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{2}\left[|00\rangle_{a_jb_j}\left(\alpha|0\rangle + \beta|1\rangle\right) + |01\rangle_{a_jb_j}\left(\alpha|1\rangle + \beta|0\rangle\right)\right] \\ &+ \frac{1}{2}\left[|10\rangle_{a_jb_j}\left(\alpha|0\rangle - \beta|1\rangle\right) + |11\rangle_{a_jb_j}\left(\alpha|1\rangle - \beta|0\rangle\right)\right]. \end{aligned} \tag{2.25}$$

Quando o vetor (a_j, b_j) chegar até Eva, ela aplica no *j*-ésimo qubit teleportado a operação $Z^{a_j}X^{b_j}$. Como $|\psi\rangle$ pertence ao conjunto $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$, existem erros na teleportação desses qubits que são imperceptíveis. Para os qubits da base retangular, $\{|0\rangle, |1\rangle\}$, somente as correções de erros do tipo bit-flip, X, são relevantes. Da mesma forma, para a base diagonal, $\{|+\rangle, |-\rangle\}$, somente os erros de inversão de fase são relevantes. Contudo, se o qubit não for alterado, a chance de ***V***enganar Eva, modificando um bit do vetor (a_j, b_j), tem probabilidade 1/2, exatamente a probabilidade de ***V*** acertar a transformação para a qual a sua aplicação naquele qubit é irrelevante.

Capítulo 3

Protocolo quântico de compromisso de informação e a prova de conhecimento nulo para toda linguagem $\mathcal{NP}$

Neste capítulo é aplicado um esquema quântico de compromisso de informação para a construção de um sistema de prova de conhecimento nulo usando grafos tricoloríveis. Uma breve introdução histórica é apresentada sobre a discórdia quanto a segurança do protocolo quântico de compromisso de informação nos últimos anos. Na seção 3.2 são postos os fundamentos da prova de Lo e Chau da inexistência do protocolo quântico de compromisso de informação incondicionalmente seguro. Por fim, na seção 3.3 é apresentado um compromisso de informação quântica baseado em estados coerentes da luz e este esquema é usado para construir um sistema de prova de conhecimento.

3.1 Introdução

O protocolo de compromisso de informação, no inglês *Bit Commitment* (BC), é um importante protocolo de criptografia que tem importantes aplicações em sistemas criptográficos maiores. Por exemplo, sistemas de prova de conhecimento nulo para toda linguagem $\mathcal{NP}$ [9], sistemas de votação eletrônica [25], moedas eletrônicas [28] e esquemas de identificação [27].

Um esquema de compromisso de informação é executado entre dois agentes, Alice e Bob, que não confiam um no outro. Um exemplo simples de aplicação desse esquema é o protocolo de lançamento de moeda. O protocolo de lançamento de moeda nasce da necessidade entre duas partes em conflito tomarem uma decisão baseada na sorte. Como em [39], supõe-se a seguinte situação: Alice e Bob estão divorciados e não querem mais ver um ao outro novamente.

Adicionalmente, eles não confiam em uma terceira parte atuando como um juiz. Então, eles concordam em decidir num lançamento de moeda quem ficará com o cachorro do casal. Se Bob não está vendo o lançamento da moeda, como ele poderia estar certo de que Alice está sendo honesta quando ela diz "O resultado é cara. Você perdeu."? Uma solução para este problema pode ser dada da seguinte maneira: Alice lança uma moeda e fecha o resultado numa caixa com uma chave. Ela envia a caixa fechada para Bob como compromisso de que lançou a moeda. Não conseguindo ver o que há na caixa, Bob faz a sua aposta e a envia para Alice. Finalmente Alice envia a chave a Bob, para que ele abra a caixa e se certifique de quem realmente ganhou a aposta.

Em criptografia clássica, a caixa usada para esconder o compromisso são as funções de sentido único ou permutações de sentido único [36]. Este simples protocolo criptográfico se dá em duas fases:

- *Fase de compromisso*. Alice escolhe um valor b e gera aleatoriamente outro valor c. Ela envia como compromisso o valor $f_c(b)$. Sem o conhecimento de c, Bob não tem conhecimento da informação b que representa $f_c(b)$.

- *Fase de revelação*. Alice envia (b, c) a Bob para que ele certifique-se de que $f_c(b)$ representava b.

Durante as duas fases do protocolo, ambas as partes não confiam uma na outra. Para um esquema de compromisso de informação ser confiável ele deve satisfazer dois requerimentos conflitantes:

- *Oculto*. Até que chegue a fase de revelação, Bob não pode ter nenhum conhecimento sobre o valor do compromisso que foi enviado. Esse requerimento tem que ser satisfeito sempre que Bob tenta trapacear.

- *Obrigatório*. Realizada a fase de compromisso, na fase de revelação, Bob deve receber um valor que ele aceita como uma efetiva revelação do compromisso. Esse requerimento tem que ser satisfeito mesmo quando Alice tenta trapacear.

A primeira versão quântica do compromisso de informação, no inglês *Quantum Bit Commitment* (QBC), foi proposta por Bennett e Brassard em 1984 [13]. Na versão quântica do lançamento de moeda discutida neste trabalho, a caixa é representada por um estado quântico. Alice codifica o resultado do lançamento da moeda dela em uma sequência de estados quânticos, escolhendo uma entre várias séries de estados não ortogonais. Sem prévio conhecimento dos estados, Bob não tem certeza dos estados que possui. Nesse momento, Bob faz a aposta dele

e informa a Alice. Alice avisa quais estados ela enviou e Bob realiza as medições para verificar a honestidade de Alice. Em [13], os autores mostraram que este protocolo é seguro contra uma trapaça passiva, na qual Alice inicialmente assume um compromisso de um bit com valor k e então tenta revelar o valor $1 - k$. No entanto, eles também provaram que Alice pode trapacear com uma estratégia mais sofisticada, na qual ela pode preparar um par de estados maximamente entrelaçado, mantendo uma partícula de cada par no laboratório dela e enviando a segunda partícula para Bob. Por consequência direta do efeito EPR (Eisntein-Podolsky-Rosen) [41], Alice pode então revelar os bits dela depois da medição de suas partículas em bases apropriadas e Bob não tem como perceber a diferença.

Subseqüentes propostas de QBC tentaram evitar este tipo de ataque forçando os agentes a realizarem suas medições e comunicarem classicamente como eles idealizaram o protocolo. Até 1993, Brassard e outros apresentaram um QBC que foi geralmente aceito como um protocolo incondicionalmente seguro numa conferência sobre segurança [42]. No entanto, em 1996 foi cogitado por Lo e Chau [43, 44], e independentemente por Mayers [45–47], que todas as propostas prévias de QBC são vulneráveis a um generalizado ataque EPR. O resultado deles é ligeiramente estendido para quaisquer propostas de QBC em geral. Posteriormente, estes resultados continuaram a ser válidos quando ambos os jogadores são restringidos pelas regras de punição [48]. Portanto, embora as propostas de QBC sejam de difícil ataque com tecnologias atuais, nenhuma delas é incondicionalmente segura. Spekkens e Rudolph [49] estenderam estes resultados para fornecer limites explícitos para medir o grau de ocultação e obrigatoriedade.

Lo-Chau-Mayers têm continuamente modificado as suas demonstrações. Yuen e outros têm repetidamente expressado dúvidas com relação à prova de Mayers [47], argumentando que a prova apresentada não é geral o suficiente para excluir todo QBC oculto. Vários protocolos têm sido propostos [50, 51], e trabalhos a respeito da controvérsia têm se manifestado [52–54]. Os protocolos de Yuen visam reforçar a posição de Bob com a ajuda de "parâmetros secretos" ou "estados anônimos", de modo que Alice carece de alguma informação para trapacear com êxito. Desta maneira, o teorema de Uhlmann ainda iria implicar na existência de uma transformação unitária usada na trapaça como descrito anteriormente, porém esta transformação poderia ser desconhecida por Alice, impossibilitando assim, a manipulação do estado que foi entregue como compromisso. Até aí, dois campos estavam formados. Um grande grupo, compreendendo a maior parte da comunidade, aceita a impossibilidade do protocolo quântico de compromisso de informação de acordo com a prova de Lo-Chau-Mayers, e Yuen e outros faziam propostas de novos protocolos, apesar de não serem provadamente seguros. A discussão tratava ligeiramente de diferentes abordagens para o problema. Até que em 2007 foi feita uma análise da discussão [54]. Segundo D'Ariano e outros, uma boa maneira de identificar a base da discórdia é através

do clássico princípio de Kerckhoffs [55]. Esse princípio estabelece que a segurança de um protocolo criptográfico não deve confiar num sistema que mantém o algoritmo secreto. Um procedimento secreto sempre é um forte ponto de fracasso, podendo sempre cair nas mãos do inimigo. Um exemplo foi o roubo da máquina de cifragem dos alemães, Enigma, que foi cair nas mãos dos ingleses. Por essa razão, autores de sistemas de criptográficos geralmente devem pensar em seus algoritmos como sendo executados por máquinas, cujas matrizes podem ser publicadas sem colocar em perigo a segurança do sistema. Assim, o resultado da discórdia ficou favorável aos argumentos de Lo-Chau-Mayers.

3.2 Prova de insegurança do protocolo quântico de compromisso de informação

Em essência, o procedimento geral para qualquer esquema quântico de compromisso de informação pode ser modelado da seguinte maneira, [43]:

1. Alice escolhe o valor de um bit para ser o compromisso a ser enviado a Bob. Se $b = 0$, ela prepara o estado

$$|0\rangle = \sum_i \alpha_i |e_i\rangle_A |\phi_i\rangle_B. \tag{3.1}$$

   Em que $\langle e_i|e_j\rangle = \delta_{ij}$, mas os estados $|\phi_i\rangle_B$'s não são necessariamente ortogonais entre si. Similarmente, se $b = 1$, ela prepara o estado

$$|1\rangle = \sum_j \alpha_j |e'_j\rangle_A |\phi'_j\rangle_B. \tag{3.2}$$

   É assumido que Alice e Bob conhecem os estados $|0\rangle$ e $|1\rangle$;

2. Uma Alice honesta realiza a medição do seu registro e determina o valor i se $b = 0$ (j se $b = 1$);

3. Alice envia o segundo registro para Bob como compromisso de informação;

4. Mais tarde, Alice abre o compromisso declarando o valor de b e de i ou j;

5. Bob realiza as medições no segundo registro e verifica se de fato Alice realizou um compromisso do bit b.

Pode-se verificar que o esquema é oculto. Para ter certeza de que Bob não terá nenhuma informação sobre o bit de compromisso b, as matrizes densidades descrevendo o segundo registro são as mesmas para o bit 0 e 1, ou seja,

$$\mathrm{Tr}_A|0\rangle\langle 0| = \rho_0^B = \rho_1^B = \mathrm{Tr}_A|1\rangle\langle 1|. \tag{3.3}$$

Isto garante que Bob não tenha qualquer informação sem que antes Alice revele o compromisso. No entanto, o protocolo quântico de compromisso de informação descrito anteriormente não é obrigatório. O fato é que Alice pode aplicar uma transformação unitária local U_A para transformar o estado $|0\rangle$ no estado $|1\rangle$ e vice-versa. Mais precisamente, considere a seguinte estratégia de trapaça: No primeiro passo, Alice prepara o estado $|0\rangle$ correspondendo a $b = 0$. Então ela pula o segundo passo e envia o segundo registrador pra Bob como descrito no terceiro passo. Agora, ela decide o valor de b para somente revelá-lo no quarto passo. Se a sua escolhe for zero, ela executa o protocolo honestamente. Mas se a sua escolha for $b = 1$, ela aplica a operação unitária U_A para transforma o estado $|0\rangle$ no estado $|1\rangle$ e executa a revelação como se tivesse feito o compromisso do bit 1.

O ataque acima é construído dando todos os poderes a Alice (memória quântica por tempo necessário, transmissão livre de erros, e preservação do entrelaçamento até o fim do protocolo). Outra direção nas pesquisas sobre o protocolo quântico de compromisso de informação é a investigação de barreiras físicas que impeçam o ataque EPR [56].

3.3 Protocolo quântico de compromisso de informação com estados coerentes

Uma proposta bem realística de QBC é feita em [57, 58]. A idéia consiste no uso de estados coerentes da luz para criar um modelo de cifra que não pode ser mudado seu estado depois de feito o compromisso. O protocolo proposto não requer memória quântica, isto é, Bob não precisa armazenar o estado quântico até que Alice faça a revelação. A vantagem desse protocolo quântico é que ele pode ser construído com tecnologia atualmente existente. A implementação do esquema quântico de compromisso de informação como proposto em [57] é mostrada na Figura 3.1.

Como pode ser visto na Figura 3.1.a, apenas três possíveis escolhas são consideras e cada escolha de Alice é codificada num estado de polarização representado pelo estado coerente bi-

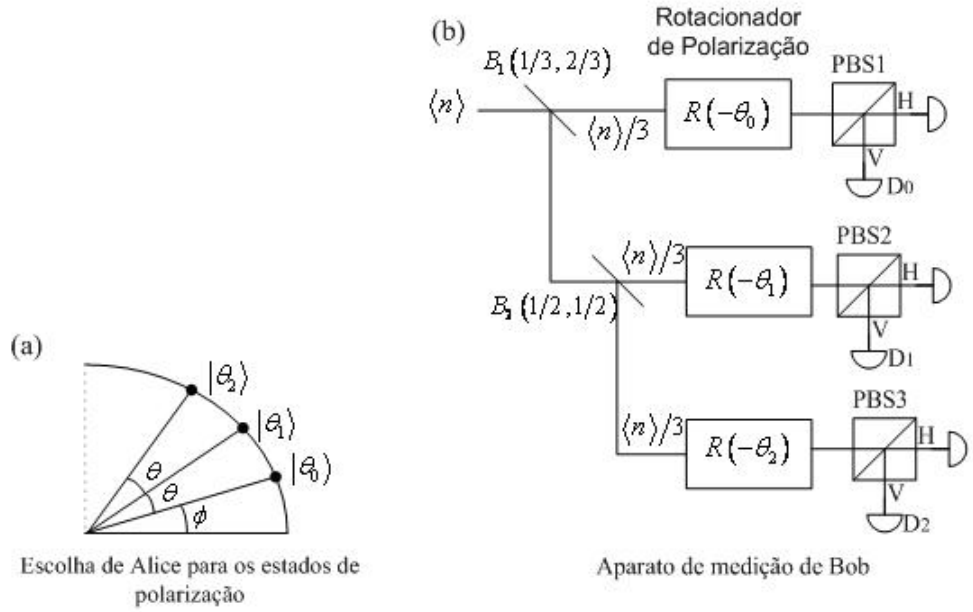

Figura 3.1: Protocolo quântico de compromisso de informação baseado em estados coerentes e sem uso de memória quântica. B_1 e B_2 são divisores de feixe, PBS é um divisor de feixes de polarização e R é um rotacionador de polarização.

modal:

$$|\alpha\cos(\phi), \alpha\,\mathrm{sen}(\phi)\rangle \tag{3.4}$$

$$|\alpha\cos(\phi+\theta), \alpha\,\mathrm{sen}(\phi+\theta)\rangle \tag{3.5}$$

$$|\alpha\cos(\phi+2\theta), \alpha\,\mathrm{sen}(\phi+2\theta)\rangle \tag{3.6}$$

Aqui, os estados restringem-se aos casos nos quais α é um número real ($\langle n\rangle = \alpha^2$), considerando somente a polarização linear da luz. Na Figura 3.1.b, pode ser visto um aparato para medir o estado quântico enviado por Alice. Esse aparato é composto por divisores de feixes ($B_{1,2}$) que dividem o feixe incidente em dois; por rotacionadores de polarização (R), que adicionam um valor ($\theta_j, j = 0, 1, 2$) ao ângulo do argumento das funções cosseno e seno; por divisores de feixes por polarização ($PBS_{1,2,3}$), que separam as duas componentes do feixe e por detectores de fótons isolados, que detectam ou não a presença do estado quântico. A evolução dos estados quânticos no aparato de Bob, como na Figura 3.2, quando Alice escolhe e envia o estado $|\theta_k\rangle$ $k = 0, 1, 2$, é da forma:

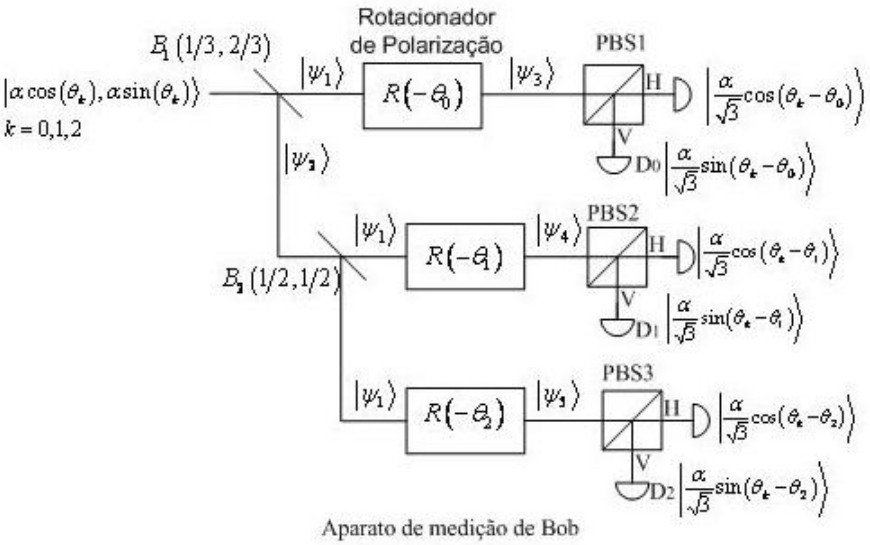

Figura 3.2: Evolução dos estados quânticos no aparato de Bob.

$$|\psi_1\rangle = |\frac{\alpha}{\sqrt{3}}\cos(\theta_k), \frac{\alpha}{\sqrt{3}}\,\mathrm{sen}(\theta_k)\rangle; \tag{3.7}$$

$$|\psi_2\rangle = |\frac{\alpha\sqrt{2}}{\sqrt{3}}\cos(\theta_k), \frac{\alpha\sqrt{2}}{\sqrt{3}}\,\mathrm{sen}(\theta_k)\rangle; \tag{3.8}$$

$$|\psi_3\rangle = |\frac{\alpha}{\sqrt{3}}\cos(\theta_k - \theta_0), \frac{\alpha}{\sqrt{3}}\,\mathrm{sen}(\theta_k - \theta_0)\rangle; \tag{3.9}$$

$$|\psi_4\rangle = |\frac{\alpha}{\sqrt{3}}\cos(\theta_k - \theta_1), \frac{\alpha}{\sqrt{3}}\,\mathrm{sen}(\theta_k - \theta_1)\rangle; \tag{3.10}$$

$$|\psi_5\rangle = |\frac{\alpha}{\sqrt{3}}\cos(\theta_k - \theta_2), \frac{\alpha}{\sqrt{3}}\,\mathrm{sen}(\theta_k - \theta_2)\rangle. \tag{3.11}$$

As probabilidades de Bob obter uma detecção nos detectores verticais D_0, D_1 e D_2 (considerados ideais) são dadas, respectivamente, por:

$$P_{D_0} = 1 - \exp\left\{-\frac{\alpha^2}{3}\,\mathrm{sen}^2(\theta_k - \theta_0)\right\}; \tag{3.12}$$

$$P_{D_1} = 1 - \exp\left\{-\frac{\alpha^2}{3}\,\mathrm{sen}^2(\theta_k - \theta_1)\right\}; \tag{3.13}$$

$$P_{D_2} = 1 - \exp\left\{-\frac{\alpha^2}{3}\,\mathrm{sen}^2(\theta_k - \theta_2)\right\}. \tag{3.14}$$

De acordo com os resultados das medições, em alguns casos, Bob estará certo do estado enviado por Alice (detecções verticais em duas saídas: D_0 e D_1, D_0 e D_2, ou D_1 e D_2), em outros

casos ele estará certo sobre o estado não enviado por Alice (detecção vertical somente em uma das saídas: D_0, D_1 ou D_2) e, em último caso, ele não terá certeza sobre nada (nenhuma detecção vertical nas saídas). Isso ocorre, porque quando o estado enviado coincide com o valor do rotacionador, o argumento do seno em uma das equações (3.12)-(3.14) se anula, tornando também nula a probabilidade de detecção no correspondente detector vertical. Todas essas situações são descritas na Tabela 2.1, em que o valor '1' indica detecção.

D_0	D_1	D_2	Possíveis estados enviados por Alice
0	0	0	$\{\|\theta_0\rangle, \|\theta_1\rangle, \|\theta_2\rangle\}$
0	0	1	$\{\|\theta_0\rangle, \|\theta_1\rangle\}$
0	1	0	$\{\|\theta_0\rangle, \|\theta_2\rangle\}$
0	1	1	$\{\|\theta_0\rangle\}$
1	0	0	$\{\|\theta_1\rangle, \|\theta_2\rangle\}$
1	0	1	$\{\|\theta_1\rangle\}$
1	1	0	$\{\|\theta_2\rangle\}$

Tabela 3.1: Detecções verticais no aparato de Bob e suas conclusões.

Protocolo 3. *Um simples compromisso de informação com estados coerente*
Estágio de compromisso

1. *Alice escolhe um dos estados $\{|\theta_0\rangle, |\theta_1\rangle, |\theta_2\rangle\}$ e o envia para Bob;*

2. *Bob usa o aparato mostrado na Figura 3.1.b para medir o estado quântico enviado por Alice e ele armazena o resultado clássico obtido em uma memória clássica (em geral, memória de um computador).*

Estágio de revelação

1. *Alice informa a Bob o estado quântico enviado;*

2. *Bob verifica se a informação de Alice está em concordância com o resultado de suas medições. Por exemplo, suponha que Bob obteve detecção vertical na saída D_2. Se Alice disser para ele que enviou $|\theta_2\rangle$, Bob saberá que ela está mentindo.*

A probabilidade de Bob obter, sem ambiguidade, o valor correto do estado enviado por Alice, antes do estágio de revelação, é igual à probabilidade de Bob identificar, sem ambiguidade, se a componente horizontal do estado coerente enviado por Alice é um dos estados $\{|\alpha\cos(\phi)\rangle, |\alpha\cos(\phi+\theta)\rangle, |\alpha\cos(\phi+2\theta)\rangle\}$. Alternativamente, Bob poderia checar se a componente vertical do estado coerente enviado por Alice é um dos estados $\{|\alpha\,\mathrm{sen}(\phi)\rangle, |\alpha\,\mathrm{sen}(\phi+$

$\theta)\rangle, |\alpha \operatorname{sen}(\phi + 2\theta)\rangle\}$. Usando o aparato de medição proposto em [59], as probabilidades de sucesso, P_{B_H} para a componente horizontal e P_{B_V} para a componente vertical, são dadas por:

$$\begin{aligned} P_{B_H} &= \frac{1}{3}\left[\sum_{j=1}^{3}\prod_{k\neq j}^{3}\left(1-e^{-\frac{1}{\sqrt{2}}[\alpha_k-\alpha_j]^2}\right)\right] \\ &= \frac{1}{3}\left[1-e^{-\frac{\langle n\rangle}{\sqrt{2}}[\cos(\phi+\theta)-\cos(\phi)]^2}\right]\left[1-e^{-\frac{\langle n\rangle}{\sqrt{2}}[\cos(\phi+2\theta)-\cos(\phi)]^2}\right] \\ &+ \frac{1}{3}\left[1-e^{-\frac{\langle n\rangle}{\sqrt{2}}[\cos(\phi)-\cos(\phi+\theta)]^2}\right]\left[1-e^{-\frac{\langle n\rangle}{\sqrt{2}}[\cos(\phi+2\theta)-\cos(\phi+\theta)]^2}\right] \\ &+ \frac{1}{3}\left[1-e^{-\frac{\langle n\rangle}{\sqrt{2}}[\cos(\phi)-\cos(\phi+2\theta)]^2}\right]\left[1-e^{-\frac{\langle n\rangle}{\sqrt{2}}[\cos(\phi+\theta)-\cos(\phi+2\theta)]^2}\right] \end{aligned} \tag{3.15}$$

$$\begin{aligned} P_{B_V} &= \frac{1}{3}\left[\sum_{j=1}^{3}\prod_{k\neq j}^{3}\left(1-e^{-\frac{1}{\sqrt{2}}[\beta_k-\beta_j]^2}\right)\right] \\ &= \frac{1}{3}\left[1-e^{-\frac{\langle n\rangle}{\sqrt{2}}[\operatorname{sen}(\phi+\theta)-\operatorname{sen}(\phi)]^2}\right]\left[1-e^{-\frac{\langle n\rangle}{\sqrt{2}}[\operatorname{sen}(\phi+2\theta)-\operatorname{sen}(\phi)]^2}\right] \\ &+ \frac{1}{3}\left[1-e^{-\frac{\langle n\rangle}{\sqrt{2}}[\operatorname{sen}(\phi)-\operatorname{sen}(\phi+\theta)]^2}\right]\left[1-e^{-\frac{\langle n\rangle}{\sqrt{2}}[\operatorname{sen}(\phi+2\theta)-\operatorname{sen}(\phi+\theta)]^2}\right] \\ &+ \frac{1}{3}\left[1-e^{-\frac{\langle n\rangle}{\sqrt{2}}[\operatorname{sen}(\phi)-\cos(\phi+2\theta)]^2}\right]\left[1-e^{-\frac{\langle n\rangle}{\sqrt{2}}[\operatorname{sen}(\phi+\theta)-\operatorname{sen}(\phi+2\theta)]^2}\right] \end{aligned} \tag{3.16}$$

Consequentemente, a probabilidade de sucesso de Bob é $P_B = P_{B_H} + P_{B_V} - P_{B_H}P_{B_V}$. Por outro lado, seguindo o protocolo, a probabilidade de Alice enganar Bob (enviando um estado no estágio de compromisso e informando outro estado no estágio de revelação), P_{A_1}, é:

$$P_{A_1} = p_{000} + \frac{1}{2}(p_{001} + p_{010} + p_{100}) \tag{3.17}$$

$$p_{000} = \frac{1}{3}e^{-\frac{\langle n\rangle}{3}\operatorname{sen}^2(\theta)}\left\{e^{-\frac{\langle n\rangle}{3}\operatorname{sen}^2(\theta)} + 2e^{-\frac{\langle n\rangle}{3}\operatorname{sen}^2(2\theta)}\right\} \tag{3.18}$$

$$p_{001} = p_{100} = \frac{1}{3}e^{-\frac{\langle n\rangle}{3}\operatorname{sen}^2(\theta)}\left\{2 - e^{-\frac{\langle n\rangle}{3}\operatorname{sen}^2(2\theta)} - e^{-\frac{\langle n\rangle}{3}\operatorname{sen}^2(\theta)}\right\} \tag{3.19}$$

$$p_{010} = \frac{2}{3}e^{-\frac{\langle n\rangle}{3}\operatorname{sen}^2(2\theta)}\left\{1 - e^{-\frac{\langle n\rangle}{3}\operatorname{sen}^2(\theta)}\right\} \tag{3.20}$$

Na equação (3.17), p_{000} é a probabilidade de não haver nenhuma detecção vertical, p_{001} (p_{010}, p_{100}) é a probabilidade de detecção somente em D_2 (D_1, D_0). Se Bob não teve nenhuma detecção vertical, então a probabilidade de Alice enganá-lo sem ser descoberta é 1. Se Bob teve uma detecção vertical em D_i, então ele pode detectar uma mentira se Alice disser durante o estágio de revelação que enviou $|\theta_i\rangle$. Conseqüentemente, a probabilidade de Alice enganar Bob

sem ser descoberto, nesse caso, é 1/2. Por fim, se Bob tem detecção vertical em duas saídas, então a probabilidade de Alice enganá-lo sem ser descoberta é 0, neste caso Bob estará certo sobre o estado enviado por Alice.

Um outro ataque que Alice pode realizar é, em vez de seguir o protocolo usando estados do conjunto $\{|\theta_0\rangle, |\theta_1\rangle, |\theta_2\rangle\}$, usar os estados de polarização intermediária, $|\theta_{01}\rangle = |\alpha\cos(\phi + \theta/2), \alpha\,\mathrm{sen}(\phi+\theta/2)\rangle$ e $|\theta_{12}\rangle = |\alpha\cos(\phi+3\theta/2), \alpha\,\mathrm{sen}(\phi+3\theta/2)\rangle$. Nesse caso, a probabilidade de Alice enganar Bob com sucesso, é:

$$
\begin{aligned}
P_{A_2} &= p_{000} + \frac{1}{2}(p_{001} + p_{010} + p_{100}); && (3.21)\\
p_{000} &= e^{-\frac{\langle n\rangle}{3}\left[2\,\mathrm{sen}^2\left(\frac{\theta}{2}\right)+\mathrm{sen}^2\left(\frac{3\theta}{2}\right)\right]}; && (3.22)\\
p_{001} &= p_{100} = \frac{1}{2}e^{-\frac{\langle n\rangle}{3}\,\mathrm{sen}^2\left(\frac{\theta}{2}\right)}\left\{P+Q\right\}; && (3.23)\\
P &= e^{-\frac{\langle n\rangle}{3}\,\mathrm{sen}^2\left(\frac{\theta}{2}\right)}\left(1-e^{-\frac{\langle n\rangle}{3}\,\mathrm{sen}^2\left(\frac{3\theta}{2}\right)}\right);\\
Q &= e^{-\frac{\langle n\rangle}{3}\,\mathrm{sen}^2\left(\frac{3\theta}{2}\right)}\left(1-e^{-\frac{\langle n\rangle}{3}\,\mathrm{sen}^2\left(\frac{\theta}{2}\right)}\right);\\
p_{010} &= e^{-\frac{\langle n\rangle}{3}\left[\mathrm{sen}^2\left(\frac{\theta}{2}\right)+\mathrm{sen}^2\left(\frac{3\theta}{2}\right)\right]}\left\{1-e^{-\frac{\langle n\rangle}{3}\,\mathrm{sen}^2\left(\frac{\theta}{2}\right)}\right\}. && (3.24)
\end{aligned}
$$

Para um protocolo quântico de compromisso de informação ideal, deve-se ter $P_A = P_B = 0$, em que $P_A = \max\{P_{A_1}, P_{A_2}\}$. Observando (3.15)-(3.24) nota-se que aumentando α^2, P_A tende a zero e P_B tende a um. Por outro lado, reduzindo α^2, P_A tende a um, enquanto que P_B tende zero. Assim, não é possível ter simultaneamente ambos iguais a zero.

Num ataque de Bob, o objetivo é reduzir a ambigüidade na identificação do estado de polarização (estado coerente bimodal), a ambiguidade na identificação de estados coerentes modais (horizontal e vertical), usando o setup proposto em [59]. Assim, a probabilidade de Bob ler sem ambiguidade o compromisso de Alice depende de ϕ, uma vez que a probabilidade de identificar os estados coerentes sem ambiguidade depende do número de fótons e de ϕ. Isso é mostrado claramente em (3.15) e (3.16). Já que Bob pode trocar ϕ em (3.4)-(3.6), aplicando uma rotação na polarização antes de realizar a tarefa de identificação do estado, é importante encontrar o valor de ϕ que maximiza P_B. A Figura 3.3 mostra P_{B_H}, P_{B_V} e P_B, versus ϕ para $\theta = \pi/12$ e $\langle n\rangle = 20$. Como pode ser visto na Figura 3.3, o melhor valor de ϕ é 1,302 rad.

Agora, usando $\phi = 1,302$ e $\theta = \pi/12$ são apresentadas na Figura 3.4 as probabilidades P_{A_1}, P_{A_2} e P_B versus o número médio de fótons.

Na Figura 3.4, para $\langle n\rangle = 22$ ($\langle n\rangle = 20$), encontra-se $P_A \approx 0,57$ (0,5239) e $P_B \approx 0,57$ (0.5239). É interessante notar que os valores de probabilidade ainda são altos e tornam o protocolo quântico de compromisso de bit inadequado para uso em protocolos de prova de conheci-

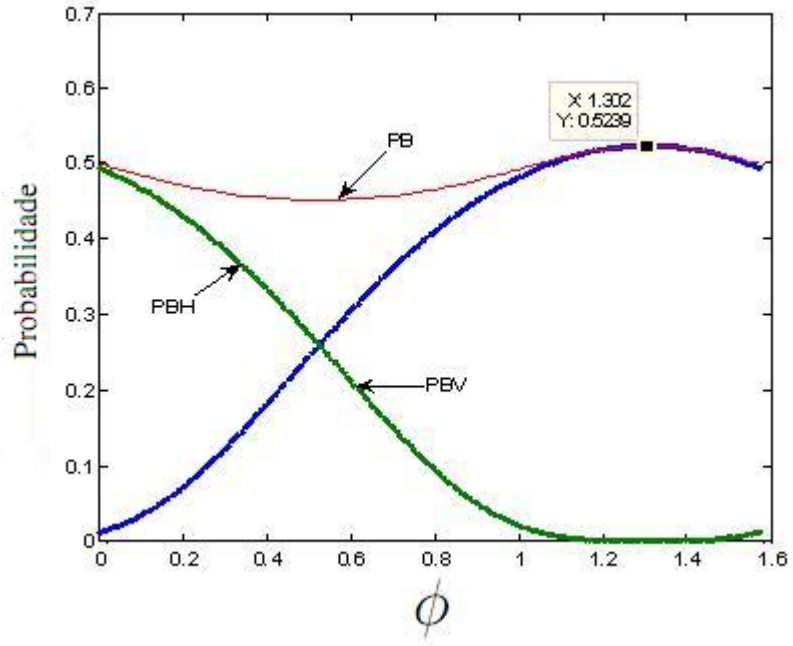

Figura 3.3: Probabilidade de sucesso no ataque de Bob versus ϕ, tendo como parâmetros fixos os valores $\theta = \pi/12$ e $\langle n \rangle = 20$.

mento nulo. Entretanto, em [57] foi ainda feita uma extensão do protocolo objetivando reduzir a probabilidade de sucesso nos ataques para valores assintoticamente próximos de zero. Deve-se considerar novamente a situação em que Alice tem que escolher uma entre apenas três possíveis escolhas, denominadas B, R e Y. Cada escolha possível é codificada por uma sequência de m bits, $B \rightarrow b_B$, $R \rightarrow b_R$, $Y \rightarrow b_Y$, e cada sequência difere das outras duas, pelo menos, $m/2$ bits. Assim, as distâncias de Hamming são: $H(b_B, b_R) \geq m/2$; $H(b_B, b_Y) \geq m/2$ e $H(b_R, b_Y) \geq m/2$. Cada bit de $b_k (k = B, R, Y)$ é a paridade de uma sequência de n bits formada por $2n$ estados quânticos enviados por Alice. Por exemplo, (i-ésimo bit de b_k) é a paridade de $|\psi_i\rangle = |\theta_1^1\rangle|\theta_2^i\rangle \ldots |\theta_{2n}^i\rangle$ dada por:

$$\text{XOR}\left(b(|\theta_1^i\rangle|\theta_2^i\rangle), b(|\theta_3^i\rangle|\theta_4^i\rangle), \ldots, b(|\theta_{2n-1}^i\rangle|\theta_{2n}^i\rangle)\right) \tag{3.25}$$

Na equação (3.25), $b(|\theta_j^i\rangle|\theta_k^i\rangle)$ é o bit que representa o par de estados quânticos $|\theta_j^i\rangle|\theta_k^i\rangle$, conforme a codificação: $\{|\theta_0\rangle|\theta_1\rangle, |\theta_1\rangle|\theta_2\rangle, |\theta_2\rangle|\theta_0\rangle\}$ representam o bit '0' enquanto que os pares $\{|\theta_0\rangle|\theta_2\rangle, |\theta_1\rangle|\theta_0\rangle, |\theta_2\rangle|\theta_1\rangle\}$ representam o bit '1'. Portanto, a adaptação no protocolo pode ser então descrita como segue:

Protocolo 4. *protocolo quântico de compromisso de informação.*
Estágio de compromisso

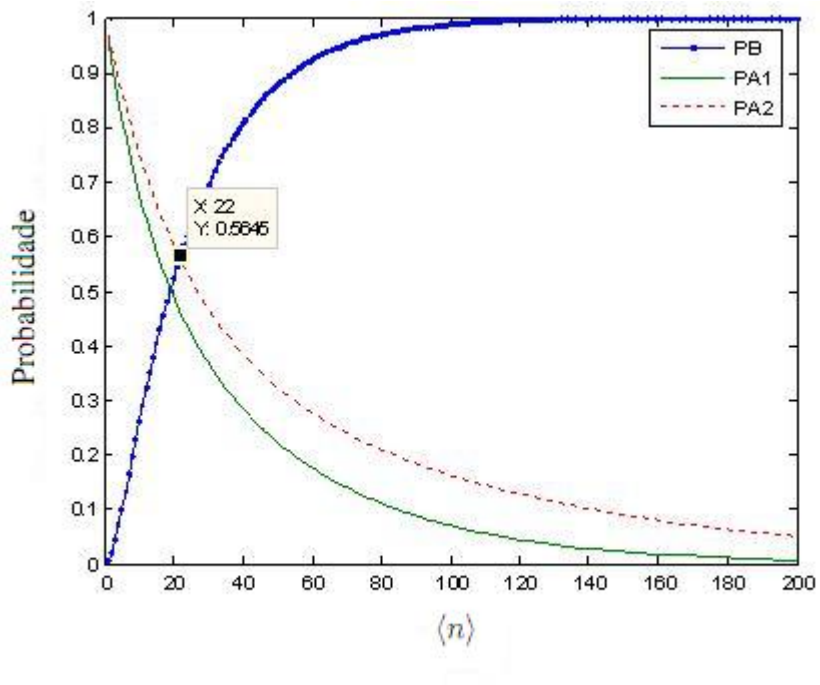

Figura 3.4: Probabilidade de sucesso nos ataques de Alice e Bob versus o número médio de fótons, $\langle n \rangle$.

1. *Alice envia para Bob os estados quânticos* $|\psi_1\rangle|\psi_2\rangle, \ldots, |\psi_m\rangle$*, sendo* $|\psi_i\rangle = |\theta_1^i\rangle, \ldots, |\theta_{2n}^i\rangle$.

2. *Bob usa o aparato mostrado na Figura 3.1.b para medir os estados quânticos enviados por Alice e armazenar os resultados das medições.*

Estágio de revelação

1. *Alice informa a Bob a sequência de m bits comprometida e os estados quânticos enviados.*

2. *Bob verifica se a informação fornecida por Alice está em concordância com os resultados das medições.*

A probabilidade de Bob desvendar a sequência de bits enviada por Alice sem a ajuda dela, considerando os parâmetros ($\phi = 1.302$ rad, $\theta = \pi/12$ and $\langle n \rangle = 22$), é, no melhor caso, $P_B \approx (0,57)^{2n}$, uma vez que Bob terá que saber corretamente pelo menos um bit da sequência de bits comprometida por Alice, isto é, ele terá que acertar com certeza uma sequência de $2n$ estados quânticos. Por outro lado, se Alice quer enganar Bob, ela tem que mentir, pelo menos, em $m/2$ bits da sequência e, para fazer isto, ela tem que mentir sobre no mínimo $m/2$ estados quânticos enviados. A probabilidade de Alice não ser apanhada mentindo é, no melhor caso,

$P_A \approx (0,57)^{m/2}$; por conseguinte, P_A e P_B podem ser próximos de zero se forem escolhidos valores de n e m grandes o suficiente. Entretanto o custo a ser pago é a quantidade de estados quânticos usados e medições realizadas. Como exemplo, consideremos o seguinte caso: $m = 6$, $n = 6$, $b_B = 001100$, $b_R = 010101$ e $b_Y = 100111$. Supõe-se que Alice escolheu b_Y. Nesse caso, Alice pode fazer as escolhas mostradas na Tabela 3.2.

1	0	0	1	1	1
$0\rightarrow\|\theta_0\rangle\|\theta_1\rangle$	$0\rightarrow\|\theta_2\rangle\|\theta_0\rangle$	$1\rightarrow\|\theta_0\rangle\|\theta_2\rangle$	$0\rightarrow\|\theta_2\rangle\|\theta_0\rangle$	$1\rightarrow\|\theta_0\rangle\|\theta_2\rangle$	$1\rightarrow\|\theta_2\rangle\|\theta_1\rangle$
$0\rightarrow\|\theta_2\rangle\|\theta_0\rangle$	$0\rightarrow\|\theta_0\rangle\|\theta_1\rangle$	$1\rightarrow\|\theta_1\rangle\|\theta_0\rangle$	$1\rightarrow\|\theta_0\rangle\|\theta_2\rangle$	$0\rightarrow\|\theta_1\rangle\|\theta_0\rangle$	$1\rightarrow\|\theta_1\rangle\|\theta_0\rangle$
$1\rightarrow\|\theta_1\rangle\|\theta_0\rangle$	$0\rightarrow\|\theta_1\rangle\|\theta_2\rangle$	$0\rightarrow\|\theta_2\rangle\|\theta_0\rangle$	$0\rightarrow\|\theta_1\rangle\|\theta_2\rangle$	$1\rightarrow\|\theta_1\rangle\|\theta_0\rangle$	$1\rightarrow\|\theta_0\rangle\|\theta_2\rangle$
$1\rightarrow\|\theta_1\rangle\|\theta_0\rangle$	$0\rightarrow\|\theta_2\rangle\|\theta_0\rangle$	$0\rightarrow\|\theta_2\rangle\|\theta_0\rangle$	$1\rightarrow\|\theta_2\rangle\|\theta_1\rangle$	$0\rightarrow\|\theta_1\rangle\|\theta_2\rangle$	$1\rightarrow\|\theta_0\rangle\|\theta_2\rangle$
$1\rightarrow\|\theta_0\rangle\|\theta_2\rangle$	$0\rightarrow\|\theta_1\rangle\|\theta_2\rangle$	$1\rightarrow\|\theta_0\rangle\|\theta_2\rangle$	$0\rightarrow\|\theta_1\rangle\|\theta_0\rangle$	$1\rightarrow\|\theta_2\rangle\|\theta_1\rangle$	$1\rightarrow\|\theta_2\rangle\|\theta_1\rangle$
$0\rightarrow\|\theta_2\rangle\|\theta_0\rangle$	$0\rightarrow\|\theta_1\rangle\|\theta_2\rangle$	$1\rightarrow\|\theta_1\rangle\|\theta_0\rangle$	$1\rightarrow\|\theta_2\rangle\|\theta_1\rangle$	$0\rightarrow\|\theta_2\rangle\|\theta_0\rangle$	$0\rightarrow\|\theta_1\rangle\|\theta_0\rangle$

Tabela 3.2: Exemplo de escolhas de Alice quando ela quer comprometer a sequência b_Y=100111.

Para o exemplo em que $1 = \text{XOR}(0,0,1,1,1,0)$ na coluna 1 da Tabela 3.2, a sequência '001110' foi escolhida aleatoriamente. O mesmo ocorre para a sequência em todas as colunas. Usando os estados mostrados na Tabela 3.2, Alice deve enviar para Bob os estados quânticos (concatenação dos estados em cada coluna da Tabela 2.2) mostrados nos estados quânticos em (3.26).

$$\begin{aligned}
|\psi_1\rangle &= |\theta_0\rangle|\theta_1\rangle|\theta_2\rangle|\theta_0\rangle|\theta_1\rangle|\theta_0\rangle|\theta_1\rangle|\theta_0\rangle|\theta_0\rangle|\theta_2\rangle|\theta_2\rangle|\theta_0\rangle,\\
|\psi_2\rangle &= |\theta_2\rangle|\theta_0\rangle|\theta_0\rangle|\theta_1\rangle|\theta_1\rangle|\theta_2\rangle|\theta_2\rangle|\theta_0\rangle|\theta_1\rangle|\theta_2\rangle|\theta_1\rangle|\theta_2\rangle,\\
|\psi_3\rangle &= |\theta_0\rangle|\theta_2\rangle|\theta_1\rangle|\theta_0\rangle|\theta_2\rangle|\theta_0\rangle|\theta_2\rangle|\theta_0\rangle|\theta_0\rangle|\theta_2\rangle|\theta_1\rangle|\theta_0\rangle,\\
|\psi_4\rangle &= |\theta_2\rangle|\theta_0\rangle|\theta_0\rangle|\theta_2\rangle|\theta_1\rangle|\theta_2\rangle|\theta_2\rangle|\theta_1\rangle|\theta_1\rangle|\theta_0\rangle|\theta_2\rangle|\theta_1\rangle,\\
|\psi_5\rangle &= |\theta_0\rangle|\theta_2\rangle|\theta_1\rangle|\theta_0\rangle|\theta_1\rangle|\theta_0\rangle|\theta_1\rangle|\theta_2\rangle|\theta_2\rangle|\theta_1\rangle|\theta_2\rangle|\theta_0\rangle,\\
|\psi_6\rangle &= |\theta_2\rangle|\theta_1\rangle|\theta_1\rangle|\theta_0\rangle|\theta_0\rangle|\theta_2\rangle|\theta_0\rangle|\theta_2\rangle|\theta_2\rangle|\theta_1\rangle|\theta_1\rangle|\theta_0\rangle. \qquad (3.26)
\end{aligned}$$

Os estados quânticos acima são enviados durante a fase de compromisso quando Alice quer comprometer a informação b_Y=100111.

Para que Bob decifre a sequência comprometida por Alice sem a ajuda dela, no presente caso, é suficiente para Bob descobrir o primeiro bit (uma vez que b_B e b_R começam com bit'0'). Para isso, ele tem que medir corretamente os 12 estados de $|\psi_1\rangle$. Isso acontece com probabilidade $P_{B1} \approx (0,57)^{12} \approx 0,001176$. Agora, suponha que, durante a fase de revelação, Alice afirme

a Bob que ela comprometeu a sequência b_R. Nesse caso, a probabilidade de Alice não ser descoberta mentindo é $P_A \approx (0,57)^3 \approx 0,185$, uma vez que ela deve ter mentido sobre um estado em $|\psi_1\rangle$, um em $|\psi_2\rangle$ e um em $|\psi_5\rangle$. Se Alice comprometeu b_B ou b_R, Bob deve estimar corretamente dois bits da sequência. A probabilidade de sucesso nesse caso é $P_B \approx (0.57)^{24}$.

Protocolo 5. *Prova de conhecimento nulo para uma linguagem $\mathcal{NP}$ usando protocolo quântico de compromisso de informação*

1. ***P** e **V** concordam com os números inteiros k e j, sendo k o número de bits da palavra código que codifica as cores B, R e Y; k/2 é a mínima distância de Hamming entre as duas palavras códigos usadas; j é o número de bits da string usado para calcular, através de uma função XOR, cada bit de uma palavra código.*

2. ***P** escolhe aleatoriamente uma permutação em S_3. Para cada vértice, **P** envia para **V** um conjunto de estados polarizados com $\langle n \rangle$=22 fótons, de acordo com a codificação usada.*

3. ***V** escolhe aleatoriamente uma aresta α e a envia para **P**.*

4. ***P** informa a **V** os estados quânticos enviados que correspondem aos vértices que pertencem a aresta α.*

5. *De acordo com o protocolo quântico de compromisso de informação, **V** verifica se a informação enviada por **P** realmente corresponde ao estado quântico medido por **V**.*

*Esses quatro passos são repetidos m^2 vezes. **V** aceita que o grafo G é tricolorível, se o Passo 4 tem sempre uma checagem positiva.*

Como explanado no protocolo quântico de compromisso de informação, ***V*** pode determinar a string enviada por ***P*** com probabilidade, no melhor caso, igual a $(0,57)^{2j}$. Assim, a probabilidade de ***V*** determinar todas as cores do grafo é, no melhor caso, $(0,57)^{n2j}$. ***V*** pode tentar isso m^2 vezes. Por outro lado, se o grafo não é tricolorível, a probabilidade de ***P*** enganar ***V*** com sucesso, por cada rodada, no melhor caso, é:

$$\frac{m-1}{m} + \frac{1}{m}\left[\frac{1}{2}(0,57)^{k/2} + \frac{1}{2}(0,57)^{k/2}\right] = 1 - \frac{1-(0,57)^{k/2}}{m} \tag{3.27}$$

Consequentemente, a probabilidade de ***P*** enganar ***V*** com sucesso durante todo o protocolo é

$$\left[1 - \left(1-(0,57)^{k/2}\right)/m\right]^{m^2}. \tag{3.28}$$

Quando *k* aumenta, essa probabilidade tende a e^{-m}. É importante enfatizar que, num protocolo de conhecimento nulo para linguagens $\mathcal{NP}$, nenhuma informação pode ser vazada. Usando o protocolo proposto, deve-se alcançar esse objetivo tornando *k* e *j* grandes o suficiente.

Capítulo 4

Dispositivo quântico à prova de falsificação

Este capítulo apresenta aplicações do conceito de dispositivo à prova de falsificação em protocolos de segurança. O capítulo segue o seguinte roteiro: na seção 4.2, o dispositivo quântico à prova de falsificação é usado para construir um acordo entre o verificador e uma terceira parte que quebra o anonimato do provador após a execução do sistema de prova de conhecimento nulo; na seção 4.3, é mostrado como um dispositivo quântico à prova de falsificação pode ser usado para provar a autoria de uma assinatura anônima.

4.1 Introdução

Stephen Wiesner escreveu o artigo intitulado *Conjugate Coding* em que fazia propostas inéditas de aplicação da mecânica quântica [11]. A idéia consistia basicamente em:

1. Produção de notas de dinheiro totalmente imunes à falsificação;

2. Um método para a combinação de duas mensagens em uma única transmissão quântica, de modo que o receptor pudesse escolher uma delas, mas não as duas simultaneamente. A leitura de uma implicava automaticamente na destruição da outra.

O artigo de Wiesner, publicado em 1983, lançou as bases da criptografia quântica. A idéia original de Wiesner para o dinheiro quântico era, em princípio teórico, possível, mas na prática era inviável, devido à dificuldade de armazenar fótons, manter os seus estados inalterados e não medidos por um longo período de tempo. No entanto, a idéia levantou um novo paradigma em sistemas de segurança. O dispositivo de Wiesner é essencialmente um dispositivo quântico à prova de falsificação (DQPF). Em essência, trata-se de uma máquina quântica em que os estados internos não podem ser acessados para impedir a previsão de resultados nas saídas.

Em [20], os autores destacam um DQPF para quebrar uma propriedade de sistemas de prova de conhecimento nulo. A idéia é construir um acordo entre duas partes que tira o poder de simulação de uma das partes. Assim, o anonimato do provador após uma interação com o verificador é quebrado. Watrous, em [16], destaca por que o paradigma da simulação não pode ser aplicado diretamente a verificadores com poder computacional quântico. As razões são as seguintes:

1. O estado quântico não pode ser copiado;

2. As medições são irreversíveis e seus efeitos não podem ser desfeitos.

Se o simulador é executado uma vez como uma caixa preta pelo verificador e a simulação não atinge um resultado satisfatório, não fica claro na simulação como reiniciar o processo e tentar novamente. Os estados de transição não podem ser copiados e a execução do verificador pode ter evoluído para um resultado irreversível.

Em [20], as propriedades desse dispositivo são discutidas e uma aplicação para assinaturas de contrato é apresentada. Neste trabalho, o DQPF é definido como um autômato quântico segundo a generalização de autômato quântico descrita em [60].

Definição 10. *Dispositivo quântico à prova de falsificação Um dispositivo quântico à prova de falsificação é um autômato quântico formado pela tupla* $Q = \{I, \Gamma, O, \mathcal{H}, |\psi_0\rangle, U, A\}$ *em que:*

1. I *é um conjunto finito de símbolos de entrada;*

2. Γ *é um conjunto finito de símbolos de observação;*

3. $O \subseteq \mathbb{R}$ *é um conjunto finito de símbolos de saída;*

4. $\mathcal{H}$ *é um espaço de Hilbert de dimensão finita;*

5. $|\psi_0\rangle \in \mathcal{H}$ *é um vetor unitário em* $\mathcal{H}$ *chamado de estado inicial;*

6. $U = \{U_i\}_{i \in I}$ *é uma família de transformações unitárias em* $\mathcal{H}$ *chamada de família de transformações;*

7. $A = \{A_\gamma\}_{\gamma \in \Gamma}$ *é uma família de observáveis sobre* $\mathcal{H}$*, chamada de família de observáveis, tal que o espectro de* A_γ *está contido em* O *para todo* $\gamma \in \Gamma$.

Estudando o poder computacional de um sistema físico podem-se extrair idéias significativas da estrutura e dinâmica do sistema. No autômato da definição 10, duas entradas são possíveis: entradas de transição $i \in I$ e entradas de observação $\gamma \in \Gamma$. Entradas de transição estão associadas às transformações $U = \{U_i\}_{i \in I}$, enquanto que as entradas de observação estão associadas

aos observáveis, $A = \{A_\gamma\}_{\gamma\in\Gamma}$. Nesse caso, o espectro de A_γ está contido em O para todo $\gamma \in \Gamma$. Em outras palavras, o conjunto de saídas $O \subseteq \mathbb{R}$ contém os autovalores de todos os observáveis A_γ do autômato. Respeitando o postulado da mecânica quântica, o autômato inicia no estado $|\psi_0\rangle$, evolui deterministicamente quando as transições de entrada são lidas, e evolui probabilisticamente quando as entradas de observação são lidas. Assim, quando a transição i é lida, os estado $|\psi_0\rangle$ do autômato evolui para $U_i|\psi_0\rangle = |\psi_i\rangle$, sem apresentar qualquer valor na saída. Quando um símbolo de observação γ é lido, então o estado $|\psi_i\rangle$ evolui para $P_o|\psi_i\rangle/||P_o|\psi_i\rangle||$ com probabilidade $||P_o|\psi_i\rangle||$ para $o \in O$ de A_γ, em que P_o é a projeção do auto-espaço de A_γ associado à saída o.

4.2 Uma memória quântica transfere a prova de interação entre o provador e o verificador a uma terceira parte

A impossibilidade de transferência de prova é uma propriedade conhecida como resistente a ataques clássicos, mas foi mostrado em [19] que não é resistente a ataques quânticos com o uso de estados de Bell. Inicialmente, estados de Bell são preparados e a terceira parte, Eva, compartilha-os com o verificador. Durante o ataque, o verificador pode somente realizar dois tipos de medições nos qubits do par de Bell que estão em seu laboratório. Essa é a única entrada permitida no dispositivo quântico à prova de falsificação. Essas restrições são suficientes para impedir a simulação do verificador. Ao final, Eva tem como confirmar se o verificador foi honesto quanto ao uso do dispositivo.

Nesta seção, para entender a aplicação de uma memória quântica no impedimento de uma simulação, deve-se imaginar a seguinte situação: Eva armazena em uma memória quântica um estado $|\psi_a^b\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, em que b representa a base de medição (0 para a base $\{|0\rangle, |1\rangle\}$ e 1 para a base $\{|+\rangle, |-\rangle\}$) e a representa o valor lógico do qubit (0 se o estado quântico $|0\rangle$ ou $|+\rangle$ e 1 se o estado quântico é $|1\rangle$ ou $|-\rangle$). Os estados quânticos $|+\rangle$ e $|-\rangle$ são definidos pelas superposições: $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ e $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Depois desse qubit estar armazenado em uma memória quântica, Eva envia a memória para Virgínia, que deve medir o estado e depois enviar o resultado da sua medição para Eva. Ressalta-se que Virgínia não conhece o estado quântico que está armazenado na memória quântica. Dessa maneira, Virgínia escolhe aleatoriamente uma base de medição β, realiza a medição, e obtém o resultado α. Realizada esta ação, Virgínia envia para Eva o par de valores (α, β). Ao receber estes valores, Eva confere se de fato a afirmativa condiz com a ação de Virgínia. Portanto, ela realiza a seguinte verificação:

1. Se $\beta \neq b$, então Eva descarta esse valor e assume que Virgínia está falando a verdade sem ter certeza disso;

2. Se $\beta = b$, então Eva verifica se $\alpha = a$. Caso realmente $\alpha = a$, então Eva tem a certeza de que Virgínia está falando a verdade. Caso contrário, Eva tem a certeza de que Virgínia está mentindo.

Nota-se que, nesse protocolo, o argumento de Virgínia é sempre aceito quando ela está falando a verdade. Por outro lado, quando Virgínia deseja mentir sobre a medição e o resultado que obteve, enviando o par $(\tilde{\alpha}, \tilde{\beta})$, ela sempre tem sucesso quando envia $\tilde{\beta} \neq \beta = b$, pois Eva não tem como verificar a sua afirmativa, então ela assume que Virgínia está falando a verdade. No entanto, quando Virgínia mente enviando $\tilde{\beta} = b \neq \beta$, então ela engana somente se ela envia $\tilde{\alpha} = a$. Mas se $b \neq \beta$, isso implica que o resultado da medição é completamente independente do valor a, ou seja, $\text{Pr}(\alpha = a) = 1/2$, implicando que a escolha de $\tilde{\alpha}$ é uma escolha totalmente independente de a, ou seja, $\text{Pr}(\tilde{\alpha} = a) = 1/2$. Portanto, quando Virgínia resolve mentir a respeito de sua medição, ela só conseguirá mentir com sucesso quando escolher $(\tilde{\alpha}, \tilde{\beta}) = (a, b)$, no que implica que

$$\text{Pr}[(\tilde{\alpha}, \tilde{\beta}) = (a, b)] = \text{Pr}[\tilde{\alpha} = a]\text{Pr}[\tilde{\beta} = b] = 1/4. \tag{4.1}$$

Seja E o algoritmo de verificação de Eva e $\text{Pr}(E(\alpha, \beta)_{aceita})$ a probabilidade de Eva aceitar o argumento de Virgínia, então esse simples algoritmo de verificação é um algoritmo probabilístico, satisfazendo as seguintes condições:

- Se Virgínia envia (α, β) para Eva, então $\text{Pr}(E(\alpha, \beta)_{aceita}) = 1$;
- Se Virgínia envia $(\tilde{\alpha}, \tilde{\beta}) \neq (\alpha, \beta)$ para Alice, então $\text{Pr}(E(\tilde{\alpha}, \tilde{\beta})_{aceita}) = \frac{3}{4}$.

Quanto ao fato de Eva aceitar entradas falsas, de forma mais precisa, percebe-se que

$$\begin{aligned} \text{Pr}(E(\tilde{\alpha}, \tilde{\beta})_{aceita}) &= \text{Pr}[(\tilde{\alpha}, \tilde{\beta}) = (a, b)] + \text{Pr}[\tilde{\beta} \neq b] \\ &= \frac{1}{4} + \frac{1}{2} = \frac{3}{4}. \end{aligned} \tag{4.2}$$

Neste trabalho é feita uma simplificação em que somente qubits armazenados em memória quântica são usados para impedir a simulação do verificador. Será descrito o protocolo entre Eva, o verificador e o provador, que será usado para obter a evidência da interação entre o provador e o verificador em um sistema de prova de conhecimento nulo. O seguinte protocolo descreve

um traço de interação entre o provador e o verificador que não pode ser falsificado, em que o provador conhece um isomorfismo entre os grafos G_0 e G_1 com n vértices.

Protocolo 6. (*Sistema de prova interativa de conhecimento nulo com possibilidade de transferência de prova*)

1. *Eva e o verificador concordam com uma função hash $h : \mathcal{G}_n \to \{0,1\}^n$, em que $\mathcal{G}_n$ é o conjunto de todos os grafos isomorfos com n vértices.*

2. *Eva escolhe, com distribuição de probabilidade uniforme, as matrizes A e B escritas como:*

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \text{ e } B = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix}. \tag{4.3}$$

   Assim, Eva armazena os seguintes estados na memória quântica:

$$\begin{matrix} |\psi_{b_{11}}^{a_{11}}\rangle & \cdots & |\psi_{b_{1n}}^{a_{1n}}\rangle \\ \vdots & \ddots & \vdots \\ |\psi_{b_{n1}}^{a_{n1}}\rangle & \cdots & |\psi_{b_{nn}}^{a_{nn}}\rangle \end{matrix} . \tag{4.4}$$

   Eva entrega a memória quântica com esses qubits armazenados para o verificador. Pode-se dizer, que essa máquina está selada para o verificador porque ele desconhece os estados internos da memória quântica. Agora, o verificador inicia a interação de prova de conhecimento nulo com o provador. Para cada interação com o provador, $k = 1, 2, \ldots, n$, o protocolo é executado da seguinte maneira:

   (a) ***P** gera um isomorfismo aleatório $\lambda_k : G_0 \to H_k$ e envia H_k para **V**.*

   (b) ***V** recebe o grafo H_k enviado por **P**, computa n bits usando a função hash, $h(H_k) = (h_{k1}, h_{k2}, \ldots, h_{kn})$, e realiza medições com a sequência obtida (h_{kl} é a base de medição do qubit $|\psi_{b_{kl}}^{a_{kl}}\rangle$) para obter a seqüência de observações na medição $o_k = (o_{k1}, o_{k2}, \ldots, o_{kn})$, com $o_{kl} \in \{0,1\}$ e $l = 1, 2, \ldots, n$. Depois, **V** computa a paridade $p_k = \bigoplus_{l=1}^{n} o_{kl}$ e envia $p_k \in \{0,1\}$ para **P**.*

   (c) ***P** recebe p_k enviado por **V** e envia o isomorfismo $\xi_k = \lambda_k \circ \sigma^{p_k}$;*

   (d) ***V** recebe o isomorfismo enviado por **P** e checa se $(G_(p_k)) = H_k$.*

   *Quando a interação entre **V** e **P** finaliza, então **V** envia os resultados a partir do que foi medido da memória quântica junto com o traço de interação $\omega = (H_1, \xi_1, o_1) \ldots (H_n, \xi_n, o_n)$.*

3. *Para $k = 1, \ldots, n$, Eva checa se $\xi_k(G_{p_k}) = H_k$ e computa $h(H_k) = (h_{k1}, h_{k2}, \ldots, h_{kn})$. Para cada iteração, $l = 1, \ldots, n$, Eva fará como segue:*

   (a) *Caso $h_{kl} \oplus b_{kl} = 1$, Eva descarta b_{kl} e a_{kl} e assume que o verificador falou a verdade a respeito desta medição;*

   (b) *Caso $h_{kl} \oplus b_{kl} = 0$, então Eva checa se $o_{kl} = a_{kl}$. Se verdade, então Eva aceita o_{kl} e h_{kl} como prova e logo depois incrementa k, pois ela tem certeza de que o verificador falou a verdade a respeito desta medição. Caso contrário, ela rejeita a prova, pois ela tem certeza que o verificador está mentindo.*

   Se nunca houver rejeição no Passo 3, Eva obtém uma evidência da interação entre o verificador e o provador.

O Protocolo 6 traça a interação entre o verificador e o provador no sistema de prova interativa de conhecimento nulo com isomorfismo de grafo. Para mostrar que o ataque realmente quebra o anonimato do provador após a interação, vamos assumir que ***V*** deseja convencer Eva que ele realmente interagiu com ***P*** sem que isto tenha acontecido. Então, o objetivo do verificador é enviar a seqüência $\omega = (H_1, \xi_1, o_1) \ldots (H_n, \xi_n, o_n)$ para persuadir Eva de que a seqüência é um traço real de interação com o provador. Assim, com distribuição de probabilidade uniforme, o simulador escolhe aleatoriamente $c_k \in \{0, 1\}$ e gera um isomorfismo aleatório $\xi_k(G_{c_k}) = H_k$. ***V*** calcula $h(H_k) \in \{0, 1\}^n$ e usa seus bits para escolher as bases de medição, cujo resultados formam a seqüência de bits $o_k \in \{0, 1\}^n$. Logo depois, ele calcula a paridade de $p_k = \oplus_{m=1}^{n} o_{km}$ e compara com c_k. Se eles são iguais, ***V*** envia (H_k, ξ_k, o_k) para Eva. Neste caso, que ocorre em metade dos grafos porque a probabilidade de $p_k = c_k$ é $1/2$, a simulação foi computada com sucesso. Por outro lado, para outra metade dos casos em que $p_k \neq c_k$, ***V*** pode pegar uma colisão de H'_k, tal que $h(H'_k) = h(H_k)$, calcula ξ'_k de forma que $\xi'_k(G_{c_k}) = H'_k$ e envia (H'_k, ξ'_k, o_k) para Eva. Apesar da probabilidade de encontrar colisões para função h ser negligenciável quando executado em tempo polinomial, pois o hash é uma função difícil de inverter, ainda assim, será assumido que a imagem de h de cada grafo testado difere apenas de um bit do grafo original em testes em tempo eficiente.

O Passo 3 computado por Eva será denotado por $S_3(\cdot)$. De forma similar ao que foi descrito no protocolo em que Virgínia envia o resultado da medição de um estado quântico, quando o verificador envia $(h(H'_k), o'_k) \neq (h(H_k), o_k)$ para Eva, então

$$\text{Prob}(S_3(h(H'_k), o'_k)_{aceita}) = 3/4. \tag{4.5}$$

Em outras palavras, a probabilidade de Eva aceitar a entrada $(h(H'_k), o'_k)$ como prova de intera-

ção é $3/4$, quando somente um bit é modificado na saída da função hash.

4.2.1 Um outro protocolo para quebra da impossibilidade de transferência de prova de conhecimento nulo

O segundo protocolo, apresentado em [10, 21], mais complexo do que o protocolo anterior, também transfere o traço de interação entre o provador e o verificador. Nesse protocolo, o traço de interação entre o provador e o verificador é construído sem o uso de uma função hash. Os cálculos das probabilidades de sucesso para cada ação do verificador na tentativa de simulação do verificador encontram-se no Capítulo 2.

No lugar da função hash é usada uma função bijetiva $f(G) = g(n)$, que mapeia todo grafo $G \in \mathcal{G}_n$ numa sequência de $g(n)$ bits (função de fácil inversão). Primeiramente, Eva compartilha com ***V*** um conjunto com $ng(n)/3$ pares de Bell $(|00\rangle_{VE} + |11\rangle_{VE})/\sqrt{2}$ e envia $ng(n)/3$ estados quânticos $\{|\theta_1\rangle, \ldots |\theta_{ng(n)}\rangle\}$ para o verificador, sendo que $|\theta_i\rangle$ pertence a $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ para $i = 1, 2, \ldots, ng(n)$. O novo ataque quântico para o sistema de transferência de prova de conhecimento nulo é realizado como descrito a seguir:

Protocolo 7. *Protocolo para impedir a simulação do verificador em sistemas de prova interativa de conhecimento nulo. Esse protocolo não faz uso da função hash, portanto a dificuldade de inversão de uma função de sentido único não é fator de segurança. Os seguintes passo são executados n vezes:*

1. ***P** gera um isomorfismo aleatório $\lambda : G_0 \to H$ e envia H a **V**;*
2. ***V** calcula $f(H)$ que define uma transformação unitária sobre os qubits $|\theta_1\rangle, \ldots, |\theta_{g(n)/3}\rangle$ enviados por Eva, depois introduz o resultado $|\phi_1\rangle, \ldots, |\phi_{g(n)/3}\rangle$ no circuito de teleportação (utilizando $g(n)/3$ qubits da parte que lhe pertence nos pares de Bell) e mede os estados que lhe pertencem na operação de teleportação, obtendo assim os pares de seqüência de bits $D = (a_1, b_1), ..., (a_{g(n)/3}, b_{g(n)/3})$, em que a_i e b_i são os bits resultantes da teleportação de $|\phi_i\rangle$. O resultado da paridade de D, Par(D), é enviado a **P**, $c = \text{Par}(D) = a_1 \oplus b_1 \oplus \cdots \oplus a_{g(n)/3} \oplus b_{g(n)/3}$;*
3. ***P** envia o isomorfismo $\xi = \lambda \circ \sigma^c$ a **V**;*
4. ***V** checa se $\xi(G_c) = H$;*
5. *Os Passos de 1-4 são repetidos n vezes e é suposto que **V** realmente verificou que **P** tem o segredo. Depois disso, **V** envia para Eva todos os grafos H (na seguinte ordem*

*$H_1, \ldots, H_n$), todos os isomorfismos (na seguinte ordem $\xi_1, \ldots, \xi_n$) recebidos de **P** e todas as seqüências resultantes da sua medição na realização da teleportação (na seguinte ordem $D_1, \ldots, D_n$);*

6. *Recebendo a seqüência D_k, Eva completa a teleportação aplicando as correções. Para o k-ésimo H recebido, H_k para $k = 1, 2, \ldots, n$, Eva recupera os estados quânticos $|\theta_{1,k}\rangle, \ldots, |\theta_{g(n)/3,k}\rangle$ a partir dos qubits teleportados $|\phi_{1,k}\rangle, \ldots, |\phi_{g(n)/3,k}\rangle$, pois ela calcula $f(H)$ para obter a transformação unitária inversa. Por fim, conhecendo a base correta de medição para cada estado, Eva mede os seus qubits e sabe que ela deverá obter exatamente os valores correspondentes a seqüência de estados quânticos $|\theta_{1,k}\rangle, \ldots, |\theta_{g(n)/3,k}\rangle$. Se os resultados das medições dos estados são os resultados esperados e a relação $\xi_k(G_{c_k}) = H_k$ é satisfeita para $c_k = Par(D_k)$, isso para todos os n grafos H_k, então Eva acredita que **V** interagiu com **P**.*

O protocolo descrito anteriormente impossibilita a simulação do verificador se ele não é capaz de alterar os estados enviados para Eva. Para entendermos como isto vai funcionar neste protocolo, vamos assumir que o verificador quer convencer Eva de que interagiu com o provador sem que isto tenha de fato acontecido. Tendo em conta o procedimento de Eva, o verificador tem de enviar a ela uma seqüência de tuplas $(H_1, \xi_1, D_1), ..., (H_n, \xi_n, D_n)$. Consideramos que ***V*** não vai usar ataques de interceptação aos estados quânticos enviados por Eva, pois ele sabe que perturbará a informação e causará erros que serão facilmente percebidos por Eva. Então para a simulação de uma interação com o provador, o verificador executa os seguintes passos:

1. O verificador escolhe uma permutação ξ_k, com distribuição de probabilidade uniforme, e um bit c_k, também com distribuição de probabilidade uniforme, e calcula $\xi_k(G_{c_k}) = H_k$;

2. ***V*** calcula $f(H_k)$ que define uma transformação unitária sobre os qubits $|\theta_1\rangle, \ldots, |\theta_{g(n)/3}\rangle$ enviados por Eva, depois introduz os qubits resultantes $|\phi_1\rangle, \ldots, |\phi_{g(n)/3}\rangle$ no circuito de teleportação (utilizando $g(n)/3$ qubits da parte que lhe pertence nos pares de Bell) e mede os estados que lhe pertencem na operação de teleportação, obtendo assim os pares de seqüência de bits $D = (a_1, b_1), ..., (a_{g(n)/3}, b_{g(n)/3})$, em que a_i e b_i são os bits resultantes da teleportação de $|\phi_i\rangle$. O resultado da paridade de D, $c = \text{Par}(D) = a_1 \oplus b_1 \oplus \cdots \oplus a_{g(n)/3} \oplus b_{g(n)/3}$ é comparado com c_k:

   (a) Caso $c = c_k$, então a simulação foi feita com sucesso;

   (b) Caso $c \neq c_k$, então a simulação evolui para um resultado indesejável, como os estados que ele possuía já foram teleportados, ele não pode mais voltar para o Passo 1.

Então, nos casos em que a simulação evolui para $c \neq c_k$, ***V*** pode almejar enganar Eva substituindo todos os grafos H_k por H'_k, de forma que $f(H'_k)$ tenha apenas um bit diferente de $f(H_k)$, ou substituindo os vetores D_k, alterando apenas um bit. Então, para cada uma das respectivas tentativas citadas, temos:

1. O verificador muda um grafo H_k por H'_k. Devemos destacar que neste caso não há colisões. Portanto, o verificador deve trocar $f(H_k)$ por $f(H'_k)$, de forma que apenas um bit da imagem da função seja alterado. Ele pode fazer tal cálculo em tempo computacional viável, pois foi considerado que f é de fácil inversão. Como discutido na Subseção 2.1.1 os resultados da Tabela 2.2, existe uma probabilidade de 1/2 para cada grafo alterado para o verificador não ser flagrado trapaceando. Durante o protocolo inteiro, em média $n/2$ grafos deverão ser alterados. Portanto, a probabilidade de ***V*** não ser flagrado trapaceando durante todas as rodadas do protocolo é $1/2^{\frac{n}{2}}$;

2. O verificador altera o vetor D de forma que sua paridade se torne Par$(D) = c_k$. Para isto ele precisa mudar apenas um bit. Como, em média, ele terá que fazer isto em $n/2$ grafos, a probabilidade do verificador não ser flagrado trapaceando será de $1/2^{\frac{n}{2}}$. Pois ele acerta um palpite de uma transformação unitária irrelevante para a correção do qubit teleportado com probabilidade de 1/2 para cada qubit (veja 2.3.1).

Uma só das estratégias de trapaça usada na simulação de interação com o provador é o suficiente para ele cumprir o objetivo que deseja. Pois, a probabilidade de sucesso do verificador, em qualquer uma das estratégias, é $p_s = 1/2^{\frac{n}{2}}$, que é um valor negligenciável em n.

Deve-se ressaltar que a opção de não usar a função hash não implica que a sua presença torne o ataque menos eficiente. Tem sido provado que usando um computador quântico com o algoritmo de busca de Grover, é possível encontrar colisões da função hash com um limite superior $O(r^{\frac{1}{3}})$ [61] e um limite inferior de $O(r^{\frac{1}{5}})$ [62] sobre um número de tentativas necessárias. Embora o algoritmo de Grover permita essa redução na complexidade da busca de colisões, o tamanho do espaço de busca é exponencial. Portanto, o uso de funções hash para a quebra da propriedade de impossibilidade de transferência de prova não torna fraca a evidência de interação entre o provador e verificador.

4.3 Como vazar uma mensagem de forma anônima e depois resgatar a autoria

O problema tratado neste trabalho começa em um cenário de criptografia assimétrica, usando o conceito de funções *trapdoor*, em que cada usuário publica uma chave pública e guarda

em sigilo uma chave privada. Agora, imaginemos o seguinte cenário: Os membros de uma instituição $\mathcal{A}$ usam criprografia assimétrica para uma comunicação secreta entre eles na rede. Portanto, cada membro da instituição possui uma chave pública P_i que lhe permite cifrar em tempo polinomial qualquer string x_i, $g_{P_i}(x_i) = y_i$. O i-ésimo membro guarda em segredo uma chave secreta S_i, da qual, ele consegue calcular em tempo hábil o resultado inverso, $g_{S_i}(y_i) = x_i$.

Dentro desse cenário, vamos imaginar a seguinte situação: a Instituição $\mathcal{A}$ está em negociação com uma outra Instituição $\mathcal{B}$ para a assinatura de um acordo entre elas. Na negociação, as duas partes tomam a decisão de assinar um acordo dentro das próximas horas. Um conjunto de membros dentro da Instituição $\mathcal{A}$ tem acesso a dados internos que, vindo a público, impedem a assinatura do acordo e geram um conflito entre as duas partes no tribunal. Dentro da Instituição $\mathcal{A}$ existe um membro que deseja revelar uma informação secreta valiosa ao público (na internet) a respeito das transações da instituição. Ao revelar esta informação, o delator provoca um conflito entre as instituições $\mathcal{A}$ e $\mathcal{B}$, em que ele pode ser beneficiado ou penalizado. Dependendo de qual das partes vai vencer o conflito nos tribunais, o delator busca realizar uma assinatura que satisfaça os seguintes casos:

1. Se ele for descoberto como delator e a Instituição $\mathcal{A}$ ganhar o conflito no tribunal, ele será penalizado. Nesse caso, o interesse do membro da Instituição $\mathcal{A}$ é preservar o seu anonimato para não ser penalizado. Portanto, ninguém deve saber qual dos membros foi o delator, mas todo o público deve ter certeza de que a informação saiu de dentro da Instituição $\mathcal{A}$ para dar credibilidade à informação.

2. Se a instituição $\mathcal{B}$ ganhar o conflito, ele será beneficiado. Nesse caso, é interesse do delator que ele revele a sua identidade.

Para proteger-se da Instituição $\mathcal{A}$, o delator aplica o esquema de assinaturas em anel apresentado em [63]. O jornal de publicação dessa notícia precisa ter certeza de que essa informação veio de um membro da Instituição. Caso a Instituição $\mathcal{A}$ vença o conflito, o delator precisa ter certeza de que o seu anonimato será preservado, mesmo que o jornalista seja obrigado a revelar a fonte em um tribunal. Na abordagem proposta em [63], o informante envia a história ao jornalista assinada com um esquema de assinaturas em anel, em que o delator usa a assinatura de todos os membros da Instituição $\mathcal{A}$, de forma a ser computacionalmente indistinguível qual dos membros tenha produzido a assinatura. Embora a assinatura seja construída pelas funções públicas dos membros da Instituição $\mathcal{A}$, somente quem pode calcular a inversa é capaz de produzir a assinatura em anel. O jornalista pode verificar o anel de assinaturas na mensagem e saber que ela, definitivamente, veio de um membro da Instituição $\mathcal{A}$. Ele pode até mesmo postar a assinatura em anel em seu trabalho ou página da web, para provar aos seus leitores que a história

veio de uma fonte confiável. No entanto, nem ele, nem seus leitores podem determinar a verdadeira origem do vazamento, já que, o delator tem proteção perfeita, mesmo que o jornalista seja forçado mais tarde a revelar a sua "fonte" a um juiz.

No cenário desse protocolo também há uma entidade confiável que fornece partículas de pares de Bell. Para cada par, a entidade fornece uma partícula e guarda a outra em seu laboratório. Também ela não permite que qualquer usuário insira uma partícula em seu laboratório, ou seja, nenhum usuário pode ter acesso aos estados quânticos internos da entidade. Além disso, um estado quântico só é publicado quando existe uma solicitação do usuário para tal atitude. Assim, vamos considerar que a entidade compartilha $(r-1)b$ pares de Bell com o membro delator,

$$\left(\frac{|00\rangle_{E,T_s} + |11\rangle_{E,T_s}}{\sqrt{2}}\right)^{(r-1)b}. \tag{4.6}$$

Consideramos que o membro delator $T_s \in \{T_1, T_2, \ldots T_r\}$ é um dentre os r membros da Instituição $\mathcal{A}$. Assim, dada uma mensagem m, uma seqüência de chaves públicas P_1, P_2, ..., P_r (cada chave púbica P_i específica uma função de sentido único g_i), uma seqüência de chaves secretas S_1, S_2, ..., S_r (cada chave privada S_i específica a função inversa g_i^{-1}), então o delator, para causar a crise, gera uma assinatura que é calculada da seguinte forma:

Protocolo 8. *Cálculo da assinatura com anonimato controlado pelo assinante.*

1. *O assinante calcula um valor k que é o hash da mensagem m, $h(m) = k$ (h é uma função hash predeterminada). O valor de k é para selecionar uma função de encriptação E_k como em* [64]*;*

2. *O assinante escolhe aleatóriamente com distribuição de probabilidade uniforme um valor de inicialização $v \in \{0,1\}^b$;*

3. *O assinante tem v como um seqüencia de bases de medição para as partículas que estão em seu laboratório. Portanto, as medições são realizadas da seguinte maneira:*

   - *Para $i = 1, 2, \ldots, r-1$ faça:*
   - *Para $j = 1, 2, \ldots, b$ faça:*
     (a) *Se $v_j = 0$, então a medição é feita na base retangular, $\{|0\rangle, |1\rangle\}$. O resultado é atribuído em x_{ij};*
     (b) *Se $v_j = 1$ a medição é feita na base diagonal, $\{|+\rangle, |-\rangle\}$. O resultado é atribuído em x_{ij}.*

   Com distribuição de probabilidade uniforme, $r-1$ entradas x_i, $1 \leq i \leq r-1$ são obtidas nas medições, tal que $x_i \in \{0,1\}^b$. Assim o assinante delator computa $y_i = g_i(x_i)$;

4. *O delator soluciona a equação do anel para* y_s

$$C_{(k,v)}(y_1, y_2, y_3, ..., y_r) = v.$$

O assinante T_s *é capaz de resolver a equação em tempo hábil se ele for capaz de calcular* $g_s^{-1}(y_s) = x_s$*. Ele só é capaz desse feito se possuir a chave secreta* S_s*.*

5. *A mensagem* m *é assinada com a tupla (*$P_1, ..., P_r$*;* v*;* $x_1, ..., x_r$*).*

A assinatura pode ser verificada para dois diferentes casos. No primeiro caso, a verificação é feita de forma pública em que o delator permanece como autor anônimo da mensagem. No segundo caso, ele pode sair do anonimato apresentando uma prova que está correlacionada com a assinatura, de forma que qualquer pessoa fique convencida de que a assinatura foi gerada por ele.

Protocolo 9. *Verificação da validade da assinatura* $(P_1, ..., P_r; v; x_1, ..., x_r)$.

1. *Para* $i = 1, 2, \ldots, r$ *o verificador calcula* $g_i(x_i)$*;*
2. *O verificador calcula o* $h(m) = k$ *para obter* E_k*;*
3. *O verificador checa se todo* $g_i(x_i)$ *satisfaz* $C_{(k,v)}\left(g_1(x_1), \ldots, g_r(x_r)\right) = v$
4. *Finalmente, se o grupo* $\mathcal{A}$ *vencer o o conflito,* T_s *não se manifesta. Caso contrário, quando o grupo* $\mathcal{B}$ *vence o conflito, então ele afirma ter* $b(r-1)$ *partículas de pares de Bell na entidade confiável e autoriza esta a realizar medições como descritas por ele (as medições seguem a mesma ordem que foi apresentada no protocolo da geração da assinatura em anel). Assim, todos vêm que a assinatura (*$P_1, ..., P_r$*;*v*;* $x_1, ..., x_r$*) foi calculada a partir destes resultados.*

O delator pode proteger-se da punição do grupo pela segurança do anonimato apresentada em [63]. A assinatura é facilmente conferida calculando a função $C_{(k,v)}(g_1(x_1), ..., g_r(x_r)) = v$. Percebe-se que a legitimidade da assinatura está assegurada pela capacidade que qualquer um dos membros da instituição $\mathcal{A}$ tem de inverter a função de sentido único. Embora os valores $y_1, ..., y_r$ sejam facilmente calculados por qualquer usuário, a equação $C_{(k,v)}$ (y_1, y_2, y_3, ..., y_r)=v só é facilmente resolvida, se ao menos uma inversão puder ser facilmente computável, $g_s^{-1}(y_s) = x_s$. Em [63] é definida uma equação que pega como entrada uma chave k, um valor de inicialização v e valores arbitrários y_1, ...,y_r em $\{0,1\}^b$. Esse algoritmo usa como subrotina E_k e produz uma saída $z \in \{0,1\}^b$, tal que, dada qualquer entrada fixada k e v, as seguintes propriedades são satisfeitas:

1. **Permutação em cada entrada** - Para cada $s \in \{1, \ldots, r\}$ e para quaisquer valores fixados de todas as entradas y_i, $i \neq s$, a função $C_{k,v}(y_1, \ldots, y_r) = z$ é um mapeamento de y_s para z;

2. **A equação é eficientemente solúvel** - Para cada $i \in \{1, \ldots, r\}$, dada uma entrada z de b bits para toda entrada y_i, é possível encontrar eficientemente uma entrada y_i de b bits tal que $C_{k,v}(y_1, \ldots, y_r) = z$;

3. **Impraticável verificar a solução da equação por entradas de funções de sentido único** - Dado k, v e z é impraticável para um adversário solucionar a equação

$$C_{(k,v)}(g_1(x_1), g_2(x_2), ..., g_r(x_r)) = z$$

para y_1, y_2, ...,y_r (dado acesso para cada g_i e E_k) se o adversário não pode inverter qualquer das funções de sentido único $g_1, g_2, \ldots, g_r$.

Os autores resolveram aplicar uma permutação pseudo-aleatória após cada operação XOR. Na proposta [63], $C_{(k,v)}$ é calculada usando funções de encriptação simétrica, E_k (a função E_k é uma função de permutação pseudo-aleatória sobre $\{0,1\}^b$). Portanto $C_{(k,v)}$ é definida por

$$\begin{aligned} C_{(k,v)}(y_1, ..., y_r) &= E_k(y_r \oplus E_k(y_{(r-1)} \oplus E_k(y_{(r-2)} \\ &\oplus E_k(... \oplus E_k(y_1 \oplus v)...))). \end{aligned} \tag{4.7}$$

Essa função é aplicada para a sequência (y_1, y_2, ..., y_r), em que $y_i = g_i(x_i)$, como mostrado

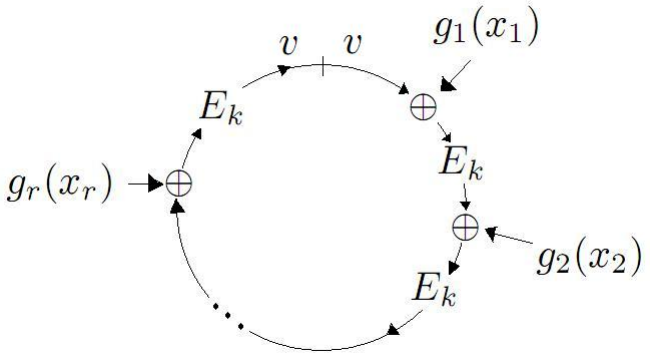

Figura 4.1: Assinatura em anel

na Fig. 4.1. Essa equação é claramente uma permutação sobre cada entrada após uma operação XOR. Além disso, ela é eficientemente resolvida para qualquer entrada dado o conhecimento

de k, o que torna possível executar o cálculo à frente a partir de um valor inicial v e para trás a partir do final z, excepcionalmente, a fim de calcular qualquer valor em falta de y_i. Essa função pode ser usada para verificar assinaturas usando uma função hash do m para a escolha de uma chave simétrica k, e forçar a saída z a ser igual à entrada v. A prova para a primeira condição do protocolo é a prova apresentada em [63].

Agora, vamos tratar do caso em que o grupo B sai vitorioso e o assessor quer provar a autoria da mensagem. Primeiro, devemos mencionar que, nesse momento, todos os assessores estão interessados em receber a recompensa do grupo B. Também, todos eles são capazes de afirmar que as suas chaves podem produzir essa assinatura. Mas, quando T_s afirma haver partículas quânticas na entidade confiável, medidas na base v fornecem os dados da assinatura. Assim, apenas com probabilidade $1/2^{b(r-1)}$, qualquer outro dos membros pode gerar a mesma assinatura, sendo essa probabilidade um valor negligenciável no tamanho da assinatura. O dispositivo à prova de falsificação proíbe a simulação dos outros assessores em gerar a mesma assinatura.

Deve ser ressaltado, que o esquema de assinatura em anel que usa funções *trapdoor* do tipo RSA e Rabin perde a sua validade diante de computadores quânticos que executem o algoritmo de Shor, [15]. Pois, com esses computadores, qualquer um que conheça a chave pública é capaz de produzir a assinatura. Portanto, o argumento de que a informação veio de dentro da Instituição $\mathcal{A}$ perde a sua validade. No entanto, a propriedade de resgate da autoria, continua válida, independente da existência do algoritmo de Shor. Mas para isso é necessário que uma função trapdoor exista independente da fatoração de números inteiros e da inversão do logaritmo discreto. Em sistemas de criptografia clássica, as únicas propostas válidas de funções trapdoor são os esquemas de encriptação RSA e o método de Rabin, pois as outras propostas falharam ao longo dos anos. No entanto, esquemas de funções trapdoor quânticas têm surgido [65–67]. Em [65], um esquema de função trapdoor quântica é construído a partir do problema de automorfismo de grafos. Encontrar um automorfismo de grafos não trivial para um conjunto de grafos é um problema $\mathcal{NP}$-completo. Este trabalho mostra que, se um computador quântico é capaz de decifrar em tempo polinomial uma mensagem cifrada por este esquema de assinatura, sem possuir a chave secreta, então o computador quântico resolverá em tempo polinomial os problemas da classe $\mathcal{NP}$. Para este esquema de assinaturas, fica como proposta futura, a construção de um anel de assinatura usando funções trapdoor quânticas.

4.3.1 Anel de assinatura quântica anônima em que apenas um delator assina

Nesse problema, deve-se considerar uma Instituição que contém um grupo de membros que mantém relações com uma autoridade dentro da instituição, a quem chamamos de $\mathcal{B}$ (o chefe). Todos eles se comunicam através de teleportação de um para o outro de qualquer lugar em que estejam. Considera-se que todo membro $A_i \in \{A_1, A_2, \ldots, A_r\}$ compartilha o estado quântico

$$\left(\frac{|00\rangle_{A_i\ A_{i+1}} + |11\rangle_{A_i\ A_{i+1}}}{\sqrt{2}}\right)^{\otimes n}$$

com o membro A_{i+1}. O mesmo compartilhamento de estados quânticos é feito entre a autoridade $\mathcal{B}$ e o membro A_1, e entre o membro A_r e a autoridade $\mathcal{B}$. Ressalta-se que a comunicação clássica requerida na teleportação é segura, ou seja, a comunicação é pública e devidamente autenticada entre os usuários da teleportação.

Agora é importante considerar a seguinte situação: o chefe está sempre interessado que os membros vigiem uns aos outros, portanto, ele sempre busca alguma informação de irregularidade a respeito dos membros. No entanto, ele sabe que os membros trabalham sempre cooperando uns com os outros e um delator que faça qualquer denúncia de irregularidade a respeito de um dos membros pode perder a cooperação dos demais. Então, $\mathcal{B}$ deve prover um método de denúncia que mantenha o anonimato do delator. Para construir tal sistema de denúncia, $\mathcal{B}$ sempre passa um estado quântico que dever ser repassado para todos os membros da instituição, $\{A_1, A_2, \ldots, A_r\}$. É importante considerar esse estado quântico como uma folha em branco em que qualquer membro pode assinar para fazer uma denúncia a respeito de um outro membro da mesma Instituição. Então, quando o membro A_s sabe um segredo a respeito de um outro membro A_y, ele aproveita esse momento para denunciá-lo. O membro A_y acredita que nenhum outro membro sabe da sua atitude irregular e ele não imagina que alguém possa fazer tal denúncia. Dentro desse cenário, o método de denúncia provido por $\mathcal{B}$ é executado da seguinte maneira:

Protocolo 10. *Assinatura privada em anel usando estados quânticos*

1. *Inicialmente $\mathcal{B}$ prepara aleatoriamente um estado quântico $|\psi_b^a\rangle = \bigotimes_{k=1}^{n} |\psi_{b_k}^{a_k}\rangle$, lembrando que $|\psi_{b_k}^{a_k}\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$;*

2. *O estado quântico $|\psi_b^a\rangle$ é teleportado para o membro A_1, depois A_1 teleporta-o para A_2, e assim sucessivamente, até que A_r teleporta este estado para $\mathcal{B}$;*

3. *O membro A_s que conhece uma informação secreta a respeito de um outro membro, do qual ninguém sabe que ele sabe desta informação, resolve fazer uma denúncia para $\mathcal{B}$.*

Assim, ele aplica a transformação unitária $U_x = \bigotimes_{k=1}^{n}(ZX)^{x_k}$ no estado quântico recebido e teleporta para o membro A_{s+1} o estado $|\psi_b^{a\oplus x}\rangle = \bigotimes_{k=1}^{n}|\psi_{b_k}^{a_k\oplus x_k}\rangle$;

4. *Quando o estado chegar no usuário $\mathcal{B}$, ele mede o estado que foi teleportado a ele, obtendo o resultado $a \oplus x$ na medição. Assim, ele aplica $a \oplus a \oplus x$ pra extrair a string x.*

5. *Mais tarde, ele recebe a denúncia publicamente assinada por $m, h_x(m)$. Em que m é a mensagem que faz a denúncia e $h_x(\cdot)$ é uma função hash universal escolhida de dentro de uma família de funções hash com 2^n funções.*

Antes de explicarmos o protocolo, devemos justificar porque

$$\bigotimes_{k=1}^{n}(ZX)^{x_k}|\psi_b^a\rangle = |\psi_b^{a\oplus x}\rangle.$$

Sem perda de generalidade, considera-se o caso de $n = 1$. Por conseguinte, temos $x \in \{0, 1\}$. operação X inverte o valor lógico dos qubits $|0\rangle$ e $|1\rangle$, desta maneira $X|\psi_0^y\rangle$, em que $y \in \{0, 1\}$, resulta no estado $|\psi_0^{y\oplus 1}\rangle$. No entanto, a operação X nada de efetivo faz sobre os qubits da base diagonal, ou seja, $X|\psi_1^y\rangle$ resulta no estado quântico $(-1)^y|\psi_1^y\rangle$. Considerando que a fase global não afeta a medição, ela será desconsiderada a partir de agora. De forma análoga, a transformação Z só é relevante para a mudança do valor lógico dos qubits da base diagonal. Portanto, quando o produto XZ é aplicado no estado $|\psi_t^y\rangle$ temos $|\psi_t^{y\oplus 1}\rangle$ para todo $t \in \{0, 1\}$. Finalmente, consideramos que $(XZ)^0 = I$. Portanto, $(XZ)^x|\psi_t^y\rangle = |\psi_t^{y\oplus x}\rangle$. Maiores detalhes destas operações em estados quânticos podem ser encontrados no Apêndice 2, na Seção 2.1.1.

A primeira questão sobre o Protocolo 10 que devemos investigar é: A denúncia é completamente anônima? O estado quântico é desconhecido de todos os membros da instituição, portanto, se um deles resolver medir o estado, não poderá reconstruí-lo para que a informação possa ser lida mais tarde. Assim, o usuário que resolver medir o estado quântico invalida totalmente o esquema de assinaturas, impossibilitando $\mathcal{B}$ de ler qualquer mensagem autenticada. Portanto, aquele que assina a mensagem tem a sua identidade preservada porque somente $\mathcal{B}$ pode ler o que foi escrito sem saber qual dos membros escreveram a assinatura.

Devemos destacar que o esquema está restrito apenas a um delator. Pois somente quem conhece a denúncia, como pressuposto inicialmente, gera a assinatura mantendo-se anônimo, de forma que, todos os membros são suspeitos de terem assinado esta mensagem.

Para resgatar a autoria da assinatura, o delator simplesmente revela x a $\mathcal{B}$, pois este dado não é público e somente quem gerou a assinatura pode fornecer esta informação.

Capítulo 5

Conclusão

Neste trabalho foram discutidos protocolos quânticos aplicado a sistema de prova de conhecimento nulo. No Capítulo 3 foi aplicado um protocolo quântico de compromisso de informação para a construção de um sistema de prova de conhecimento nulo para toda linguagem $\mathcal{NP}$. Como perspectiva futura fica o desenvolvimento da prova de segurança do protocolo quântico de compromisso de informação usando estados coerentes da luz.

No Capítulo 4 foi discutido o uso de um dispositivo quântico a prova de falsificação para impedir a simulação de protocolos clássicos. Em primeira proposta, foi discutido o uso de uma memória quântica, sem estados entrelaçados, para a transferência de prova de interação em sistema de prova de conhecimento nulo. Depois foi apresentado um protocolo que realiza a mesma transferência de prova, mas sem o uso de uma função hash. Ambos protocolos quebram o anonimato do provador em um sistema de prova de conhecimento como afirmado em [20]. Depois foi apresentada uma maneira para quebrar o anonimato de um assinante num esquema de assinatura em anel. Basicamente, o usuário que pertence a um conjunto de usuários que usam funções trapdoors para comunicação secreta é capaz de gerar uma assinatura em anel usando estados de Bell para provar a origem da assinatura. Assim, ele pode escolher em permanecer, ou não, anônimo. Como futuras propostas de investigação são sugeridas:

- A elaboração de esquemas de assinatura em anel usando funções trapdoor quânticas;
- Descoberta de outros protocolos clássicos para sugestões de aplicações de dispositivos quânticos a prova de falsificação, construindo de novas propriedades de segurança ou elaborando novos ataques.

Referências Bibliográficas

[1] C. E. Shannon. Communication theory of secrecy systems. *Bell Systems Technical Journal*, 28:656–715, 1949.

[2] W. Diffie and M. E. Hellman. New directions in cryptography, 1976.

[3] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978.

[4] S. Goldwasser and S. Micali. Probabilistic encryption & how to play mental poker keeping secret all partial information. In *STOC '82: Proceedings of the fourteenth annual ACM symposium on Theory of computing*, pages 365–377, New York, NY, USA, 1982. ACM.

[5] A. C. Yao. Theory and application of trapdoor functions. In *SFCS '82: Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*, pages 80–91, Washington, DC, USA, 1982. IEEE Computer Society.

[6] M. Blum and S. Goldwasser. An efficient probabilistic public key encryption scheme which hides all partial information. In *Proceedings of CRYPTO 84 on Advances in cryptology*, pages 289–302, New York, NY, USA, 1985. Springer-Verlag New York, Inc.

[7] S. Micali, C. Rackoff, and B. Sloan. The notion of security for probabilistic cryptosystems. In *Proceedings on Advances in cryptology—CRYPTO '86*, pages 381–392, London, UK, 1987. Springer-Verlag.

[8] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof-systems. In *STOC '85: Proceedings of the seventeenth annual ACM symposium on Theory of computing*, pages 291–304, New York, NY, USA, 1985. ACM.

[9] O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield nothing but their validity or all languages in np have zero-knowledge proof systems. *J. ACM*, 38(3):690–728, 1991.

[10] J. C. do Nascimento and R. V. Ramos. Quantum protocols for zero-knowledge systems. *Quantum Information Processing*, 2009.

[11] Stephen W. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983.

[12] Hoi-Kwong Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283(5410):2050 – 2056, 1999.

[13] C. H. Bennett and G. Brassard. Quantum cryptography: Public-key distribution and coin tossing. *Advances in Cryptology: Proceedings of Crypto 84*, pages 475 – 480, 1984.

[14] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68(21):3121–3124, 1992.

[15] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[16] J. Watrous. Zero-knowledge against quantum attacks. In *STOC '06: Proceedings of the thirty-eighth annual ACM symposium on Theory of computing*, pages 296–305, New York, NY, USA, 2006. Association for Computing Machinery.

[17] J. Watrous. Limits on the power of quantum statistical zero-knowledge. In *In Proceedings of the 43rd Annual Symposium on Foundations of Computer Science*, pages 459–468. IEEE Computer Society, 2002.

[18] H. Kobayashi. General properties of quantum zero-knowledge proofs. In *Theory of Cryptography*, volume 4948. Springer Berlin / Heidelberg, 2008.

[19] P. Mateus, F. Moura, and J. Rasga. Transfering proofs of zero-knowledge systems with quantum correlations. *First International Conference on Quantum, Nano, and Micro Technologies*, 0:9, 2007.

[20] J. Bouda, P. Mateus, N. Paunkovic, and J. Rasga. On the power of quantum tamper-proof device. *International Journal of Quantum Information*, 6:281 – 302, 2008.

[21] J. C. do Nascimento and R. V. Ramos. Quantum protocols for transference of proof of zero-knowledge systems. In *Anais do SBrT 2007*, 2007.

[22] J. C. do Nascimento and R. V. Ramos. Ataque quântico a sistemas de transferência de prova de conhecimento nulo. In *2° Workshop-Escola de Computação e Informação Quântica*, 2007.

[23] P. R. M. Contador. *Matemática: uma breve história*, volume II. Livraria da Física, 2008.

[24] G. Cardano. *Artis Magnæ Sive de Regulis Algebraicis*. 1545.

[25] R. Cramer, R. Gennaro, and B. Schoenmakers. A secure and optimally efficient multi-authority election scheme. In *Advances in Cryptology - EUROCRYPT'97*, pages 103–118. Springer-Verlag, 1997.

[26] J. D. Cohen and M. J. Fischer. A robust and verifiable cryptographically secure election scheme. In *SFCS '85: Proceedings of the 26th Annual Symposium on Foundations of Computer Science*, pages 372–382, Washington, DC, USA, 1985. IEEE Computer Society.

[27] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. *Advances in Cryptology - CRYPTO'86*, 163:186–197, 1987.

[28] D. Chaum, A. Fiat, and M. Naor. Untraceable electronic cash. In *CRYPTO '88: Proceedings on Advances in cryptology*, pages 319–327, New York, NY, USA, 1990. Springer-Verlag New York, Inc.

[29] A. M. Turing. On computable numbers: With an application to the entscheidungsproblem. In *Proceedings of the London Mathematical Society*, pages 230–265. Mathematical Society, 1936.

[30] A. Cobham. The intrinsic computational difficulty of functions. In *Procedings of the 1964 International Congress for Logic. Methodology, and Philosophy of Science*, pages 24–30. Elsevier, 1964.

[31] J. Edmonds. Minimum partition of a matroid into independent subsets. In *J. Res. Nat. Bur. Standard Sect. B*, volume 69, pages 67–72, 1965.

[32] J. von Neumann. *A certain zero-sum two-person game equivalent to the optimal assignment problem*, volume II. Princenton University Press, 1953.

[33] S. A. Cook. The complexity of theorem-proving procedures. In *STOC '71: Proceedings of the third annual ACM symposium on Theory of computing*, pages 151–158, New York, NY, USA, 1971. ACM.

[34] L. A. Levin. Universal sequential search problems. *Jour Probl. Peredachi Inf.*, 9:115–116, 1973.

[35] H. Chernoff. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *Annals of Mathematical Statistics*, 23:493–509, 1952.

[36] O. Goldreich. *Foundations of Cryptography: Basic Tools*, volume 1. Cambridge University Press, 2001.

[37] S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Science*, 28:270–299, 1984.

[38] J. Torán, A. Theoretische Informatik, and O. Eselsberg. On the hardness of graph isomorphism. In *SIAM J. Comput*, pages 180–186. Society Press, 2000.

[39] M. Blum. Coin flipping by telephone a protocol for solving impossible problems. *SIGACT News*, 15(1):23–27, 1983.

[40] M. Naor. Bit commitment using pseudo-randomness. In *Advances in Cryptology - CRYPTO'89 Proceedings*, number 128-136, 1990.

[41] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47(10):777–780, 1935.

[42] G Brassard, C Crepeau, R Jozsa, and D Langlois. A quantum bit commitment scheme provably unbreakable by both parties. Technical report, Bristol, UK, UK, 1993.

[43] Hoi-Kwong Lo and H. F. Chau. Is quantum bit commitment really possible? *Phys. Rev. Lett.*, 78(17):3410–3413, 1997.

[44] Hoi-Kwong Lo and H. F. Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. In *PhysComp96: Proceedings of the fourth workshop on Physics and computation*, pages 177–187, Amsterdam, The Netherlands, The Netherlands, 1998. Elsevier Science Publishers B. V.

[45] D. Mayers. The trouble with quantum bit commitment, 1996.

[46] G. Brassard, Crepeau C, D. Mayers, and L. Salvail. A brief review on the impossibility of quantum bit commitment. 1997.

[47] D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.*, 78(17):3414–3417, 1997.

[48] A. Kitaev, D. Mayers, and J. Preskill. Superselection rules and quantum protocols. *Phys. Rev. A*, 69(5):052326, 2004.

[49] R. W. Spekkens and T. Rudolph. Degrees of concealment and bindingness in quantum bit commitment protocols. *Phys. Rev. A*, 65(1):012310, 2001.

[50] H. P. Yuen. Unconditionally secure quantum bit commitment is possible, 2000.

[51] H. P. Yuen. How to build unconditionally secure quantum bit commitment protocols, 2003.

[52] G. M. D'Ariano. The quantum bit commitment: a finite open system approach for a complete classification of protocols, 2002.

[53] G. M. D'Ariano. The quantum bit commitment: a complete classification of protocols, 2002.

[54] G. M. D'Ariano, D. Kretschmann, D. Schlingemann, and Reinhard F. Werner. Reexamination of quantum bit commitment: The possible and the impossible. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 76(3):032328, 2007.

[55] A. Kerckhoffs. La cryptographie militaire. *Journal des sciences militaires*, IX:5–83, 1883.

[56] C. Crepéau. Quantum oblivious transfer. *Journal of Modern Optics*, 41:2445–2454, 1994.

[57] F. A. Mendonca and R. V. Ramos. Quantum bit commitment protocol without quantum memory. *Arquivo interno do DETI-UFC*, 2008.

[58] F. A. Mendonça and R. V. Ramos. Quantum bit string commitment protocol using polarization of mesoscopic coherent states. *Physics Letters A*, 372 (8):1190–1193, 2008.

[59] M. Sedlák, M. Ziman, O. Přibyla, V. Bužek, and M. Hillery. Unambiguous identification of coherent states: Searching a quantum database. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 76(2):022326, 2007.

[60] C. Moore and J. P. C. Eld. Quantum automata and quantum grammars. *Theoretical Computer Science*, 237:2000, 2000.

[61] Gilles Brassard, Peter Høyer, and Alain Tapp. Quantum cryptanalysis of hash and claw-free functions. *SIGACT News*, 28(2):14–19, 1997.

[62] Scott Aaronson. Quantum lower bound for the collision problem. In *STOC '02: Proceedings of the thiry-fourth annual ACM symposium on Theory of computing*, pages 635–642, New York, NY, USA, 2002. ACM.

[63] R. L. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. *Communications of the ACM*, 22(22):612–613, 2001.

[64] M. Luby and C. Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM J. Comput.*, 17(2):373–386, 1988.

[65] A. Kawachi, T. Koshiba, and T. Yamakami H. Nishimura. A quantum trapdoor one-way function that relies on the hardness of the graph automorphism problem. In *Quantum Information Science Workshop*, pages 115–116, 2003.

[66] G. M. Nikolopoulos. Applications of single-qubit rotations in quantum public-key cryptography. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 77(3):032348, 2008.

[67] T. Okamoto, K. Tanaka, and S. Uchiyama. Quantum public-key cryptosystems. In *CRYPTO '00: Proceedings of the 20th Annual International Cryptology Conference on Advances in Cryptology*, pages 147–165, London, UK, 2000. Springer-Verlag.

Trabalhos Publicados Pelo Autor

1. José Cláudio do Nascimento, Rubens Viana Ramos. “Quantum protocols for transference of proof of zero-knowledge systems. ”. *Anais do XXV Simpósio Brasileiro de Telecomunicações* (SBrT 2007), Recife, Pernambuco, Brasil, Setembro 2007.

2. José Cláudio do Nascimento, Rubens Viana Ramos. “Ataque quântico a sistemas de transferência de prova de conhecimento nulo”. *Anais do 2º Workshop-Escola de Computação e Informação Quântica* (WECIQ’2007), Campina Grande, Paraíba, Brasil, pg. 158-163, Outubro 2007.

3. José Cláudio do Nascimento, Rubens Viana Ramos. “Quantum protocols for zero-knowledge systems”. *Quantum information processing*, Agosto 2009.

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo