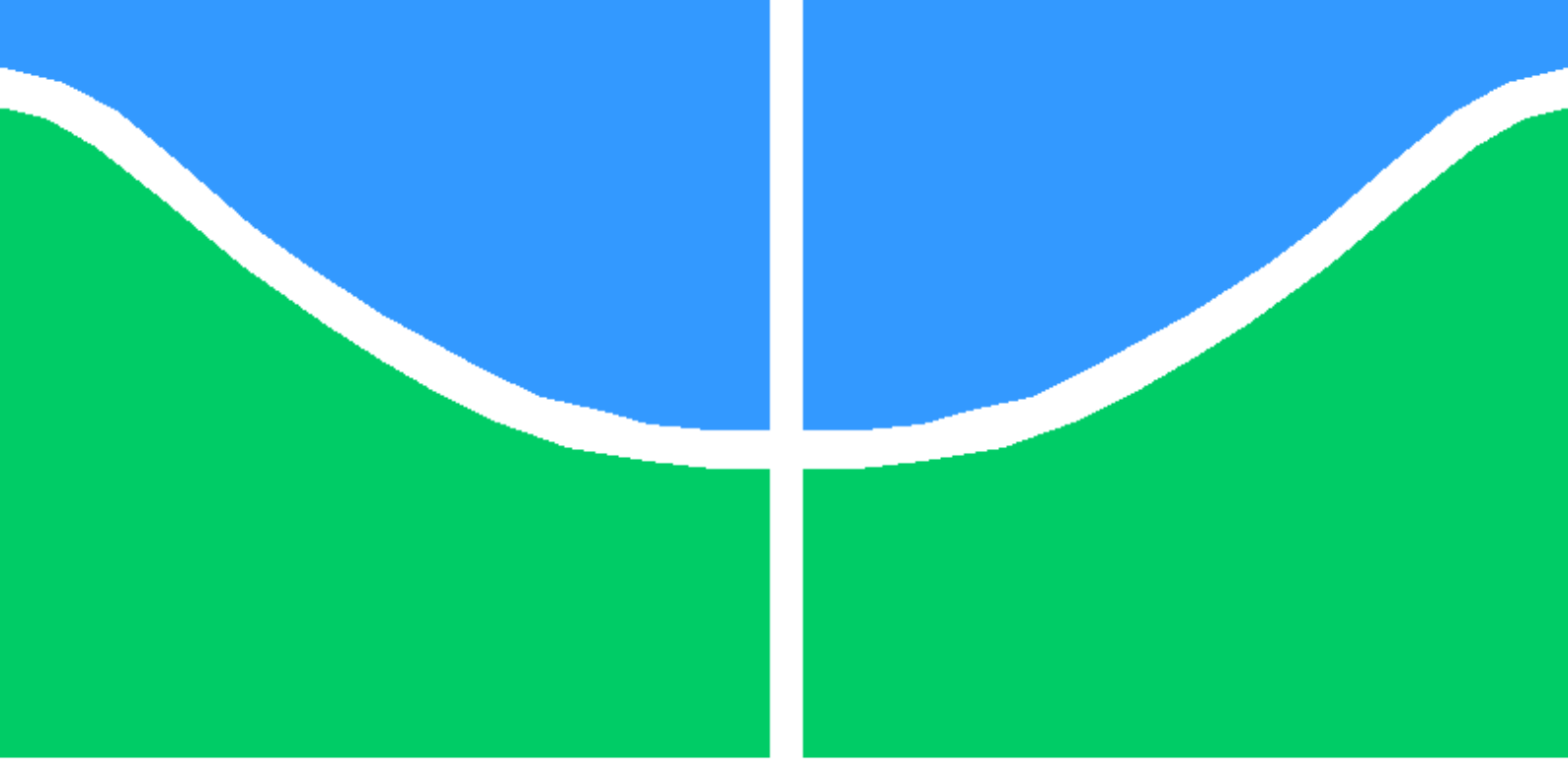

DISSERTAÇÃO DE MESTRADO

PROTOCOLO DE COMPROMETIMENTO DE BIT EFICIENTE COM SEGURANÇA SEQUENCIAL BASEADO NO MODELO DE MEMÓRIA LIMITADA

VINÍCIUS DE MORAIS ALVES

Brasília, Fevereiro de 2010

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASILIA
Faculdade de Tecnologia
Departamento de Engenharia Elétrica

DISSERTAÇÃO DE MESTRADO

PROTOCOLO DE COMPROMETIMENTO DE BIT EFICIENTE COM SEGURANÇA SEQUENCIAL BASEADO NO MODELO DE MEMÓRIA LIMITADA

VINÍCIUS DE MORAIS ALVES

ORIENTADOR: ANDERSON CLAYTON ALVES NASCIMENTO.

PUBLICAÇÃO: PPGENE 419/2010.

BRASÍLIA/DF: FEVEREIRO/2010.

FICHA CATALOGRÁFICA

Alves, Vinícius de Morais

Protocolo de Comprometimento de Bit Eficiente com Segurança Sequencial Baseado no Modelo de Memória Limitada

[Distrito-Federal], Fevereiro de 2010.

xii, 59 p. (ENE/FT/UnB, Mestre em Ciências, 2010)

Dissertação de Mestrado - Universidade de Brasília.

Faculdade de Tecnologia.

Departamento de Engenharia Elétrica.

1. Segurança Incondicional
2. Primitivas Criptográficas
3. Comprometimento de Bit
4. Modelo de Memória Limitada
5. *Commitment Capacity*
6. *Everlasting Security*

I. ENE/FT/UnB

II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

Alves, Vinícius de Morais (2010). Protocolo de Comprometimento de Bit Eficiente com Segurança Sequencial Baseado no Modelo de Memória Limitada. Dissertação de Mestrado, Publicação PPGENE 419/2010, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF,

CESSÃO DE DIREITOS

GRAU / ANO: Mestre em Ciências / 2010.

VINÍCIUS DE MORAIS ALVES

QI 23, LOTE 2/6, Bl. I, Apto 504, Guará II.

CEP 71060-632 - Brasília - DF - Brasil.

Dedico esta obra à você, Lílian, amor da minha vida! Também dedico ao meu pai, Paulo César, a quem devo toda minha paixão pela matemática.

Agradecimentos

Agradeço inicialmente a Deus, que mediante sua graça possibilitou mais essa conquista em minha vida. Gostaria de agradecer profundamente ao Prof. Dr. Anderson C. A. Nascimento por sua inestimável ajuda e por sempre buscar me motivar durante meus estudos do mestrado. Aos colegas de laboratório, sou grato pelos muitos momentos maravilhosos, tanto de estudo como de descontração. Agradeço à banca examinadora pelo tempo dispensado para avaliar essa obra e pelas valiosas sugestões. Sou especialmente grato aos meus pais, que me deram apoio incondicional e suporte financeiro para concluir meus estudos, além de ser grato a toda minha família, pela qual tenho grande afeto. Por fim, mas não menos especial, gostaria de agradecer a minha noiva, Lílian, por sua interminável paciência e compreensão comigo, pelas muitas vezes que me incentivou, pelas horas que tive de abdicar de sua companhia para estudar e por todo o amor que tem por mim.

VINÍCIUS DE MORAIS ALVES

RESUMO

O Comprometimento de Bit é uma primitiva criptográfica fundamental usada para construir provas de conhecimento nulo e computação segura distribuída. Ueli Maurer [Mau93] introduziu o modelo de memória limitada no contexto de criptografia incondicionalmente segura. O modelo de Maurer limita o tamanho máximo da memória de um participante desonesto, ao contrário da abordagem usual em criptografia moderna, que limita a capacidade de processamento do adversário. Dedicou-se no presente trabalho à elaboração de um protocolo de comprometimento de bit baseado apenas no paradigma de memória limitada, sem a adoção de hipóteses computacionais não comprovadas. Até a presente data, esse é o primeiro protocolo de comprometimento de bit no modelo de memória limitada clássico[1]. Embora se saiba que a existência da primitiva criptográfica conhecida como *Oblivious Transfer*, implementada no modelo de memória limitada pela primeira vez em [CCM98], implique na existência de comprometimento de bit, uma implementação direta tem a vantagem de ser mais eficiente e mais simples, em geral. A intenção do protocolo é maximizar a quantidade de bits que o emissor consegue se comprometer e, simultaneamente, minimizar a quantidade de bits amostrados pelo mesmo durante a fase de transmissão, de modo a atingir a máxima capacidade de comprometimento. O conceito de capacidade de comprometimento apresentado aqui difere em certos aspectos do conceito presente no trabalho [WNI03] sobre canais ruidosos, sendo o principal deles o fato de a capacidade de comprometimento definida aqui ser dependente do limite no tamanho da memória do adversário. Além disso, fez-se uma contribuição adicional com a elaboração de um modelo geral para os protocolos de comprometimento de bit baseados em memória limitada. Para essa família de protocolos foram demonstrados limites ótimos, como o tamanho mínimo da memória dos participantes e a quantidade máxima de bits que o emissor pode se comprometer.

[1] Um protocolo de comprometimento de bit baseado no modelo de memória quântica limitada foi introduzido em [DFSS05].

ABSTRACT

The Bit commitment is a fundamental cryptographic primitive used to construct zero-knowledge proofs and multi-party computation. Ueli Maurer introduced the bounded storage model in the context of information-theoretical security on [Mau93]. Unlike the usual approach in modern cryptography, the Maurer's bounded storage model restricts the adversaries' memory size instead of their computing power. In this thesis we develop a protocol of bit commitment based on solely in the bounded storage assumption, without the assumption of unproved hard problems. Up to date, there are no results in the literature about the implementation of commitment schemes in the classical bounded storage model[2]. Although is known that the existence of a cryptographic primitive called oblivious transfer, implemented in the bounded storage model at first time on [CCM98], implies the existence of bit commitment, a directly implementation usually is better in terms of simplicity and efficiency. The intention of our protocol is maximize the length of the string that the sender may commits to and, at the same time, minimize the length of the string sampled by the sender during the broadcast phase, to achieve the commitment capacity. The concept of commitment capability presented here differs in some aspects of the concept on [WNI03] about noisy channels, and the main reason is due to the commitment capacity defined here to depend on memory size of the opponent. In addition, we made a further contribution elaborating a general model for the bit commitment protocols based on bounded storage. For this family of protocols, we have demonstrated optimal bounds, as the minimum size of the player's memory and the maximum length of the string that the sender may commits to.

[2]Commitment schemes in the bounded quantum-storage model were presented in [DFSS05].

SUMÁRIO

LISTA DE FIGURAS

LISTA DE SÍMBOLOS

Variáveis aleatórias

X	Longa Sequência binária aleatória transmitida	$\{0,1\}^n$
X_a	Sequência amostrada de X por Alice	$\{0,1\}^k$
X_b	Sequência amostrada de X por Bob	$\{0,1\}^l$
V	Domínio das sequências do comprometimento de Alice	$\{0,1\}^m$
K	Saída da função extratora de aleatoriedade	$\{0,1\}^m$
T	Comunicação em claro trocada entre Alice e Bob	$\{0,1\}^*$
U_a	Aleatorieda local de Alice	$\{0,1\}^r$
U_b	Aleatorieda local de Bob	$\{0,1\}^r$
$\mathsf{C}_{\mathsf{comp}}$	Cifra one-time-pad contendo o comprometimento de Alice	$\{0,1\}^{\delta k}$

Parâmetros

n	Tamanho da sequência X transmitida.
k	Tamanho da amostra dos participantes honestos.
l	Tamanho da amostra de Bob malicioso.
s	Parâmetro de segurança positivo do protocolo.
r	Tamanho das aleatoriedades obtidas localmente pelos participantes.
α	Taxa de entropia por bit da fonte.
ν	Percentual de limite na memória do adversário em relação à min-entropia de X.
δ	Taxa de entropia por bit da amostra de Alice dada a visão de Bob do protocolo.
ω	Razão entre o tamanho da saída da função Hash e $\lvert X_a\rvert$.
γ	Probabilidade de falha da função amostrador mediano
τ	Variável que representa a redução da taxa de entropia da fonte no processo de amostragem.
ϵ	Usado de modo geral como variável auxiliar para representar limites.
ε	Distância estatística máxima entre $\lVert\mathsf{Ext}(X_a) - U_m\rVert$.
ε'	$\frac{2^{-k}\left(2^{-s}+\left(\gamma+2^{-q\tau n}\right)^{1-\lambda}\right)}{1-2^{-k}\left(2^{-s}+(\gamma+2^{-q\tau n})^{1-\lambda}\right)}$.

Funções

Ext	Função extratora forte de aleatoriedade	$\{0,1\}^k \rightarrow \{0,1\}^{\delta k}$
Hash	Função de hash 2-universal	$\{0,1\}^k \rightarrow \{0,1\}^{\omega k}$
Samp	Função amostrador mediano	$\{0,1\}^r \rightarrow [n]^t$
Test	Função que representa as verificações de Bob	$\{0,1\}^* \rightarrow \{ACK, REJ\}$
f^*	Função Probabilística Arbitrária	$\{0,1\}^n \rightarrow \{0,1\}^{\gamma n}$

Siglas

OT	Oblivious Transfer.
XOR	Operação de OU-Exclusivo bit-a-bit.

Capítulo 1

Introdução

Este capítulo introduz o tema e apresenta os diversos conceitos envolvidos com o desenvolvimento do protocolo de comprometimento de bit baseado no modelo de memória limitada. No decorrer do capítulo, destacam-se os fatores que motivaram o desenvolvimento do trabalho, os relevantes melhoramentos obtidos com o protocolo proposto e as desvantagens comparativas entre este e os outros protocolos existentes na literatura, visando elucidar as principais características que tornam relevante a elaboração deste trabalho.

1.1 Computação segura distribuída

A criptografia moderna é uma ciência recente, embora diversas técnicas criptográficas já fossem aplicadas desde a época do Império Romano e até mesmo antes. Talvez o grande fato histórico que consolidou a necessidade de uma abordagem séria, rigorosa e científica das técnicas criptográficas tenha sido a segunda grande guerra mundial, a qual, para muitos, foi vencida com grandiosa contribuição de matemáticos, físicos, inventores e cientistas que ajudaram a decifrar as comunicações secretas dos alemães feitas com o auxílio da famosa máquina Enigma.

No século XX surgiram tanto a teoria da informação como a teoria da computação, as quais sofreram enormes avanços mediante às brilhantes contribuições de diversos pesquisadores como Claude Shannon, Alan Turing, Norbert Wiener, Warren Weaver, Andrei Kolmogorov, David Hilbert, John von Neumann, Aaron Wyner, dentre muitos outros. Dentre todas as contribuições para a área da criptografia moderna, talvez o trabalho de Shannon [Sha49], entitulado "*Communication Theory of Secrecy Systems*", e o trabalho de Diffie e Helmann [DH76], entitulado "*New Directions in Cryptography*", tenham sido os dois prin-

cipais pilares de sustentação dessa recente área de pesquisa, fornecendo os fundamentos do atual estágio de desenvolvimento da criptografia.

Em criptografia moderna, há um famoso problema conhecido como *Computação segura distribuída*, introduzido por Andrew C. Yao [Yao82] em importante trabalho publicado na FOCS em 1982, entitulado "*Protocols for Secure Computations*". Nessa publicação apareceu o famoso **Problema Dos Milionários**: *Alice e Bob são dois milionários que desejam descobrir quem é mais rico, mas sem revelarem um ao outro quanto dinheiro possuem.* Yao apresentou solução que permite Alice e Bob descobrirem quem é o mais rico sem, no entanto, violar qualquer das restrições impostas no enunciado do problema.

A formulação teórica para esse problema foi posteriormente generalizada, permitindo solucionar a computação de funções seguras distribuídas entre muitas partes. Ou seja, dado um conjunto de participantes $p_1, p_2, \ldots, p_n$ e tendo cada um entradas privadas $x_1, x_2, \ldots, x_n$, respectivamente, pode-se computar o resultado $f(x_1, x_2, \ldots, x_n)$ de modo que cada participante saiba apenas a sua entrada, a saída da função e o que pode ser computado localmente a partir dessas informações. Um protocolo de computação distribuída é dito seguro se nenhum participante for capaz de calcular algo a mais do que é possível a partir da descrição da função pública, do resultado obtido por ele ao final do protocolo e de sua própria entrada.

Um problema muito famoso em computação segura distribuída foi proposto por Manuel Blum em 1981 na CRYPTO [Blu83]. Conhecido como "Jogando cara-ou-coroa pelo telefone", o protocolo apresentado por Blum propõe uma solução para a seguinte situação hipotética:

"*Alice e Bob se divorciaram e querem decidir por telefone, pois não desejam mais se ver, quem vai ficar com o cachorro. Eles preferem não envolver outras pessoas na briga, de modo a evitarem exposição excessiva. Para isso, eles resolvem jogar cara-ou-coroa, porém um não confia no outro. Como proceder nessa situação para que Bob possa confiar na escolha de Alice, de modo a não ser possível ela mudar de idéia, sem ser detectada, após Bob anunciar seu resultado?*"

Esse é um exemplo de computação segura de duas partes, onde os participantes se engajam na obtenção de um resultado, mas sem terem confiança mútua e sem possibilitarem que o outro descubra alguma informação além do necessário. Percebe-se que tal computação pode ser realizada facilmente com a ajuda de uma terceira parte confiável. Entretanto, conforme visto no exemplo acima, os participantes preferem não confiar em uma terceira parte.

Objetiva-se, assim, encontrar um protocolo de computação segura de duas partes sem auxílio de uma terceira parte confiável. Contudo, sabe-se que essa é uma tarefa impossível de se realizar do zero, ou seja, sem ao menos uma hipótese adicional. Por outro lado, há hipóteses extremamente simples e elementares, como a existência de um canal ruidoso, que permitem a realização desse tipo de computação de modo incondicionalmente seguro, ou seja, a chance de um participante malicioso obter informação adicional, mesmo tendo

poder computacional ilimitado, não é maior que tentar advinhar essa informação, processo usualmente chamado de força bruta. Há implementações no ambiente computacional, ou seja, seguras contra adversários que apenas têm limitado poder computacional. No entanto, a segurança de tais implementações são baseadas em problemas matemáticos considerados difíceis, porém sem comprovação. Por exemplo, conjectura-se que a fatoração do produto de dois números primos grandes e a obtenção do logarítmo discreto são difíceis.

Isso posto, percebe-se que é desejável basear a segurança de um protocolo de computação segura entre duas partes em hipóteses que sejam o mais simples possível. Protocolos de comprometimento de bit são primitivas criptográficas que permitem um emissor se comprometer a enviar um bit ao receptor, o qual pode verificar de forma indubitável se o bit recebido corresponde de fato ao comprometimento prévio. O valor do bit deverá permanecer completamente desconhecido para o receptor até o instante em que o emissor decida revelá-lo. Por outro lado, o emissor não deverá ser capaz de revelar um valor diferente do qual se comprometeu.

1.2 Protocolos de Comprometimento de Bit

A noção de comprometimento é uma das primitivas fundamentais tanto na teoria quanto na prática da criptografia moderna. O conceito de comprometimento como primitiva criptográfica foi introduzido por Manuel Blum [Blu83]. É uma ferramenta essencial na construção de inúmeros protocolos criptográficos, como provas gerais de conhecimento nulo (*general zero knowledge proofs*) [BCC88, GMW86], assim como computação segura distribuída [CDvdG87]. Extensivos estudos em criptografia moderna foram feitos à respeito dessa primitiva, como se pode observar nos trabalhos [Nao90], [Ken98], [IBP97], [Dam99], [IBDS99], [Kil91], dentre outros.

Um protocolo de comprometimento de bit consiste de duas fases, *Comprometimento* e *Abertura*, executadas por dois participantes, um emissor, Alice, e um receptor, Bob. Na fase de comprometimento, Alice se compromete com um valor v, enviando certa informação contendo vestígios sobre v para Bob. No caso ideal, Bob não deve ser capaz de descobrir o valor v, por conta própria, a partir dessa informação vestigial e de possíveis interações com Alice. Posteriormente, Alice e Bob podem executar a fase de abertura do protocolo, que revelará para Bob o valor v e o permitirá verificar se a informação vestigial recebida na fase anterior corresponde, de fato, ao valor v. Note que, em princípio, a fase de abertura pode não ser executada.

Com base em problemas computacionais é possível construir um protocolo de comprometimento de bit incondicionalmente seguro para o receptor, mas computacionalmente seguro para o emissor (veja [Nao90]). De modo análogo, também é possível construir protocolos que sejam incondicionalmente seguros para o emissor e computacionalmente seguros

para o receptor [CDvdG87]. A segurança baseada nesse paradigma envolve a suposição de que alguns problemas são intratáveis para adversários cujo poder computacional é suposto polinomial. Em paradigmas onde a segurança é incondicional tanto para o emissor quanto para o receptor, nenhuma restrição é feita sobre a capacidade computacional do adversário. Naturalmente, deseja-se obter segurança incondicional para ambos os participantes do protocolo, mas não é possível construir um comprometimento que seja incodicionalmente seguro para ambos os participantes sem o auxílio de uma hipótese adicional.

A razão para isso está na chamada condição de simetria em relação ao conhecimento mútuo dos participantes. Quando ambos os participantes possuem toda a transcrição da comunicação que realizam, cada um deles pode determinar com exatidão o que o outro sabe sobre seus dados. Dessa forma, não é possível para as partes esconder informação alguma uma da outra usando os dados obtidos na realização do protocolo. Uma das formas de se quebrar a condição de simetria foi apresentada por Crépeau e Kilian em [CK88]. A idéia deles se baseou na construção de um protocolo de comprometimento de bit baseado em canais ruidosos. Nesse trabalho, os autores mostraram uma redução da primitiva criptográfica *oblivious transfer*(OT) ao canal binário simétrico (CBS), o que, de fato, implica na redução de comprometimento de bit ao CBS, já que é conhecida uma redução caixa preta da primitiva OT para a primitiva comprometimento de bit [Kil88].

Crepeau, em [Cré97], introduziu um protocolo de comprometimento de bit baseado diretamente no canal binário simétrico, obtendo uma implementação mais eficiente. Em geral, implementações diretas de comprometimento de bit são mais eficientes do que aquelas obtidas via uma redução de OT. Esse é inclusive um dos fatores que motivaram a elaboração deste trabalho.

Finalmente, um esquema de comprometimento de bit baseado em uma hipótese mais fraca e mais realista, onde os participantes têm controle parcial sobre o ruído introduzido no canal, conhecida como *unfair noisy channel*, foi proposta por Damgård, Kilian e Salvail em [IBDS99]. Em outro trabalho, Winter, Nascimento e Imai [WNI03] definiram a capacidade de comprometimento de um canal como sendo a razão entre a quantidade de bits que Alice se compromete e o número de vezes que o canal ruidoso é usado quando executado o protocolo. A capacidade de comprometimento de um canal discreto sem memória se mostrou igual a equivocação do canal depois de removidas quaisquer redundâncias triviais.

1.3 Modelo de Memória Limitada

Em um artigo memorável [Mau93], Ueli Maurer introduziu o modelo de memória limitada no contexto de criptografia incondicionalmente segura. Ao contrário da abordagem usual em criptografia moderna, o modelo de memória limitada de Maurer restringe o tamanho da memória dos participantes, ao invés da capacidade de processamento. Além

disso, assume-se que há uma fonte de alta taxa de transmissão de aleatoriedade pública e que o limite no tamanho da memória dos participantes os impede de guardar toda a aleatoriedade vinda da fonte. Destaca-se que assumindo apenas essa simples hipótese é possível construir cripto-sistemas incondicionalmente seguros, sem assumir hipóteses computacionais adicionais. Intuitivamente, uma chave pré-compartilhada pode ser usada pelos participantes honestos para amostrar bits da longa sequência binária irradiada pela fonte, sendo que o adversário obtém pouca informação sobre esses bits, dado o limite em sua memória. Com o auxílio de algum processamento, os participantes honestos podem comprimir esses bits de modo que a sequência resultante se torne estatísticamente próxima de uniforme sob a ótica do adversário, o que permite o seu uso para fins criptográficos, por exemplo como chave de uma cifra one-time-pad.

Há uma lista de trabalhos melhorando a segurança e o desempenho de protocolos nesse modelo [CM97], [AR99], [ADR02], [DM02], [Lu04]. Em particular, o trabalho de Aumann, Ding e Rabin [ADR02] mostra que uma importante vantagem de protocolos nesse modelo está em sua propriedade de segurança conhecida como *everlasting*. Essa propriedade implica na incapacidade do adversário comprometer a segurança do protocolo mesmo no caso de adquirir memória ilimitada após a execução da primeira fase do protocolo ou se a chave usada inicialmente for fornecida ao adversário ao final do protocolo, diferentemente do que ocorre com protocolos clássicos em criptografia baseados em problemas como o do logarítmo discreto, pois quando o adversário adquiri poder computacional suficiente, mesmo que no futuro, ou mesmo a chave usada anteriormente, ele pode decifrar toda a comunicação feita no passado.

Em trabalho publicado no *Jornal of Cryptology* em 2004, Lu [Lu04] mostrou que protocolos no modelo de memória limitada podem ser implementados com auxílio de extratores fortes de aleatoriedade. Extratores, introduzidos por Nisan and Zuckerman [NZ96], são procedimentos para se extrair bits quase-uniformes de fontes enviesadas que apresentam bits correlacionados. Essas poderosas ferramentas têm sido muito estudadas e apresentam uma vasta área de aplicação na teoria da computação [NTS99]. Uma das primeiras aplicações que se deu a extratores foi a construção de geradores de pseudo-aleatoriedade para computadores com restrição de memória. Então, parece que essa é uma ferramenta naturalmente relacionada com o modelo de memória limitada, o que de fato Lu mostrou em seu trabalho ao provar que a existência de extratores fortes de aleatoriedade implica na construção de cripto-sistemas de chave simétrica incondicionalmente seguros no modelo de memória limitada.

Crepeau, em [CCM98], apresentou o primeiro protocolo de oblivious transfer no modelo de memória limitada. Uma das desvantagens do protocolo presente nesse trabalho é o tamanho da memória dos participantes honestos, que devem armazenar $k = O(n^{2/3})$ bits da sequência binária aleatória irradiada, de tamanho n e distribuição uniforme. Uma de suas vantagens é possibilitar que o tamanho da memória do adversário seja até νn, para

todo $\nu < 1$. Ainda nesse protocolo, a probabilidade de um participante desonesto aprender informação sobre as duas entradas é $k^{-\Omega(1)}$ e a quantidade de mensagens trocadas para se executar o hash interativo em uma das fases do protocolo era linear em n. Uma versão modificada desse protocolo apareceu no trabalho de Yan Zong Ding [Din01]. Nessa versão, os participantes honestos precisam de apenas $O(\sqrt{n})$ de memória e a probabilidade de falha do protocolo é de $O(2^{-\sqrt{n}})$. Porém, o protocolo tratava o comprometimento de um único bit e apresentava muitas mensagens trocadas entre as partes ainda. Esse resultado foi generalizado para tratar *one-out-of-k* OT em [HCR02]. Contudo, todos esses protocolos apresentavam a desvantagem de terem que trocar algo em torno de $O(k^{\Omega(1)})$ mensagens entre os participantes, onde k é o tamanho da memória dos participantes honestos. Essa complexidade de comunicação foi um fator significativamente melhorado em [DHRS07], que além de manter todos os melhoramentos dos trabalhos anteriores, reduziu o número de mensagens trocadas entre os participantes para apenas 5.

1.4 Resultados obtidos

Uma importante observação sobre todo o trabalho que foi feito na área de memória limitada está no fato de que nenhum deles abordou a implementação direta de um protocolo de comprometimento de bit. Assim, até a presente data, este é o primeiro protocolo de comprometimento de bit no modelo clássico de memória limitada[1]. Embora se saiba que a existência da primitiva criptográfica conhecida como *Oblivious Transfer*, implementada no modelo de memória limitada pela primeira vez em [CCM98], implique na existência de comprometimento de bit, uma implementação direta tem a vantagem de ser mais eficiente e mais simples, em geral. Além disso, contribuiu-se com a elaboração de um modelo geral para os protocolos de comprometimento de bit baseados em memória limitada, de modo que qualquer possível protocolo de comprometimento nesse paradigma seja uma instância desse modelo geral.

Para essa família de protocolos, estabeleceu-se limiares importantes, como o tamanho mínimo da memória dos participantes honestos, o fato da memória do adversário ter tamanho arbitrariamente menor do que a quantidade de aleatoriedade irradiada e a quantidade máxima de bits que o emissor pode se comprometer, tendo sido demonstrada a otimalidade dessas cotas. Além disso, resultados importantes quanto ao desempenho do protocolo também foram obtidos, como a exigência de pequenas sementes para que Alice e Bob possam obter suas amostras, complexidade de comunicação pequena, com a troca de apenas 3 mensagens, além da manutenção de todas as outras vantagens obtidas anteriormente para as outras primitivas. Contudo, algumas desvantagens congêneres do modelo permaneceram no protocolo apresentado nesse trabalho. Por exemplo, o tamanho da se-

[1] Um protocolo de comprometimento de bit baseado no modelo de memória quântica limitada foi introduzido em [DFSS05].

quência binária irradiada é extremamente grande, a qual mesmo em meios com elevadas taxas de transmissão pode levar dias para ser transmitida.

1.5 Visão Geral

Esse trabalho está organizado da seguinte forma. No capítulo 2 há uma apresentação da notação usada em todo o trabalho e uma descrição das principais ferramentas matemáticas necessárias para a compreensão das provas de segurança e do funcionamento do protocolo. No capítulo 3, aborda-se o modelo teórico de comprometimento adotado e certos limites são deduzidos, sendo demonstrada a otimalidade de alguns. No capítulo 4 é provada a segurança do esquema de comprometimento de bit proposto, sendo demonstrado que o protocolo atende as condições de segurança e atinge os limites ótimos previamente estabelecidos no modelo geral. No capítulo 5 são feitas certas escolhas para os valores dos parâmetros de segurança, de modo a se realizar uma análise mais prática do protocolo. Finaliza-se o trabalho com as conclusões, bibliografia e um compêndio em anexo sobre limites de probabilidade e a prova de um lema interessante conectando o conceito de distância de hamming com funções de hash universal.

Capítulo 2

Preliminares

Esse capítulo apresenta a notação adotada no trabalho e introduz brevemente alguns conceitos relacionados com o desenvolvimento matemático da prova de segurança do esquema de comprometimento de bit. Além disso, as principais definições e os lemas centrais são estabelecidos, visando consolidar em um único capítulo todas as ferramentas matemáticas necessárias para a construção do protocolo.

2.1 Notação

Denotar-se-á por letras maiúsculas X as variáveis aleatórias, por letras caligráficas $\mathcal{X}$ o domínio das variáveis aleatórias, e por letras minúsculas x uma realização da variável aleatória. Os conjuntos serão representados tanto por letras maiúsculas como caligráficas, dependendo da conveniência no texto, e um elemento do conjunto será representado por letra minúscula. A cardinalidade do conjunto, ou o tamanho do alfabeto, será denotada por $|\mathcal{X}|$ ou, similarmente, por $|X|$.

Exceto quando dito ao contrário, far-se-á referência às variáveis aleatórias discretas. Para uma variável aleatória X com alfabeto $\mathcal{X}$, seja $P_r[X = x]$ a probabilidade de que a variável X assuma o valor x, podendo ser abreviada por $P_X(x)$, sendo sua distribuição de probabilidade dada por $P_X : \mathcal{X} \to [0, 1]$ com $\sum_{x\in\mathcal{X}} P_X(x) = 1$. Para denotar a distribuição de probabilidade conjunta $P_{XY} : \mathcal{X} \times \mathcal{Y} \to [0, 1]$, seja $P_X(x) := \sum_{y\in\mathcal{Y}} P_{XY}(x, y)$ a distribuição de probabilidade marginal, considerando a abreviação $P_{XY}(x, y)$ para $P_r[X = x, Y = y]$, e seja $P_{X|Y=y}(x) := P_{XY}(x, y)/P_Y(y)$ a distribuição de probabilidade condicional quando $P_Y(y) \neq 0$. Denominar-se-á por U_r a variável aleatória uniformemente distribuída sobre $\{0, 1\}^r$, o domínio das sequências binárias de comprimento r.

Se uma função f for probabilística, então será denotado por $f(x; r)$ o resultado da

computação de f na entrada x com aleatoriedade r. Se x_a e x_b são duas sequências binárias de mesma ordem, então $x_a \oplus x_b$ representa a operação de ou-exclusivo, daqui para frente XOR, entre elas de modo bit-a-bit, e $\mathsf{HD}(x_a, x_b)$ representa a distância de Hamming entre as sequências, isto é, o número de posições em que elas diferem.

2.2 Entropias

A entropia de Shannon é uma medida útil e importante na teoria da informação, particularmente em processos de extração de aleatoriedade. Nesse trabalho, define-se a função de entropia como sendo $H(X) = -\sum_i p_i(x) \log p_i(x)$, sendo a entropia binária dada por $h(x) := -x \log x - (1-x)\log(1-x)$. Logarítmos usados nessas funções estão sempre na base 2, exceto quanto dito o contrário. Como é usual, tem-se as seguintes relações para entropia condicional, entropia conjunta e informação mútua, respectivamente:

$$H(X|Y) = H(XY) - H(Y)$$

$$H(XY) = H(X) + H(Y) - I(X;Y)$$

$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = I(Y;X)$$

A entropia relativa $\mathcal{D}(P||Q)$ mede a ineficiência de assumir que a distribuição de uma variável aleatória X é $Q_X(x)$ quando a distribuição verdadeira é $P_X(x)$. Por exemplo, caso se saiba a distribuição verdadeira da variável aleatória X, é possível construir um código com comprimento médio $H(X)$. No entanto, usar um código desenhado para uma distribuição $Q_X(x)$ implica em uma construção inadequada com base na variável aleatória, sendo necessários $H(X) + \mathcal{D}(P||Q)$ bits, em média, para se conseguir construir o código.

Definição 2.1 (divergência de Kullback-Leibler). *A entropia relativa $\mathcal{D}(P||Q)$ entre duas distribuições $P_X(x)$ e $Q_X(x)$ é definida por*

$$\mathcal{D}(P||Q) \stackrel{def}{=} \sum_{x \in \mathcal{X}} p(x) \log \frac{p(x)}{q(x)}$$

Neste trabalho, adotou-se a seguinte convenção de notação para a entropia relativa binária $\mathsf{d}(p||q)$, onde as distribuições P e Q assumem apenas os valores p, $1-p$ e q, $1-q$, respectivamente. Assim, define-se a entropia relativa binária a seguir:

Definição 2.2. *A entropia relativa binária $\mathsf{d}(p||q)$ entre duas probabilidades p e q é definida por*

$$\mathsf{d}(p||q) = p \log \frac{p}{q} + (1-p) \log \frac{1-p}{1-q}$$

Além dessas definições básicas de entropia, será necessário introduzir outras mais específicas, já que a entropia de Shannon passa a idéia da quantidade de informação média sobre um conjunto, enquanto se está interessado na quantidade de informação miníma sobre um conjunto. Nesse caso, a entropia de Shannon capta apenas uma solução parcial do problema, uma vez que os limiares podem estar bem distantes da média. Quando se analisa a eficiência de um processo de extração de aleatoriedade no caso de repetições identicamente distribuidas, então a entropia de Shannon é a resposta. Porém, quando se está interessado em extração de aleatoriedade em casos sem repetição, que ocorrem possivelmente uma única vez, a chamada entropia de Rényi obtém limites melhores.

Para um alfabeto finito $\mathcal{X}$, a min-entropia da variável aleatória $X \in \mathcal{X}$ é definida como:

$$H_\infty(X) = \min_x \log(1/P_X(x)).$$

A versão condicional da min-entropia, definida sobre o alfabeto finito $\mathcal{Y}$, é dada por:

$$H_\infty(X|Y) = \min_y H_\infty(X|Y = y).$$

Para um alfabeto finito $\mathcal{X}$, a max-entropia da variável aleatória $X \in \mathcal{X}$ é definida como:

$$H_0(X) = \log |\{x \in X | P_X(x) > 0\}|$$

A versão condicional da max-entropia, definida sobre o alfabeto finito $\mathcal{Y}$, é dada por:

$$H_0(X|Y) = \max_y H_0(X|Y = y).$$

A distância estatística entre duas distribuições de probabilidade P_X e P_Y sobre algum domínio $\mathcal{V}$ é

$$\mathsf{SD}(P_X, P_Y) = \|P_X - P_Y\| := \frac{1}{2} \sum_{v \in \mathcal{V}} |P_X(v) - P_Y(v)|.$$

Para $\epsilon \geq 0$, as versões ϵ-suaves da entropia de Rényi estão definidas a seguir:

$$H_\infty^\epsilon(X) = \max_{X' : \|P_{X'} - P_X\| \leq \epsilon} H_\infty(X'),$$

$$H_\infty^\epsilon(X|Y) = \max_{X'Y' : \|P_{X'Y'} - P_{XY}\| \leq \epsilon} H_\infty(X'|Y'),$$

$$H_0^\epsilon(X) = \min_{X' : \|P_{X'} - P_X\| \leq \epsilon} H_0(X'),$$

$$H_0^\epsilon(X|Y) = \min_{X'Y' : \|P_{X'Y'} - P_{XY}\| \leq \epsilon} H_0(X'|Y').$$

No decorrer do trabalho, será necessário usar a regra da cadeia da entropia de suave [RW05] condicionada a uma variável aleatória adicional Z. Para todo $\varepsilon, \varepsilon', \varepsilon'' \geq 0$, essas desigualdades estão definidas a seguir:

$$H_{\infty}^{\varepsilon}(X|YZ) \leq H_{\infty}^{\varepsilon+\varepsilon'}(XY|Z) - H_{\infty}^{\varepsilon'}(Y|Z)$$

$$H_{\infty}^{\varepsilon+\varepsilon'+\varepsilon''}(X|YZ) > H_{\infty}^{\varepsilon'}(XY|Z) - H_{0}^{\varepsilon''}(Y|Z) - \log(1/\varepsilon)$$

$$H_{0}^{\varepsilon+\varepsilon'+\varepsilon''}(X|YZ) < H_{0}^{\varepsilon'}(XY|Z) - H_{\infty}^{\varepsilon''}(Y|Z) + \log(1/\varepsilon)$$

$$H_{0}^{\varepsilon}(X|YZ) \geq H_{0}^{\varepsilon+\varepsilon'}(XY|Z) - H_{0}^{\varepsilon'}(Y|Z)$$

2.3 Funções de Hash 2-Universal

Devido ao papel central na construção do protocolo proposto neste trbalho, faz-se de suma importância relembrar a definição de função de hash 2-universal, assim como introduzido por Carter and Wegman [CW79]. Uma família, indexada por uma semente de r-bits, consiste de um conjunto de funções de hash 2-universal que mapeiam mensagens de um domínio $\mathcal{K} = \{0,1\}^k$ em uma imagem $\mathcal{H} = \{0,1\}^m$. A seguir, define-se a propriedade de resistência à colisão, onde a probabilidade de ocorrência em funções de hash 2-universal é estabelecida, dado que a função é escolhida com distribuição uniforme:

Definição 2.3 (Funções de Hash 2-Universal). *Uma classe $\mathcal{G}$ de funções que mapeiam $\mathcal{K} \to \mathcal{H}$ é* 2-universal *se, para quaisquer valores distintos $x_1, x_2 \in \mathcal{K}$, A probabilidade de que $g(x_1) = g(x_2)$ é no máximo $|\mathcal{H}|^{-1}$, onde g é escolhida aleatoriamente com distribuição uniforme da classe $\mathcal{G}$.*

2.4 Extratores de Aleatoriedade

Definir-se-á agora a noção de extratores fortes de aleatoriedade [NZ96, DORS08].

Definição 2.4 (Extratores Fortes de Aleatoriedade). *Seja* Ext *um algoritmo de extração de aleatoriedade baseado em $\leftarrow G : \{0,1\}^k \times \{0,1\}^r \to \{0,1\}^m$ uma função de hash probabilística de tempo polinomial que usa r bits de aleatoriedade. Diz-se que* Ext *é um eficiente $(k, \delta k, m, \epsilon)$ –* extrator forte *se para toda distribuição de probabilidade P_X, com $\mathcal{X} = \{0,1\}^k$ tal que $H_{\infty}(X) \geq \delta k$, tem-se que $\mathsf{SD}(P_{\mathsf{Ext}(X;U_r),U_r}, P_{U_m,U_r}) \leq \epsilon$, onde $r = \log k + O(\log m + \log(1/\epsilon))$.*

Extratores fortes podem extrair no máximo $m = \delta k - 2\log(1/\epsilon) + O(1)$ bits de aleatoriedade aproximadamente com distribuição uniforme e este limite pode ser alcançado por meio da aplicação do famoso lema *Leftover-Hash*, que faz uso de funções de hash 2-universal.

2.5 O lema *Leftover-Hash*

O lema conhecido como Leftover-Hash, citado em [CG88, ILL89, HILL99, BBR88, BBCM95, DORS08, CV08], estabelece que uma função de hash 2-universal permite extrair $m = \delta k - 2\log(\epsilon^{-1}) + 2$ bits de aleatoriedade de uma fonte com min-entropia maior ou igual a δk, para k suficientemente grande.

Lema 2.1 (O Lema Leftover-Hash). *Assuma que uma classe $\mathcal{G}$ de funções $G : \{0,1\}^k \to \{0,1\}^m$ é 2-universal. Então para G selecionado aleatoriamente com distribuição uniforme de $\mathcal{G}$, tem-se que*

$$\mathsf{SD}(P_{G(X),G}, P_{U_m,G}) \leq \frac{1}{2}\sqrt{2^{-H_\infty(X)}2^m}.$$

*Em particular, funções de hash 2-universal são $(k, \delta k, m, \epsilon)-$*extratores fortes *sempre que $m \leq \delta k - 2\log(\epsilon^{-1}) + 2$.*

2.6 Alguns Lemas Técnicos Úteis

Os seguintes lemas estabelecem formas de medir a min-entropia de uma variável aleatória X que modela uma fonte, cuja distribuição de aleatoriedade não é uniforme, quando condicionada à ocorrência do evento $\{Y = y\}$, onde Y é uma variável aleatória de cardinalidade menor do que a da fonte e possivelmente dependente dela. Esses lemas são essenciais para obtenção de informação de uma variável aleatória X, que se apresente na forma de uma longa sequência binária, do ponto de vista de uma máquina de turing probabilística com memória limitada que armazena apenas uma parte da informação de X mediante procedimento de amostragem modelado por Y.

Inicialmente será apresentada a definição de uma αn-fonte de aleatoriedade, que terá grande importância para a sintese da notação dos resultados seguintes.

Definição 2.5. *Uma fonte de aleatoriedade é definida como qualquer dispositivo físico capaz de emitir sequências binárias de qualquer comprimento, tendo aleatoriedade com distribuição arbitrária. Seja $X \in \mathcal{X} = \{0,1\}^n$ a variável aleatória que modela essa fonte, então uma αn-fonte será tal que, para todo $0 < \alpha < 1$, tem-se:*

$$H_\infty(X) \geq \alpha n$$

O próximo lema aparece em [CCM98]. Incluiu-se a prova dele aqui por ser bastante instrutiva para a compreensão dos lemas seguintes, que estabelecem um resultado importante e mais complexo.

Lema 2.2. *Seja X uma variavel aleatória representando uma αn-fonte e Y uma variável aleatória arbitrária definida sobre $\mathcal{Y}$, onde $\beta > 0$. Então, com probabilidade pelo menos $1 - 2^{-\beta}$ sobre a realização $y \leftarrow Y$, obterá-se um valor y tal que*

$$H_\infty(X|Y = y) \geq \alpha n - \log|\mathcal{Y}| - \beta$$

Prova: Seja $p_0 = 2^{-\beta}/|\mathcal{Y}|$ e $B = \{y|P_Y(y) < p_0\}$. Então, $\sum_{y\in B} P_Y(y) < 2^{-\beta}$. Segue que para todo y com $P_Y(y) \geq p_0$

$$\begin{aligned} H_\infty(X|Y = y) &= -\log \max_{x\in\mathcal{X}} \left(P_{X|Y=y}(x)\right) \\ &= -\log \max_{x\in\mathcal{X}} \left(\frac{P_X(x) \cdot P_{Y|X=x}(y)}{P_Y(y)}\right) \\ &\geq -\log \max_{x\in\mathcal{X}} \left(\frac{P_X(x)}{p_0}\right) \\ &= H_\infty(X) + \log(p_0) \\ &= \alpha n - \log|\mathcal{Y}| - \beta \end{aligned}$$

O que prova o lema. ■

O passo da amostragem é baseado no lema fundamental de Nisan e Zuckerman [NZ96], o qual estabelece que se uma amostragem uniforme é feita de uma fonte com aleatoriedade fraca, a taxa de min-entropia da fonte é (aproximadamente) preservada. De modo mais preciso, se $X \in \{0,1\}^n$ é uma αn-fonte e $X_S \in \{0,1\}^t$ é uma projeção de X em um conjunto aleatório $S \subset [n]$ de t posições, então, com alta probabilidade, X_S é ε-próximo de uma $\alpha' t$-fonte, para algum α' dependente de α. Assim, torna-se possível simplesmente aplicar um extrator de aleatoriedade sobre X_S e dessa forma obter $\alpha' t$ bits com distribuição de probabilidade aproximadamente uniforme. Isso é, uma parte da semente é usada para amostrar de forma aleatória bits da sequência irradiada e a outra parte é usada para extrair aleatoriedade dessa amostra, o que se chama de extração de aleatoriedade localmente computável.

Escolher um conjunto S aleatório com distribuição uniforme é extremamente ineficiente em termos de tamanho da semente e possivelmente em termos da complexidade computacional. Contudo, como nenhuma limitação em termos de poder de processamento é feita sobre os participantes do protocolo, essa não é uma questão relevante, embora para a praticidade do protocolo seja interessante.

Por isso, para tornar eficiente esse processo de amostragem e tornar o tamanho da semente prático, Nisan e Zuckerman mostraram que o conjunto S pode ser amostrado de modo aleatoriamente eficiente, usando *k-wise independence and random walks on expander*

graphs. Para obter uma performance ainda melhor, Vadhan impôs uma restrição um pouco mais forte e utilizou o que é conhecido amplamente na literatura [BR94, CEG95, Zuc97, Gol97] como *averaging (oblivious) samplers*, traduzidos como amostradores medianos.

A definição a seguir de um amostrador mediano é devida à Vadhan [Vad03] e difere um pouco da definição padrão na literatura, mas se encaixa melhor em nossos propósitos. Para fins de uniformização da notação, seja $[n]$ o conjunto $\{1, 2, \ldots, n\}$ e $[n]^t$ o domínio dos subconjuntos de $[n]$ com cardinalidade t.

Definição 2.6. *Uma função* $\mathsf{Samp}\colon \{0,1\}^r \to [n]^t$ *é um* (μ, θ, γ) ***amostrador mediano*** *se para cada função* $f : [n] \to [0,1]$ *com média* $\frac{1}{n}\sum_{i\in[n]} f(i) \geq \mu$*, vale a seguinte desigualdade:*

$$\Pr_{\{i_1,\ldots,i_t\}\leftarrow\mathsf{Samp}(U_r)}\left[\frac{1}{t}\sum_{j=1}^{t} f(i_j) < \mu - \theta\right] \leq \gamma$$

Samp *tem* ***amostras distintas*** *se para todo* $x \in \{0,1\}^r$*, as amostras produzidas por* $\mathsf{Samp}(x)$ *são todas distintas.*

Assim, para qualquer função f que o valor médio seja pelo menos μ, com alta probabilidade (i. e., pelo menos $1-\gamma$), o amostrador sorteia uma amostra de posições nas quais o valor médio de f não é muito menor do que μ. O objetivo de construir amostradores medianos geralmente é minimizar o tamanho da aleatoriedade r e da complexidade da amostragem t.

Usando amostradores medianos junto com uma idéia presente no trabalho de Ta-Shma [TS02] é possível obter um aperfeiçoamento no lema de Nisan-Zuckerman [NZ96]. Especificamente, eles demonstraram que amostrar bits de uma αn-fonte fornece uma $(\alpha n)/\log(1/\alpha)$-fonte. O método em [Vad03] permite obter uma $(\alpha - 3\tau)n$-fonte, para τ quão pequeno se queira.

Para uma sequência $x \in \{0,1\}^n$ e um subconjunto $\mathcal{S} = \{i_1, i_2, \ldots, i_t\} \subset_R [n]^t$, define-se $x_{\mathcal{S}} \in \{0,1\}^t$ como sendo a sequência $x_{i_1}x_{i_2}\ldots x_{i_t}$. Destaca-se que, para um par de variáveis aleatórias conjuntamente distribuídas (A, B), a notação $B|_{A=a}$ denota a variável B condicionada a ocorrência do evento $A = a$.

Lema 2.3 (Refinando Nisan-Zuckerman [NZ96]). *Seja* $0 \leq 3\tau \leq \alpha \leq 1$*. Suponha que* $\mathsf{Samp} : \{0,1\}^r \to [n]^t$ *é um* (μ, θ, γ) *amostrador mediano com amostras distintas para* $\mu = (\alpha - 2\tau)/\log(1/\tau)$ *e* $\theta = \tau/\log(1/\tau)$*. Então, para cada* αn*-fonte* X *com domínio* $\{0,1\}^n$*, a variável aleatória* $(U_r, X_{\mathsf{Samp}(U_r)})$ *é* $\left(\gamma + 2^{-\Omega(\tau n)}\right)$*-próximo de* (U_r, W)*, sendo que para todo* $a \in \{0,1\}^r$*, a variável aleatória* $W|_{U_r=a}$ *é uma* $(\alpha - 3\tau)t$*-fonte.*

Para os propósitos deste trabalho é conveniente estabelecer o lema (2.3) de Vadhan [Vad03] de uma forma distinta. Para isso, a definição de *amostrador de min-entropia* será introduzida a seguir:

Definição 2.7 (Amostrador de Min-Entropia). *A função* $\mathsf{Samp} : \{0,1\}^r \to [n]^t$ *com amostras distintas é um* $(\alpha, \alpha', \phi, \epsilon)$-***amostrador de min-entropia*** *se para toda* αn*-fonte* X *com domínio* $\{0,1\}^n$ *há um conjunto* $A \subseteq \{0,1\}^r$ *tal que para todo* $a \in A$ *a distribuição* $X_{\mathsf{Samp}(a)}$ *é* ϵ*-próxima de uma* $\alpha' t$*-fonte, com probabilidade pelo menos* $1 - \phi$*.*

Com a notação estabelecida acima, torna-se possível reescrever o lema 2.3, conforme a seguir:

Lema 2.4 (Refinando o lema de Vadhan [Vad03]). *Seja* $0 \leq 3\tau \leq \alpha \leq 1$*. Suponha que* $\mathsf{Samp} : \{0,1\}^r \to [n]^t$ *é um* (μ, θ, γ) *amostrador mediano com amostras distintas para* $\mu = (\alpha - 2\tau)/\log(1/\tau)$ *e* $\theta = \tau/\log(1/\tau)$*. Então, há uma constante* $q > 0$ *tal que, para todo* $0 < \lambda < 1$*,* Samp *é um* $\left(\alpha, \alpha - 3\tau, (\gamma + 2^{-q\tau n})^{1-\lambda}, (\gamma + 2^{-q\tau n})^{\lambda}\right)$*-amostrador de min-entropia.*

Prova: O refinamento do lema de Vadhan [Vad03] aparece no trabalho de Ding [DHRS07], estando reproduzido a seguir. Seja q a constante omitida no enunciado do lema 2.3. Isto é, $(U_r, X_{\mathsf{Samp}(U_r)})$ é $(\gamma + 2^{-q\tau n})$-próximo da variável aleatória (U_r, W), sendo que para todo $a \in \{0,1\}^r$, a variável aleatória $W|_{U_r=a}$ é uma $(\alpha - 3\tau)t$-fonte. Seja B o conjunto de todo $a \in \{0,1\}^r$ tal que $X_{\mathsf{Samp}(U_r)}$ não seja $(\gamma + 2^{-q\tau n})^{\lambda}$-próximo de uma $(\alpha - 3\tau)t$-fonte. Segue que sua densidade é dada por $\phi = \sum_{a \in B} P_{U_r}(a) \leq (\gamma + 2^{-q\tau n})^{1-\lambda}$. Para ver isso, basta perceber que para satisfazer a condição da distância estatística que aparece no lema 2.3, tem-se que:

$$\mathsf{SD}(P_{U_r, X_{\mathsf{Samp}(U_r)}}, P_{U_r, W}) \leq \gamma + 2^{-q\tau n}$$
$$\therefore \phi \left(\gamma + 2^{-q\tau n}\right)^{\lambda} \leq \gamma + 2^{-q\tau n}$$
$$\therefore \phi \leq \left(\gamma + 2^{-q\tau n}\right)^{1-\lambda}$$

Por fim, assuma que o conjunto A é o complemento de B. Logo, o lema segue. ■

Existe uma construção, apresentada no trabalho de Vadhan [Vad03], que permite obter um amostrador mediano quase ótimo. Essa construção está expressa no lema a seguir:

Lema 2.5. *Para todo* $n \in N, 0 < \theta < \mu < 1$ *e* $\gamma > 0$*, existe um* (μ, θ, γ)*-amostrador mediano* $\mathsf{Samp} : \{0,1\}^d \to [n]^t$ *que usa:*

- t *amostras distintas* $\quad \forall \quad t \in [t_0, n]$*, onde* $t_0 = O\left(\frac{1}{\theta^2} \log \frac{1}{\gamma}\right)$*, e*
- $d = \log(n/t) + O\left(t_0 \cdot \log(1/\theta)\right)$ *bits aleatórios.*

2.7 Teste de Hipóteses

O teste de hipóteses é uma tarefa de decisão entre duas assertivas, chamadas de Λ_0 e Λ_1, dado certa informação representada por uma variável aleatória arbitrária X. A distribuição

de probabilidade da variável X quando Λ_0 é a hipótese correta é denotada por $C_X(x)$. A distribuição de probabilidade da variável X quando Λ_1 é a hipótese correta é denotada por $E_X(x)$. Seja $\digamma$ uma regra de decisão tal que, se $\digamma(X) = 0$, então Λ_0 é a hipótese correta, e se $\digamma(X) = 1$, então Λ_1 é a hipótese correta. A seguir, duas probabilidades de falha são definidas:

Definição 2.8. *Dado $\digamma$, uma regra de decisão, seja a probabilidade de falha η definida como sendo a probabilidade de $\digamma(X) = 0$ dado que Λ_1 é a hipótese correta.*

Definição 2.9. *Dado $\digamma$, uma regra de decisão, seja a probabilidade de falha ρ definida como sendo a probabilidade de $\digamma(X) = 1$ dado que Λ_0 é a hipótese correta.*

Segue do teorema de Neyman-Pearson [NP33] que o teste ótimo está em assumir Λ_0 como sendo a hipótese correta se e somente se

$$\log \frac{C_X(x)}{E_X(x)} \geq L$$

sendo L um limiar dependente de η, x o resultado da medição e $E_X(x) \neq 0 \ \ \forall \ \ x \in \mathcal{X}$.

Um dos maiores resultados em teste de hipóteses estabelece uma proporcionalidade entre η e ρ. O teorema a seguir, presente no trabalho de Blahut [Bla74], estabelece essa relação:

Teorema 2.1. *Em um teste de hipóteses, as probabilidades de falha η e ρ satisfazem a seguinte relação:*

$$\eta \log \frac{\eta}{1-\rho} + (1-\eta) \log \frac{1-\eta}{\rho} \leq \sum_{x \in \mathcal{X}} C_X(x) \log \frac{C_X(x)}{E_X(x)}$$

$$\therefore \ \mathsf{d}(\eta||1-\rho) \leq \mathcal{D}(C||E)$$

O teorema acima pode ser generalizado para o caso em que informação paralela adicional, modelada pela variável aleatória V com alfabeto $\mathcal{V}$ e distribuição P_V, esteja disponível [Bla74].

Teorema 2.2. *As probabilidades médias de falha $\bar{\eta} = \sum_{v \in \mathcal{V}} P_V(v)\eta(v)$ e $\bar{\rho} = \sum_{v \in \mathcal{V}} P_V(v)\rho(v)$ satisfazem a seguinte relação*

$$\mathsf{d}(\bar{\eta}||1-\bar{\rho}) \leq \sum_{v \in \mathcal{V}} P_V(v) \sum_{x \in \mathcal{X}} C_{X|V=v}(x|v) \log \frac{C_{X|V=v}(x|v)}{E_{X|V=v}(x|v)}$$

Capítulo 3

Modelo Geral e Limites Teóricos

Esse capítulo apresenta um modelo teórico geral para protocolos de comprometimento de bit no paradigma de memória limitada, onde são definidos os procedimentos que qualquer protocolo de comprometimento baseado nesse paradigma deve realizar. As fases e os algoritmos do esquema de comprometimento proposto são detalhadamente descritos e uma construção eficiente é apresentada. Por fim, demonstra-se certas cotas na probabilidade de falha e no desempenho do esquema proposto, sendo provada a otimalidade desses limites.

3.1 Modelo Geral

Neste capítulo, elabora-se um modelo geral para os protocolos de comprometimento de bit baseados em memória limitada, de modo que qualquer protocolo de comprometimento baseado nesse paradigma seja uma instância do modelo proposto. Com isso, pode-se demonstrar que certos limites irão existir para todo protocolo de comprometimento baseado em uma restrição na memória dos participantes, como uma cota inferior em torno de $\sqrt{n}$ no tamanho mínimo da memória dos participantes, ainda que honestos, onde n é o comprimento da sequência aleatória transmitida no início do protocolo.

Todo protocolo de comprometimento de bit baseado no modelo de memória limitada consistirá de três fases: transmissão, comprometimento e abertura. De modo mais formal, um protocolo de comprometimento é uma família de protocolos indexados por um parâmetro de segurança n. Por questão de simplicidade, não será explicitamente mencionada na notação a dependência do protocolo em relação ao parâmetro de segurança.

Nos protocolos de comprometimento há ao menos dois participantes, um emissor do comprometimento, a partir daqui chamado de Alice, e um receptor do comprometimento,

Bob. Nos protocolos em que a sequência binária aleatória não for transmitida por Alice haverá um terceiro participante, sendo uma fonte transmissora de bits aleatórios chamada de distribuidor. O distribuidor participa apenas na fase de transmissão, na qual ele realiza a transmissão via broadcast de uma longa sequência binária aleatória.

A transmissão da longa sequência binária aleatória é modelada pela variável aleatória X, a amostragem feita dessa sequência por Alice é modelada pela variável aleatória X_a e a amostragem feita por Bob, pela variável aleatória X_b. Caso algum participante se comporte de modo malicioso, sua memória pode ser muito maior que a requerida de participantes honestos. Se o adversário for Alice, poderá armazenar até toda a sequência irradiada, não sendo necessária restrição em sua capacidade de processamento ou de armazenamento. Já quando o adversário for Bob, este não poderá ter memória suficiente para armazenar toda a informação transmitida pelo distribuidor. Como é usual, supõe-se que as mensagens sem ruído trocadas pelos participantes e as aleatoriedades locais são todas discretas e binárias, por questão de simplicidade.

A seguir são definidos os objetivos de cada uma das fases que qualquer protocolo de comprometimento de bit baseado no modelo clássico de memória limitada deve apresentar:

Fase de Transmissão: Inicialmente, um distribuidor transmite uma longa sequência binária aleatória, modelada pela variável aleatória X, de comprimento n bits. Caso não haja um participante específico para desempenhar o papel de distribuidor, Alice pode assumir esse papel, se não houver no protocolo específico alguma restrição que a impeça de conhecer toda a informação transmitida nessa fase. Os participantes armazenam uma parte da informação transmitida, a qual é obtida por meio de um processo de amostragem arbitrário realizado sobre X. Um participante malicioso pode armazenar a saída de uma função arbitraria aplicada sobre a sequência transmitida $\mathfrak{f}(X)$. Se o adversário for Bob, então o comprimento da saída dessa função deve ser no máximo $\nu\alpha n$, onde α é a taxa de entropia por bit da fonte X, para todo $0 < \nu < 1$.

Fase de Comprometimento: Alice tem uma entrada $v \in \mathcal{V}$ com a qual ela quer se comprometer. Alice e Bob podem se comunicar por meio de um canal autenticado e sem ruído. Seja T a variável aleatória que representa todas as mensagens trocadas pelos participantes. Seja $view_A$ a variável que representa todos os dados em posse de Alice ao término da execução desta fase, e $view_B$, similarmente, a visão de Bob do protocolo. Ao final da comunicação, Bob deve possuir dados vestigiais relativos à v, $\mathsf{C}_{\mathsf{comp}}$, que representem o comprometimento de Alice. Quando Alice se comportar honestamente, a variável $\mathsf{C}_{\mathsf{comp}}$ deve depender de v, de aleatoriedades obtidas localmente por ambos os participantes e de X_a, variável que representa a amostragem realizada por Alice, já que essa é a única informação disponível no paradigma de memória limitada que viabiliza a quebra da condição de simetria existente entre os participantes. Porém, caso ela aja maliciosamente, Bob deve ser capaz

de detectar esse comportamento. Por outro lado, quando Bob agir maliciosamente, ele não deve ser capaz de obter informação alguma sobre v antes do final da fase de abertura.

Fase de Abertura: Os participantes se comunicam por um canal autenticado e sem ruído. Alice envia v' e X'_a para Bob, que deve ser capaz de verificar a validade do comprometimento a partir desses dados. Caso Alice se comporte honestamente, então $(v' = v \wedge X'_a = X_a)$ e Bob constata que $\mathsf{C}_{\mathsf{comp}}$ corresponde a v'. Por outro lado, se Alice for desonesta, então $(v' \neq v \vee X'_a \neq X_a)$ e a verificação realizada por Bob deve falhar.

Assim, o esquema proposto a seguir é um exemplo de um protocolo que pode ser tratado como uma instância do modelo apresentado acima. A vantagem do esquema instanciado neste trabalho está no fato de ser eficiente e atingir os limites ótimos preconizados pelo modelo geral, além de ser o primeiro proposto na literatura da área.

3.2 Descrição do protocolo

Nesta seção se descreve em detalhes o funcionamento do esquema de comprometimento proposto no presente trabalho.

O esquema de comprometimento construído a seguir apresenta segurança incondicional para ambos os participantes. Alice e Bob, enquanto participantes honestos, precisam armazenar uma pequena parte de uma longa sequência binária aleatória transmitida. Prova-se, inclusive, que essa quantidade é ótima, não existindo protocolo baseado nesse paradigma em que as partes armazenem menos informação para se comprometerem. Nenhuma hipótese ou limitação é assumida sobre Alice, sendo imposta restrição apenas no tamanho da memória de Bob, que não deve ser capaz de armazenar toda a informação transmitida durante a execução da fase de transmissão. Contudo, essa restrição só é necessária durante a primeira fase, após a qual Bob passa a ser ilimitado em todos os aspectos computacionais.

A primeira fase do esquema é a **Fase de Transmissão**, onde o distribuidor transmite uma longa sequência binária aleatória X de comprimento n bits e $H_\infty(X) \geq \alpha n$. A min-entropia de X deve ser maior que todo o espaço da memória de armazenamento de Bob quando ele se comporta maliciosamente. Essa restrição é importante para a segurança de Alice, pois só haverá assimetria entre a informação obtida pelas partes se Bob não for capaz de obter toda a informação transmitida. Neste passo, Alice e Bob amostram a realização x, obtendo sequências x_A e x_B, respectivamente, por meio da seleção de bits em posições aleatórias de x. Esses subconjuntos de posições aleatórias são obtidos por meio da aplicação da função de amostragem $\mathsf{Samp}(u) \subset_R [n]^k$ sobre uma pequena semente $u \leftarrow U_*$, o que resulta em subconjuntos aleatórios de $[n]$ com k posições. Caso Bob se comporte maliciosamente, o método de amostragem usado será arbitrário, modelado pela aplicação da função $f^*(X)$, tendo o tamanho da saída restrito à $\nu\alpha n$, imposto por hipótese do modelo

sobre a memória do adversário. Para participantes honestos, o protocolo requer que cada um seja capaz de armazenar $O\left(\sqrt{cn}\right)$ bits, onde c é o valor esperado de colisões entre as sequências amostradas, um parâmetro de segurança do protocolo. Vale ressaltar que, após essa fase, nenhuma restrição é imposta aos participantes.

A segunda fase do protocolo é chamada **Fase de Comprometimento**. Inicialmente, Bob sorteia uma semente $u_b \leftarrow U_r$, com distribuição uniforme e comprimento r bits, e a envia para Alice, de modo a especificar uma função de hash 2-universal $g(\cdot; u_b)$. Essa escolha é importante por duas razões. Primeiro, Bob é quem escolhe a função de hash para evitar que Alice maliciosamente tente manipular as possíveis pré-imagens da função de hash. Segundo, Bob faz sua escolha e tem que enviar a semente antes de Alice anunciar o conjunto $\mathcal{A} = \{i_1, i_2, \ldots, i_k\} \leftarrow \mathsf{Samp}(U_r)$ das posições amostradas por ela, caso contrário essa situação lhe permitiria manipular a escolha da função de hash de modo a vazar informação além do esperado.

Ao receber a semente enviada por Bob através de um canal de comunicação autenticado e sem ruído, Alice aplica a função de hash definida por Bob em sua amostra x_A, obtendo $\mathsf{Hash} = g(x_A; u_b)$ e envia esse resultado para Bob. Além disso, Alice envia para Bob o conjunto $\mathcal{A} = \{i_1, i_2, \ldots, i_k\} \leftarrow \mathsf{Samp}(U_r)$ das posições amostradas por ela da sequência x transmitida pela fonte X, o distribuidor. Depois disso, Bob verifica se $|\mathcal{C} := \mathcal{A} \bigcap \mathcal{B}| \geq k^2/2n$, um teste que permite avaliar se há pelo menos $c/2$ colisões entre as posições anunciadas por Alice e as posições amostradas por ele, sendo $c = k^2/n$ a esperança matemática de colisões entre posições de x_A e x_B. Caso o número de colisões seja menor do que esse limiar, Bob aborta o protocolo. Além disso, dada essa informação, Bob é capaz de detectar tentativas de trapaça de Alice com probabilidade tendendo assintoticamente a 1, enquanto sua incerteza sobre x_A permanece elevada.

Em seguida, Alice sorteia uma semente $u_a \leftarrow U_r$ para a função extratora $g(\cdot; u_a)$ e a aplica em sua amostra x_A, obtendo $\mathsf{Ext} = (x_A; u_a)$. Sendo v a informação que Alice deseja se comprometer, a sequência obtida como saída da função extratora é então usada como chave de uma cifra one-time-pad, computada por Alice como sendo $\mathsf{C_{comp}} = \mathsf{Ext} \oplus v$. Então, Alice envia para Bob u_a e $\mathsf{C_{comp}}$. Com alta probabilidade, Bob não será capaz de obter informação sobre o comprometimento v, devido ao XOR entre o comprometimento e a saída da função extratora, que é aleatória, tornando a operação incondicionalmente segura.

A intuição por trás da aplicação da função extratora está em ampliar a incerteza de Bob sobre a amostra x_A de Alice, sendo necessário, portanto, compactar a amostra para eliminar os bits conhecidos por Bob e as possíveis redundâncias, tornando o resultado da extração, sob o ponto de vista de Bob, uma variável aleatória com distribuição ϵ-próxima de uniforme, para ϵ quão pequeno se queira. A quantidade de bits do comprometimento v tem que ser no máximo igual à da saída da função extratora para que o esquema seja incondicionamente seguro, embora seja possível obter comprometimentos de maior tamanho se a segurança desejada for apenas computacional.

A terceira fase é chamada de **Fase de Abertura**. Quando executada, Alice envia para Bob x'_A e v'. Então, Bob verifica se as posições que Alice afirma ter amostrado correspondem aquelas também amostradas por ele, ou seja, $(x'_A)_C = (x_B)_C$. Além disso, ele verifica se o hash enviado anteriormente corresponde ao da amostra enviada por Alice, $g(x'_A; u_b) = \mathsf{Hash}$, e verifica se a informação que Alice afirma ter se comprometido é consistente com os vestígios recebidos anteriormente, ou seja, $v' = \mathsf{C_{comp}} \oplus g(x'_A; u_a)$. Finalmente, após concluir todas essas verificações, caso não ocorram falhas nesse processo de detecção de trapaça, Bob "aceita" o resultado da fase de abertura como comprometimento de Alice.

A seguir, tem-se um esquema que sintetiza os detalhes do protocolo de comprometimento de bit descrito anteriormente:

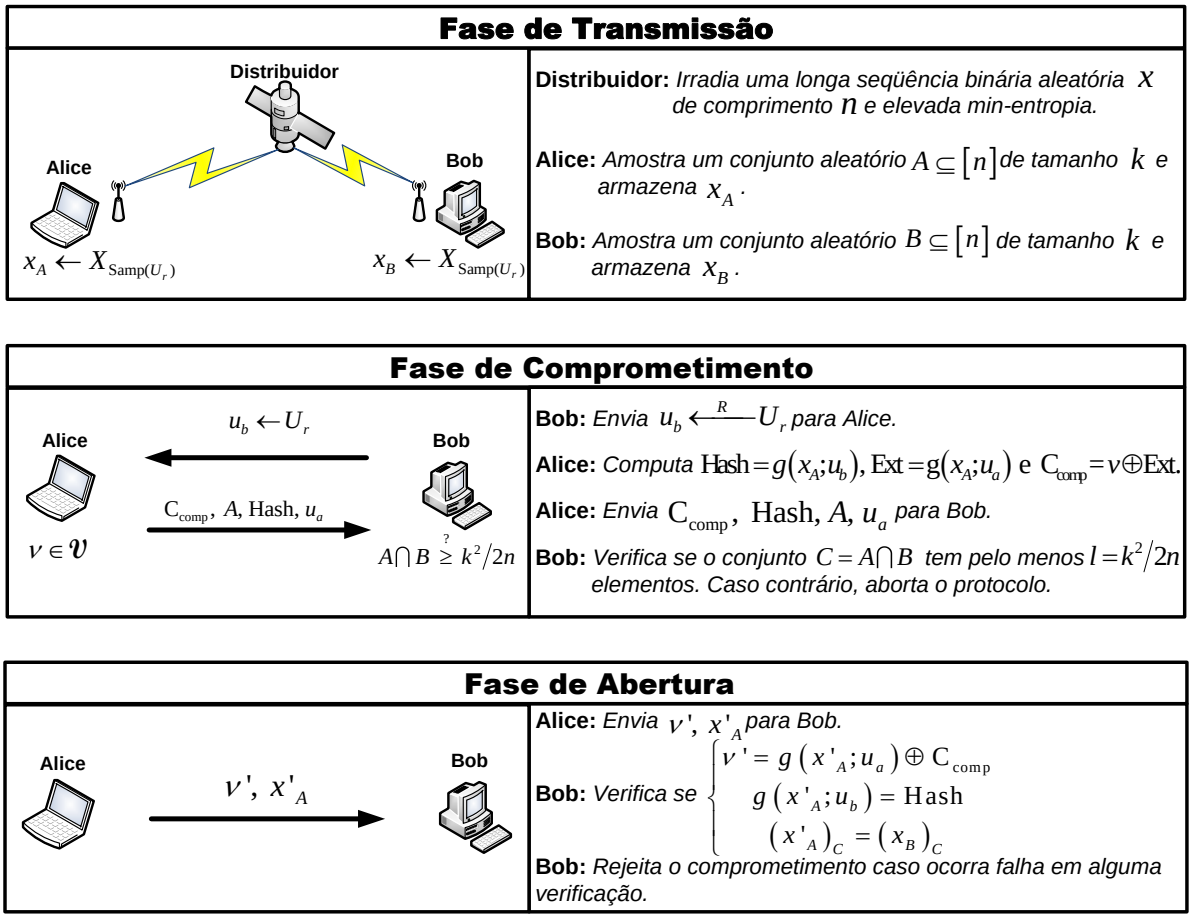

Figura 3.1: Esquema do protocolo de comprometimento de bit proposto.

3.3 Algoritmos em detalhes

Para melhor compreensão do protocolo, uma apresentação detalhada dos algoritmos usados na computação feita pelos participantes durante a execução do protocolo de comprometimento é feita a seguir, sendo esses algoritmos vistos como subrotinas chamadas durante o processamento feito por Alice e Bob em suas máquinas de Turing probabilísticas.

O algoritmo 1 apresenta uma possível construção para $g(\cdot;\cdot)$, a função de hash 2-univeral usada no protocolo, com saída de tamanho m. Assuma que p é um número primo publicamente conhecido, o qual estabelece a família de funções de hash a ser usada. A seguir, temos a especificação do funcionamento desse algoritmo:

Algorithm 1 $g(x;u)$: Computa a função de hash 2-universal da sequência binária x.

Require: $x \in \{0,1\}^n$, $u \leftarrow U_r$ e $p \in_R \mathbb{G}$, onde $|p| = m$.

Ensure: O valor do hash $\mathsf{Hash} = g(x;u)$ de tamanho fixo $|\mathsf{Hash}| = m$.

$s||t \leftarrow u$

$\mathsf{Hash} = s \cdot x + t \bmod p$

return Hash

O algoritmo 2 apresenta uma possível construção para a função Samp, e para isso implementa um *expander graph* e faz uso de caminhadas aleatórias por esse grafo para gerar as posições do subconjunto de $\mathcal{S} \subset_R [n]^k$, usando uma semente com $O(t + \log n)$ bits, onde t é uma variável relacionada com a probabilidade de falha do amostrador mediano.

Algorithm 2 $\mathsf{Samp}(u)$: Gera um subconjunto $\mathcal{S} \subset_R [n]^k$.

Require: k, $u \leftarrow U_{O(t+\log n)}$ e $p \in_R \mathbb{G}$, onde $|p| = O(k)$.

Ensure: Uma lista de k posições aleatórias, $\mathcal{S} = \{s_1, s_2, \ldots, s_k\}$.

Seja $\boldsymbol{G}(V,E)$ o grafo expansor.

$V \subset \mathbb{Z}_p$

$x \neq 0 \Rightarrow, E_0(x, x-1), E_1(x, x+1)$ e $E_2(x, x^{-1})$.

$x = 0 \Rightarrow E_1(0,0), E_2(0,1)$ e $E_3(0, p-1)$.

$Y_0||D[t] \leftarrow u$

$Y := Y_0$

$e := E_j$

$l := 0$; $i := 0$; $j := 0 \bmod 3$

repeat

  if $D[i] = 0$ **then**

    $j{+}{+} \bmod 3$

  else

    $s_l \leftarrow e(Y)$,

    $l{+}{+}$

  end if

  $i{+}{+} \bmod t$

until $l = k$

$\mathsf{S} \leftarrow \{s_1, s_2, \ldots, s_k\}$

return S

3.4 Limites Teóricos

A seguir, os limites nas complexidades computacional e de comunicação presentes na família dos protocolos de comprometimento de bit baseados no modelo de memória limitada são provados. A primeira cota apresentada vem de trabalhos anteriores que estudaram a viabilidade de protocolos de comprometimento de bit baseados em dados pré-distribuidos [NMQO+03], [Riv99].

Lema 3.1. *A probabilidade média de Alice trapacear $\bar{\xi}$ é limitada inferiormente por $2^{-H(X_b|X_a)}$.*

Prova: É claro que se Alice puder chutar corretamente os dados X_b obtidos por Bob, ela deve ser capaz de trapacear com sucesso, uma vez que a segurança do protocolo se baseia no sigilo das variáveis X_a, X_b. Como a única informação que Alice possui para auxiliá-la na tentativa de descobrir X_b é a sua própria amostra X_a, já que a única mensagem enviada por Bob independe de sua amosta, então sua incerteza sobre a amostra de Bob é $H(X_b|X_a)$. Sendo a entropia de Shannon uma medida assintótica, então a probabilidade média de erro de Alice ao tentar advinhar os dados secretos de Bob é limitada inferiormente por:

$$\bar{\xi} \geq 2^{-H(X_b|X_a)}$$

■

Outra forma de visualizar esse limite no modelo proposto está no fato de a verificação realizada por Bob, ao final da fase de abertura, ser entendida como um teste de hipóteses. Assim, suponha que o receptor do comprometimento deseja distinguir entre duas situações:

- O emissor se comporta honestamente, hipótese Λ_0.
- O emissor tenta trapacear, hipótese Λ_1.

Seja $(X_a, X_b|T)$ a variável aleatória que representa as informações de Alice e Bob honestos, dadas as mensagens trocadas entre eles. No caso da hipótese Λ_0, denota-se por $C_{(X_a,X_b|T)}$ a distribuição de probabilidade verdadeira, gerada pelas especificações do protocolo. Para a hipótese Λ_1 é gerada outra distribuição de probabilidade $E_{(X'_a,X_b|T)}$, a qual representa uma estratégia arbitrária de trapaça de Alice. A seguir, prova-se que

Proposição 3.1. *Em qualquer esquema de comprometimento be bit baseado no modelo de memória limitada, o emissor sempre tem uma probabilidade média de trapaçear maior ou igual a:*

$$\bar{\rho} \geq 2^{-I(X_a;X_b)}$$

Prova: Lembrando que ρ é igual a probabilidade de que ocorra um falso positivo, ou seja, Bob aceite um comprometimento desonesto de Alice, e η é igual a probabilidade de

que ocorra um falso negativo, ou seja, Bob rejeite um comprometimento honesto de Alice. Fazendo $C_{X|V=v}(x|v) = P_{X_a,X_b|T}$ e $E_{X|V=v}(x|v) = P_{X'_a}P_{X_b|T}$ no teorema em 2.2, segue que:

$$\mathsf{d}(\bar{\eta}||1-\bar{\rho}) \leq \sum_{t\in\mathcal{T}} P_T(t) \sum_{x_a,x_b\in\mathcal{X}} P_{(X_a,X_b|T)}(x_a,x_b|t) \log \frac{P_{(X_a,X_b|T)}(x_a,x_b|t)}{P_{X'_a}(x'_a)P_{X_b|T}(x_b|t)}$$

$$\mathsf{d}(\bar{\eta}||1-\bar{\rho}) \leq I(X_a;X_b|T)$$

Entretanto, pode-se assumir que a comunicação sem ruído T não fornece informação alguma a Alice sobre os dados de Bob no protocolo proposto, uma vez que a única mensagem enviada por Bob à Alice é uma semente com distribuição uniforme, logo independente de X_b. Então:

$$I(X_a;X_b|T) = I(X_a;X_b)$$

Usando a definição $\mathsf{d}(\bar{\eta},1-\bar{\rho})$ apresentada anteriormente, segue que:

$$\eta \log \frac{\eta}{1-\rho} + (1-\eta)\log\frac{1-\eta}{\rho} \leq I(X_a;X_b)$$

A partir da condição de corretude do esquema de comprometimento de bit, tem-se que $\lim_{n\to\infty}\eta \to 0$, sendo n o parâmetro de segurança. Logo, tem-se que:

$$\log\frac{1}{\rho} \leq I(X_a;X_b)$$

$$\therefore \bar{\rho} \geq 2^{-I(X_a;X_b)}$$

o que prova o resultado. ■

Segue da proposição anterior que, se os dados amostrados por Alice e Bob durante a fase de transmissão não forem correlacionados, qualquer esquema de comprometimento de bit é impossível. A partir de resultados que tratam sobre a capacidade de comprometimento em sistemas sem memória presentes em [WNI03], é possivel obter também o seguinte limite ótimo no tamanho da sequência binária com a qual Alice pode se comprometer:

Proposição 3.2. *Em um esquema de comprometimento no modelo de memória limitada,*

$$\log|\mathcal{V}| \leq H(X_a|X_b)$$

Trabalhos anteriores sobre o modelo de memória limitada demonstraram que no cenário de estabelecimento de chaves (key agreement) Alice e Bob têm que armazenar pelo menos $\sqrt{n}$, sendo n o tamanho da sequência binária irradiada. Esse resultado se estende trivialmente para o caso de Oblivious Tranfer, já que OT implica em estabelecimento de chaves [Kil88]. Demonstra-se que a mesma cota existe também para protocolos de comprometimento de bit baseados no modelo de memória limitada. A prova apresentada se assemelha aquela presente em [DM08]. Inicialmente, introduzir-se-á uma definição e um lema auxiliar, presentes em [DM08].

Definição 3.1. *Uma lista $Z_0, \cdots, Z_n$ de variáveis aleatória é simétrica com relação à variável aleatória Y se para cada sequência $i_1, \ldots, i_w$ e $i'_1, \ldots, i'_w$, tem-se $P_{Y,Z_{i_1},\cdots,Z_{i_w}} = P_{Y,Z_{i'_1},\cdots,Z_{i'_w}}$ para todo $y, z_1, z_2, \cdots, z_w$.*

A seguir, introduz-se o lema sobre a simetria entre variáveis aleatórias e a informação mútua entre elas.

Lema 3.2. *Se $Z_0, \cdots, Z_n$ são simétricos com relação à Y, então existe $i \in \{0, \ldots, n\}$ tal que:*

$$I(Y; Z_0 | Z_1, \ldots, Z_i) \leq \frac{H(Y)}{n+1}$$

Além disso, fora observado em [DM08] que, se $Z_0, \cdots, Z_n$ são simétricos com relação a Y, então $Z_0, \cdots, Z_n$ são simétricos com relação a qualquer função arbitrária $f(Y)$.

Para provar que um limiar semelhante vale para esquemas de comprometimento baseados no modelo de memória limitada, apresenta-se um modelo para o comportamento de um receptor malicioso.

Assuma Alice honesta, que ao final da fase de transmissão armazena X_a, enquanto Bob malicioso armazena $X_{b_1}, \cdots, X_{b_{\frac{\nu n}{k}}}$, onde $X_{b_i}, 1 \leq i \leq \frac{\nu n}{k}$ são $\frac{\nu n}{k}$ instâncias independentes e aleatórias representando o que um participante honesto poderia armazenar durante a fase de transmissão.

Inicialmente, nota-se que $X_{b_1}, \cdots, X_{b_{\frac{\nu n}{k}}}$ são simétricas em relação a X_a. Então, tem-se que existe algum i tal que

$$I(X_a; X_{b_1} | X_{b_2}, \cdots, X_{b_i}) \leq \frac{H(X_a)}{\frac{\nu n}{k} + 1}$$

Como $I(X_a; X_{b_1} | X_{b_2}, \cdots, X_{b_i}) \geq I(X_a; X_{b_1})$ e Alice honesta armazena no máximo k bits, portanto $H(X_a) \leq k$. Logo,

$$I(X_a; X_{b_1}) \leq \frac{k}{\frac{\nu n}{k} + 1} \leq \frac{k^2}{\nu n}$$

Uma vez que essa estratégia é válida para o adversário suposto, que se comporta da forma mais simples possível, então ela é válida para qualquer outro comportamento malicioso mais elaborado. Assim, para se obter uma probabilidade de trapaça desprezível, os participantes devem armazenar pelo menos $\sqrt{n}$ bits durante a fase de transmissão. Com isso, prova-se o seguinte:

Lema 3.3. *Seja um adversário ilimitado em todos os aspectos, exceto por uma restrição na sua capacidade de armazenamento durante a transmissão de uma sequência aleatória inicial. Então, para todo protocolo de comprometimento de bit baseado no modelo de memória limitada, onde a sequência transmitida inicialmente tem tamanho n e os participantes honestos armazenam uma amostra de k bits, a probabilidade de o adversário conseguir trapacear será desprezível sempre que os participantes honestos armazenarem pelo menos $k = O(\sqrt{n})$.*

Capítulo 4

Análise de Segurança

Esse capítulo apresenta as provas de segurança do protocolo proposto, demonstrando a realização do comprometimento de bit com segurança incondicional para ambos os participantes. Isso implica em satisfazer as condições de corretude do protocolo, de segurança para o destinatário e de segurança para o remetente. As condições são satisfeitas estatísticamente, existindo, portanto, uma probabilidade de falha, embora desprezível, em cada fase do protocolo.

4.1 Visão Geral da Prova de Segurança

A segurança do protocolo de comprometimento de bit proposto se fundamenta no conceito de segurança baseada em lista. Assim, pretende-se demonstrar que o esquema é seguro desde que certas propriedades fundamentais, apresentadas numa lista, sejam garantidas. Embora essa seja a forma mais comum de se provar a segurança de protocolos, há um conceito mais geral que baseia a prova de segurança em simuladores.

A grosso modo, a prova de segurança baseada em simuladores estabelece que um adversário, ao lidar com o simulador, não consegue distinguir entre interações em uma situação real e em uma situação ideal. Sendo o protocolo seguro na situação ideal, então ele também será seguro na situação real, uma vez que a indistinguibilidade perante à atuação do simulador implica no fato de o adversário não ter mais poderes nessa do que naquela situação.

A metodologia de prova nesse distinto paradigma baseado em simuladores é, no entanto, bastante complexa e exige que se possa definir de modo rigoroso o comportamento de uma funcionalidade ideal de comprometimento de bit, a qual define o funcionamento do protocolo no caso ideal, exigindo a aplicação de um conjunto de ferramentas matemáticas elaboradas

especificamente para esse fim [Can01]. Com isso, preferiu-se utilizar a metodologia clássica de prova, baseada em lista, para o esquema de comprometimento de bit proposto, que é suficiente para a maior parte das situações de interesse.

Assim sendo, precisa-se entender quais são essas propriedades e porque quando satisfeitas elas garantem a segurança do esquema de comprometimento de bit. A idéia por trás da prova de segurança clássica se assemelha à baseada em simuladores. O que se pretende é constituir um cenário no qual o esquema seja seguro e, a partir dessa situação ideal, derivar as propriedades fundamentais que o tornam seguro. Então, conjectura-se que o esquema real que detenha essas propriedades fundamentais é da mesma forma seguro. A partir dessa premissa, a prova consiste em demonstrar que o funcionamento dos protocolos práticos asseguram a existência das propriedades listadas.

Nos esquemas de comprometimento ideais, a característica de segurança mais simples que o protocolo deve apresentar é o funcionamento adequado quando os participantes são todos honestos. É evidente que qualquer protocolo, para ser seguro, tem que ser infalível quando todos os participantes seguem as regras. essa característica é capturada pela propriedade fundamental chamada de *correctness*, ou corretude do protocolo. No esquema de comprometimento de bit proposto, mostrar-se-á que quando os participantes seguem o protocolo este irá funcionar corretamente a menos de uma probabilidade desprezível de falha, que decresce exponencialmente em k, o tamanho da memória dos participantes honestos.

Outra característica que um esquema de comprometimento ideal deve apresentar é a segurança dos participantes honestos na presença de participantes maliciosos. Nesse caso, como estamos tratando de uma computação segura de duas partes, temos duas situações distintas, sendo a segurança do remetente quando o destinatário é malicioso e a segurança do destinatário quando o remetente é malicioso. O primeiro caso é quando Alice vai se comprometer com v e Bob é malicioso, ou seja, tentará descobrir o valor v antes do final do protocolo. O segundo caso é quando Alice é maliciosa e tenta se comprometer com Bob, que se comporta honestamente, enviando-lhe dados na fase de comprometimento que a permita revelar v e v' distintos na fase de abertura. Observe que os esquemas de comprometimento não precisam garantir absolutamente nada quando ambos os participantes são desonestos, uma vez que o sentido de segurança só é relevante para as partes honestas.

4.2 Definições de Segurança

Neste tópico se definirá a segurança de um protocolo de comprometimento de bit. Um protocolo de comprometimento de bit deve satisfazer certas condições para ser seguro. A seguir, tem-se a descrição dessas condições de segurança em termos do comportamento dos participantes:

- **Correctness**: *Se ambos os participantes são honestos, então Bob aceita o compro-*

metimento de Alice.

- **Hiding**: *Se Alice é honesta e Bob malicioso, então a execução da fase de comprometimento não revela informação sobre o comprometimento v de Alice para Bob.*
- **Binding**: *Se Bob é honesto e Alice maliciosa, então existe apenas um valor v que Alice consegue revelar na fase de abertura aceito por Bob como válido.*

De modo mais formal, pode-se definir matematicamente a segurança de um protocolo de comprometimento de bit. Sejam X_a e X_b as variáveis aleatórias que representam as sequências de comprimento k amostradas por Alice e Bob, respectivamente, X a variável aleatória que modela a fonte transmissora da sequência aleatória, $v \in \mathcal{V}$ o valor que Alice deseja se comprometer e $t \in \mathcal{T}$ as mensagens trocadas entre Alice e Bob. Assumir-se-á que $\mathsf{Test} : \{0,1\}^k \times \{0,1\}^k \times \mathcal{T} \times \mathcal{V} \to \{\text{ACK}, \text{NEG}\}$ é uma função conhecida publicamente e permite a Bob verificar a validade do comprometimento de Alice, assim como checar se há posições coincidentes suficientes entre os subconjuntos amostrados, ainda durante a fase de comprometimento. Logo, tem-se que:

Definição 4.1. *Um protocolo de comprometimento de bit baseado no modelo de memória limitada é (φ, μ, β)-seguro se, e somente se, satifaz as seguintes condições:*

- *φ-Correctness: Se Alice e Bob são honestos, então o comprometimento de Alice será aceito por Bob com alta probabililidade.*

$$\Pr[\mathsf{Test}(x_a, x_b, t, v) = \text{ACK}] \geq 1 - \varphi$$

- *μ-Hiding: Se Alice é honesta, então uma quantidade desprezível de informação sobre v é revelada para Bob na fase de comprometimento.*

$$I(V; view_B) \leq \mu$$

- *β-Binding: Se Bob é honesto, a probabilidade de Alice conseguir trapacear sem ser detectada é pequena.*

$$\Pr[\mathsf{Test}(x_a, x_b, t, v) = \text{ACK} \wedge \mathsf{Test}(x'_a, x_b, t, v') = \text{ACK}] \leq \beta$$

Um protocolo de comprometimento é dito incondicionalmente seguro se φ, μ e β são desprezíveis em função do parâmetro de segurança k.

4.3 Prova de Corretude do Protocolo

Essa prova consiste em mostrar que o esquema proposto funciona quando as partes seguem o protocolo. Conforme descrição apresentada na seção 3.2, o protocolo aborta

quando falha em ao menos uma das verificações realizadas por Bob. As verificações feitas por Bob na fase de abertura resultam da aplicação de funções de hash 2-universal sobre os valores informados por Alice. Como, por definição, os participantes são honestos e a comunicação é autenticada e livre de ruído, então essas verificações feitas por Bob obtém sucesso com probalidade igual a 1, já que os valores enviados por Alice na fase de comprometimento correspondem aos enviados na fase de abertura.

Porém, o outro caso em que o esquema proposto pode falhar é na verificação feita por Bob durante a fase de comprometimento. enfatiza-se que nessa fase, após Alice anunciar suas posiçoes, existe uma chance de Bob abortar o protocolo. Isso decorre da possibilidade de Bob rejeitar as informações enviadas por Alice e parar a execução do protocolo caso as posições amostradas por ambos não coincidam em uma certa quantidade mínima previamente estabelecida, conforme os parâmetros públicos de segurança do protocolo.

Mesmo quando os participantes seguem as regras do protocolo, amostrando com distribuição uniforme posições de uma longa sequência binária transmitida por uma fonte de elevada aleatoriedade, existe a chance de não se obter uma quantidade desejada de interseções entre ambos os subconjuntos de posições amostradas. O valor esperado de posições coincidentes entre as amostras de Alice e Bob é $c = k^2/n$. Essas posições coincidentes, daqui para frente denominadas de colisões, têm probabilidade desprezível de ocorrerem em quantidade inferior a $c - \epsilon$, tendendo exponencialmente a zero no parâmetro ϵ, dada uma realização qualquer.

Com isso, é preciso mostrar que, embora exista a probabilidade de o número de colisões ser insuficiente, ela é desprezível em função do parâmetro de segurança. Como essa é a única situação em que pode falhar o esquema proposto, obtém-se a probabilidade de falha φ da condição de corretude, definida na seção anterior, baseada apenas nessa verificação efetuada por Bob, demonstrando-se que o esquema proposto funciona, com probabilidade tendendo a 1, quando os participantes seguem o protocolo.

Assim, dar-se-á início à prova de corretude apresentando um limite inferior de $O(\sqrt{n})$ no tamanho da memória dos participantes. Além disso, demonstra-se a otimalidade dessa cota, já que a probabilidade de ocorrerem colisões se torna desprezível quando as partes amostram uma quantidade de posições menor que essa, evidenciando a eficiência do esquema proposto, já que esse é o limiar mínimo para qualquer protocolo de comprometimento de bit baseado no modelo de memória limitada, conforme demonstrado no capítulo 3, seção 3.4.

Lema 4.1. *Sejam x_A e x_B sequências amostradas por Alice e Bob, respectivamente, a partir da transmissão de x feita pela fonte X, conforme o protocolo descrito na seção 3.2. A probabilidade de $|\mathcal{C}| = 0$ é limitada superiormente por e^{-2c}, sendo $c = k^2/n$ o valor esperado de colisões, n o comprimento da sequência x, em bits, e k o tamanho da memória dos participantes.*

Prova: Por hipótese, $\mathcal{A}$ e $\mathcal{B}$ são subconjuntos amostrados com distribuição uniforme por Alice e Bob, respectivamente, tendo cada um k posições escolhidas dentre as n da sequência x, e $\mathcal{C}$ o subconjunto das posições em colisão, ou seja, $\mathcal{C} = \mathcal{A} \bigcap \mathcal{B}$. Então, seja $W = |\mathcal{C}|$ a variável aleatória que modela a distribuição de probabilidade sobre a quantidade de colisões entre os subconjuntos amostrados pelos participantes, e W_j a variável aleatória que representa a ocorrência de colisão na j-ésima posição de x. A probabilidade que i posições dentre k amostradas por cada participante colidam é dada a seguir:

$$P_r[W = i] = \frac{\left(\begin{array}{c} k \\ i \end{array} \right) \left(\begin{array}{c} n-k \\ k-i \end{array} \right)}{\left(\begin{array}{c} n \\ k \end{array} \right)}$$

A expressão acima elucida que a probabilidade desejada é resultante de uma simples contagem. Inicialmente, os casos favoráveis são contabilizados, ou seja, efetua-se o produto entre a combinação de todas as possíveis i colisões dentre k posições amostradas e a combinação de todos os $k - i$ elementos restantes dentre as $n - k$ posições não amostradas de x. Então, divide-se os casos favoravéis pelos casos possíveis, ou seja, todos os subconjuntos de k posições dentre n disponíveis. Note que a probabilidade calculada acima não é uma desigualdade, o que permite obter um resultado mais preciso. Assim, a probabilidade de $W = |\mathcal{C}| = 0$ é dada por:

$$P_r[W = 0] = \frac{\left(\begin{array}{c} k \\ 0 \end{array} \right) \left(\begin{array}{c} n-k \\ k-0 \end{array} \right)}{\left(\begin{array}{c} n \\ k \end{array} \right)} = \frac{\left(\begin{array}{c} n-k \\ k \end{array} \right)}{\left(\begin{array}{c} n \\ k \end{array} \right)} = \frac{(n-k)!^2}{n!(n-2k)!}$$

Usando a aproximação de Stirling, tem-se que, quando o limite de n tende ao infinito, vale a igualdade a seguir:

$$\lim_{n\to\infty} P_r[W = 0] = \lim_{n\to\infty} \frac{2\pi \left(\frac{n-k}{e}\right)^{2(n-k)+1}}{\sqrt{2\pi n}\left(\frac{n}{e}\right)^n \sqrt{2\pi(n-2k)}\left(\frac{n-2k}{e}\right)^{n-2k}} = \lim_{n\to\infty} \frac{(n-k)^{2n-2k+1}}{n^{n+\frac{1}{2}}(n-2k)^{n-2k+\frac{1}{2}}}$$

Agora, colocando n em evidência, tanto na base quanto no expoente, obtém-se:

$$\lim_{n\to\infty} P_r[W = 0] = \lim_{n\to\infty} \left[\frac{\left(1-\frac{k}{n}\right)^{2\left(1-\frac{k}{n}\right)+\frac{1}{n}}}{\left(1-\frac{2k}{n}\right)^{1-\frac{2k}{n}+\frac{1}{2n}}} \right]^n$$

Lembrando que $\lim_{n\to\infty} \left(1+\frac{x}{n}\right)^n = e^x$, pode-se reescrever a expressão acima da seguinte forma:

$$\lim_{n\to\infty} P_r[W = 0] = \frac{e^{-k\left[2\left(1-\frac{k}{n}\right)+\frac{1}{n}\right]}}{e^{-2k\left[1-\frac{2k}{n}+\frac{1}{2n}\right]}} = \frac{e^{-k\left(-\frac{2k}{n}\right)}}{e^{-k\left(-\frac{4k}{n}\right)}} = e^{-\frac{2k^2}{n}}$$

Finalmente, $e^{-\frac{2k^2}{n}}$ irá para zero se $\frac{k^2}{n} >> 0$. Dado que o valor esperado de colisões c deve ser um valor inteiro maior que zero para que Bob não aborte o comprometimento, já que as sequências amostradas pertencem a um domínio discreto, então o valor $k \geq O(\sqrt{n})$ é um limite inferior no tamanho da memória dos participantes para que se tenha probabilidade desprezível de falha. Logo, isso prova que o protocolo proposto é ótimo, pois atinge o limiar demonstrado na seção 3.4.

Finalmente, demonstrar-se-á que o valor esperado de colisões corresponde, de fato, a taxa obtida no expoente da probabilidade calculada acima, ou seja, $E[W] = k^2/n$. A função esperança matemática de uma variável aleatória pode ser calculada conforme a seguir:

$$E[W] = \sum_{i=-\infty}^{\infty} i \cdot P_r[W = i] = \sum_{i=1}^{k} i \cdot \frac{\binom{k}{i}\binom{n-k}{k-i}}{\binom{n}{k}} \tag{4.1}$$

$$E[W] = \sum_{i=1}^{k} i \cdot \frac{\frac{k}{i}\binom{k-1}{i-1}\binom{n-k}{k-i}}{\frac{n}{k}\binom{n-1}{k-1}} \tag{4.2}$$

$$E[W] = \frac{k^2}{n} \sum_{i=0}^{k-1} \frac{\binom{k-1}{i}\binom{n-k}{k-i-1}}{\binom{n-1}{k-1}} = \frac{k^2}{n} \cdot \frac{\binom{n-1}{k-1}}{\binom{n-1}{k-1}} \tag{4.3}$$

$$E[W] = \frac{k^2}{n} \tag{4.4}$$

As etapas acima são tais que, em (4.1), utilizou-se a definição da função esperança matemática e se restringiu os limites da variável muda no somatório, já que quando $\{i < 0 \cup i > k\}$ temos $P_r[W = i] = 0$, e quando $i = 0$ temos o produto $i \cdot P_r[W = i] = 0$. Em (4.2) fora utilizada a *identidade de absorção*, conforme consta em [RLG94, Chapter 5, pages 157-159]. Por fim, em (4.3), aplicou-se a convolução de Vardermonde para resolver o somatório.

O próximo teorema estabelece que o protocolo proposto atende a condição de corretude, φ-*Correctness*, com probabilidade de falha φ desprezível, tendendo exponencialmente a zero no parâmetro de segurança c.

Teorema 4.1. *O esquema de comprometimento proposto satisfaz a condição de corretude, onde Bob aborta o protocolo apenas quando o número de colisões é menor do que $c/2$, com probabilidade de falha limitada superiormente por*

$$\varphi < \left(\frac{e}{2}\right)^{-c/2}$$

feita quão pequena se queira para c suficientemente grande.

Prova: Supondo inicialmente que o protocolo irá falhar apenas quando nenhuma colisão for detectada por Bob após Alice anunciar as posições que amostrou, então a probabilidade de falha φ será igual a probabilidade de que não haja colisões. Isso significa que $\varphi = P_r[W = 0] = e^{-2c}$, a qual decresce exponencialmente no parâmetro c.

Considerando um caso mais real, o protocolo irá falhar não só quando não houver colisão, mas também quando o número de colisões for menor do que um certo limiar. Assim, assumindo de forma geral que esse limiar inferior será dado por $c - \epsilon$ colisões, deve-se demonstrar que para valores razoáveis de $\epsilon > 0$ a probabilidade de Bob abortar o protocolo ainda será desprezível.

Uma questão que surge naturalmente é se o valor absoluto da variável aleatória W tende a permanecer em torno da esperança $E[W]$, o que é desejável para um funcionamento eficiente do protocolo. Essa questão pode ser respondida usando uma poderosa ferramenta de teoria da probabilidade, a desigualdade de Chernoff-Hoeffding. Devido sua importância, deduziu-se essa desigualdade neste trabalho, entretanto, a apresentação dessa prova foi deixada para o apêndice. A seguir, apresentamos o lema da desigualdade de interesse, cuja prova se encontra no apêndice I.3.

Lema 4.2 (A desigualdade de Chernoff-Hoeffding). *Sejam $X_1, X_2, \ldots, X_n$ variáveis aleatórias independentes com $P_r[X_i = 1] = p_i$, a probabilidade do i-ésimo evento ocorrer, e $P_r[X_i = 0] = 1 - p_i$, caso contrário. Seja $X = \sum_{i=1}^{n} X_i$ a quantidade de eventos ocorridos após n realizações independentes e seja $E[X]$ o valor esperado de ocorrências. Então, a seguinte desigualdade é válida para todo $0 \leq \delta < 1$:*

$$\Pr\left[X \leq (1-\delta)E[X]\right] < \left(\frac{e^{-\delta}}{(1-\delta)^{1-\delta}}\right)^{E[X]}$$

Trocando X por W na desigualdade acima, e realizando a mudança de variável $\epsilon = \delta E[W]$, pode-se utilizar essa relação como limite da probabilidade de falha do protocolo, obtendo-se um resultado positivo para o comportamento desejado. Assim, tem-se que:

$$\varphi = \Pr\left[W \leq c - \epsilon\right] < \left(\frac{c}{c-\epsilon}\right)^{c-\epsilon} \cdot e^{-\epsilon}$$

A relação acima mostra que a probabilidade de a variável aleatória W assumir um valor distante da esperança c decresce exponencialmente com o afastamento, representado por ϵ. Outro detalhe relevante sobre o comportamento dessa expressão está no fato de a probabilidade do número de colisões ser maior do que o valor esperado também diminuir exponencialmente em ϵ, o que pode ser visto como uma garantia para Alice que, com alta probabilidade, $E[W]$ é de fato o número de colisões conhecidas por Bob.

Para terminar a prova do teorema, basta calcular a probabilidade de W ser menor do que metade do valor esperado de colisões, ou seja, escolhendo $\epsilon = c/2$. Logo, segue que:

$$\Pr\left[W \leq c - \frac{c}{2}\right] < \left(\frac{c}{c-\frac{c}{2}}\right)^{c-\frac{c}{2}} \cdot e^{-\frac{c}{2}}$$

$$\varphi = \Pr\left[W \leq \frac{c}{2}\right] < \left(\frac{e}{2}\right)^{-c/2}$$

■

Para melhor entendimento da desigualdade obtida, segue um gráfico de seu comportamento em função de ϵ, para três valores de esperança distintos, sendo $c = 64$, $c = 256$ e $c = 1024$ bits. Nesse gráfico, o eixo das abcissas mede o afastamento percentual que a variável aleatória W adquire em relação ao valor esperado $E[W]$ e o eixo das ordenadas, a probabilidade que esse afastamento ocorra.

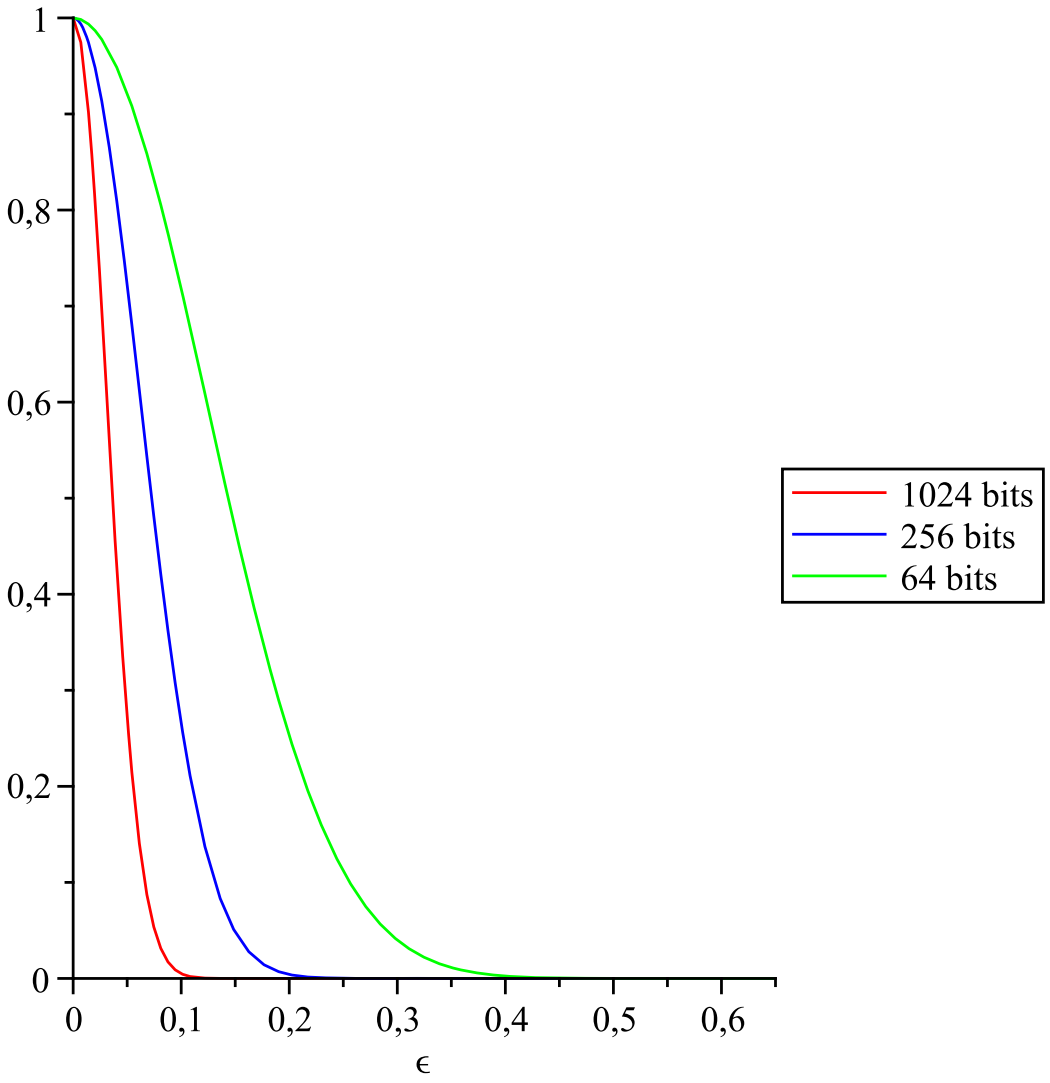

Figura 4.1: Desigualdade de Chernoff-Hoeffding para Afastamento do Valor Esperado.

De fato, percebe-se que o comportamento desse limite é exponencial em ϵ, podendo ser obtido um limite inferior ainda melhor para ϵ suficientemente grande. Entretanto, para valores próximos da média, a desigualdade de Chebyshev pode apresentar limite mais apertado. Um tratamento detalhado sobre esse assunto será apresentado no próximo capítulo.

4.4 Prova de Segurança para o Emissor

Nesta seção, demonstra-se a segurança de Alice quando Bob se comporta de modo malicioso, provando que ele obtém, com alta probabilidade, apenas uma quantidade desprezível de informação sobre o comprometimento dela. Essa prova consiste em mostrar que a sequência de bits obtida por Alice, ao aplicar uma função extratora sobre sua amostra, é estatísticamente indistinguível de uma sequência aleatória com distribuição uniforme para Bob. Com isso, Alice pode usar essa sequência como chave de uma cifra one-time-pad em seu comprometimento, tornando-o incondicionalmente seguro.

Bob conseguiria trapacear com sucesso caso não houvesse limite no tamanho de sua memória. Isso é evidente, já que ambos estariam de posse das mesmas informações, existindo uma condição de simetria entre eles. Nessa situação, Bob seria capaz de computar a sequência usada por Alice como chave da cifra, usando as mensagens trocadas na fase de comprometimento e a sequência X, armazenada integralmente. Entretanto, essa situação se assemelha à enfrentada por protocolos que limitam a capacidade de processamento do adversário, que pode quebrar o protocolo caso disponha de poder computacional superior à restrição imposta. Pórem, uma vantagem do modelo de memória limitada está em não precisar se basear em nenhuma hipótese matemática não provada, tal como a dificuldade de se fatorar o produto de numeros primos grandes ou o problema do logaritmo discreto, para obter a primitiva de comprometimento de bit, o que é recorrente nos protocolos baseados em restrição na capacidade de processamento. Outra vantagem desse modelo está no fato de o adversário ter restrição de armazenamento apenas durante a fase de transmissão, permitindo que ele adquira memória ilimitada após essa etapa, sem comprometer a segurança do protocolo. Além disso, o parâmetro de segurança do protocolo pode ser estimado a partir da razão do valor da informação pelo custo da memória necessária para o adversário quebrar o protocolo, o que torna mais clara e objetiva a escolha desse parâmetro.

No protocolo proposto, Bob não consegue trapacear ativamente porque sua interação com Alice se restringe ao envio de uma única mensagem, na fase de comprometimento, descrevendo a função de hash a ser utilizada por Alice. Contudo, o hash computado por Alice só serve para garantir a própria segurança de Bob, implicando que a mensagem enviada deve ser sorteada uniformemente, a fim de garantir maior segurança. No resto do protocolo, apenas Alice envia mensagens para Bob. Com isso, a melhor estratégia dele é tentar computar informações sobre o comprometimento com base nas mensagens recebidas. Todavia, como Alice cifra seu comprometimento via one-time-pad com uma chave ε-próximo da distribuição uniforme, independente do poder computacional que Bob tenha, a probabilidade de se obter alguma informação a partir desse comprometimento será limitada superiormente por uma probabilidade desprezível, proporcional a ε.

Como a única restrição sobre o participante malicioso é o limite no espaço de armazenamento durante a fase de transmissão, dado seu poder computacional ilimitado, pode-se

modelar a forma como o adversário amostra a sequência irradiada por meio da aplicação de uma função arbitrária, possivelmente ineficiente, com restrição apenas no tamanho de sua saída, que deve ser igual a $l = \nu\alpha n$, para todo $0 \leq \nu < 1$, sendo α a taxa de entropia por bit da fonte.

Assim, será demonstrado que o protocolo proposto atende a condição de *hiding*, garantindo a segurança do emissor honesto. Inicialmente, provar-se-á que a incerteza de Bob sobre X dado que obtém X_b, computada por meio da aplicação de uma função probabilística arbitrária sobre X, será limitada inferiormente por $(1-\nu)\alpha n - s$, tendo a fonte que irradia X min-entropia $H_\infty \geq \alpha n$. O proximo lema estabelece essa relação:

Lema 4.3. *Seja $f^* : \{0,1\}^n \rightarrow \{0,1\}^l$ uma função probabilística arbitrária (possivelmente ineficiente), que permite obter a amostra X_b a partir de X. Então, dado que $H_\infty(X) \geq \alpha n$ e $l = \nu\alpha n$, para todo $0 \leq \nu < 1$, tem-se que a incerteza sobre X dada a realização $f^*(x) = x_b$ será, com probabilidade pelo menos $1 - 2^{-s}$, limitada inferiormente por*

$$H_\infty(X|X_b = x_b) \geq (1-\nu)\alpha n - s$$

onde s é o parâmetro de segurança.

Prova: Essa prova se baseia no resultado apresentado no lema 2.2. A idéia está em mostrar que a incerteza sobre a variável aleatória X, de elevada min-entropia, dada a saída de uma função arbitrária Y aplicada sobre essa variável aleatória está limitada inferiormente, com alta probabilidade, pela diferença entre a min-entropia de X e o comprimento de Y.

Assim, invocando o lema 2.2, tem-se que X é uma αn-fonte, substitui-se Y por X_b, a saída da função probabilística arbitrária, e fazemos $\beta = s$. Logo, segue que:

$$H_\infty(X|Y = y) \geq H_\infty(X) - \log|\mathcal{Y}| - \beta$$

$$\therefore H_\infty(X|X_b = x_b) \geq \alpha n - \nu\alpha n - s$$

$$\therefore H_\infty(X|X_b = x_b) \geq (1-\nu)\alpha n - s$$

Com probabilidade $1 - 2^{-s}$, onde s é um parâmetro de segurança. ■

Fica claro da expressão acima que o tamanho da memória do adversário não deve exceder a min-entropia da fonte que irradia X para que o protocolo funcione e seja seguro. Além disso, esse resultado demonstra a incapacidade de Bob compactar toda a informação contida na sequência binária irradiada X em uma variável X_b menor, limitada ao tamanho de sua memória, com probabilidade tendendo exponencialmente para 1. Com isso, restará à Bob uma incerteza inerente acerca de X.

Agora, o próximo passo é provar que essa incerteza se conserva acerca de X_a, a amostra de Alice. É claro que a incerteza de Bob sobre X_a deve ser menor do que sua incerteza sobre X, uma vez que X_a é uma amostra muito menor do que X. Porém, o que se pretende

mostrar é que uma taxa de incerteza se conserva entre as duas variáveis, ou seja, a incerteza por bit que Bob tem em relação à X será aproximadamente a mesma em relação à X_a. O próximo lema captura essa intuição.

Lema 4.4. *Sejam X_a e X_b variáveis aleatórias correlacionadas, $view_B$ a variável aleatória que representa a visão de Bob sobre o protocolo e X a sequência irradiada por uma αn-fonte. Ainda, Seja $X_a = X_{\mathsf{Samp}(U_r)}$ a saída de um $\left(\alpha, \alpha - 3\tau, (\gamma + 2^{-q\tau n})^{1-\lambda}, (\gamma + 2^{-q\tau n})^{\lambda}\right)$-amostrador de min-entropia e assuma $X_b = f^*_{\{0,1\}^n \to \{0,1\}^l}(X)$ obtido de uma função probabilística arbitrária aplicada sobre X pelo adversário, onde $l = \nu\alpha n$. Assim, quando Alice se compromete com Bob seguindo o protocolo de comprometimento de bit proposto, a incerteza de Bob em relação à amostra de Alice é limitada inferiormente por:*

$$H_\infty^{\varepsilon+\varepsilon'}(X_a|view_B) > ((1-\nu)\alpha - \omega - s/n - 3\tau)\, k + \varepsilon' \log \varepsilon' - \log(1/\varepsilon)$$

onde s é um parâmetro de segurança positivo, k é o tamanho mínimo da memória dos participantes, $\varepsilon' = \frac{2^{-k}\left(2^{-s} + \left(\gamma + 2^{-q\tau n}\right)^{1-\lambda}\right)}{1 - 2^{-k}\left(2^{-s} + (\gamma + 2^{-q\tau n})^{1-\lambda}\right)}$ e $\varepsilon = 2^{-s}$.

Prova: Conforme o lema 4.3, sabe-se que $(1-\nu)\alpha - s/n$ é a taxa de incerteza por bit de Bob em relação à X, com probabilidade $1 - 2^{-s}$. Então, amostrar bits de X via aplicação de um amostrador de min-entropia, a função de amostragem $\mathsf{Samp}(U_r)$, para se obter $X_a = X_{\mathsf{Samp}(U_r)}$ faz com que a taxa de incerteza de Bob em relação à X se preserve em relação à X_a com probabilidade $1 - (\gamma + 2^{-q\tau n})^{1-\lambda}$, a menos de uma constante 3τ que pode ser feita quão pequena se queira, conforme o lema 2.4 obtido de um resultado central do trabalho de Vadhan [Vad03]. Assumindo a menor probabilidade de erro entre as anteriores, $1 - 2^{-s} - (\gamma + 2^{-q\tau n})^{1-\lambda}$, a min-entropia de X_a dada a realização $X_b = x_b$ é limitada inferiormente por:

$$H_\infty(X_a|X_b = x_b) \geq ((1-\nu)\alpha - s/n - 3\tau)\, k$$

com probabilidade maior ou igual a $1 - 2^{-s} - (\gamma + 2^{-q\tau n})^{1-\lambda}$.

Utilizando a versão ε-suave da entropia de Rényi, essa pequena probabilidade de falha pode ser absorvida de modo a se considerar uma fonte suavizada. Logo, combinando os lemas 4.1 e 4.2 apresentados em [RW05], segue que:

$$H_\infty^\epsilon(Z) \geq H_\alpha(Z) + \frac{\log(\epsilon)}{\alpha - 1} \geq H_\infty(Z) - \frac{\log(1-\epsilon)}{\alpha - 1} + \frac{\log(\epsilon)}{\alpha - 1}$$

Na expressão acima, $H_\alpha(Z)$ é a entropia de Rényi e α é a sua ordem. Assim, fazendo a substituição $(Z) = (X_a|X_b = x_b)$ e $\alpha = 1/\epsilon$, tem-se que:

$$H_\infty^\epsilon(X_a|X_b = x_b) \geq ((1-\nu)\alpha - s/n - 3\tau)\, k + \frac{\epsilon}{1-\epsilon} \log\left(\frac{\epsilon}{1-\epsilon}\right)$$

onde $\epsilon = 2^{-s} + (\gamma + 2^{-q\tau n})^{1-\lambda}$.

Com isso, sabe-se que a desigualdade anterior é valida para toda realização x_b, em especial para o valor de x_b particular que maximiza a min-entropia. Já que, mesmo no pior caso, a desigualdade deve permanecer válida, tem-se que:

$$\max_{x_b} H_\infty^\epsilon(X_a|X_b = x_b) \geq ((1-\nu)\alpha - s/n - 3\tau)\, k + \frac{\epsilon}{1-\epsilon}\log\left(\frac{\epsilon}{1-\epsilon}\right)$$

Aplicando o lema 5.2 definido em [RW05], sobre a min-entropia suave condicional, sabe-se o seguinte:

$$H_\infty^{p\epsilon}(X_a|X_b) \geq H_\infty^\epsilon(X_a|X_b = x_b)$$

onde $p := \Pr[X_b = x_b]$.

Assim, como a desigualdade é válida para x_b que maximiza, ela também vale para outro x_b qualquer. Assumindo que a probabilidade desse evento particular acontecer é dada por $p = 2^{-k}$, situação na qual Bob honesto obtém amostras equiprováveis, segue que:

$$H_\infty^{p\epsilon}(X_a|X_b) \geq ((1-\nu)\alpha - s/n - 3\tau)\, k + \frac{p\epsilon}{1-p\varepsilon}\log\left(\frac{p\varepsilon}{1-p\varepsilon}\right)$$

onde $p\epsilon = 2^{-k}\left(2^{-s} + (\gamma + 2^{-q\tau n})^{1-\lambda}\right)$.

Agora é possível obter a min-entropia suave da amostra X_a para Bob. Seja $view_B$ a variável aleatória que representa a visão de Bob sobre o protocolo. As aleatoriedades obtidas localmente não reduzem a incerteza de Bob em relação à X_a, pois são variáveis independentes. Logo, dentre as informações que Bob tem acesso, Apenas a sua amostra X_b e o Hash enviado por Alice podem reduzir sua incerteza sobre X_a. As posições amostradas por Alice também revelam informação para Bob acerca de X_a, porém esse dado está implícito no fato das amostras serem correlacionadas. A informação em $\mathsf{C_{comp}}$, por ser resultado de um XOR bit-a-bit, só pode auxiliar Bob a descobrir v quando ele conhece algum bit de $\mathsf{Ext} = g(x_A; u_a)$, o que ocorre com probabilidade desprezível ε.

Portanto, a incerteza de Bob sobre a amostra de Alice, dada sua visão do protocolo, pode ser obtida por:

$$H_\infty^{\varepsilon+\varepsilon'+\varepsilon''}(X_a|view_B) = H_\infty^{\varepsilon+\varepsilon'+\varepsilon''}(X_a|X_b, \mathsf{Hash}) > H_\infty^{\varepsilon'}(X_a, \mathsf{Hash}|X_b) - H_0^{\varepsilon''}(\mathsf{Hash}|X_b) - \log(1/\varepsilon)$$

Como a função Hash pode ser calculada a partir de X_a, assumindo que G é pública, e informação adicional somente reduz a máx-entropia suave, tem-se que:

$$H_\infty^{\varepsilon+\varepsilon'+\varepsilon''}(X_a|view_B) > H_\infty^{\varepsilon'}(X_a|X_b) - H_0^{\varepsilon''}(\mathsf{Hash}) - \log(1/\varepsilon)$$

Considerando que $|\mathsf{Hash}| = \omega k$, então $H_0^{\varepsilon''}(X) \leq H_0(X) \leq |\mathcal{X}|$, o que permite assumir $\varepsilon'' = 0$. Logo, substituindo o resultado obtido acima para a min-entropia condicional, fazendo $\varepsilon' = \frac{p\epsilon}{1-p\epsilon}$, obtém-se o resultado a seguir:

$$H_\infty^{\varepsilon+\varepsilon'}(X_a|view_B) > ((1-\nu)\alpha - s/n - 3\tau)\, k - \omega k - \log(1/\varepsilon) + \varepsilon' \log \varepsilon'$$

$$\therefore H_{\infty}^{\varepsilon+\varepsilon'}(X_a|view_B) > ((1-\nu)\alpha - \omega - s/n - 3\tau)\, k + \varepsilon' \log \varepsilon' - \log(1/\varepsilon)$$

onde $\log(1/\varepsilon)$ absorve a probabilidade de falha na aplicação da função extratora sobre a amostra de Alice. Em outros termos, ε representa a probalidade de Bob adivinhar a saída da função de hash 2-universal usada na extração de aleatoriedade. ■

Finalmente, demonstra-se que Alice consegue extrair de sua amostra, ao aplicar a função extratora forte de aleatoriedade, uma sequência binária que é, para Bob, indistinguível de uma sequência sorteada com distribuição uniforme. Com isso, esses bits podem ser usados como chave para cifrar o comprometimento de Alice. O próximo lema estabelece que os bits extraídos por Alice e uma sequência aleatória são 2^{-s}-próximos.

Lema 4.5. *Seja* Ext *uma função* $(k, \delta k, m, \varepsilon)$*-extratora forte que permite extrair* $m \leq H_{\infty}(X) - 2\log \varepsilon^{-1} + 2$ *bits de aleatoriedade de uma variável aleatória* X *com min-entropia* $H_{\infty}(X) \geq \delta k$*. Então, Alice consegue extrair* $m = ((1-\nu)\alpha - \omega - s/n - 3\tau)\, k - 3s$ *bits ao aplicar* Ext *em* X_a*, cuja distribuição de probabilidade é* $\mathsf{SD}(P_{\mathsf{Ext}(X_a),U_r}, P_{U_m,U_r}) \leq 2^{-s}$ *distante de uniforme na visão de Bob, para* s *um parâmetro de segurança positivo.*

Prova: Esse resultado é consequência direta da aplicação do lema leftover-hash 2.1, apresentado no capítulo 2, sobre a amostra de Alice para extração de bits ε-próximos de uma distribuição uniforme na visão de Bob. Assim, substituindo δk na função extratora pela min-entropia obtida no lema anterior, $((1-\nu)\alpha - \omega - s/n - 3\tau)\, k + \varepsilon' \log \varepsilon' - \log(1/\varepsilon)$, obtém-se o resultado desejado.

$$H_{\infty}^{\varepsilon+\varepsilon'}(X_a|view_B) - 2\log \varepsilon^{-1} + 2 = ((1-\nu)\alpha - \omega - s/n - 3\tau)\, k + \varepsilon' \log \varepsilon' - 3\log(1/\varepsilon) + 2$$

Com isso, realiza-se a substituição $\frac{p\varepsilon}{1-p\varepsilon} \log\left(\frac{p\varepsilon}{1-p\varepsilon}\right) = -2$, já que m pode assumir qualquer valor abaixo do limite superior estabelecido no lema 2.1, e a substituição $\varepsilon = 2^{-s}$. Logo, aplicando-se a definição 2.4 de extratores fortes de aleatoriedade é possível obter m da seguinte forma:

$$m = ((1-\nu)\alpha - \omega - s/n - 3\tau)\, k - 3s$$

Com isso, só falta mostrar que a distância estatística entre a sequência Ext obtida, de comprimento m, e uma variável aleatória U_m é no máximo ε. Aplicando-se, mais uma vez, a definição 2.4, tem-se que:

$$\begin{aligned} \mathsf{SD}(P_{\mathsf{Ext}(\mathsf{X_a}|\mathsf{view_B}),G}, P_{U_m,G}) &\leq \frac{1}{2}\sqrt{2^{-H_{\infty}^{\varepsilon+\varepsilon'}(X_a|view_B)+m}} = \frac{1}{2}\sqrt{2^{-2\log\varepsilon^{-1}+2}} \\ &\leq \frac{1}{2}2^{\log\varepsilon+1} = \varepsilon \end{aligned}$$

Finalmente, lembrando que $\varepsilon = 2^{-s}$, segue a prova do lema. ■

Uma forma similar de enunciar o resultado anterior, mas que permite avaliá-lo em termos da informação mútua entre as variáveis aleatórias envolvidas, pode ser feita usando o famoso

resultado conhecido como *Privacy Amplification*. A seguir, apresentar-se-á esse teorema, ligeiramente diferente daquele apresentado no teorema 3 em [BBCM95], na forma de um corolário do lema anterior, com a finalidade de apresentar o resultado de modo a satisfazer a condição de segurança para o emissor no protocolo proposto.

O teorema a seguir estabelece que, se Alice é honesta, então uma quantidade desprezível de informação sobre v é revelada para Bob na fase de comprometimento.

Teorema 4.2 (Privacy Amplification). *Seja* $X_a = X_{\mathsf{Samp}(U)} \in \{0,1\}^k$ *uma variável aleatória de min-entropia* $H_\infty(X_a) \geq \delta k$, *onde* Samp *é um amostrador de min-entropia, e seja* $X_b = f^*(X)$ *o resultado de uma função probabilística arbitrária aplicada sobre* X *que o adversário faz uso, com tamanho da saída restrito à* $\nu\alpha n$ *bits, para todo* $0 < \nu < 1$. *Além disso, seja* s *um parâmetro de segurança positivo. Se Alice escolhe* $\mathsf{Ext} = g(X_a; u_a)$ *como sua chave secreta, sendo* $m = ((1-\nu)\alpha - \omega - s/n - 3\tau)\, k - 3s$ *o tamanho da saída da função extratora e* g *escolhida uniformemente de uma classe* $\mathcal{G}$ *de funções de hash, então a quantidade média de informação que Bob tem sobre o segredo de Alice* V, *satisfaz a seguinte relação:*

$$I(V; view_B) \leq 2^{-s}$$

Prova: A informação mútua entre os dados que Bob possui e o comprometimento de Alice está relacionada à informação mútua entre as amostras e a comunicação realizada entre eles. Como Alice cifra o seu comprometimento via one-time-pad, A incerteza de Bob é maior ou igual à menor min-entropia dentre as variáveis V e X_a. Logo, assumindo que a incerteza de Bob sobre V é maior do que a sua incerteza sobre a amostra de Alice, dada sua visão do protocolo, tem-se que:

$$\begin{aligned} I(V; view_B) &= H(V) - H(V|view_B) \\ &\leq H_0(V) - H_\infty^{\varepsilon+\varepsilon'}(X_a|view_B) \\ &\leq m - ((1-\nu)\alpha - \omega - s/n - 3\tau)\, k + \varepsilon' \log \varepsilon' - \log(1/\varepsilon) \\ &= -2\log \varepsilon^{-1} \\ &= 2^{-s} \end{aligned}$$

Assim, Alice será capaz de extrair uma sequência ε-próxima de uniforme de tamanho $m = ((1-\nu)\alpha - \omega - s/n - 3\tau)\, k - 3s$, que poderá ser usada como chave para cifrar via one-time-pad seu comprometimento, sendo incondicionalmente seguro para Alice perante comportamentos maliciosos de Bob, exceto por uma probabilidade desprezível dada por $1 - (\gamma + 2^{-q\tau n})^{1-\lambda} - 2^{-s}$. Em média, a informação mútua μ entre a visão de Bob do protocolo e o comprometimento de Alice pode ser feita arbitrariamente pequena, em função do parâmetro de segurança s. ■

Uma análise mais detalhada desses parâmetros, de modo a avaliar questões como praticidade e eficiência, foi deixada para o capítulo 5.

4.5 Prova de Segurança para o Receptor

Para a última propriedade de segurança a ser satisfeita pelo protocolo proposto será provado que, com alta probabilidade, Alice não será capaz de reverlar mais de um valor, na fase de abertura, aceito por Bob como válido, quando ele segue as regras do protocolo honestamente.

Essa prova consiste em mostrar que a forma de Alice se comprometer com Bob, embora não vaze informação sobre seu valor secreto, a impede de mudar de idéia após o envio da informação vestigial à Bob na fase de comprometimento. Isso é possível devido ao uso da função de hash 2-universal aplicada sobre sua amostra e da divulgação das posições amostradas.

Essas informações possibilitam à Bob detectar, com alta probabilidade, qualquer tentativa maliciosa de Alice de forjar outra sequência como sendo sua amostra. Isso se deve ao hash da sequência forjada não bater com o hash que Bob possui, já que as funções de hash 2-universal têm probabilidade de colisão limitada superiormente pela cardinalidade de seu conjunto imagem. Outro impecílio está na quantidade de bits que Alice precisa modificar para forjar uma nova sequência cujo hash colida com o da amostra, podendo esse comportamento malicioso ser detectado por Bob devido às posições em claro da amostra de Alice que ele conhece.

O teorema a seguir estabelece que a probabilidade de Alice conseguir trapacear, quando Bob se comporta honestamente, é pequena em função do parâmetro de segurança k.

Teorema 4.3. *Se Bob segue honestamente as regras do protocolo proposto, então a probabilidade β de Alice trapacear com sucesso é limitada por*

$$2^{-(\alpha-3\tau)k} \leq \beta \leq e^{-\sigma c} + 2^{-\left(\omega - h(\sigma) - \frac{1}{2k}\log \sigma k\right)k}$$

Prova: O primeiro passo da prova é demonstrar o limite inferior. Dado que Bob não anuncia suas posições para Alice e segue o protocolo honestamente, realizando a amostragem $X_b = X_{\mathsf{Samp}(U_\tau)}$, então a incerteza de Alice sobre a amostra de Bob é dada por $H(X_b|X_a) = H(X_b) \geq H_\infty^\varepsilon(X_b) \geq (\alpha - 3\tau)k$, devido ao lema 2.4. Logo, fazendo uso do resultado apresentado no lema 3.1, segue o limite inferior.

Para demonstrar o limite superior, dividir-se-á a prova em duas partes. A primeira consiste em mostrar que se Alice forja sua amostra, modificando mais de σk posições, com alta probabilidade sua atividade maliciosa é detectada por Bob. A segunda consiste em provar que a probabilidade de Alice trapacear modificando menos de σk é exponencialmente pequena.

Seja $\Delta_j = 1$ quando Alice forja o j-ésimo bit de sua amostra e $\Delta_j = 0$ caso contrário. Além disso, seja $\Gamma_j = 1$ se Bob conhece o j-ésimo bit da amostra de Alice e $\Gamma_j = 0$ se não conhece. Agora, seja $Q = \sum_{j=1}^{k} \Delta_j \times \Gamma_j$ a variável aleatória que representa a quantidade de

bits forjados por Alice e detectados por Bob. A probabilidade de Alice conseguir modificar σk posições necessárias para forjar sua amostra sem ser detectada por Bob, que conhece pelo menos $c/2$ bits de sua amostra, é dada por:

$$\Pr[Q=0] = \frac{\begin{pmatrix} k-c/2 \\ \sigma k \end{pmatrix}}{\begin{pmatrix} k \\ \sigma k \end{pmatrix}} = \frac{(k-c/2)!\,(k-\sigma k)!}{k!\,(k-\sigma k-c/2)!}$$

$$\lim_{k\to\infty} \Pr[Q=0] = \lim_{k\to\infty} \frac{(k-c/2)^{k-c/2+\frac{1}{2}}\,(k-\sigma k)^{k-\sigma k+\frac{1}{2}}}{k^{k+\frac{1}{2}}\,(k-\sigma k-c/2)^{k-\sigma k-c/2+\frac{1}{2}}}$$

Na expressão acima foi utilizada a aproximação de Stirling e algumas simplificações foram feitas. A seguir, a variável k será colocada em evidência, tanto na base quanto no expoente, será aplicado o limite $\lim_{x\to\infty}\left(1+\frac{n}{x}\right)^x = e^n$, e será feita a substituição da igualdade assintótica pela desigualdade, uma vez que a aproximação de stirling adotada é uma cota superior. Logo, segue que:

$$\begin{aligned}
\lim_{k\to\infty} \Pr[Q=0] &= \lim_{k\to\infty} \left[\frac{\left(1-\frac{c/2}{k}\right)^{1-\frac{c/2}{k}+\frac{1}{2k}}\,(1-\sigma)^{1-\sigma+\frac{1}{2k}}}{\left(1-\sigma-\frac{c/2}{k}\right)^{1-\sigma-\frac{c/2}{k}+\frac{1}{2k}}} \right]^k \\
\Pr[Q=0] &\leq \frac{e^{-(c/2)\left[1-\frac{c/2}{k}+\frac{1}{2k}\right]} e^{-\sigma k\left[1-\sigma+\frac{1}{2k}\right]}}{e^{-(\sigma k+c/2)\left[1-\sigma-\frac{c/2}{k}+\frac{1}{2k}\right]}} \\
&\leq e^{-\sigma c}
\end{aligned}$$

O próximo passo é demonstrar que a probabilidade de Alice trapacear com sucesso modificando menos de σk bits de sua amostra é desprezível. Assim, seja x_i uma sequência qualquer e x_a uma realização qualquer de X_a, ambas de tamanho k. Se Alice modifica σk ou menos bits de sua amostra, então existe um conjunto Z formado pelas sequências vizinhas da amostra, tal que $Z = \{x_i | \mathsf{HD}(x_a, x_i) \leq \sigma k\}$. Ou seja, $|Z|$ é igual ao número máximo de sequências que podem resultar da tentativa de trapaça de Alice. Essa quantidade pode ser calculada a partir da seguinte expressão:

$$|Z| = \sum_{i=1}^{\sigma k} \begin{pmatrix} k \\ i \end{pmatrix}$$

O somatório de coeficientes binomiais geralmente é difícil de ser calculado e não apresenta expressões fechadas. Uma boa cota superior dessa soma pode ser encontrada em [Wor94], conforme proposição a seguir:

Proposição 4.1. *Seja $2 < a < b \in o(k)$. Então, para todo $\varepsilon > 0$ e k suficientemente grande, tem-se que*

$$\sum_{i=k/b}^{k/a} \begin{pmatrix} k \\ i \end{pmatrix} \leq \frac{(1+\epsilon)}{\sqrt{2\pi}} \left(\sqrt{k}(b-a) + \frac{ab}{\sqrt{k}}\right) \sqrt{\frac{1}{b^2(a-1)}} \left[a^{\frac{1}{a}} \left(\frac{a}{a-1}\right)^{\frac{a-1}{a}} \right]^k$$

Na expressão acima, ao substituir a por $1/\sigma$ e b por k, obtém-se a desigualdade desejada. Com isso, obtém-se o seguinte:

$$\sum_{i=1}^{\sigma k} \left(\begin{array}{c} k \\ i \end{array} \right) \leq \frac{(1+\epsilon)}{\sqrt{2\pi}} \left(\sqrt{k}(k - 1/\sigma) + \frac{k}{\sigma\sqrt{k}} \right) \sqrt{\frac{1}{k^2(1/\sigma - 1)}} \left[\left(\frac{1}{\sigma}\right)^{\sigma} \left(\frac{1}{1-\sigma}\right)^{1-\sigma} \right]^k$$

Fazendo a substituição $\epsilon = \sqrt{2\pi(1-\sigma)} - 1$ e observando que $\left(\frac{1}{\sigma}\right)^{\sigma} \left(\frac{1}{1-\sigma}\right)^{1-\sigma} = 2^{h(\sigma)}$, onde $h(\sigma)$ é a entropia binária definida na seção 2.2, a expressão anterior pode ser reescrita da seguinte forma:

$$\sum_{i=1}^{\sigma k} \left(\begin{array}{c} k \\ i \end{array} \right) \leq \sqrt{\sigma k} \ \cdot \ 2^{h(\sigma)k}$$

Enfim, levando em conta o fato que $\sqrt{\sigma k} = 2^{\frac{1}{2}\log \sigma k}$, o volume da hiperesfera de centro em x_a é cotada superiormente por:

$$\sum_{i=1}^{\sigma k} \left(\begin{array}{c} k \\ i \end{array} \right) \leq 2^{h(\sigma)k + \frac{1}{2}\log \sigma k}$$

Uma função de hash 2-universal, por definição, tem a probabilidade de colisão menor ou igual ao inverso da cardinalidade de sua imagem, ou seja, para x_1 e x_2 quaisquer sequências distintas $\Pr[g_u(x_1) = g_u(x_2)] \leq 2^{-\omega k}$. Com isso, quando Alice muda no máximo σk bits de sua amostra, a probabilidade de ocorrer colisão entre alguma sequência da hiperesfera e sua amostra será menor do que o produto da probabilidade de colisão do hash 2-universal por $|Z|$. Assim, tem-se que:

$$\Pr\left[g(x_a; u_a) = g(x_i; u_a) \ \forall \ x_i \in Z\right] \leq \sum_{x_i \in Z} P_r[g(x_a; u_a) = g(x_i; u_a)] \leq 2^{h(\sigma)k + \frac{1}{2}\log \sigma k} \times 2^{-\omega k}$$

$$\therefore \Pr\left[g(x_a; u_a) = g(x_i; u_a) \ \forall \ x_i \in Z\right] \leq 2^{-\left(\omega - h(\sigma) - \frac{1}{2k}\log \sigma k\right)k}$$

Como $\frac{1}{2k}\log \sigma k$ é desprezível em função de k, pode-se afirmar que essa probabilidade será pequena desde que $\omega > h(\sigma)$. Uma vez que esses são parâmetros de livre escolha, é possível tornar essa probabilidade arbitrariamente pequena, para k grande o suficiente.

Finalmente, se Alice conseguir trapacear em qualquer dos casos, então sua estratégia será bem sucedida. Assim, a probabilidade de Alice ser bem sucedida ao tentar trapacear é limitada superiormente por:

$$\beta \leq \Pr[Q = 0] + \Pr\left[g(x_a; u_a) = g(x_i; u_a) \ \forall \ x_i \in Z\right]$$

$$\therefore \beta \leq e^{-\sigma c} + 2^{-\left(\omega - h(\sigma) - \frac{1}{2k}\log \sigma k\right)k}$$

Para k grande o suficiente e $\omega > h(\sigma)$.

Por outro lado, demonstrou-se que essa probabilidade é no mínimo $2^{-(\alpha - 3\tau)k}$. Logo, segue que:

$$2^{-(\alpha - 3\tau)k} \leq \beta \leq e^{-\sigma c} + 2^{-\left(\omega - h(\sigma) - \frac{1}{2k}\log \sigma k\right)k}$$

o que prova o teorema. ■

Capítulo 5

Análise dos resultados

Neste capítulo é feita uma breve análise sobre as condições dos parâmetros do protocolo, de modo a demonstrar a existência de escolhas interessantes para casos práticos. Além disso, apresenta-se o exemplo de uma situação teórica de funcionamento do protocolo, com o intuito de elucidar questões como eficiência e restrições de desempenho.

5.1 Análise dos parâmetros

Considerando a tecnologia atual, um limite de 512 TeraBytes na memória de Bob parece bastante razoável. Atualmente, o custo para se adquirir essa quantidade de memória ainda é alto, sem contar as dificuldades quanto à mudança de local dos dispositivos físicos de armazenamento, a velocidade de leitura e escrita, espaço físico para acomodar esses dispositivos, dentre outras dificuldades relacionadas existentes.

Assim, suponha que o distribuidor irá fazer a transmissão de uma sequência binária de 2 PetaBytes, ou seja, 2^{54} bits. Isso quer dizer que o adversário pode ter uma memória de quase 2 petabytes, embora esteja se considerando uma restrição na memória do adversário de 512 terabytes de espaço para armazenamento de dados, não se assumindo limites na memória de processamento. Entretanto, faz-se importante explicar que o limite na memória só é necessário na fase de transmissão e como resultado final da computação que o adversário faz sobre a sequência transmitida, ou seja, ele pode armazenar toda a sequência, fazer o processamento que desejar, ocupando uma memória RAM muitas vezes maior do que o tamanho da própria sequência irradiada, mas deve armazenar um resultado restrito ao limite de memória imposto, além de apagar todos os dados de sua memória volátil após o processamento dessa função arbitrária sobre a sequência transmitida.

Dado que o link de transmissão utilizado pelo distribuidor opera na faixa dos 100 Gbps, taxa essa atualmente encontrada em backbones de fibra ótica com certa facilidade, a duração

da transmissão será de, aproximadamente, dois dias. Terminada a fase de transmissão, os participantes terão armazenado 4 GigaBytes de dados, a fim de obterem um valor esperado de 65536 bits de colisão entre suas amostras. Com isso, após Alice anunciar suas posições, Bob deve conhecer pelo menos 32768 posições em claro da amostra de Alice, caso contrário ele aborta o protocolo. A probabilidade de falha nessa fase, quando as partes seguem o protocolo, será no máximo $\varphi \leq (e/2)^{-c/2} \leq (1,36)^{-32768} \doteq 0$.

Para amostrar esses dados, cada participante honesto precisa de uma semente dada pela relação $r = \log k + O(\log m + \log(1/\epsilon))$ para a função extratora e $d = \log(n/t) + O(t_0 \cdot \log(1/\theta))$ para a função de amostragem. Isso implica em obter uma aleatoriedade local de $O(\sqrt{k}) \approx 1$ MegaByte para determinar uma caminhada aleatória por um grafo expansor que servirá para especificar as posições em que os bits devem ser amostrados e então aplicar o extrator localmente para se obter uma saída com distribuição 2^{-s}-próxima de uniforme, onde o parâmetro γ está relacionado com a probabilidade de falha do amostrador mediano. Esse fato é importante por dois motivos. Primeiro para garantir que o resultado da função extratora será realmente próximo de uniforme e que será possível computar esses dados em tempo polinomial. Segundo para se estabelecer uma relação de compromisso entre a complexidade computacional e a complexidade de comunicação. Note que ao invés de Alice enviar em claro o conjunto $\mathcal{A}$ das posições amostradas de X, ela pode enviar para Bob apenas a semente usada no algorítmo de caminhada aleatória pelo grafo, permitindo que Bob compute essas posições, já que a descrição da função Samp é pública.

Um importante parâmetro é o tamanho do hash que Alice envia para Bob. Ao mesmo tempo que esse hash garante a segurança de Bob, dificultando o trabalho de Alice para revelar uma sequência diferente da que amostrou, ele não pode ser muito grande, dado que quanto maior for o tamanho do hash, menor será o tamanho da sequência que Alice poderá se comprometer de forma segura. Precisa-se levar em conta o fato de que a probabilidade de Bob detectar Alice trapaceando por meio de bits que ela modifica é limitada superiormente por $e^{-\sigma c}$. Além disso, há a restrição $\omega > h(\sigma)$, obtida na seção da prova de segurança do receptor, que impõe a necessidade de a razão $|\mathsf{Hash}|/|X_a|$ ser maior que a entropia binária do percentual de bits que Alice precisa mudar para forjar X'_a. Assim, escolhendo a $\sigma = 1/2048$, tem-se que $e^{-65536/2048} = e^{-32} \approx 10^{-14}$ e a probabilidade de não haver outra sequência que colida dada por $2^{-\left(\omega - h(\sigma) - \frac{1}{2k}\log \sigma k\right)k} = 2^{-\left(\omega - 0{,}0060754 - 10^{-10}\right)\cdot 2^{35}} = 2^{-0{,}000005\cdot 2^{35}} \doteq 0$ para a escolha do parâmetro $\omega = 0,00608$. Ou seja, o tamanho do hash é algo em torno de $|\omega k| \approx 26$ MegaBytes. Com isso, a função de hash 2-universal que foi especificada como exemplo na seção 3.3 precisará de apenas 128Bytes de aleatoriedade para ser especificada, já que $r = \log 2^{35} + O(\log 2^{33} + \log(1/2^{-32})) \approx 35 + 16 \times 65 = 1075$ bits. Veja que essa função de hash garante que a probabilidade de colisão de $2^{-0{,}000005\cdot 2^{35}}$, efetivamente zero.

Já para especificar a função extratora, a aleatoriedade necessária será maior, caso seja usada a mesma função de hash 2-universal. Nesse caso, como o tamanho da saída do extrator deve ser o maior possível, pois será usada como chave do ciframento simétrico

utilizado no comprometimento, para alcançar a capacidade de comprometimento máxima do modelo, tem-se que $\delta \approx (1-\nu)\alpha - \omega - \epsilon$, onde α é a taxa de entropia da fonte, ν a taxa de armazenamento de Bob, ω a taxa de compressão da função de hash 2-universal e ϵ uma quantidade desprezível para n grande. Para esse exemplo, assumir-se-á como sendo $\alpha = 0,75$, $\nu = 0,25$, $\omega = 0,00608$ e $\epsilon = 10^{-5}$. Então, $\delta \approx 0,55$, ou seja, nesse caso algo em torno de 55% da quantidade de bits amostrada poderá ser usado para se comprometer, permitindo que Alice escolha uma sequência de pelo menos 2 GB de comprimento como seu comprometimento.

5.2 Comparando o desempenho das desigualdades

Uma última análise interessante está no detalhe comentado na prova de segurança da condição de corretude do protocolo, seção 4.3. O comportamento das desigualdades de Chebyshev e Chernoff-Hoeffding não implica que um seja uma assíntota para a outra em toda a extensão do limite de probabilidade. Isso pode ser observado com mais clareza no gráfico a seguir:

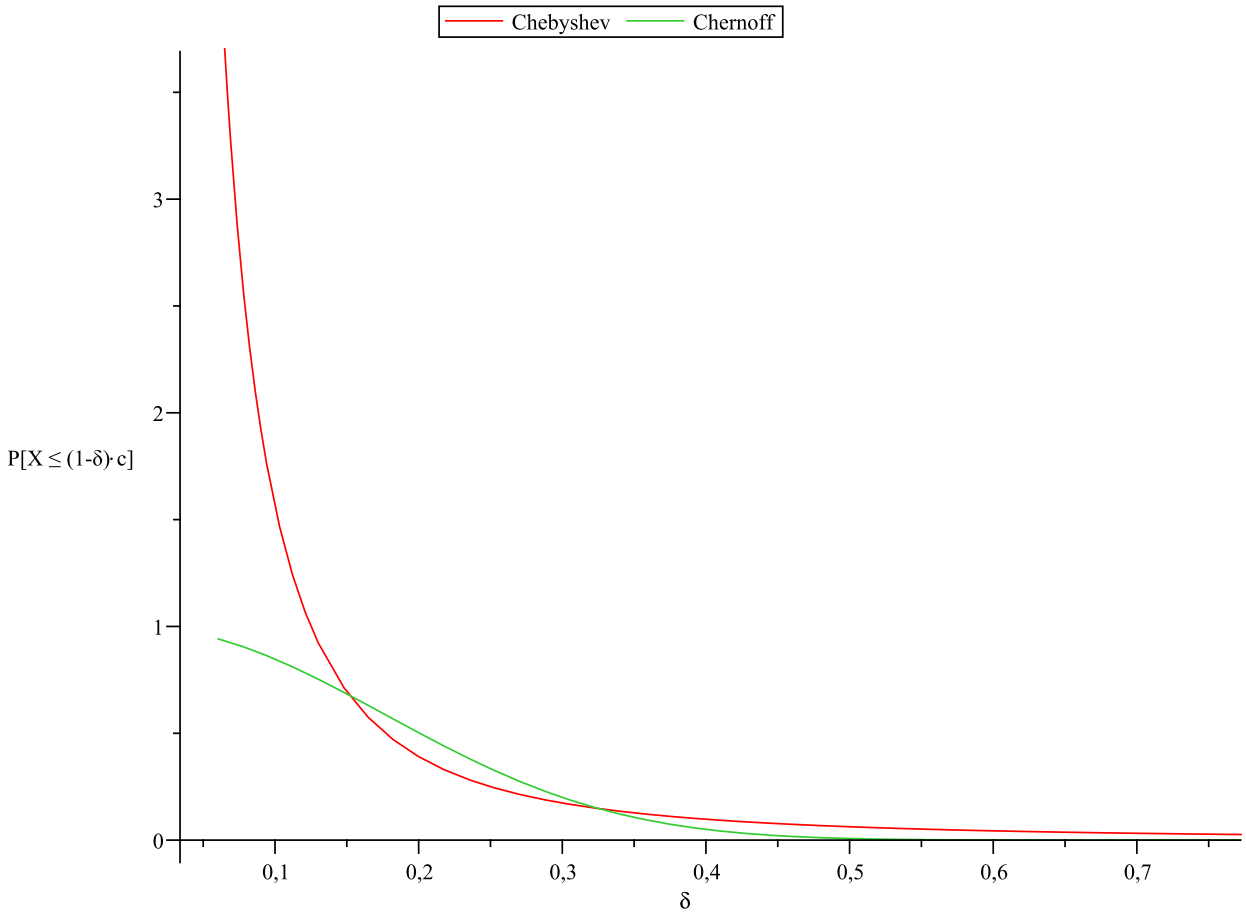

Figura 5.1: Comparação entre as desigualdades de Chebyshev e Chernoff.

Com isso, tornou-se importante deduzir os dois limites de probabilidade, já que num caso prático, é bem provavel que a escolha do parâmetro ϵ caia justamente na faixa em que a desigualdade de chebyshev limita de modo mais apertado a probabilidade de falha do que a desigualdade de Chernoff. A idéia é perceber que é possível optar sempre pela melhor situação entre os dois casos, ou qualquer outra desigualdade que surja futuramente melhorando ainda mais essas cotas, principalmente de forma não assintótica, como ocorre na maioria das aplicações. Contudo, esses limites, embora não sejam ótimos, são quase ótimos dado n, o parâmetro de segurança, suficientemente grande.

Capítulo 6

Conclusões

O presente trabalho propôs a elaboração do primeiro protocolo de comprometimento de bit baseado no modelo clássico de memória limitada. Para o funcionamento do protocolo, os participantes honestos precisam armazenar apenas $O(\log(n))$ bits dos n transmitidos por uma fonte de alta taxa de transmissão, o que se provou ser ótimo, ou seja, a probabilidade de falha cresce exponencialmente para valores menores. Embora o mesmo limite já tivesse sido provado para outras primitivas, como estabelecimento de chaves e OT, não era óbvio que o mesmo limite valeria para a primitiva de comprometimento, significativamente mais fraca.

Além disso, a segurança obtida é incondicional para ambos os participantes, não importando, portanto, o poder computacional que detêm. Inclusive, a restrição será apenas no espaço de memória durante a execução da primeira fase do protocolo, não sendo necessário impor nenhuma restrição em nenhum dos participantes após isso. Demonstrou-se também que a quantidade de bits que Alice pode se comprometer em cada execução atinge o limite superior, sendo essa quantidade dada pela incerteza de bob sobre a amostra de Alice, conceito denominado de equivocação em um contexto ligeiramente distinto do abordado no protocolo proposto.

Alguns aspectos do protocolo demonstraram ser bastante eficientes e práticos, já outros nem tanto. Devido ao fato que para o protocolo funcionar a quantidade de bits aleatórios irradiados deve ser maior do que a memória do adversário, a qual pode ser muito grande, há uma dificuldade inerente na transmissão desses dados, primeiro quanto a geração e segundo quanto a capacidade do canal para realizar esse tipo de transmissão. Contudo, considerando-se casos mais práticos, onde a memória do adversário não será tão grande, como é o caso de dispositivos RFID e smartcards, o modelo se torna bastante viável. As principais vantagens estão na simplicidade com que se pode implementar o protocolo, no nível de segurança obtido para os participantes e na eficiência do protocolo em termos da quantidade de bits que os participantes honestos precisam armazenar, limite provado como ótimo, e o tamanho do comprometimento de Alice, ótimo a menos de um fator constante.

Alguns aspectos que devem ser abordados posteriormente são a tentativa de se provar a segurança do protocolo no modelo de composição universal, baseado no paradigma da simulação, e uma natural generalização para o caso de múltiplos participantes. Além disso, relacionar os limiares obtidos para o caso clássico com o caso quântico, verificando se os mesmos existem, se são possíveis, ou se seria possível melhorá-los. Ainda, uma generalização do caso clássico com a ocorrência de ruído na transmissão e um adversário que tenha controle parcial sobre o canal usado para transmitir a longa sequência aleatória inicial. Enfim, essas são propostas que parecem pertinentes à realização de possíveis bons trabalhos futuros.

REFERÊNCIAS BIBLIOGRÁFICAS

[ADR02] Yonatan Aumann, Yan Zong Ding, and Michael O. Rabin, *Everlasting security in the bounded storage model*, IEEE Transactions on Information Theory **48** (2002), no. 6, 1668–1680.

[AR99] Yonatan Aumann and Michael O. Rabin, *Information theoretically secure communication in the limited storage space model*, CRYPTO (Michael J. Wiener, ed.), Lecture Notes in Computer Science, vol. 1666, Springer, 1999, pp. 65–79.

[BBCM95] Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Ueli M. Maurer, *Generalized privacy amplification*, IEEE Transactions on Information Theory **41** (1995), no. 6, 1915–1923.

[BBR88] Charles H. Bennett, Gilles Brassard, and Jean-Marc Robert, *Privacy amplification by public discussion*, SIAM J. Comput. **17** (1988), 210–229.

[BCC88] Gilles Brassard, David Chaum, and Claude Crépeau, *Minimum disclosure proofs of knowledge*, J. Comput. Syst. Sci. **37** (1988), no. 2, 156–189.

[Bla74] Richard E. Blahut, *Hypothesis testing and information theory*, Information Theory, IEEE Transactions on **20** (1974), no. 4, 405 – 417.

[Blu83] Manuel Blum, *Coin flipping by telephone a protocol for solving impossible problems*, SIGACT News **15** (1983), no. 4, 23–27.

[BR94] Mihir Bellare and John Rompel, *Randomness-efficient oblivious sampling*, FOCS, IEEE, 1994, pp. 276–287.

[Can01] Ran Canetti, *Universally composable security: A new paradigm for cryptographic protocols*, FOCS, 2001, pp. 136–145.

[CCM98] Christian Cachin, Claude Crépeau, and Julien Marcil, *Oblivious transfer with a memory-bounded receiver*, FOCS, 1998, pp. 493–502.

[CDvdG87] David Chaum, Ivan Damgård, and Jeroen van de Graaf, *Multiparty computations ensuring privacy of each party's input and correctness of the result*,

CRYPTO (Carl Pomerance, ed.), Lecture Notes in Computer Science, vol. 293, Springer, 1987, pp. 87–119.

[CEG95] Ran Canetti, Guy Even, and Oded Goldreich, *Lower bounds for sampling algorithms for estimating the average*, Inf. Process. Lett. **53** (1995), no. 1, 17–25.

[CG88] Benny Chor and Oded Goldreich, *Unbiased bits from sources of weak randomness and probabilistic communication complexity*, SIAM J. Comput. **17** (1988), no. 2, 230–261.

[CK88] Claude Crépeau and Joe Kilian, *Achieving oblivious transfer using weakened security assumptions (extended abstract)*, FOCS, IEEE, 1988, pp. 42–52.

[CM97] Christian Cachin and Ueli M. Maurer, *Unconditional security against memory-bounded adversaries*, CRYPTO (Burton S. Kaliski Jr., ed.), Lecture Notes in Computer Science, vol. 1294, Springer, 1997, pp. 292–306.

[Cré97] Claude Crépeau, *Efficient cryptographic protocols based on noisy channels*, EUROCRYPT, 1997, pp. 306–317.

[CV08] Kai-Min Chung and Salil P. Vadhan, *Tight bounds for hashing block sources*, APPROX-RANDOM (Ashish Goel, Klaus Jansen, José D. P. Rolim, and Ronitt Rubinfeld, eds.), Lecture Notes in Computer Science, vol. 5171, Springer, 2008, pp. 357–370.

[CW79] Larry Carter and Mark N. Wegman, *Universal classes of hash functions*, J. Comput. Syst. Sci. **18** (1979), no. 2, 143–154.

[Dam99] Ivan Damgård, *Commitment schemes and zero-knowledge protocols*, Lectures on Data Security, Modern Cryptology in Theory and Practice, Summer School, Aarhus, Denmark (London, UK), Springer-Verlag, 1999, pp. 63–86.

[DFSS05] Ivan Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner, *Cryptography in the bounded quantum-storage model*, FOCS, IEEE Computer Society, 2005, pp. 449–458.

[DH76] Whitfield Diffie and Martin E. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory **22** (1976), no. 6, 644–654.

[DHRS07] Yan Zong Ding, Danny Harnik, Alon Rosen, and Ronen Shaltiel, *Constant-round oblivious transfer in the bounded storage model*, J. Cryptology **20** (2007), no. 2, 165–202.

[Din01] Yan Zong Ding, *Oblivious transfer in the bounded storage model*, CRYPTO (Joe Kilian, ed.), Lecture Notes in Computer Science, vol. 2139, Springer, 2001, pp. 155–170.

[DM02] Stefan Dziembowski and Ueli M. Maurer, *Tight security proofs for the bounded-storage model*, STOC, 2002, pp. 341–350.

[DM08] ———, *The bare bounded-storage model: The tight bound on the storage requirement for key agreement*, IEEE Transactions on Information Theory **54** (2008), no. 6, 2790–2792.

[DORS08] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith, *Fuzzy extractors: How to generate strong keys from biometrics and other noisy data*, SIAM J. Comput. **38** (2008), no. 1, 97–139.

[GMW86] Oded Goldreich, Silvio Micali, and Avi Wigderson, *Proofs that yield nothing but their validity and a methodology of cryptographic protocol design (extended abstract)*, FOCS, IEEE, 1986, pp. 174–187.

[Gol97] Oded Goldreich, *A sample of samplers - a computational perspective on sampling (survey)*, Electronic Colloquium on Computational Complexity (ECCC) **4** (1997), no. 20.

[HCR02] Dowon Hong, Ku-Young Chang, and Heuisu Ryu, *Efficient oblivious transfer in the bounded-storage model*, ASIACRYPT '02: Proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security (London, UK), Springer-Verlag, 2002, pp. 143–159.

[HILL99] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby, *A pseudorandom generator from any one-way function*, SIAM J. Comput. **28** (1999), no. 4, 1364–1396.

[IBDS99] Joe Kilian Ivan B. Damgård and Louis Salvail, *On the (im)possibility of basing oblivious transfer and bit commitment on weakened security assumptions*, Advances in Cryptology, EUROCRYPT 99 (Berlin / Heidelberg), vol. 1592, Springer, 1999, pp. 56–73.

[IBP97] Torben P. Pedersen Ivan B.Damgård and Birgit Pfitzmann, *On the existence of statistically hiding bit commitment schemes and fail-stop signatures*, Journal of Cryptology **10** (1997), no. 3, 163–169.

[ILL89] Russell Impagliazzo, Leonid A. Levin, and Michael Luby, *Pseudo-random generation from one-way functions (extended abstracts)*, STOC, ACM, 1989, pp. 12–24.

[Ken98] Adrian Kent, *Unconditionally secure bit commitment*, Physical Review Letters **83** (1998), no. 7, 1447–1450.

[Kil88] Joe Kilian, *Founding cryptography on oblivious transfer*, STOC, ACM, 1988, pp. 20–31.

[Kil91] ———, *A general completeness theorem for two-party games*, STOC, ACM, 1991, pp. 553–560.

[Lu04] Chi-Jen Lu, *Encryption against storage-bounded adversaries from on-line strong extractors*, J. Cryptology **17** (2004), no. 1, 27–42.

[Mau93] Ueli M. Maurer, *Secret key agreement by public discussion from common information*, IEEE Transactions on Information Theory **39** (1993), no. 3, 733–742.

[Nao90] Moni Naor, *Bit commitment using pseudo-randomness*, CRYPTO '89: Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology (London, UK), Springer-Verlag, 1990, pp. 128–136.

[NMQO+03] Anderson C. A. Nascimento, Jörn Müller-Quade, Akira Otsuka, Goichiro Hanaoka, and Hideki Imai, *Unconditionally secure homomorphic pre-distributed bit commitment and secure two-party computations*, ISC (Colin Boyd and Wenbo Mao, eds.), Lecture Notes in Computer Science, vol. 2851, Springer, 2003, pp. 151–164.

[NP33] J. Neyman and E. S. Pearson, *On the problem of the most efficient tests of statistical hypotheses*, Philosophical Transactions of the Royal Society of London. Series A, Containing Papers of a Mathematical or Physical Character **231** (1933), no. 694-706, 289–337.

[NTS99] Noam Nisan and Amnon Ta-Shma, *Extracting randomness: A survey and new constructions*, J. Comput. Syst. Sci. **58** (1999), no. 1, 148–173.

[NZ96] Noam Nisan and David Zuckerman, *Randomness is linear in space*, J. Comput. Syst. Sci. **52** (1996), no. 1, 43–52.

[Riv99] Ronald L. Rivest, *Unconditionally secure commitment and oblivious transfer schemes using private channels and a trusted initializer*, Tech. report, Laboratory for Computer Science, Massachusetts Institute of Technology, 1999.

[RLG94] Oren Patashnik Ronald L. Graham, Donald E. Knuth, *Concrete mathematics: A foundation for computer science*, second ed., 0201558025, Addison-Wesley Professional, USA, March 1994.

[RW05] Renato Renner and Stefan Wolf, *Simple and tight bounds for information reconciliation and privacy amplification*, ASIACRYPT (Bimal K. Roy, ed.), Lecture Notes in Computer Science, vol. 3788, Springer, 2005, pp. 199–216.

[Sha49] Claude Elwood Shannon, *Communication theory of secrecy systems*, Bell Systems Technical Journal **28** (1949), 656–715.

[TS02] Amnon Ta-Shma, *Almost optimal dispersers*, Combinatorica **22** (2002), no. 1, 123–145.

[Vad03] Salil P. Vadhan, *On constructing locally computable extractors and cryptosystems in the bounded storage model*, CRYPTO (Dan Boneh, ed.), Lecture Notes in Computer Science, vol. 2729, Springer, 2003, pp. 61–77.

[WNI03] Andreas Winter, Anderson C. A. Nascimento, and Hideki Imai, *Commitment capacity of discrete memoryless channels*, CoRR **cs.CR/0304014** (2003).

[Wor94] Thomas Worsch, *Lower and upper bounds for (sums of) binomial coefficients*, 1994.

[Yao82] Andrew Chi-Chih Yao, *Protocols for secure computations (extended abstract)*, FOCS, 1982, pp. 160–164.

[Zuc97] David Zuckerman, *Randomness-optimal oblivious sampling*, Random Struct. Algorithms **11** (1997), no. 4, 345–367.

ANEXOS

I. LIMITES DE PROBABILIDADE

A seguir temos as desigualdades usadas na prova de segurança do protocolo. A desigualdade de Markov é apresentada por ser essencial para demonstrar a desigualdade de Chebyshev.

I.1 A desigualdade de Markov

Essa desigualdade é uma simples consequência da relação conhecida como função indicadora. A seguir temos o lema que estabele a desigualdade de Markov.

Lema I.1. *Se X é uma variável aleatória não negativa, então para todo $a > 0$*

$$P_r[X \geq a] \leq \frac{E[X]}{a}$$

Prova: Como toda função de probabilidade, tem-se que $\Pr[X \geq a] \leq 1$. Assim, a desigualdade de Markov é util apenas quando $E[X]/a$ é menor do que 1. Considere a variável aleatória $a \cdot I_{[a;1)}(X)$, que é a função indicadora. Essa variável aleatória assume o valor zero se $X < a$ e assume o valor a se $X \geq a$. Logo,

$$E[aI_{[a;1)}(X)] = 0 \cdot P_r[X < a] + a \cdot P_r[X \geq a] = a \cdot P_r[X \geq a]$$

Agora, observe que $a \cdot I_{[a;1)}(X) \leq X$. Para melhor compreensão, veja que o lado esquerdo dessa desigualdade só pode ser zero ou a, conforme definição da função indicador. Se for zero, não há problemas porque X é uma variável aleatória não negativa. Se for a, isso implicará em $I_{[a;1)}(X) = 1$, mas isso significa que $X \geq a$. Finalmente, aplicando a função esperança e dividindo por a ambos os lados da desigualdade em questão, obtem-se a desigualdade de Markov:

$$P_r[X \geq a] = \frac{E[aI_{[a;1)}(X)]}{a} \leq \frac{E[X]}{a}$$

I.2 A desigualdade de Chebyshev

A cota superior estabelecida por Markov pode ser melhorada com a simples observação feita por Chebyshev, a qual está expressa no lema a seguir:

Lema I.2. *Seja X uma variável aleatória arbitrária. Para $a > 0$, tem-se que:*

$$P_r[|X| \geq a] \leq \frac{E[X^2]}{a^2}$$

Para provar a desigualdade de Chebyshev, tem-se que $\{|X| \geq a\} = \{|X|^2 \geq a^2\}$. Como os dois conjuntos são iguais, eles têm a mesma distribuição de probabilidade. Logo,

$$P_r[|X| \geq a] = P_r[|X|^2 \geq a^2] \leq \frac{E[|W|^2]}{a^2}$$

onde o último passo segue diretamente da desigualdade de Markov.

O seguinte caso especial da desigualdade de Chebyshev é relevante, já que se está interessado na probabilidade de X estar em torno de $E[X]$. Se $c = E[X]$ for finito, então tomando $|W|$ como sendo $|X - c|$ e definindo $a = \varepsilon\sigma$, onde σ é o desvio padrão de X, a desigualdade pode ser reescrita como:

$$P_r[|W| \geq a] \leq \frac{E[|X - c|^2]}{(\varepsilon\sigma)^2} \leq \frac{E[|X^2 - 2cX + c^2|]}{(\varepsilon\sigma)^2} \leq \frac{E[X^2] - E[X]^2}{(\varepsilon\sigma)^2}$$

Note que $\sigma^2 = E[X^2] - E[X]^2$, o que implica

$$P_r[|X - c| \geq \varepsilon\sigma] \leq \frac{1}{\varepsilon^2}$$

Percebe-se que para $\varepsilon \leq 1$ nenhuma informação útil é obtida. O limiar apenas se torna desprezível para um número grande de desvios padrões de afastamento da média. Entretanto, o intuito de se mostrar essa desigualdade está no seu melhor desempenho, quando comparada com a desigualdade de Chernoff, nas proximidades da média. Uma boa estimativa pode ser feita tomando-se $\varepsilon = \delta\sqrt{c}$. Segue que:

$$P_r[X \leq c - (\delta\sqrt{c})\sigma] \leq \frac{1}{2c\delta^2}$$

A desigualdade acima pode ser obtida, já que o módulo foi removido, levando-se em conta apenas a calda inferior da função que limita superiormente a probabilidade, que é simétrica. Para se determinar o valor de σ, note que $\sigma^2 = var(X) = E[X^2] - E[X]^2$, e o segundo momento de X pode ser obtido conforme a seguir:

$$E[X^2] = \sum_i i^2 \cdot P_r[X = i] = \sum_{i=1}^{k} i^2 \frac{\begin{pmatrix} k \\ i \end{pmatrix}\begin{pmatrix} n-k \\ k-i \end{pmatrix}}{\begin{pmatrix} n \\ k \end{pmatrix}}$$

$$E[X^2] = \sum_{i=1}^{k} i^2 \frac{\frac{k}{i}\begin{pmatrix} k-1 \\ i-1 \end{pmatrix}\begin{pmatrix} n-k \\ k-i \end{pmatrix}}{\frac{n}{k}\begin{pmatrix} n-1 \\ k-1 \end{pmatrix}} = \frac{k^2}{n}\sum_{i=1}^{k} i \frac{\begin{pmatrix} k-1 \\ i-1 \end{pmatrix}\begin{pmatrix} n-k \\ k-i \end{pmatrix}}{\begin{pmatrix} n-1 \\ k-1 \end{pmatrix}}$$

$$E[X^2] = \frac{k^2}{n}\left\{\sum_{i=2}^{k} i - 1 \frac{\frac{k-1}{i-1}\begin{pmatrix} k-2 \\ i-2 \end{pmatrix}\begin{pmatrix} n-k \\ k-i \end{pmatrix}}{\frac{n-1}{k-1}\begin{pmatrix} n-2 \\ k-2 \end{pmatrix}} + \sum_{i=1}^{k} \frac{\begin{pmatrix} k-1 \\ i-1 \end{pmatrix}\begin{pmatrix} n-k \\ k-i \end{pmatrix}}{\begin{pmatrix} n-1 \\ k-1 \end{pmatrix}}\right\}$$

$$E[X^2] = \frac{k^2}{n}\left\{\frac{(k-1)^2}{n-1}\sum_{i=2}^{k}\frac{\binom{k-2}{i-2}\binom{n-k}{k-i}}{\binom{n-2}{k-2}} + \sum_{i=1}^{k}\frac{\binom{k-1}{i-1}\binom{n-k}{k-i}}{\binom{n-1}{k-1}}\right\}$$

Observe que quando $k \geq \sqrt{n}\ \forall\ n \to \infty$ implica que $\frac{(k-1)^2}{n-1} \cong \frac{k^2}{n}$. Aplicando a convolução de Vandermonde para resolver ambos os somatórios, obtem-se:

$$E[X^2] = \frac{k^2}{n}\left(\frac{k^2}{n} + 1\right) = c^2 + c$$

Logo, o desvio padrão é dado por:

$$\sigma = \sqrt{E[X^2] - E[X]^2} = \sqrt{c^2 + c - c^2} = \sqrt{c}$$

Para k suficientemente grande. Portanto, segue que:

$$P_r\left[X \leq (1-\delta)c\right] \leq \frac{1}{2c\delta^2}$$

■

I.3 A desigualdade de Chernoff-Hoeffding

A limitação imposta por essa desigualdade tende a ser melhor assintoticamente, embora isso nem sempre ocorra para faixas específicas, conforme mostrado no capítulo 5. A seguir, obtém-se a desigualdade conhecida como Chernoff-Hoeffding:

Lema I.3. *Sejam $X_1, X_2, \ldots, X_n$ variáveis aleatórias independentes com $\Pr[X_i = 1] = p_i$ a probabilidade do i-ésimo evento ocorrer e $\Pr[X_i = 0] = 1 - p_i$, caso contrário. Seja $X = \sum_{i=1}^{n} X_i$ o número de ocorrências de eventos após n realizações independentes e seja $E[X]$ o valor esperado dessas ocorrências. Então, a seguinte desigualdade é válida para todo $0 < \delta < 1$:*

$$P_r\left[X \leq (1-\delta)E[X]\right] < \left(\frac{e^{-\delta}}{(1-\delta)^{1-\delta}}\right)^{E[X]}$$

Prova: Para provar essa desigualdade, far-se-á uso das mesmas ferramentas das desigualdades anteriores. Logo, os eventos definidos a seguir são todos iguais, já que são funções de uma mesma variável aleatória, portanto, tendo todos a mesma probabilidade:

$$\{X \leq a\} = \{-X \geq -a\} = \{-sX \geq -sa\} = \{e^{-sX} \geq e^{-sa}\}$$

$$P_r\left[X \leq a\right] = P_r\left[e^{-sX} \geq e^{-sa}\right] \leq \frac{E[e^{-sX}]}{e^{-sa}}$$

obtendo-se a desigualdade do último passo com a aplicação da desigualdade de Markov.

Observa-se agora que a desigualdade vale para todo $s > 0$, e o lado esquerdo da expressão não depende de s. Então, é possível minimizar o lado direito da expressão de modo a se obter um limite apertado. Logo, segue que:

$$P_r\left[X \leq a\right] \leq \inf_{s>0} \frac{E[e^{-sX}]}{e^{-sa}} \leq \inf_{s>0} \frac{E\left[e^{-s(X_1+\ldots+X_n)}\right]}{e^{-sa}} \leq \inf_{s>0} \frac{E\left[e^{-sX_1}\cdots e^{-sX_n}\right]}{e^{-sa}}$$

$$P_r\left[X \leq a\right] \leq \inf_{s>0} \frac{\prod_{i=1}^{n} E\left[e^{-sX_i}\right]}{e^{-sa}}$$

Seja p_i a probabilidade de $X_i = 1$ e $1 - p_i$ a probabilidade de $X_i = 0$. Note que essa definição é bastante geral, uma vez que a probabilidade de cada ocorrência pode ser diferente. Em outras palavras, os eventos só precisam ser independentes, não sendo necessário serem identicamente distribuídos.

É possível calcular a função esperança matemática obtida no último passo da expressão acima como sendo:

$$E\left[e^{-sX_i}\right] = \sum_{x=0}^{1} P_X(x) \cdot e^{-sx} = (1 - p_i) + p_i \cdot e^{-s}$$

Reescrevendo $(1-p_i)+p_i \cdot e^s$ como $p_i(e^s-1)+1$ e lembrando que $1+x \leq e^x$, com estrita desigualdade sempre que $x > 0$, pode-se assumir que $x = p_i(e^s - 1)$. Dada a substituição, segue que:

$$\Pr\left[X \leq a\right] < \inf_{s>0} \prod_{i=1}^{n} \frac{(1 - p_i) + p_i \cdot e^{-s}}{e^{-sa}} < \inf_{s>0} \prod_{i=1}^{n} \frac{e^{p_i(e^{-s}-1)}}{e^{-sa}} < \inf_{s>0} \frac{e^{(e^{-s}-1)\sum_{i=1}^{n} p_i}}{e^{-sa}}$$

Na última manipulação feita acima, utilizou-se a propriedade de multiplicação de potências para se realizar a transformação do produtório na base em somatório no expoente. Sendo $E[X] = E\left[\sum_{i=1}^{n} X_i\right] = \sum_{i=1}^{n} E[X_i] = \sum_{i=1}^{n} p_i$, obtem-se:

$$\Pr\left[X \leq a\right] < \inf_{s>0} \frac{e^{(e^{-s}-1)E[X]}}{e^{-sa}}$$

Fazendo $a = (1 - \delta)E[W]$, para todo $0 < \delta < 1$, e substituindo a na expressão obtida acima, tem-se que:

$$\Pr\left[X \leq (1 - \delta)E[X]\right] < \inf_{s>0} \frac{e^{(e^{-s}-1)E[X]}}{e^{-s(1-\delta)E[X]}}$$

Agora é possível minimizar o lado direito da desigualdade acima para se obter uma cota superior apertada, bastando para isso encontrar a derivada da função em termos da variável muda s e igualá-la a zero. Logo:

$$\frac{d}{ds} e^{(e^{-s}-1)+s(1-\delta)} = e^{(e^{-s}-1)+s(1-\delta)} \cdot \left[-e^{-s} + (1 - \delta)\right] = 0$$

Dado que $s > 0$, então a função $e^{(e^{-s}-1)+s(1-\delta)}$ será sempre diferente de zero. Como o produto de duas funções reais é zero se e somente se uma delas for zero, então:

$$-e^{-s} + (1-\delta) = 0$$

$$e^{-s} = (1-\delta)$$

Finalmente, substituindo esse resultado na desigualdade anterior,

$$P_r\left[W \leq (1-\delta)E[W]\right] < \left(\frac{e^{-\delta}}{(1-\delta)^{1-\delta}}\right)^{E[W]}$$

o lema segue. ■