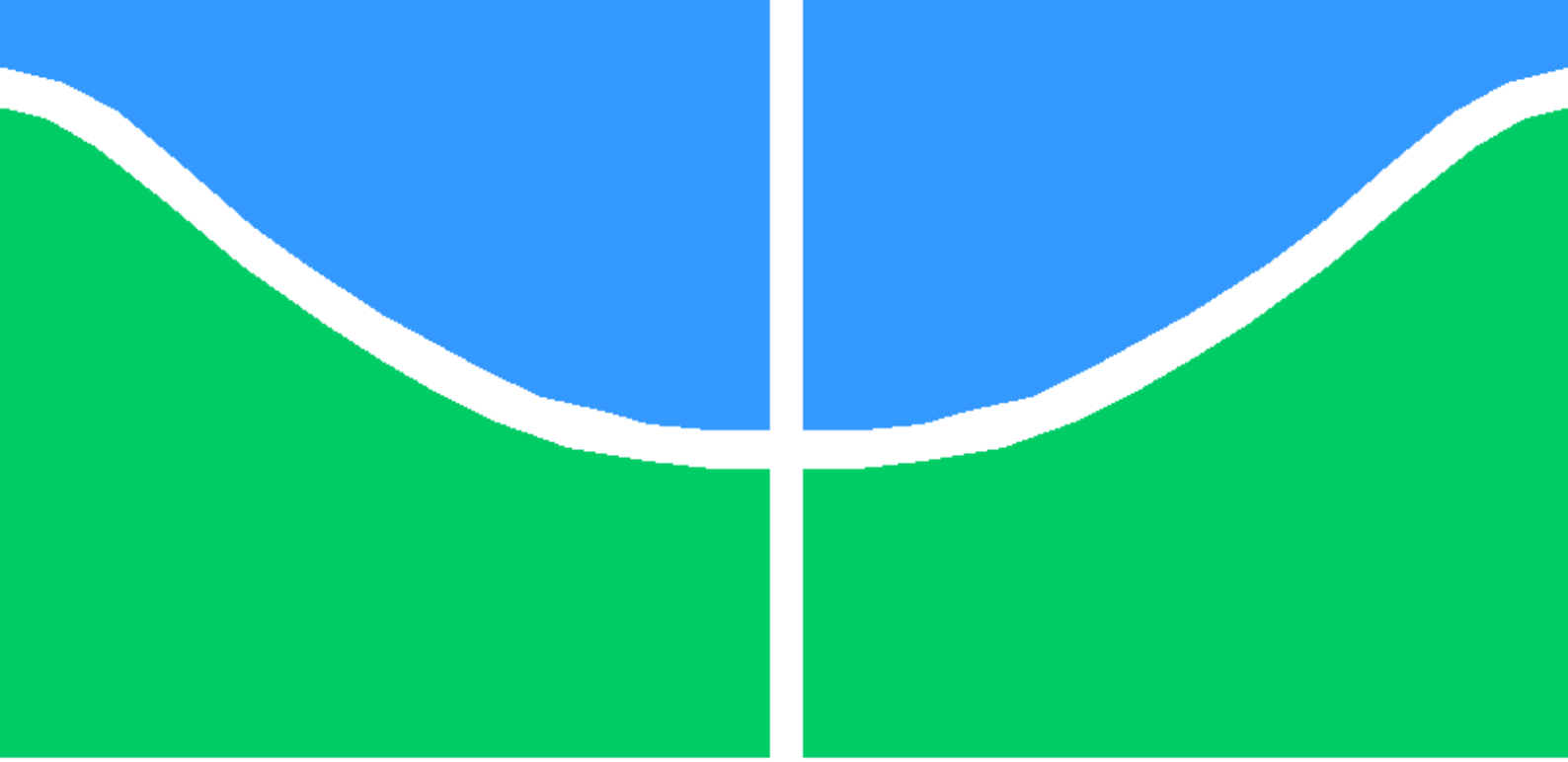

PROTOCOLO DE COMPROMETIMENTO COM SEGURANÇA INCONDICIONAL BASEADO NO CANAL COM RUÍDO DE REORDENAMENTO DE PACOTES

Vinícius de Morais Alves

TESE DE DOUTORADO
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

Brasília, 2 de dezembro de 2021

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

PROTOCOLO DE COMPROMETIMENTO COM SEGURANÇA INCONDICIONAL BASEADO NO CANAL COM RUÍDO DE REORDENAMENTO DE PACOTES

VINÍCIUS DE MORAIS ALVES

Orientador: RAFAEL TIMÓTEO DE SOUSA JR., UNB, PHD.

TESE DE DOUTORADO EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO PPGEE.TD - 182/22
BRASÍLIA-DF, 2 DE DEZEMBRO DE 2021.

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

PROTOCOLO DE COMPROMETIMENTO COM SEGURANÇA INCONDICIONAL BASEADO NO CANAL COM RUÍDO DE REORDENAMENTO DE PACOTES

VINÍCIUS DE MORAIS ALVES

TESE DE DOUTORADO ACADÊMICO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE DOUTOR EM ENGENHARIA ELÉTRICA.

APROVADA POR:

Rafael Timóteo de Sousa Jr., UnB, PhD.
Orientador

William Ferreira Giozza, UnB, PhD.
Examinador interno

Bernardo Machado David, ITU, PhD.
Examinador Externo

Georges Daniel Amvame Nze, UnB, PhD.
Examinador Externo

BRASÍLIA, 2 DE DEZEMBRO DE 2021.

FICHA CATALOGRÁFICA

VINÍCIUS DE MORAIS ALVES
Protocolo de Comprometimento com Segurança Incondicional Baseado no Canal com Ruído de Reordenamento de Pacotes. [Distrito Federal] 2021.
xiii, 107p., 201x297 mm (ENE/FT/UnB, Doutor, Engenharia Elétrica, 2021)
Tese de Doutorado – Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. Criptografia	2. Segurança Incondicional
3. Protocolo de Comprometimento	4. Reordenamento de Pacotes
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

VINÍCIUS DE MORAIS ALVES (2021) Protocolo de Comprometimento com Segurança Incondicional Baseado no Canal com Ruído de Reordenamento de Pacotes. Tese de Doutorado em Engenharia Elétrica, Publicação PPGEE.TD - 182/22, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 107p.

CESSÃO DE DIREITOS

AUTOR: Vinícius de Morais Alves
TÍTULO: Protocolo de Comprometimento com Segurança Incondicional Baseado no Canal com Ruído de Reordenamento de Pacotes.
GRAU: Doutor ANO: 2021

Vinícius de Morais Alves
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
Faculdade de Tecnologia - FT
Departamento de Engenharia Elétrica (ENE)
Brasília - DF CEP: 70919-970
e-mail: vinicius.alves@redes.unb.br

À minha mãe, Madalena, por me amar sem medidas; Ao meu pai, Paulo, por sempre me entusiasmar; À minha esposa, Lílian, por me apoiar incondicionalmente, por sua paciência, sua ternura e seu amor; E aos meus filhos, Tarcísio e Olívia, as razões de ser de toda a minha vida!

Vinícius de Morais Alves

AGRADECIMENTOS

Agradeço em primeiro lugar a Deus, por mais essa bênção. Aos meus familiares e amigos, sou grato por todo o apoio e incentivo que sempre me deram.

Agradeço também a cada um dos colegas com quem me relacionei durante todo esse tempo na pós-graduação, pelos prazerosos momentos de criação, discussão, estudo, comunhão e descontração.

Agradeço, ainda, ao meu orientador, Prof. Dr. Rafael Timóteo de Sousa Jr., e ao meu coorientador, Prof. Dr. Anderson C. A. Nascimento, por toda a atenção, a paciência, o aprendizado e a dedicação de ambos a mim.

Por fim, agradeço o apoio técnico e computacional do Laboratório de Tecnologias para Tomada de Decisão - LATITUDE, da Universidade de Brasília, que conta com apoio do CNPq - Conselho Nacional de Pesquisa (Outorgas 312180/2019-5 PQ-2, BRICS2017-591 LargEWiN e 465741/2014-2 INCT em Cibersegurança), da CAPES - Coordenação de Aperfeiçoamento do Pessoal de Nível Superior (Outorgas PROAP PPGEE/UnB, 23038.007604/2014-69 FORTE, e 88887.144009/2017-00 PROBRAL), da FAP-DF - Fundação de Amparo à Pesquisa do Distrito Federal (Outorgas 0193.001366/2016 UIoT e 0193.001365/2016 SSDDC), do Ministério da Economia (Outorgas 005/2016 DIPLA e 083/2016 ENAP), da Secretaria de Segurança Institucional da Presidência da República do Brasil (Outorga ABIN 002/2017), do Conselho Administrativo de Defesa Econômica (Outorga CADE 08700.000047/2019-14), da Advocacia Geral da União (Outorga AGU 697.935/2019), do Departamento Nacional de Auditoria do SUS (Outorga DENASUS 23106.118410/2020-85), da Procuradoria Geral da Fazenda Nacional (Outorga PGFN 23106.148934/2019-67) e dos Decanatos de Pesquisa e Inovação e de Pós-Graduação da Universidade de Brasília (Outorga 23106.067186/2021-37).

Vinícius de Morais Alves

RESUMO

Um grande esforço de pesquisa foi envidado nos últimos 50 anos para desenvolver primitivas criptográficas incondicionalmente seguras baseadas em condições físicas, como a existência de ruído em canais de comunicação, capacidade de armazenamento limitada ou as leis da mecânica quântica. Em trabalho desenvolvido por Paolo Palmieri e Olivier Pereira, demonstrou-se que a variação no atraso sofrido por pacotes enviados através de canais de comunicação pode ser usada como uma hipótese plausível e eficaz para se obter a primitiva criptográfica incondicionalmente segura de *Oblivious Transfer* contra adversários passivos. Além disso, os autores observaram que a variação do atraso implica no efeito de reordenamento dos pacotes. No presente trabalho, pavimentamos o caminho para essa possibilidade, propondo uma nova definição para canais com ruído do tipo reordenamento de pacotes. A nossa finalidade é facilitar a obtenção de medidas estatísticas e entrópicas relativas ao canal. Finalmente, propomos a primeira implementação direta de uma primitiva criptográfica de comprometimento incondicionalmente segura contra adversários maliciosos baseada no canal de reordenamento de pacotes.

Keywords: Criptografia, Segurança incondicional, protocolo de comprometimento, reordenamento de pacotes.

ABSTRACT

A lot of research effort has been deployed in the last 50 years on achieving unconditionally secure cryptographic primitives based on physical assumptions, such as noisy channels, bounded storage capacity or quantum mechanics laws. In a work of Paolo Palmieri and Olivier Pereira, it was demonstrated the variable delay of packets sent by communication channels could be used as a reasonable and an effective assumption to achieve the unconditionally secure cryptographic primitive of Oblivious Transfer against passive adversaries. Furthermore, the authors observed that variable delays implies packet reordering effect. In the present work, we pave the path into this possibility by establishing a new definition of the Packet Reordering noisy channel. Our purpose is to simplify the calculation of statistical and entropic measures. Finally, we show the first directly implemented unconditionally secure commitment scheme against malicious adversaries based on the packet reordering noisy channel.

Keywords: Cryptography, Unconditional security, commitment schemes, packet reordering.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SÍMBOLOS

Variáveis Aleatórias

X^n	Sequência de pacotes escolhida por Alice
$\overline{X^n}$	Sequência de pacotes anunciada por Alice na fase de abertura
$\widetilde{X^n}$	Sequência de pacotes forjada pelo adversário
Y^n	Sequência de pacotes recebida por Bob
K	Quantidade de inversões realizadas pelo canal
V	Comprometimento de Alice
T	Comunicação realizada entre Alice e Bob
C	Inversões realizadas pelo canal e por Alice maliciosa (colisões)
$C_{\mu(i+1,i)}$	Indica se a referida inversão é ou não uma colisão
F	V. A. uniformemente distribuida sobre a família de funções de hash 2-universal $\mathcal{F}$
G	V. A. uniformemente distribuida sobre a família de funções de hash 2-universal $\mathcal{G}$

Parâmetros

ℓ	tamanho dos pacotes, cujo mínimo é dado por $\lceil \log(n) \rceil$
n	Quantidade de pacotes enviada por Alice para Bob
s	Parâmetro de segurança do protocolo
ρ	Parâmetro característico do ruído do canal
v	Valor com a qual Alice se compromete
τ	Limiar de inversões realizadas por uma Alice maliciosa
m	tamanho do comprometimento de Alice
ε	parâmetro de margem de erro do canal
φ	Máxima probabilidade de falha do protocolo quando as partes são honestas
ϵ	Máximo de informação sobre v que vaza para Bob
θ	Máxima chance de Bob ser trapaceado por Alice
β	$1 - 2\rho/[(n-1)(1-\rho)]$
α	$\varepsilon(1-\rho)/(1+\varepsilon\rho)$
p	$\rho/(1+\rho)$

Funções

$f(\cdot)$	Bob amostra uma realização $f \leftarrow F$ e envia sua descrição para Alice
$g(\cdot)$	Alice amostra uma realização $g \leftarrow G$ e utiliza como extrator de aleatoriedade
hash	Hash 2-universal enviado por Alice para Bob, dado por $f(x^n)$
commit	comprometimento de Alice, dado por $g(x^n) \oplus v$
$M(n,k)$	Triângulo de Mahonian
$T(n,k)$	Número de permutações dentre aquelas em $M(n,k)$ contendo uma dada inversão $\mu(i+1;i)$ de ordem-1
$S_i(\rho)$	Série geométrica
$E[K]$	$(n-1)\rho/(1-\rho)$
$\langle n-1 \rangle^i$	$(n-1)n(n+1)(n+2)\cdots(n-1+i-1)$
$\sigma_n(\rho)$	$(1-\rho)(1-\rho^2)\cdots(1-\rho^n)/(1-\rho)^n$

Siglas

PRNC	Packet Reordering Noisy Channels (*Canal com Ruído de Reordenamento de Pacotes*)
BDDC	Binary Discrete-time Delaying Channel
BEC	Binary Erasure Channel
BSC	Binary Symmetric Channel
WNC	Weak Noisy Channel
WEC	Weak Erasure Channel
WBSC	Weak Binary Symmetric Channel
XOR	eXclusive-OR (*OU-Exclusivo*)
NAND	Not-AND
OT	Oblivious Transfer
BC	Bit Commitment
OTP	One Time Pad
QKD	Quantum Key Distribution
QSDC	Quantum Secure Direct Communication
LDPC	Low-Density Parity-Check codes
MDS	Maximum Distance Separable codes
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
IP	Internet Protocol
MIMO	Multiple-Input and Multiple-Output
IEEE	Institute of Electrical and Electronics Engineers
FOCS	IEEE Symposium on Foundations of Computer Science
OEIS	On-line Encyclopedia of Integer Sequences
ASIC	Application Specific Integrated Circuit

Capítulo 1

Introdução

1.1 Dos Primórdios à Criptografia Moderna

Desde a invenção da escrita[1], comunicar-se de forma secreta já era uma necessidade humana. Técnicas criptográficas rudimentares foram utilizadas na escrita dos hieróglifos da tumba de Khnumhotep II no Egito antigo, quase 2 mil anos antes de Cristo. Da época do Império Romano, há documentos históricos contendo relatos sobre o uso de cifras de substituição na codificação de mensagens secretas enviadas aos generais em campos de batalha pelo famoso imperador Júlio César. O esquema de ciframento utilizado por ele ainda hoje é ensinado e carrega seu nome em homenagem.

No decorrer das idades média e moderna, a cifra de César e de modo geral as técnicas de criptoanálise foram aperfeiçoadas por vários estudiosos na Europa, Asia e no Oriente Médio. Al Kindi, estudioso árabe, escreveu o manuscrito "*Sobre a decifração de mensagens criptografadas*"em 841 d.c. [2], o qual contém a descrição mais antiga conhecida de criptoanálise por frequência. Uma das cifras mais famosas desenvolvidas com o propósito de dificultar essa técnica de criptoanálise é a chamada cifra de Vigenère, um método de criptografia que usa uma série de diferentes cifras de César baseadas em letras de uma senha, sendo classificada como uma cifra de substituição polialfabética. Por muitos anos, acreditaram se tratar de um código indecifrável. Porém, Charles Babbage mostrou, no século XIX, como a cifra poderia ser criptoanalisada com o uso de computação e estatística quando o texto cifrado é suficientemente grande, devido a repetição da chave.

Certamente, o grande fato histórico que consolidou a necessidade de uma abordagem com rigor científico da criptografia foi a Segunda Guerra Mundial. Para muitos autores [1, 3, 4], a guerra foi vencida com grandiosa contribuição de engenheiros, matemáticos, físicos e cientistas, com destaque para Alan Turing, os quais ajudaram a decifrar as comunicações secretas alemãs realizadas por meio das máquinas Enigma e Lorenz SZ40. A decodificação das mensagens criptografadas por essas máquinas foi realizada pelos Aliados com auxílio do computador britânico Colossus, considerado

[1]Os fatos históricos narrados neste capítulo e outras informações interessantes sobre a história da criptografia podem ser encontrados no livro de Simon Singh, intitulado "*The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*"[1].

o primeiro computador digital eletrônico programável de grande escala do mundo, mantido em Bletchley Park, nas proximidades de Londres.

1.2 Segurança Perfeita

O principal objetivo da criptografia é possibilitar a comunicação segura entre remetente e destinatário, de modo que a informação seja irrecuperável no caso de o texto cifrado ser interceptado por uma terceira parte não autorizada. Além disso, a criptografia também tem como finalidade clássica possibilitar a autenticação entre partes, seja por meio do uso de senhas, chaves ou certificados.

Em meados do século XX, surgiram tanto a Teoria da Informação como a Teoria da Computação, baseadas inicialmente nos trabalhos de seus fundadores, Claude Shannon e Alan Turing, respectivamente. Em conjunto, essas teorias formam os fundamentos teóricos da Criptografia Moderna, inaugurada no trabalho de Shannon intitulado "*Communication Theory of Secrecy Systems*"[5]. Porém, no decorrer da segunda metade do século, a Criptografia Moderna sofreu enorme avanço mediante as contribuições de diversos pesquisadores, conforme detalhado no capítulo 2, o que possibilitou o atual estágio de desenvolvimento dessa teoria.

Claude Shannon é o fundador da Teoria da Informação, assim como da Criptografia Moderna. Seu trabalho [5] estabeleceu a definição de segurança perfeita em relação à confidencialidade de um texto cifrado. Uma cifra com segurança perfeita torna a tarefa de criptoanálise tão difícil quanto advinhar a mensagem na ausência de qualquer outra informação que não seja o tamanho da mensagem. Shannon demonstrou que a cifra *One Time-Pad* (OTP) apresenta segurança perfeita, desde que a chave secreta utilizada seja aleatória, ao menos do mesmo tamanho da mensagem e não seja utilizada mais de uma vez.

1.3 Segurança Computacional

Posteriormente, já na década de 1970, pesquisadores começaram a lidar com o resultado negativo apresentado por Shannon, pois a geração de aleatoriedade em grande quantidade para se estabelecer a chave secreta e o compartilhamento dessa chave entre as partes confiáveis são problemas complexos de se solucionar [6]. Assim, diversas pesquisas surgiram com o intuito de relaxar as restrições do resultado de segurança perfeita, mas mantendo ainda o nível de segurança das comunicações adequado. Evidentemente, o primeiro problema que surgiu foi definir o conceito de nível de segurança. Esses estudos se bifurcaram em duas trilhas principais.

A primeira frente se baseou no conceito de **segurança computacional** para relaxar as premissas de segurança perfeita. Há duas hipóteses basilares nesse caso. A primeira é a limitação do poder computacional disponível, onde se presume que a quantidade de computações que se pode realizar em um dado intervalo de tempo tem um limite máximo para qualquer participante do protocolo. A segunda é a existência de problemas matemáticos complexos intratáveis. Ou seja, presume-se que a quantidade mínima de computações necessárias para se resolver certos proble-

mas cresce exponencialmente com o tamanho da variável. Dito de outra forma, não se conhece algoritmo capaz de resolver certas operações de modo eficiente, havendo sempre uma quantidade mínima elevada de computações para se obter uma solução.

Além disso, a dificuldade no compartilhamento da chave é resolvida com a criativa solução de se utilizar um par de chaves. Dessa forma, uma delas, a chave privada, é mantida em segredo por seu portador, enquanto a outra, a chave pública, é divulgada publicamente para que qualquer interessado seja capaz de se comunicar secretamente com o portador. Os sistemas criptográficos que funcionam baseados nesse paradigma são conhecidos como Criptossistemas de Chave Pública.

A vantagem dessa abordagem reside na possibilidade de se estimar com razoável precisão um limite superior na capacidade computacional disponível para um adversário, o que torna precificável o nível de segurança do protocolo, baseado no custo computacional para se quebrar a cifra. A desvantagem está no fato de os problemas computacionais utilizados para se implementar os protocolos criptográficos não serem comprovadamente intratáveis, além do fato de a restrição física imposta também ser frágil, sendo possível que sejam criptoanalisados caso se descubra um algoritmo eficiente para resolvê-los ou algum avanço tecnológico inovador torne a capacidade computacional disponível muito maior.

Com o advento da Internet, os serviços em nuvem e o avanço de *malwares*, é cada vez mais difícil estimar o real poder computacional do adversário, que pode processar de forma distribuída em milhões de máquinas e dispositivos espalhados pelo mundo, ou mesmo em diversos serviços em nuvem, com relativa facilidade. A lei de Moore, observação feita por Gordon E. Moore sobre a tendência da indústria de microchips produzir processadores onde o número de transistores contidos dobra a cada dois anos a um custo fixo, tem se confirmado nos últimos 50 anos. O recente desenvolvimento de computadores quânticos por empresas como Google e IBM, em uma corrida pela supremacia dessa tecnologia, também representa uma quebra de paradigma, ao trazer à tona a possibilidade de fatoração em tempo polinomial, como preconizado pelo algoritmo de Shor [7]. Esses são alguns exemplos dos casos citados anteriormente que podem comprometer protocolos criptográficos construídos com base em segurança computacional.

A frente de pesquisa em criptografia com segurança computacional demonstrável foi inaugurada pelos pesquisadores Whitfield Diffie e Martin Hellman [8], com um método de troca de chaves batizado com os seus sobrenomes. Em seguida, Ronald Linn Rivest, Adi Shamir e Leonard Adleman criaram o primeiro criptossistema de chave pública, conhecido como RSA [9], acrônimo formado pelas letras iniciais de seus sobrenomes. O trabalho desenvolvido por Shafi Goldwasser e Silvio Micali em cifras probabilísticas e em segurança demonstrável [10] também representa um importante avanço na área, pois introduziu o tratamento matemático para formalizar a definição de nível de segurança. A área de estudos em criptografia com segurança computacional é atualmente a mais relevante em criptologia.

O jornalista Patrick Sawer [11] relata que os cientistas ingleses James H. Ellis, Clifford Christopher Cocks e Malcolm John Williamson, que trabalhavam para inteligência britânica na década de 1970, anteciparam a criação da criptografia de chave pública, o que eles chamaram de "*non-secret encryption*". Contudo, como o trabalho para o serviço secreto era classificado, somente no

ano de 1997 veio a público o conhecimento desse feito, quando o sigilo dos documentos foi retirado. De toda forma, não há evidências claras se esses pesquisadores tiveram a visão do impacto que essas tecnologias poderiam ter no meio acadêmico e comercial.

1.4 Segurança Incondicional

A segunda frente, denominada **segurança incondicional**, busca por alguma hipótese física que permita estabelecer a assimetria entre os participantes de um protocolo criptográfico sem limitar a capacidade computacional destes e, principalmente, sem depender de problemas matemáticos considerados intratáveis. Nessa área, a principal observação se baseia no fato de o canal não apresentar ruído na comunicação entre os participantes no resultado sobre segurança perfeita apresentado por Shannon. Evidentemente, esse não é o caso na prática.

Geralmente visto como uma dificuldade a ser vencida por engenheiros de comunicação, o ruído é uma poderosa ferramenta para criptógrafos. Portanto, assumindo que a comunicação entre as partes se dá por meio de canais ruidosos, os pesquisadores dessa vertente demonstraram ainda ser possível a comunicação secreta entre as partes legítimas, independente do poder computacional do adversário ou das partes.

Aaron Wyner é o fundador dessa vertente com a publicação "*The Wire-Tap Channel*"[12]. Em seu resultado, Wyner demonstra a possibilidade de comunicação sigilosa entre as partes autênticas mesmo na presença de um adversário passivo, desde que o canal por onde o adversário realiza o "grampo" esteja concatenado ao canal principal, conforme ilustra a figura a seguir:

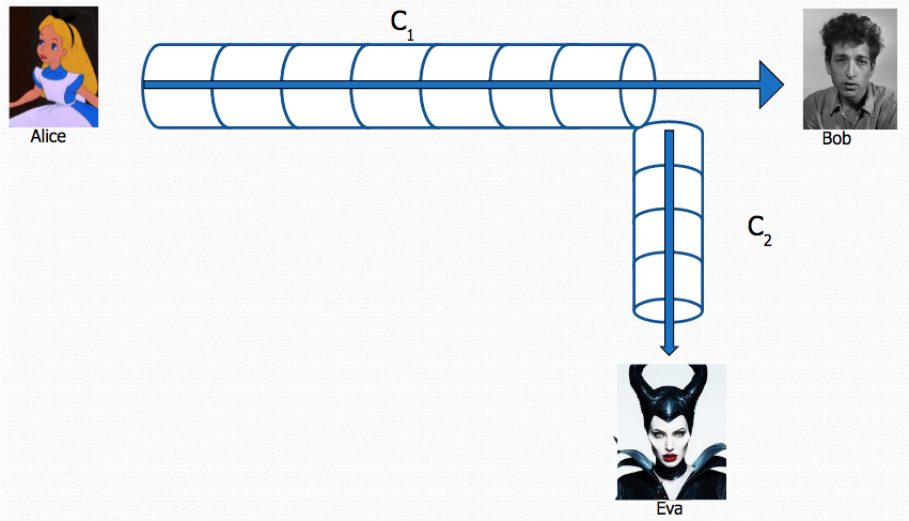

Figura 1.1: *The Wire-Tap Channel* proposto por Wyner
(adaptada das fontes `https://segredosdomundo.r7.com/alice-no-pais-das-maravilhas/`, `https://pt.wikipedia.org/wiki/Maleficent` e `https://english.worldmagazine.it/164616/`)

Imre Csiszár e János Körner [13] mostraram que não há necessidade de o canal da parte adversária ser concatenado ao canal principal, podendo ser independente, desde que seja mais

ruidoso do que o canal entre os participantes honestos. Ueli Maurer [14] foi além e mostrou que existindo um canal de comunicação acessório bidirecional sem ruído ligando as partes, além de poder ser independente, o canal do adversário não precisa ser mais ruidoso que o canal entre as partes legítimas para se obter comunicação sigilosa.

A ideia introduzida por Wyner de utilizar o canal ruidoso como uma primitiva criptográfica fundamental na transmissão de informação secreta entre pares na presença de um adversário foi ampliada, onde extensos trabalhos baseados em canais ruidosos surgiram a partir dessas contribuições. Atualmente, essa ideia é aplicada na construção de protocolos para acordo de chave secreta com base em canais com ruído dos tipos gaussiano, binário simétrico, *erasure*, entre outros. Também são derivações feitas a partir do trabalho de Wyner os extratores de aleatoriedade determinísticos e estatísticos, *privacy amplification*, geradores de pseudoaleatoriedade, assim como a construção de primitivas criptográficas incondicionalmente seguras de *Bit Commitment* (BC) e de *Oblivious Transfer* (OT). Uma revisão sobre essa área da literatura de criptologia será apresentada no capítulo 2.

Por ser uma disciplina cada vez mais ampla, que lida com assuntos muito além das tarefas clássicas de ciframento e autenticação, a relevância da criptografia tem se destacado entre os teóricos das principais áreas das ciências naturais, como computação, matemática e física. Por conta disso, os modelos teóricos tratados na área apresentam um nível de abstração e complexidade cada vez maior.

1.5 Visão geral da tese

Esta tese está organizada da seguinte forma. Neste Capítulo, fizemos uma breve introdução a respeito da criptografia. No Capítulo 2, apresentamos uma revisão da literatura da área relacionada ao escopo desta tese. No Capítulo 3, tratamos sobre as nossas motivações para a realização do trabalho e as suas contribuições à literatura da área. No Capítulo 4 introduzimos algumas medidas de informação e resultados importantes em matemática e estatística utilizados no decorrer do texto. No Capítulo 5, introduzimos uma nova definição para o canal com ruído de reordenamento de pacotes e apresentamos o desenvolvimento matemático do novo modelo. No Capítulo 6, apresentamos o modelo geral de um comprometimento, a sua definição de segurança e descrevemos em detalhes o funcionamento do protocolo de comprometimento proposto. No Capítulo 7, apresentamos as provas matemáticas de corretude e de segurança incondicional do protocolo para ambos os participantes. No Capítulo 8, tratamos da análise sobre o desempenho do protocolo proposto, com um caso de uso para faixas de valores dos parâmetros que caracterizam o canal PRNC em estado de operação, demonstrando sua viabilidade em condições reais. O Capítulo 9 e último traz um resumo do que foi apresentado na tese com a conclusão, as possíveis extensões do resultado e as diversas linhas de trabalhos futuros.

Capítulo 2

Revisão da Literatura

2.1 Computação Segura Distribuída

Na Computação Segura Distribuída, duas ou mais partes sem confiança mútua querem colaborar de forma segura, a fim de alcançar um objetivo comum. Podemos citar como exemplos a realização de uma eleição eletrônica, a obtenção do processamento de dados em nuvem sem o vazamento de informações ou a consulta a uma base de dados de forma privada sem que o administrador da base tenha ciência do que foi consultado.

O problema introduzido por Andrew C. Yao em trabalho publicado no IEEE *Symposium on Foundations of Computer Science* (FOCS) em 1982 e intitulado "*Protocols for Secure Computations*" [15] caracteriza o conceito para o caso de duas partes. Nessa publicação apareceu o famoso **Dilema dos Milionários**: *Alice e Bob são dois milionários que desejam descobrir quem é mais rico, porém sem revelarem um ao outro quanto dinheiro possuem.* Yao apresentou solução que permite Alice e Bob saberem quem é o mais rico sem, no entanto, violar qualquer das restrições impostas no enunciado do problema.

Exemplos de funções específicas em computação segura entre duas partes são a Avaliação Segura de Função, na qual cada parte tem uma entrada para uma função e a sua saída deve ser calculada de tal forma que nenhuma parte revele informações desnecessárias sobre a sua entrada, e a Recuperação Privada de Informação, na qual uma das partes tem acesso a uma parte das informações disponibilizadas por outra parte, mas sem possibilitar o rastreamento do que foi acessado.

A formulação teórica para esse problema foi posteriormente generalizada, buscando a solução para se computar de forma distribuída uma função entre várias partes, dado um conjunto de participantes $p_1, p_2, \ldots, p_n$ e de entradas privadas $d_1, d_2, \ldots, d_n$. Nesse caso, as partes desejam calcular o resultado da aplicação de uma função pública F de n variáveis no ponto $(d_1, d_2, \ldots, d_n)$.

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. Além disso, uma preocupação central desses protocolos é sobre a corretude do processamento, de modo a garantir que as partes desonestas não

consigam deturpar o resultado obtido na saída da função computada publicamente pelos demais participantes honestos.

Outros resultados importantes sobre a generalidade de computação segura distribuída aparecem em [16] e em [17], onde os autores apresentam resultados sobre a quantidade mínima de participantes honestos para uma implementação segura ser possível e reduções computacionais ao problema de troca de segredo de forma segura. Infelizmente, não é possível assumirmos que os participantes de um protocolo de computação segura distribuída possuem capacidades computacionais ilimitadas e ainda obtermos segurança incondicional sem uma hipótese adicional.

Essa hipótese precisa garantir a assimetria necessária entre as partes para possibilitar a implementação de primitivas incondicionalmente seguras. Por exemplo, a existência de um canal quântico entre dois participantes computacionalmente ilimitados não é suficiente para permitir a construção de protocolos incondicionalmente seguros, conforme demonstraram de forma independente Mayers, e Lo e Chau [18, 19]. Porém, a existência de praticamente qualquer canal ruidoso possibilita o estabelecimento de primitivas incondicionalmente seguras, especialmente no caso de computação segura entre duas partes [20].

2.2 Estabelecimento de Chave Secreta

Os protocolos de estabelecimento de chave secreta são fundamentais em criptografia, uma vez que permitem a comunicação de forma segura entre partes que jamais se encontraram. As primeiras ideias sobre o estabelecimento de chave secreta tratam da possibilidade de as partes se encontrarem previamente para compartilharem um segredo que as possibilitem se comunicar sigilosamente a posteriori.

Como aperfeiçoamento natural dessa ideia, surgiram as primeiras propostas de estabelecimento de chave a distância, sem a necessidade de as partes se encontrarem pessoalmente. Então, uma corrente de pesquisadores propôs protocolos de estabelecimento de chave com base em limitações computacionais do adversário, como nos casos dos famosos protocolos de Diffie-Hellman [8] e do RSA [9]. Esses protocolos se demonstraram bastante práticos e são usados na atualidade em virtualmente todos os protocolos criptográficos. Porém, a segurança dessas implementações tem se tornado fator crítico, devido ao vertiginoso crescimento do poder computacional e da melhoria dos algoritmos matemáticos de fatoração. Assim, o interesse por protocolos alternativos, com segurança independente de restrições computacionais do adversário, tem crescido muito no meio acadêmico e na indústria.

2.3 Canais Ruidosos

Desde 1975, a proposta de Wyner [12] já pavimentava a área de protocolos com segurança incondicional, ao propor o uso do ruído existente no canal que conecta as partes confiáveis como forma de extrair uma chave secreta para estas se comunicarem de forma segura. No artigo *The*

wire-tap channel, Wyner modelou o cenário onde dois canais discretos sem memória C_1 e C_2 estão disponíveis, um entre Alice e Bob, e o outro entre Bob e Eva, respectivamente, conforme a figura 1.1. Wyner provou que esse modelo atinge a capacidade de sigilo do canal *(Secrecy Capacity)* quando C_1 é um canal sem ruído (com correção de erro) e C_2 é um canal binário simétrico (*Binary Symmetric Channel* - BSC - em inglês), caracterizada da seguinte forma: Para todo $\epsilon > 0$, existe um esquema de codificação da informação com taxa $R > C_s - \epsilon$ que satisfaz os requisitos de confiabilidade e segurança. Por outro lado, não existe esquema de codificação que satisfaça esses requisitos a uma taxa superior a C_s.

Desde então, o resultado de Wyner foi bastante estudado e generalizado. Surgiram construções baseadas em canais ruidosos gaussianos, com alfabetos contínuos [21]. Outra generalização importante apareceu no trabalho sobre canais de *broadcast* com mensagem confidencial [13], onde Csiszar e Körner incluíram a possibilidade de o canal entre Alice e Eva ser independente do canal entre Alice e Bob, desde que seja mais ruidoso. Ozarow e Wyner estenderam o resultado aos canais que impõem restrições combinatoriais (ao invés de probabilísticas) ao adversário [22], que pode observar quaisquer k dentre n símbolos transmitidos pelo canal.

Posteriormente, esses resultados foram generalizados por Maurer, em seu trabalho intitulado *"Secret-Key Agreement by public Discussion"* [23], onde o autor demonstra que a existência de um canal de *broadcast* autenticado e livre de ruído interligando as partes possibilita a obtenção de taxas positivas no estabelecimento de chave secreta, mesmo quando o canal entre Alice e Eva é independente e menos ruidoso do que o canal entre Alice e Bob. A grande maioria dos protocolos derivados dessa linha de pesquisa são muito restritivos quanto aos requisitos do canal e exigem grande poder computacional das partes confiáveis para computar as codificações e decodificações previstas, inviabilizando a implementação desses protocolos em aplicações práticas.

De fato, a literatura sobre *wire-tap channels* engloba, atualmente, centenas de publicações, sendo inviável abordá-las todas nesta sucinta revisão. Entretanto, a grande maioria desses trabalhos está baseada em argumentos não construtivos envolvendo códigos aleatórios para demonstrar seus principais resultados. Esses resultados provam a existência de códigos que atingem a capacidade de sigilo do canal, mas são de pouca utilidade quando se objetiva projetar protocolos de codificação e decodificação que sejam práticos e eficientes. Existem soluções construtivas para o problema do *wire-tap channel* em alguns casos especiais.

O primeiro caso é quando o canal principal é sem ruído e o *wire-tap channel* é um canal do tipo *Binary Erasure Channel* (BEC). Um esquema de codificação e decodificação para esse caso foi apresentado em [24] e em [25], onde usando códigos de Verificação de Paridade de Baixa Densidade (*Low-Density Parity-Check* - LDPC - em inglês) para o canal BEC os autores provaram atingir a capacidade de sigilo. Outro caso especial é quando o adversário é limitado combinatorialmente. Essa situação foi estudada por Ozarow e Wyner em [22] e tratada como uma variação combinatorial do canal BEC. Esquemas de codificação comprovadamente ótimos podem ser construídos com base em códigos com Máxima Distância de Separação - MDS [26], ou também usando extratores [27]. Entranto, deve-se destacar que mesmo para casos simples onde o canal principal é tratado como sem ruído, poucas codificações atingem a capacidade de sigilo do canal.

2.4 Oblivious Transfer

Uma primitiva criptográfica de fundamental importância para a computação segura distribuída e, especialmente, na área de computação segura entre duas partes é conhecida como *Oblivious Transfer* (OT). Os primeiros resultados sobre a primitiva OT podem ser encontrados em trabalhos dos anos de 1970, quando Wiesner introduziu uma primitiva similar chamada por ele de *Quantum Conjugate Coding* ou Multiplexação de Canal Quântico [28]. Seu trabalho, entretanto, foi publicado apenas após uma década, em 1983, sem que ele vislumbrasse uma aplicação criptográfica para o protocolo proposto. Contudo, Rabin [29] foi quem introduziu OT como um protocolo de aplicação criptográfica, em um relatório técnico manuscrito para o Laboratório Aiken Computation, na Universidade de Harvard.

A implementação que ele propôs, conhecida como Rabin-OT, é um esquema de comunicação onde Bob e Alice possuem *bits* secretos S_B e S_A, respectivamente, e desejam trocá-los sem auxílio de uma terceira parte ou de um hardware seguro. Para isso, Rabin assume que Alice envia *bits* para Bob, que os recebe com probabilidade $p = 0,5$, sem que Alice saiba quando isso ocorre. Essa versão de OT é bastante similar a um canal BEC com probabilidade $p = 0,5$.

Uma variação conhecida como *one-out-of-two oblivious transfer*, ou resumidamente 1-2 OT, foi posteriormente introduzida por Even, Goldreich e Lempel [30]. Nessa construção, Alice tem 2 *bits* secretos, b_0 e b_1, e deseja comunicar um deles para Bob, sem revelá-los simultaneamente. Bob deseja conhecer o valor do *bit* b_s sem revelar para Alice sua escolha, enquanto permanece leigo sobre o valor do outro *bit* b_{1-s}. As duas construções de OT são equivalentes, conforme demonstrado por Crépeau [31].

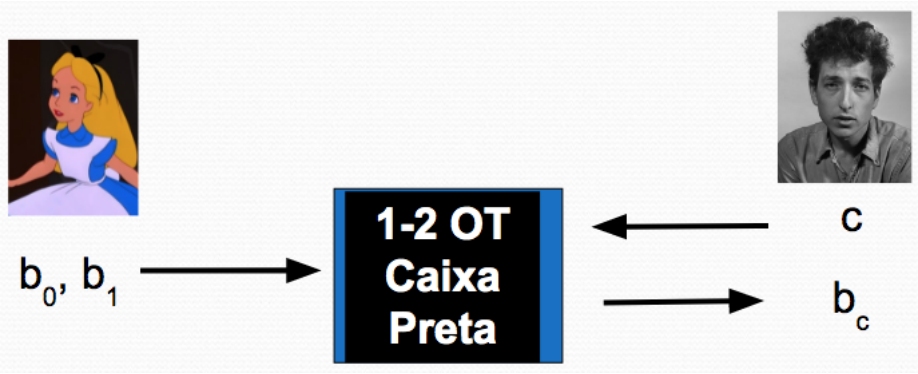

Figura 2.1: *One-out-of-two Oblivious Transfer*
(adaptada das fontes `https://segredosdomundo.r7.com/alice-no-pais-das-maravilhas/` e `https://english.worldmagazine.it/164616/`)

De forma geral, existem outras variações da primitiva, tais como m-out-of-n OT, onde Alice possui como entrada do protocolo um conjunto de n *bits* secretos e deseja transmitir para Bob apenas $m < n$ dentre eles; ou o *string*-OT, onde *strings* binárias são apresentadas como entradas do protocolo, ao invés de *bits*. A relevância de OT se deve à sua universalidade, pois quando está disponível, qualquer computação segura pode ser implementada por meio de redução como

caixa preta a essa primitiva, conforme provou Kilian em [32]. A primitiva OT está para protocolos criptográficos assim como a porta Não-E (NAND) está para circuitos eletrônicos.

Palmieri e Pereira [33] apresentaram o primeiro protocolo de OT baseado em canais com atraso variável. A grande vantagem desse tipo de canal está na sua maior aderência a modelos realistas de ruído comumente presentes em redes como a Internet. Além disso, a dependência do conhecimento exato do nível de ruído para o funcionamento de protocolos que implementam primitivas como OT é menor, conforme demonstrado em [34]. Palmieri e Pereira também demonstraram que as suas premissas eram bastante práticas por meio da implementação em software do protocolo de OT em uma rede TCP/IP.

2.5 Coin Flipping

Um problema muito conhecido em computação segura entre duas partes foi proposto por Manuel Blum em 1981 [35]. O protocolo apresentado por Blum propõe uma solução para a seguinte situação hipotética:

"*Alice e Bob se divorciaram e querem decidir à distância, pois não desejam mais se ver, quem vai ficar com o carro. Eles preferem não envolver outras pessoas na briga, de modo a evitarem exposição excessiva. Para isso, eles resolvem jogar cara-ou-coroa pelo telefone, porém um não confia no outro. Como proceder neste caso, tal que Bob possa confiar na escolha de Alice, garantindo que ela não possa trapacear?*"

Esse é um exemplo de primitiva criptográfica conhecida na literatura da área de computação segura entre duas partes como *Coin Flipping*, onde os participantes se engajam na obtenção do resultado de um sorteio, entretanto sem terem confiança mútua e sem possibilitarem que o outro trapaceie. Percebe-se que tal computação pode ser realizada trivialmente com o auxílio de uma terceira parte confiável. Entretanto, conforme visto no exemplo acima, comumente os participantes preferem não se expor.

Assim, o objetivo é encontrar protocolos de computação segura entre duas partes apenas, sem a necessidade do auxílio externo de uma terceira parte confiável. Contudo, sabe-se que essa é uma tarefa impossível de se realizar do nada, ou seja, sem ao menos uma hipótese adicional. Há implementações cuja hipótese se baseia em restrições computacionais, ou seja, seguras contra adversários com poder computacional polinomial limitado. No entanto, a segurança de tais implementações é baseada ainda em problemas matemáticos considerados intratáveis, mas não comprovadamente, como a fatoração do produto de dois números primos grandes ou o cálculo do logaritmo discreto em corpos finitos com muitos elementos.

Por outro lado, há hipóteses que permitem a realização dessa tarefa computacional de modo incondicionalmente seguro. Ou seja, mesmo um adversário com poder computacional ilimitado não possui uma estratégia melhor do que advinhar ao tentar obter informação adicional indevida. É desejável se obter primitvas criptográficas incondicionalmente seguras baseadas em hipótese menos restritiva ou mais simples possível.

2.6 Comprometimento de Bit

Bit Commitment (BC), Comprometimento de Bit em português, é uma primitiva criptográfica introduzida por Manuel Blum [35] que permite a um emissor se comprometer com o valor de um *bit* através do envio de informação vestigial ao receptor, mas sem revelar o verdadeiro valor do *bit*. Caso o receptor exija comprovação do valor comprometido, o emissor envia informação adicional ao receptor, permitindo verificar indubitavelmente se o *bit* anunciado corresponde àquele comprometido previamente. O receptor irá permanecer completamente ignorante sobre o real valor do *bit* antes de o emissor revelá-lo, enquanto o remetente não conseguirá mudar o valor comprometido, enviando uma informação vestigial falsa ao destinatário, sem ser detectado.

A primitiva de BC é a versão digital da funcionalidade do envelope selado, comum em partidas de xadrez. Para que os jogadores possam descansar ao final da noite, quando o jogo ainda não terminou, o árbitro da partida solicita ao jogador da vez a inscrição de seu próximo lance em uma folha de papel, que é guardada em um envelope opaco e selado. Essa é a chamada Fase de Comprometimento de uma primitiva de BC, ilustrada abaixo:

Figura 2.2: Fase de comprometimento de um protocolo de BC
(adaptada de `https://www.nytimes.com/2020/10/16/arts/television/queens-gambit-chess-netflix.html`)

No dia seguinte, ao reiniciar a partida, o árbitro abre o envelope na frente de ambos os jogadores e realiza o movimento anotado no papel. Com isso, o jogador que estava na vez não disporá do tempo de descanço durante a noite para pensar em seu lance, assim como o jogador adversário também não terá essa possibilidade, uma vez que não fica sabendo do lance que será efetuado antes do recomeço do jogo. Essa é a chamada Fase de Abertura de uma primitiva de comprometimento (BC) e está ilustrada na figura a seguir:

Figura 2.3: Fase de abertura de um protocolo de BC
(adaptada de `https://www.nytimes.com/2020/10/16/arts/television/queens-gambit-chess-netflix.html`)

A segurança da funcionalidade ideal de BC está no fato de Bob não receber nenhuma informação sobre o comprometimento de Alice antes da fase de abertura ser executada, assim como Alice não poder mudar de ideia sobre sua escolha após a fase de comprometimento ser finalizada.

O Comprometimento de Bit é uma primitiva essencial na construção de inúmeras funcionalidades criptográficas, como provas gerais de conhecimento nulo (*general zero knowledge proofs*) [36, 37], assinaturas digitais [38], assim como computação segura distribuída [39, 40]. Extensivos estudos em criptografia moderna foram feitos à respeito dessa primitiva [41, 42, 43], baseando inclusive a construção do protocolo no uso de pseudo-aleatoriedade [44], na impossibilidade de comunicação superluminal [45], limitação do espaço em memória [46, 47, 48, 49], a existência de tokens de hardware à prova de violação [50, 51, 52], correlações ditas *non-signaling* [53], dentre outros. A composição universal de primitivas criptográficas de BC estatisticamente seguras com base em canais ruidosos também foi investigada na literatura [54, 55, 56].

A funcionalidade de *Coin Flipping* pode ser integralmente construída somente com base em BC. Da mesma forma, BC pode ser obtido com base em uma primitiva de OT. Porém, do ponto de vista da utilização de recursos, as implementações de *Coin Flipping* com base em BC são diretas e, por isso, mais eficientes que as reduções caixa preta de BC à primitiva de OT.

2.6.1 Comprometimentos Computacionalmente Seguros

A segurança baseada no paradigma computacional envolve a suposição de que alguns problemas matemáticos são intratáveis para adversários com poder computacional limitado. Com base nessa

classe de problemas computacionais é possível construir protocolos de BC incondicionalmente seguros para o receptor, mas computacionalmente seguros para o emissor [44]. De modo análogo, é possível construir protocolos incondicionalmente seguros para o emissor, mas computacionalmente seguros para o receptor [39]. Porém, não é possível construir protocolos de BC onde a segurança é incondicional tanto para o emissor quanto para o receptor.

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 no caso onde a restrição é apenas na capacidade computacional. Dessa forma, não é possível para as partes esconder informação alguma uma da outra usando os dados obtidos na realização do protocolo, apenas impor que será difícil para a outra parte realizar a tarefa de trapacear.

2.6.2 Comprometimentos Incondicionalmente Seguros

Uma das formas de se quebrar a condição de simetria foi apresentada por Crépeau e Kilian em [20]. A idéia deles se baseou na construção de um protocolo de BC baseado em canais ruidosos. Os autores mostraram uma redução da primitiva criptográfica OT ao canal BSC, o que de fato implica na redução da primitiva BC ao canal BSC, já que é conhecida uma redução caixa preta de BC para OT [32].

Crepeau, em [57], introduziu um protocolo de BC baseado diretamente no canal BSC, obtendo uma implementação mais eficiente. Em geral, implementações diretas de BC são mais eficientes do que aquelas obtidas via uma redução caixa preta a OT. Inclusive, essa é uma das motivações para a elaboração da presente tese.

Existem diversas implementações de protocolos de BC baseadas em canais ruidosos. Contudo, a grande maioria delas são apenas variações dos dois principais modelos de canais discretos sem memória: os canais BSC e BEC.

2.6.3 Weak and Unfair Noisy Channels

Um esquema de comprometimento baseado em uma hipótese mais fraca e mais realista, onde os participantes têm controle parcial sobre o ruído introduzido no canal, conhecida como canais ruidosos injustos (*unfair noisy channels*), foi proposta por Damgård, Kilian e Salvail em [42]. Nessa construção, o adversário passa a ter informação mais precisa sobre o comportamento do canal do que a parte honesta, podendo inclusive controlar parcialmente os parâmetros do canal. Ao invés de uma probabilidade de erro fixa, como no caso típico do canal BSC, os canais ruidosos injustos funcionam com ruído podendo assumir valores dentro de uma faixa de possíveis probabilidades, além de permitir ao adversário saber exatamente qual o real nível de ruído em uma dada utilização do canal, uma vantagem em relação à parte honesta. A idéia dessa abordagem é justamente tentar aproximar o cenário teórico do real, no qual as restrições impostas tornam inviável a implementação desses protocolos. Embora tenham obtido relativo sucesso nessa abordagem mais flexível, a grande maioria dos protocolos propostos ainda não é eficiente a ponto de serem implementáveis.

Em [58], Wullschleger propõe um novo tipo de canal ruidoso, o chamado *Weak Noisy Channel* (WNC), Canal Ruidoso Fraco em português. Em seu trabalho, ele redefine os dois canais ruidosos clássicos em termos do conceito da primitiva "fraca": *Weak Erasure Channel* (WEC) e o *Weak Binary Symmetric Channel* (WBSC), Canal Binário Simétrico Fraco em português. O mote do resultado apresentado em [58] é definir canais em termos de condições mínimas que devem satisfazer, mas não com base em funcionalidades pré-definidas. Dessa forma, o adversário dispõe de uma liberdade ainda maior para atuar maliciosamente, por exemplo, tendo o poder de saber com certa probabilidade se o *bit* enviado ao outro participante através do canal foi recebido sem ruído.

2.7 Taxas, Capacidade e Eficiência

O resultado central da teoria da informação é a medida da Capacidade do Canal Ruidoso [59]. Com isso, Shannon resolveu um problema que havia em aberto na sua época sobre a quantidade máxima de informação que poderia trafegar em um canal sem que o ruído provocasse perdas irreversíveis de informação. A resposta estava na Informação Mútua entre as variáveis aleatórias que modelam entrada e saída do canal.

Wyner introduziu o conceito de Capacidade de Sigilo para estabelecer a qual taxa Alice pode enviar para Bob informação por um canal ruidoso sem que Eva, o adversário, obtenha uma quantidade significativa dessa informação indevidamente [12]. Em sua construção, Wyner relaxou a premissa do resultado de Shannon, permitindo que Eva, que espiona o canal, obtenha uma versão ruidosa da saída do canal obtida por Bob, o destinatário.

Maurer [14] introduziu a possibilidade das partes disporem de um canal de comunicação bidirecional, autenticado, público e sem ruído. Com isso, conseguiu estender o resultado para casos mais gerais, onde o nível de ruído do canal do participante malicioso, Eva, é menor que o ruído do canal entre as partes honestas, Alice e Bob. Por se diferenciar do resultado de Wyner, onde a comunicação era em sentido único e feita com o envio direto da mensagem pelo canal, Maurer e Wolf [60] introduziram o modelo de observação de uma fonte discreta sem memória e obtiveram uma taxa que define o tamanho da chave destilada pelos participantes honestos em relação a quantidade de observações realizadas.

Maurer [23] e, de forma independente, Ahlswede e Csiszar [61], também definiram a Capacidade de Chave Secreta de um canal, dado pela razão entre a maior chave secreta que Alice e Bob conseguem acordar pela quantidade de dados que necessitam trafegar pelo canal ruidoso. Vários estudos foram feitos aplicando e estendendo esse conceito para casos de múltiplos terminais [62, 63], canais de múltiplo acesso (MIMO) [64, 65], canais em desvanecimento (*fading*) [66], entre outros [67]. Finalmente, Maurer e Wolf observaram que se um canal bidirecional sem ruído e autenticado estiver disponível para Alice e Bob, as partes confiáveis do protocolo, então mesmo em casos onde o ruído na saída do canal de Eva é menor do que o ruído na saída do canal de Alice e de Bob é possível obter chaves secretas com taxas estritamente positivas [60].

Nascimento e Winter [68] estabeleceram o conceito de Capacidade de Oblivious Transfer de um canal, que mede a melhor forma de se implementar *string*-OT a partir de canais ruidosos. Vários

são os resultados estendendo o estudo para diferentes canais, como no caso de *erasure channels* [69, 70, 71]. Um protocolo é tão eficiente em termos de capacidade de OT quanto maior for o tamanho da string que Alice comunica para Bob através da primitiva, dada uma quantidade fixa arbitrária de usos do canal. Os primeiros protocolos propondo implementações de OT com base em canais ruidosos apresentavam taxas assintoticamente desprezíveis [29]. Posteriormente, surgiram trabalhos onde as soluções apresentavam taxas estritamente positivas [70]. O protocolo de OT construído por Pereira e Palmieri [33] baseado em canais com atraso não trata a questão sobre a capacidade de OT do canal.

Winter, Nascimento e Imai [72] definiram a taxa de comprometimento de um canal discreto sem memória como sendo a razão entre a quantidade de *bits* que Alice se compromete e o número de vezes que o canal ruidoso é usado na execução do protocolo. A Capacidade de Comprometimento de um canal discreto sem memória se mostrou igual a equivocação deste canal, após removidas quaisquer redundâncias triviais, mesmo quando um canal de comunicação bidirecional sem ruído está disponível para os participantes. Nascimento *et al* ainda mostraram que a capacidade de comprometimento de um canal com ruído Gaussiano é infinita [73]. A capacidade de comprometimento para canais *unfair* também foi estudada [74].

Capítulo 3

Motivações e Contribuições

Palmieri e Pereira propuseram em [33] um tipo de canal ruidoso ainda pouco explorado na literatura de criptografia, o chamado *Binary Discrete-time Delaying Channel* (BDDC). Eles construíram baseado nesse tipo de canal um protocolo que implementa a primitiva criptográfica OT, segura contra um **adversário passivo**, também chamado honesto-porém-curioso. Esse tipo de adversário tenta obter informação indevida sobre os dados do outro participante, mas não se desvia do protocolo. Um **adversário ativo** (também chamado de malicioso), por outro lado, pode trapacear de forma arbitrária.

Os autores afirmam em [34] que o canal BDDC equivale a um canal de reordenamento de pacotes. Além disso, propuseram um protocolo de OT para esse novo canal, alegando ser incondicionalmente seguro. Porém, a segurança do protocolo proposto por eles foi demonstrada apenas para o caso do adversário passivo, assumindo-se uma extensão para o caso do adversário malicioso com base nos resultados [75, 76] que realizam reduções caixa preta utilizando compiladores.

Um primeiro aspecto importante a ser observado sobre a segurança dos protocolos propostos em [33, 34] está no fato de a redução caixa preta utilizando compiladores demandar a existência da primitiva de BC, segura contra um adversário malicioso. Essa primitiva ainda não havia sido definida para os canais de atraso ou de reordenamento, até a realização do presente trabalho. Ou seja, a redução só é possível nesse caso para um protocolo de BC construído sobre outro tipo de canal.

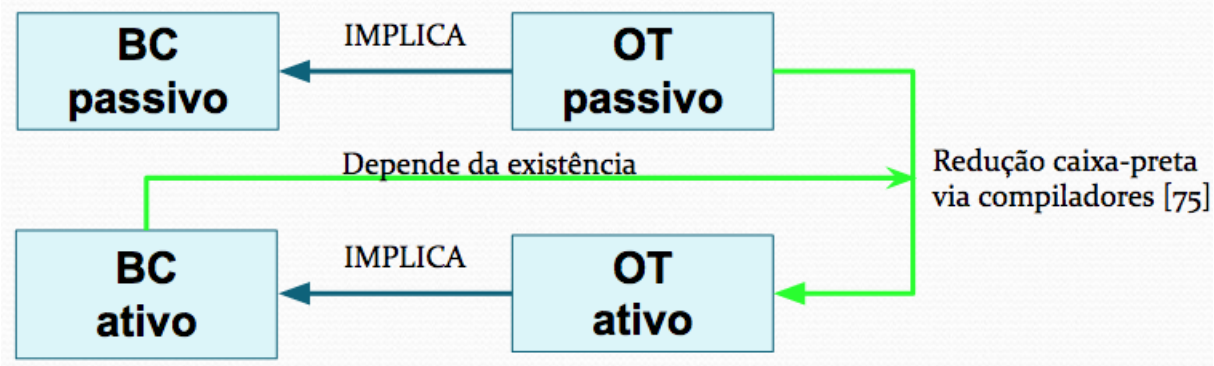

Figura 3.1: Esquema de redução caixa preta usando compiladores

A existência da primitiva de OT segura contra um adversário passivo implica na existência de uma primitiva de BC também segura apenas contra um adversário passivo. Porém, a redução via compiladores necessita de um BC incondicionalmente seguro contra adversários maliciosos. Logo, a afirmação dos autores carece da existência de uma primitiva de BC incondicionalmente segura baseada no canal de reordenamento para ser válida, conforme ilustra a Figura 3.1. Esta tese tem como uma de suas motivações fechar essa lacuna.

O efeito de reordenamento de pacotes de dados em redes de alta velocidade, como é o caso do backbone da Internet, é muito tratado na literatura de redes de comunicação, mas ainda negligenciado na literatura de criptografia. Assim, outra motivação para a elaboração desta tese foi explorar essa vertente de canais dentro da literatura de criptografia. Definimos no Capítulo 5 o Canal com Ruído de Reordenamento de Pacotes (*Packet Reordering Noisy Channel - PRNC*), ao qual passaremos a nos referir daqui em diante.

Trata-se de uma vertente diferente de canal, uma vez que a transmissão através do PRNC é do tipo único uso (*one shot*). Isso ocorre porque a transposição entre pares de pacotes vizinhos, ou inversão, torna as probabilidades de ocorrência dos eventos dependentes do comportamento de suas vizinhanças. Um canal binário simétrico (*Binary Symmetric Channel - BSC*) típico pode ser utilizado repetidas vezes para a transmissão dos dados, já que a probabilidade de um *bit* mudar de valor por conta de ruído é considerada independente da vizinhança e identicamente distribuida para cada *bit*.

Com isso, resultados que convergem para a média devido à lei dos grandes números no caso de muitas utilizações de um canal BSC não mais se aplicam ao canal PRNC. Logo, o instrumental matemático clássico da entropia de Shannon não é válido para a obtenção das medidas de capacidades e entrópicas do canal PRNC, sendo necessário utilizar o ferramental da entropia de Rényi, mais especificamente a min-entropia, que ao invés de considerar a média, leva em conta o pior caso.

Embora seja amplamente sabido que a existência de uma primitiva de OT implica na realização de qualquer tarefa criptográfica por meio de redução do tipo caixa preta, geralmente de modo muito ineficiente [32], uma das contribuições dessa tese é a construção direta de um esquema de comprometimento eficiente e incondicionalmente seguro para ambos os participantes no modelo adversarial ativo a partir de canais PRNC.

O presente trabalho estabelece uma nova formalização para canais com ruído do tipo reordenamento de pacotes. A finalidade dessa nova construção é facilitar a modelagem do efeito de reordenamento de pacotes em canais ruidosos, simplificando a obtenção de medidas de concentração, dispersão e entrópicas nos cálculos de taxas e capacidades do canal. Ainda em [34], os autores conjecturam que o canal BDDC é equivalente ao canal com ruído de reordenamento de pacotes, para alguma distribuição de probabilidade arbitrária.

Construímos o primeiro protocolo de comprometimento incondicionalmente seguro contra um adversário malicioso baseado diretamente no canal PRNC. Trata-se de uma construção de *string commitment*, cujo objetivo é maximizar o tamanho do comprometimento v de Alice em termos da quantidade n de pacotes de dados trafegados pelo canal. Nesse sentido, o protocolo proposto é eficiente, pois o tamanho do comprometimento realizado por Alice é uma função dos parâmetros

que definem o canal PRNC, sendo seu valor igual a uma fração de n. Finalmente, o protocolo é conciso, realizando apenas duas trocas de mensagens pequenas (bem menores que $|X^n|$) por meio do canal livre de ruído (com correção de erro) na fase de comprometimento, evitando que construções mais complexas, que realizam várias chamadas a uma primitiva criptográfica de BC, tenham uma elevada complexidade de comunicação, nos termos definidos por Yao em [77].

Nossa proposta tem algumas características atrativas, que constituem as principais contribuições deste trabalho. Em síntese, o protocolo de comprometimento proposto é incondicionalmente seguro para ambas as partes, não recaindo sobre qualquer hipótese matemática de intratabilidade não comprovada. O protocolo de comprometimento construído com base em um canal com ruído de reordenamento é o primeiro na literatura, pelo que sabemos. Mais ainda, não é apenas um protocolo de BC de um único *bit*, e sim um *string commitment*. Sua segurança é baseada no modelo adversarial ativo, construído para resistir às ameaças do comportamento mais geral de um participante malicioso. É uma construção direta, feita sem reduções baseadas em primitivas de OT, além de ser bastante suscinta, com baixa complexidade de comunicação.

Uma desvantagem do protocolo proposto nesta tese é a restrição imposta sobre o parâmetro $0 \leq \rho \leq 1$, que caracteriza o nível de ruído do canal de reordenamento, o qual deve estar restrito ao intervalo $0 < \rho < 1/(5+8\varepsilon)$ para que o protocolo seja seguro, embora funcione adequadamente para quaisquer valores possíveis de ρ quando as partes são honestas. Uma das propostas de trabalho futuro é justamente a extensão do resultado de modo a provar que o protocolo é seguro para todo $0 < \rho < 1$, o que exige uma análise aprofundada de casos onde as transposições de pares de pacotes vizinhos não são independentes umas das outras, adentrando no campo de limites de concentração para variáveis aleatórias dependentes.

Capítulo 4

Fundamentos Matemáticos

Apresentamos neste capítulo a notação adotada no trabalho e introduzimos os conceitos relacionados ao desenvolvimento matemático das provas de segurança do protocolo proposto. Além disso, as principais definições e os lemas centrais são estabelecidos já nesta parte do texto, visando consolidar em um único capítulo todas as ferramentas matemáticas necessárias para as construções teóricas que se seguem.

4.1 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 em negrito como caligráficas, dependendo da conveniência no texto, e um elemento do conjunto será representado por letra minúscula. A cardinalidade do conjunto é denotado por $|\mathbf{X}|$, ou o tamanho do alfabeto, por $|\mathcal{X}|$.

Exceto quando dito ao contrário, far-se-á referência às variáveis aleatórias discretas. Para uma variável aleatória X com alfabeto $\mathcal{X}$, seja $\Pr[X = x]$ 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 $\Pr[X = x, Y = y]$, e seja $P_{X|Y=y}(x) := P_{XY}(x, y)/P_Y(y)$ a distribuição de probabilidade condicional quando $P_Y(y) \neq 0$. Ainda, seja U_r a variável aleatória uniformemente distribuída sobre o domínio das sequências binárias de comprimento r, $\{0, 1\}^r$.

Se uma função f for probabilística, então será denotado por $f(x; r)$ ou $f_r(x)$ 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.

4.2 Entropias

A entropia de Shannon é uma medida útil e importante na teoria da informação, particularmente em processos de extração de aleatoriedade. Neste trabalho, os logarítmos usados nas funções estão sempre na base 2, exceto quanto dito o contrário. Define-se a função Entropia como sendo:

$$H(X) = -\sum_{x\in\mathcal{X}} P_X(x)\log P_X(x) \tag{4.1}$$

A entropia de uma variável aleatória com probabilidade binária, também conhecida como variável de Bernoulli $X \sim Bernoulli(p)$, é dada por $\mathsf{H}_b(p) := -p\log p - (1-p)\log(1-p)$. A função de entropia binária, definida como a entropia de um processo de Bernoulli com distribuição de probabilidade $\left(\frac{a}{a+b}; \frac{b}{a+b}\right)$, onde $0 \leq a \leq b$, é dada por $\mathsf{H}_b\left(\frac{a}{a+b}\right) = \frac{a}{a+b}\log\left(\frac{a+b}{a}\right) + \frac{b}{a+b}\log\left(\frac{a+b}{b}\right)$. Observe que $0 \leq \mathsf{H}_b\left(\frac{a}{a+b}\right) = \mathsf{H}_b\left(\frac{b}{a+b}\right) \leq 1$.

A definição de entropia condicional sé baseia na definição de entropia apresentada em (4.1):

$$H(X|Y) = -\sum_{y\in\mathcal{Y}} H(X|Y=y) = -\sum_{y\in\mathcal{Y}}\sum_{x\in\mathcal{X}} P_{X|Y=y}(x)\log P_{X|Y=y}(x) \tag{4.2}$$

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

$$\mathcal{D}(P||Q) = \sum_{x\in\mathcal{X}} P_X(x)\log\frac{P_X(x)}{Q_X(x)} \tag{4.3}$$

A Informação Mútua pode ser formalmente definida em termos da entropia relativa entre a distribuição de probabilidade de duas variáveis aleatórias distintas X e Y:

$$I(X;Y) = \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} P_{XY}(x,y)\log\frac{P_{XY}(x,y)}{P_X(x)P_Y(y)} \tag{4.4}$$

Neste trabalho, quando as distribuições P e Q são variáveis aleatórias de Bernoulli e assumem apenas os valores p, $1-p$ e q, $1-q$, respectivamente, adotou-se a nomenclatura Entropia Relativa Binária e a seguinte convenção para notação:

Definição 4.2. *A entropia relativa binária $\mathsf{d}(p||q)$ entre duas distribuições de probabilidade P e Q é definida como*

$$\mathsf{d}(p||q) = p\log\frac{p}{q} + (1-p)\log\frac{1-p}{1-q} \tag{4.5}$$

Além dessas definições básicas de entropia, será necessário introduzir outras mais específicas, já que a entropia de Shannon fornece apenas a incerteza média de uma fonte. Em muitos casos de interesse será necessário conhecer a incerteza miníma de uma fonte. Nesses casos, a entropia de Shannon capta apenas uma solução parcial do problema, já que o limite inferior pode estar bem abaixo 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 respostas mais apropriadas.

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

$$H_\infty(X) = \min_x \log(1/P_X(x)). \tag{4.6}$$

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

$$H_\infty(X|Y) = \min_y H_\infty(X|Y=y) = \min_x \min_y \log\left(1/P_{X|Y=y}(x)\right) \tag{4.7}$$

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

$$H_0(X) = \log|\{x \in X | P_X(x) > 0\}| \tag{4.8}$$

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

$$H_0(X|Y) = \max_y H_0(X|Y=y). \tag{4.9}$$

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

$$\mathsf{SD}(P_X, P_Y) = \|P_X - P_Y\| := \frac{1}{2}\sum_{v\in\mathcal{V}} |P_X(v) - P_Y(v)|. \tag{4.10}$$

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

$$H_\infty^\epsilon(X) = \max_{X': \|P_{X'} - P_X\| \leq \epsilon} H_\infty(X'), \tag{4.11}$$

$$H_\infty^\epsilon(X|Y) = \max_{X'Y': \|P_{X'Y'} - P_{XY}\| \leq \epsilon} H_\infty(X'|Y'), \tag{4.12}$$

$$H_0^\epsilon(X) = \min_{X': \|P_{X'} - P_X\| \leq \epsilon} H_0(X'), \tag{4.13}$$

$$H_0^\epsilon(X|Y) = \min_{X'Y': \|P_{X'Y'} - P_{XY}\| \leq \epsilon} H_0(X'|Y'). \tag{4.14}$$

A regra da cadeia da entropia suave condicionada a uma variável aleatória adicional Z foi estudada em [78]. Para todo $\varepsilon, \varepsilon', \varepsilon'' \geq 0$, essas desigualdades estão definidas a seguir:

$$H_{\infty}^{\varepsilon}(X|YZ) \leq H_{\infty}^{\varepsilon+\varepsilon'}(XY|Z) - H_{\infty}^{\varepsilon'}(Y|Z) \tag{4.15}$$

$$H_{\infty}^{\varepsilon+\varepsilon'+\varepsilon''}(X|YZ) > H_{\infty}^{\varepsilon'}(XY|Z) - H_{0}^{\varepsilon''}(Y|Z) - \log(1/\varepsilon) \tag{4.16}$$

$$H_{0}^{\varepsilon+\varepsilon'+\varepsilon''}(X|YZ) < H_{0}^{\varepsilon'}(XY|Z) - H_{\infty}^{\varepsilon''}(Y|Z) + \log(1/\varepsilon) \tag{4.17}$$

$$H_{0}^{\varepsilon}(X|YZ) \geq H_{0}^{\varepsilon+\varepsilon'}(XY|Z) - H_{0}^{\varepsilon'}(Y|Z) \tag{4.18}$$

4.3 Funções de Hash 2-Universal

Devido ao papel central na construção do protocolo proposto neste trabalho, faz-se de suma importância relembrar a definição de função de *hash* 2-universal, assim como introduzido por Carter and Wegman [79]. Uma família $\mathcal{H}$ consiste de um conjunto de funções de *hash* 2-universal que mapeiam mensagens de um domínio de tamanho $|\mathcal{M}| = \{0,1\}^m$ em uma imagem de tamanho $|\mathcal{W}| = \{0,1\}^w$. A seguir, define-se a probabilidade de ocorrência de colisão em funções de *hash* 2-universal, dado que a função h é escolhida aleatoriamente com distribuição uniforme dentre a família $\mathcal{H}$:

Definição 4.3 (Funções de Hash 2-Universal). *Uma classe $\mathcal{H}$ de funções de hash que mapeiam $\mathcal{M} \to \mathcal{W}$ é dita* 2-universal *se, para quaisquer valores distintos $m_1, m_2 \in \mathcal{M}$,*

$$\Pr[h(m_1) = h(m_2)] \leq \frac{1}{|\mathcal{W}|} \tag{4.19}$$

onde h é escolhida aleatoriamente com distribuição uniforme da classe $\mathcal{H}$.

4.4 Extratores de Aleatoriedade

Segue a definição de extratores de aleatoriedade forte, conforme estabelecido em [80].

Definição 4.4 (Strong Randomness Extractors). *Um extrator de aleatoriedade forte é uma função eficiente $\mathsf{Ext} : \{0,1\}^n \times \{0,1\}^r \to \{0,1\}^w$ que usa r bits aleatórios como entrada e que para toda distribuição de probabilidade $P_X(x)$ com $H_{\infty}(X) \geq \delta n$, é verdade que*

$$\mathsf{SD}(P_{\mathsf{Ext}(X;U_r)U_r}, P_{U_w U_r}) \leq \epsilon \tag{4.20}$$

Extratores de aleatoriedade podem obter no máximo $w = \delta n - 2\log(1/\epsilon) + O(1)$ *bits* de aleatoriedade com distribuição ϵ-próximo de uniforme. Este limite pode ser alcançado por meio da aplicação do lema *Leftover-Hash*, que para isso faz uso de funções de *hash* 2-universal.

Apresentamos a definição de uma δn-fonte de aleatoriedade, que será relevante para a sintese da notação dos resultados obtidos no decorrer do texto.

Definição 4.5. *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 δn-fonte será tal que, para todo $0 < \delta < 1$, tem-se:*

$$H_\infty(X) \geq \delta n \tag{4.21}$$

4.5 Privacy Amplification

Privacy Amplification, ou Amplificação de Privacidade, é um conceito usado com frequência quando se trata de segurança incondicional. O objetivo dessa técnica é derivar uma nova variável aleatória com distribuição próxima de uniforme e com pouquíssima redundância a partir de uma variável aleatória com distribuição enviesada e excessiva informação redundante. Esse conceito foi inicialmente introduzido por Bennett, Brassard, e Robert [81].

Na prática, quando se tem uma *string* secreta s de tamanho n, onde t desses *bits* são conhecidos pelo adversário, é possível produzir uma nova string com quase $n - t$ *bits*, sobre a qual o adversário possui pouquíssima informação. Neste trabalho, faremos uso das técnicas de amplificação de privacidade sempre com auxílio das ferramentas apresentadas abaixo, o lema *Leftover-Hash*, extratores de aleatoriedade e funções de *hash* 2-universal, com a finalidade de tornar desprezível o conhecimento de um possível adversário sobre a informação secreta de posse dos participantes.

4.6 O lema *Leftover-Hash*

O lema conhecido como *Leftover-Hash* é tratado em diversos trabalhos [80, 82, 83, 84, 81, 85, 86, 87] e estabelece que uma função de *hash* 2-universal permite extrair $w = \delta n - 2\log(1/\epsilon) + 2$ *bits* de aleatoriedade de uma fonte com min-entropia maior ou igual a δn, para n suficientemente grande. Faremos uso da mesma definição do lema *Leftover-Hash* presente em [80] que segue do resultado apresentado em [84].

Lema 4.1 (Leftover-Hash Lemma). *Assuma que a classe $\mathcal{G} : \{0,1\}^n \to \{0,1\}^w$ de funções é 2-universal. Então para g sorteada com distribuição uniforme sobre $\mathcal{G}$, tem-se que*

$$\mathsf{SD}(P_{g(X),g}, P_{U_e,g}) \leq \frac{1}{2}\sqrt{2^{-H_\infty(X)}2^w}. \tag{4.22}$$

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

4.7 Alguns Lemas Técnicos Úteis

O próximo lema aparece em [88]. A sua prova foi adicionada a seguir por ser bastante instrutiva para a compreensão dos resultados do trabalho.

Lema 4.2. *Seja X uma variavel aleatória que representa uma δn-fonte e Y uma variável aleatória arbitrária definida sobre $\mathcal{Y}$, onde $s > 0$. Então, com probabilidade pelo menos $1 - 2^{-s}$, obter-se-á um valor y tal que*

$$H_\infty(X|Y = y) \geq \delta n - \log|\mathcal{Y}| - s \tag{4.23}$$

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

$$\begin{aligned}
H_\infty(X|Y = y) &= -\log \max_{x\in\mathcal{X}} \left(P_{X|Y=y}(x)\right) && (4.24)\\
&= -\log \max_{x\in\mathcal{X}} \left(\frac{P_X(x) \cdot P_{Y|X=x}(y)}{P_Y(y)}\right) && (4.25)\\
&\geq -\log \max_{x\in\mathcal{X}} \left(\frac{P_X(x)}{p_0}\right) && (4.26)\\
&= H_\infty(X) + \log p_0 && (4.27)\\
&= \delta n - \log|\mathcal{Y}| - s && (4.28)
\end{aligned}$$

O que prova o lema. ■

O próximo lema estabelece uma cota superior em um somatório infinito convergente, central na obtenção das provas de segurança para ambas as partes do protocolo proposto nesta tese:

Lema 4.3. *Para $0 \leq \rho \leq 1$ é verdade que*

$$\sum_{i=0}^{\infty} \frac{\rho^i}{(\sum_{j=0}^{i} \rho^j)^2} \leq 1 + \rho \tag{4.29}$$

Prova: Seja a seguinte identidade

$$\frac{\rho^n}{1 + \rho + \cdots + \rho^{n-1}} - \frac{\rho^{n+1}}{1 + \rho + \cdots + \rho^n} = \frac{\rho^n}{1 + \rho + \cdots + \rho^{n-1}} \cdot \frac{1}{1 + \rho + \cdots + \rho^n} \tag{4.30}$$

Vamos provar sua validade por indução. Iniciamos mostrando que ela é válida para o caso quando $n = 1$:

$$\begin{aligned}
\frac{\rho}{1} - \frac{\rho^2}{1+\rho} &= \rho\left(1 - \frac{\rho}{1+\rho}\right) && (4.31)\\
&= \rho\left(\frac{1+\rho-\rho}{1+\rho}\right) && (4.32)\\
&= \frac{\rho}{1} \cdot \frac{1}{1+\rho} && (4.33)
\end{aligned}$$

Pelo princípio da indução matemática, assumindo que seja válido o caso para n, demonstramos a seguir que também é válido para $n + 1$:

$$\frac{\rho^{(n+1)}}{1 + \rho + \cdots + \rho^{(n+1)-1}} - \frac{\rho^{(n+1)+1}}{1 + \rho + \cdots + \rho^{(n+1)}} = \rho^{n+1}\left(\frac{1}{1 + \rho + \cdots + \rho^n} - \frac{\rho}{1 + \rho + \cdots + \rho^{n+1}}\right) \tag{4.34}$$

$$= \rho^{n+1}\left(\frac{1 + \rho + \cdots + \rho^{n+1} - \rho(1 + \rho + \cdots + \rho^n)}{(1 + \rho + \cdots + \rho^n)(1 + \rho + \cdots + \rho^{n+1})}\right) \tag{4.35}$$

$$\therefore \frac{\rho^{(n+1)}}{1+\rho+\cdots+\rho^{(n+1)-1}} - \frac{\rho^{(n+1)+1}}{1+\rho+\cdots+\rho^{(n+1)}} = \frac{\rho^{(n+1)}}{1+\rho+\cdots+\rho^{(n+1)-1}} \cdot \frac{1}{1+\rho+\cdots+\rho^{(n+1)}} \tag{4.36}$$

Logo, ela é válida para todo $n \geq 1$.

Observe que é possível desenvolver a seguinte recorrência para ρ com base na identidade acima:

$$\rho = \frac{\rho}{1+\rho} + \frac{\rho^2}{1+\rho} \tag{4.37}$$

$$= \frac{\rho}{1+\rho} + \frac{\rho^2}{1+\rho} \cdot \frac{1}{1+\rho+\rho^2} + \frac{\rho^3}{1+\rho+\rho^2} \tag{4.38}$$

$$= \frac{\rho}{1+\rho} + \frac{\rho^2}{1+\rho} \cdot \frac{1}{1+\rho+\rho^2} + \frac{\rho^3}{1+\rho+\rho^2} \cdot \frac{1}{1+\rho+\rho^2+\rho^3} + \frac{\rho^4}{1+\rho+\rho^2+\rho^3} \tag{4.39}$$

$$\vdots$$

$$= \frac{\rho}{1+\rho} + \frac{\rho^2}{1+\rho} \cdot \frac{1}{1+\rho+\rho^2} + \cdots$$

$$\cdots + \frac{\rho^{n+1}}{1+\rho+\rho^2+\cdots+\rho^n} \cdot \frac{1}{1+\rho+\rho^2+\cdots+\rho^n+\rho^{n+1}} + \cdots \tag{4.40}$$

Destacamos que cada termo da expansão infinita acima é maior que o termo correspondente da série infinita proposta. É facil verificar a validade dessa afirmação, uma vez que a diferença entre os termos da expansão e da série que têm a mesma potência de ρ no numerador é sempre positiva:

$$\frac{\rho}{1+\rho} - \frac{\rho}{(1+\rho)^2} = \frac{\rho^2}{(1+\rho)^2} \tag{4.41}$$

$$\frac{\rho^2}{1+\rho} \cdot \frac{1}{1+\rho+\rho^2} - \frac{\rho^2}{(1+\rho+\rho^2)^2} = \frac{\rho^2}{1+\rho} \cdot \frac{\rho^2}{(1+\rho+\rho^2)^2} \tag{4.42}$$

$$\frac{\rho^3}{1+\rho+\rho^2} \cdot \frac{1}{1+\rho+\rho^2+\rho^3} - \frac{\rho^3}{(1+\rho+\rho^2+\rho^3)^2} = \frac{\rho^3}{1+\rho+\rho^2} \cdot \frac{\rho^3}{(1+\rho+\rho^2+\rho^3)^2} \tag{4.43}$$

$$\vdots$$

$$\frac{\rho^{n+1}}{1+\rho+\cdots+\rho^n} \cdot \frac{1}{1+\rho+\cdots+\rho^{n+1}} - \frac{\rho^{n+1}}{(1+\rho+\cdots+\rho^{n+1})^2}$$

$$= \frac{\rho^{n+1}}{1+\rho+\cdots+\rho^n} \frac{\rho^{n+1}}{(1+\rho+\cdots+\rho^{n+1})^2} \tag{4.44}$$

Isso decorre do fato de o denominador dos termos da expansão ser sempre menor que o denominador dos termos da série, quando ambos possuem o mesmo numerador. Finalmente:

$$\sum_{i=0}^{\infty} \frac{\rho^i}{(\sum_{j=0}^{i} \rho^j)^2} = 1 + \frac{\rho}{(1+\rho)^2} + \frac{\rho^2}{(1+\rho+\rho^2)^2} + \cdots \tag{4.45}$$

$$\leq 1 + \frac{\rho}{1+\rho} + \frac{\rho^2}{(1+\rho)(1+\rho+\rho^2)} + \cdots \tag{4.46}$$

$$\leq 1 + \rho \tag{4.47}$$

■

A seguir apresentamos as desigualdades que subsidiam a computação das cotas obtidas na prova de corretude do protocolo. A desigualdade de Markov é a base para as desigualdades de Chebyshev e de Chernoff-Hoeffding, essenciais nas demonstrações de limites de concentração para variáveis aleatórias independentes.

4.7.1 As desigualdades de Markov, Chebyshev e Chernoff-Hoeffding

As desigualdades a seguir formam a base das computações dos limites de concentração da prova de corretude do protocolo. A fim de tornar as demonstrações o mais autocontido possível, resolvemos incluí-las neste trabalho. O desenvolvimento realizado foi todo baseado em [89].

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

Lema 4.4. *Se X é uma variável aleatória não negativa, então para todo $a > 0$*

$$P_r[X \geq a] \leq \frac{E[X]}{a} \tag{4.48}$$

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 seguinte variável aleatória $a \cdot I_{[a;\infty)}(X)$, 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,

$$E[aI_{[a;\infty)}(X)] = 0 \cdot \Pr[X < a] + a \cdot \Pr[X \geq a] = a \cdot \Pr[X \geq a] \tag{4.49}$$

Agora, observe que $a \cdot I_{[a;\infty)}(X) \leq X$. 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 $I_{[a;\infty)}(X) = 1$, 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 (4.48):

$$P_r[X \geq a] = \frac{E[aI_{[a;\infty)}(X)]}{a} \leq \frac{E[X]}{a} \tag{4.50}$$

■

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

$$P_r[|X| \geq a] \leq \frac{E[X^2]}{a^2} \tag{4.51}$$

Prova: 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,

$$P_r[|X| \geq a] = P_r[|X|^2 \geq a^2] \leq \frac{E[|X|^2]}{a^2} \tag{4.52}$$

onde o último passo segue diretamente da desigualdade de Markov (4.48). ■

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 $\mu = E[X]$ for finito, então tomando $|W|$ como sendo $|X - \mu|$ e definindo $a = \varepsilon\sigma$, onde σ é o desvio padrão de X, a desigualdade pode ser reescrita da seguinte forma:

$$P_r[|W| \geq a] \leq \frac{E[|W|^2]}{a^2} \leq \frac{E[|X-\mu|^2]}{(\varepsilon\sigma)^2} \leq \frac{E[|X^2 - 2\mu X + \mu^2|]}{(\varepsilon\sigma)^2} \leq \frac{E[X^2] - E[X]^2}{(\varepsilon\sigma)^2} \tag{4.53}$$

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

$$P_r[|X - \mu| \geq \varepsilon\sigma] \leq \frac{1}{\varepsilon^2} \tag{4.54}$$

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.

A limitação imposta pela desigualdade acima tende a ser melhor para faixas específicas, embora isso não ocorra para o caso assintótico. A seguir, introduzimos a desigualdade mais utilizada para obtenção de limites de concentração apertados, conhecida como Chernoff-Hoeffding:

Lema 4.6. *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 $0 < \delta < 1$:*

$$P_r\left[X \leq (1-\delta)E[X]\right] < \left(\frac{e^{-\delta}}{(1-\delta)^{1-\delta}}\right)^{E[X]} \tag{4.55}$$

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:

$$\{X \geq a\} = \{sX \geq sa\} = \{e^{sX} \geq e^{sa}\} \tag{4.56}$$

$$P_r\left[X \geq a\right] = P_r\left[e^{sX} \geq e^{sa}\right] \leq \frac{E[e^{sX}]}{e^{sa}} \tag{4.57}$$

De modo análogo, temos para a outra cauda:

$$\{X \leq a\} = \{-X \geq -a\} = \{-sX \geq -sa\} = \{e^{-sX} \geq e^{-sa}\} \tag{4.58}$$

$$P_r\left[X \leq a\right] = P_r\left[e^{-sX} \geq e^{-sa}\right] \leq \frac{E[e^{-sX}]}{e^{-sa}} \tag{4.59}$$

obtendo-se as desigualdades (4.57) e (4.59) com a aplicação da desigualdade de Markov (4.48).

Observe agora que a desigualdade (4.59) vale para todo $s > 0$, e o lado esquerdo da expressão não depende de s. Então, é possível minimizar o lado direito da expressão em (4.59) de modo a se obter um limite apertado. Logo, segue que:

$$P_r\left[X \leq a\right] \leq \inf_{s>0} \frac{E[e^{-sX}]}{e^{-sa}} \leq \inf_{s>0} \frac{E\left[e^{-s(X_1+\ldots+X_n)}\right]}{e^{-sa}} \leq \inf_{s>0} \frac{E\left[e^{-sX_1}\cdots e^{-sX_n}\right]}{e^{-sa}} \tag{4.60}$$

$$P_r\left[X \leq a\right] \leq \inf_{s>0} \frac{\prod_{i=1}^{n} E\left[e^{-sX_i}\right]}{e^{-sa}} \tag{4.61}$$

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 na expressão (4.61) acima como sendo:

$$E\left[e^{-sX_i}\right] = \sum_{x=0}^{1} P_X(x) \cdot e^{-sx} = (1 - p_i) + p_i \cdot e^{-s} \tag{4.62}$$

Reescrevendo $(1 - p_i) + p_i \cdot e^{s}$ como $p_i(e^{-s} - 1) + 1$ e lembrando que $1 + y \leq e^{y}$, com estrita desigualdade sempre que $y > 0$, pode-se assumir que $y = p_i(e^{-s} - 1)$. Realizando essa substituição em (4.62) e aplicando o resultado da esperança em (4.61), segue que:

$$\Pr\left[X \leq a\right] < \inf_{s>0} \prod_{i=1}^{n} \frac{(1 - p_i) + p_i \cdot e^{-s}}{e^{-sa}} < \inf_{s>0} \prod_{i=1}^{n} \frac{e^{p_i(e^{-s}-1)}}{e^{-sa}} < \inf_{s>0} \frac{e^{(e^{-s}-1)\sum_{i=1}^{n} p_i}}{e^{-sa}} \tag{4.63}$$

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:

$$\Pr\left[X \leq a\right] < \inf_{s>0} \frac{e^{(e^{-s}-1)E[X]}}{e^{-sa}} \tag{4.64}$$

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

$$\Pr\left[X \leq (1 - \delta)E[X]\right] < \inf_{s>0} \frac{e^{(e^{-s}-1)E[X]}}{e^{-s(1-\delta)E[X]}} \tag{4.65}$$

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:

$$\frac{d}{ds} e^{[(e^{-s}-1)+s(1-\delta)]E[X]} = e^{[(e^{-s}-1)+s(1-\delta)]E[X]} \cdot \left[-e^{-s} + (1 - \delta)\right] E[X] = 0 \tag{4.66}$$

Dado que $s > 0$, então a função $e^{[(e^{-s}-1)+s(1-\delta)]E[X]}$ 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, segue o lema:

$$P_r\left[X \leq (1 - \delta)E[X]\right] < \left(\frac{e^{-\delta}}{(1 - \delta)^{1-\delta}}\right)^{E[X]} \tag{4.67}$$

■

4.8 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 $D_X(x)$. 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 4.6. *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 4.7. *Dado $\digamma$, uma regra de decisão, seja a probabilidade de falha γ definida como sendo a probabilidade de $\digamma(X) = 1$ dado que Λ_0 é a hipótese correta.*

Segue do teorema de Neyman-Pearson [90] que o teste ótimo está em assumir Λ_0 como sendo a hipótese correta se e somente se

$$\log \frac{D_X(x)}{E_X(x)} \geq L \tag{4.68}$$

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 γ. O teorema a seguir, presente no trabalho de Blahut [91], estabelece essa relação:

Teorema 4.1. *Em um teste de hipóteses, as probabilidades de falha η e γ satisfazem a seguinte relação:*

$$\eta \log \frac{\eta}{1-\gamma} + (1-\eta) \log \frac{1-\eta}{\gamma} \leq \sum_{x \in \mathcal{X}} D_X(x) \log \frac{D_X(x)}{E_X(x)} \tag{4.69}$$

$$\therefore \ \mathsf{d}(\eta||1-\gamma) \leq \mathcal{D}(D||E) \tag{4.70}$$

O teorema acima pode ser generalizado para o caso em que informação paralela adicional, modelada pela variável aleatória A com alfabeto $\mathcal{A}$ e distribuição P_A, esteja disponível [91].

Teorema 4.2. *As probabilidades médias de falha $\bar{\eta} = \sum_{a \in \mathcal{A}} P_A(a)\eta(a)$ e $\bar{\gamma} = \sum_{a \in \mathcal{A}} P_A(a)\gamma(a)$ satisfazem a seguinte relação*

$$\mathsf{d}(\bar{\eta}||1-\bar{\gamma}) \leq \sum_{a \in \mathcal{A}} P_A(a) \sum_{x \in \mathcal{X}} C_{X|A=a}(x) \log \frac{C_{X|A=a}(x)}{E_{X|A=a}(x)} \tag{4.71}$$

Capítulo 5

Canal com Ruído de Reordenamento

Wyner introduziu a ideia de utilizar o ruído do canal para permitir a comunicação secreta. Essa simples e poderosa observação possibilita a superação da restrição mais severa do resultado negativo de Shannon sobre segurança perfeita, a produção de chave aleatória do mesmo tamanho da mensagem. Uma alternativa ao modelo de chave pública, o protocolo proposto se baseou no canal binário simétrico e demonstrou a possibilidade de comunicação incondicionalmente segura, consideradas certas características do canal entre as partes e do canal de "grampo". Desde então, o resultado foi estendido de várias formas para cobrir outros canais e cenários, como no caso onde existe, além do canal ruidoso, um canal de *broadcast* entre os participantes, o qual possibilita comunicação incondicionalmente segura entre as partes honestas, mesmo quando o canal de "grampo" é menos ruidoso que o canal principal.

Neste trabalho, modelamos um novo tipo de canal ruidoso, baseado no efeito de reordenamento de pacotes de dados, um efeito típico na Internet. O Canal com Ruído de Reordenamento de Pacotes (PRNC - *Packet Reordering Noisy Channel*, sigla em inglês) visa modelar o comportamento de *switches* e roteadores no encaminhamento de pacotes através de redes de alta velocidade, onde, devido às características de construção dos equipamentos e dos protocolos de comunicação utilizados, os pacotes de dados podem sofrer reordenamentos enquanto trafegam através desses dispositivos de rede [92]. Diversos são os fatores que podem ocasionar a permutação dos pacotes, tais como número de saltos intermediários entre os dispositivos da rede, qualidade do sinal no meio de transmissão, velocidade ponto-a-ponto dos enlaces, nível de congestionamento do tráfego de rede, roteamento por múltiplas rotas, flutuações de roteamento, diferença de tamanho dos pacotes, atraso variável no envio dos pacotes, duração do intervalo entre pacotes, retransmissões, entre outras.

5.1 Canal Binário com Atraso Discreto - BDDC

A primeira ideia de utilizar como primitiva criptográfica um canal cujo o efeito do ruído fosse o atraso dos pacotes apareceu no trabalho de Palmieri e Pereira [33]. O *Binary Discrete-time Delaying Channel* (BDDC), ou Canal Binário com Atraso Discreto em português, foi introduzido por Palmieri e Pereira como modelo para canais com esse tipo de comportamento. Na definição

dos autores, p representa a probabilidade de um elemento sofrer atraso por um intervalo discreto de tempo. No modelo proposto pelos autores, cada elemento admitido na entrada do canal em um instante $t_i \in T$ é unicamente transmitido na saída do canal com probabilidade de que ocorra no instante $u_j \in U$ dada por $Pr[u_j] = p^{(j-i)} - p^{(j-i+1)}$.

O ruído de atraso variável pode ocasionar o efeito de reordenamento de pacotes, mas as distribuições de probabilidade do atraso variável e do reordenamento de pacotes podem não ser as mesmas. Isso devido ao fato de os pacotes vizinhos, aqui chamados de pares, poderem sofrer o mesmo atraso e não permutarem de posição relativa entre eles, ou então o atraso sofrido por um pacote não ser suficiente para ocasionar a permutação de sua posição com a do pacote vizinho na saída do canal.

O efeito de reordenamento de pacotes é mais prático de ser observado e medido no tráfego típico de Internet do que o ruído de atraso variável. Isso porque a medição do reordenamento dispensa o uso de equipamentos especializados, ou considerar questões como a precisão da medida, erros instrumentais e sincronismo de *timestamps* dos pacotes. O efeito resulta na permutação de saída e sua medição é realizada pela contagem da quantidade de inversões realizadas para transformá-la na sequência de pacotes na entrada do canal.

Logo, trata-se de uma escolha mais natural utilizar o reordenamento, ao invés do atraso, para modelar um canal de comutação de pacotes que produz permutações na construção de uma primitiva criptográfica. Além disso, o reordenamento é extremamente comum em redes de comutação de pacotes de alta velocidade, como é o caso da Internet, ou mais especificamente em transmissões de streamings de video, algo em crescente e larga utilização na atualidade. O reordenamento de pacotes é um efeito muito conhecido na literatura de protocolos de comunicação de redes [92].

5.2 PRNC - uma nova definição

Nesta seção propomos uma nova forma de se modelar o efeito de reordenamento de pacotes, distinta da definição proposta por Palmieri e Pereira [33]. Nossa definição está baseada apenas na probabilidade da saída do canal, dada a sequência de pacotes na entrada. O objetivo é construir um modelo matemático para o Canal com Ruído de Reordenamento de Pacotes (*Packet Reordering Noisy Channel - PRNC*) de modo que a função massa de probabilidade para as possíveis saídas do canal seja obtida com naturalidade, de modo a facilitar sobremaneira o cálculo das medidas estatísticas e entrópicas do canal. Assim, o primeiro passo é construir uma definição matemática formal para o canal PRNC.

Uma observação importante a respeito do efeito de reordenamento é sobre o fato de as inversões de posição entre pacotes terem função massa de probabilidade condicional às inversões dos demais pacotes da vizinhança, diferentemente do que ocorre em um canal binário simétrico, onde uma mudança no valor de um *bit* em qualquer posição é independente da probabilidade de mudança do valor dos demais *bits*.

O conceito de permutação por trás do modelo do canal PRNC é uma ferramenta poderosa

para a construção de protocolos criptográficos e foi usado similarmente na técnica de rearranjo de ordem controlada nas primitivas de *Quantum Key Distribution* (QKD) [93], Distribuição de Chave Quântica em português, e de *Quantum Secure Direct Communication* (QSDC) [94], Comunicação Direta Segura Quântica, em português. Porém, destacamos que o canal realiza a permutação dos pacotes no caso do nosso modelo, enquanto os participantes realizam a permutação das partículas no caso dos protocolos quânticos supracitados.

Antes de apresentarmos uma definição formal, vamos elaborar melhor a intuição por trás do comportamento do canal proposto. Modelamos o comportamento coletivo dos vários dispositivos de rede, os possíveis atrasos de comunicação e as diversas rotas existentes, os quais são tipicamente causadores do efeito de reordenamento de pacotes no receptor, por meio de uma caixa preta contendo uma fila de entrada e uma fila de saída, conforme diagrama a seguir:

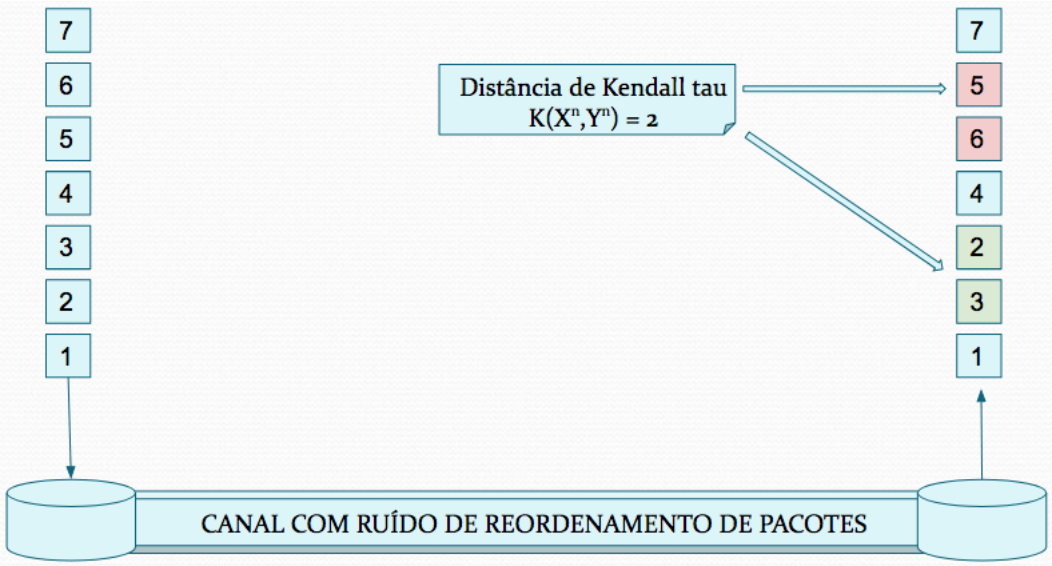

Figura 5.1: Modelo de um canal PRNC caixa preta

O PRNC é uma espécie de canal ruidoso através do qual o emissor transmite uma sequência arbitrariamente ordenada de n pacotes de dados, modelada pela variável aleatória X^n, e o receptor obtém na saída do canal uma nova versão aleatoriamente permutada da sequência original, modelada por Y^n. Para fazer isso, o canal recebe os pacotes enviados por Alice, formando uma fila de entrada $x^n = [x_1, x_2, \ldots, x_n]$. Então, o canal produz uma permutação movendo pacotes da entrada para a fila de saída, com o reordenamento de pacotes podendo ocorrer durante esse processo.

O pacote x_1 é colocado diretamente na fila de saída sem permutação com probabilidade 1. Cada um dos demais pacotes x_i (com $i \in [2, n]$) da fila de entrada é colocado logo atrás de todos os outros pacotes já movidos para a fila de saída, de x_1 até x_{i-1}, e nenhuma permutação ocorre, ou pode ocorrer a transposição de pacotes de dados adjacentes em pares (*inversões*) com cada um deles assentando em uma das $i - 1$ posições possíveis.

Seja cada K_i, para todo $i \in [1, n]$, uma variável aleatória que representa a quantidade de inversões realizadas por cada pacote x_i quando é movido pelo canal da fila de entrada para a fila de saída, onde $0 \leq K_i \leq i - 1$. Destacamos que as variáveis aleatórias $\{K_1, \ldots, K_n\}$ são

independentes, já que a quantidade de inversões que cada pacote sofre ao ser movido de fila independe do resultado anterior dos demais pacotes, porém não são identicamente distribuídas, já que para cada pacote a mais na fila de saída, o próximo pacote a ser movido a partir da fila de entrada possui mais posições de assento possíveis.

Detalhando melhor, se o pacote x_i for colocado na fila de saída atrás de todos os outros pacotes, então $K_i = 0$ e x_i se tornará o último pacote da fila até o momento. Se o pacote x_i inverter de posição com o último pacote já na fila de saída, então $K_i = 1$ e x_i se tornará o penúltimo pacote da fila até o momento. Se a inversão de posição ocorrer com os dois últimos pacotes já na fila de saída, então $K_i = 2$ e x_i se tornará o antepenúltimo pacote da fila e assim sucessivamente.

O algoritmo acima se repete até que o canal tenha movido todos os pacotes da entrada para a fila de saída. Por fim, a permutação formada na fila de saída é representada por $y^n = [y_1, y_2, \ldots, y_n]$, sendo que para algum mapeamento bijetivo b, $x_i = y_{b(i)}$ para cada i.

Definimos $K = \sum_{i=1}^{n} K_i$ como sendo a variável aleatória que representa a quantidade total de transposições de pares de elementos adjacentes (inversões) realizadas pelo canal ao produzir a permutação de saída. Essa quantidade é também conhecida com distância de Kendall tau, definida da seguinte forma:

Definição 5.1 (distância de Kendall tau [95]). *Seja x^n uma sequência de n elementos distintos e y^n uma sequência obtida a partir da permutação dos elementos de x^n. A distância de Kendall tau $K(x^n, y^n)$ entre as sequências x^n e y^n é definida como a menor quantidade de transposições de pares de elementos adjacentes, ou inversões, necessária para transformar x^n em y^n.*

Para quaisquer permutações X^n e Y^n de n elementos distintos, formadas conforme a definição anterior, a distância de Kendall tau entre elas é no mínimo 0 e no máximo

$$\begin{aligned} K(X^n, Y^n) &= \sum_{i=1}^{n} K_i && (5.1)\\ &\leq \sum_{i=1}^{n} i - 1 && (5.2)\\ &= \frac{n(n-1)}{2} && (5.3)\\ &= \mathsf{N} && (5.4) \end{aligned}$$

Para uma dada permutação x^n, o número de Mahonian $M(n, k)$ representa a quantidade de permutações y^n cuja distância de Kendall tau seja $K(x^n, y^n) = k$. Esses números formam o chamado *triângulo de Mahonian*, definido pela recorrência a seguir:

$$\begin{aligned} M(1,0) &= 1,\\ M(1,k) &= 0 \text{ for all integers } k \neq 0,\\ M(n,k) &= \sum_{i=0}^{n-1} M(n-1, k-i) \text{ for integers } n > 1. \end{aligned}$$

A tabela 5.1 abaixo apresenta as primeiras linhas do triângulo de Mahonian[1], sendo que deixamos em branco as posições iguais a zero para destacar os números do triângulo:

Tabela 5.1: Triângulo de Mahonian

n \ k	0	1	2	3	4	5	6	7	8	9	10
1	1										
2	1	1									
3	1	2	2	1							
4	1	3	5	6	5	3	1				
5	1	4	9	15	20	22	20	15	9	4	1

No triângulo de Mahonian, a soma dos termos da n-ésima linha é dada por $n!$. Não é conhecida uma fórmula simples e geral para se obter cada um dos termos, como no caso do triângulo de Pascal. Em [96], o autor apresenta uma complicada expressão para o caso $k \leq n$, cuja quantidade de termos para n grande é da ordem de $1,6\sqrt{k}$. Em [97], Janjić apresenta uma expressão fechada para todo n, bastante complexa, a primeira da literatura pelo que se sabe.

Agora, seja $S_i(\rho)$ a série geométrica

$$S_i(\rho) = \sum_{j=0}^{i-1} \rho^j \tag{5.5}$$

$$= \frac{1-\rho^i}{1-\rho}. \tag{5.6}$$

A função massa de probabilidade de cada variável aleatória K_i pode ser definida usando um parâmetro $0 \leq \rho \leq 1$ que caracteriza o canal. Quando $\rho = 0$, trata-se de um canal trivialmente sem ruído e quando $\rho = 1$, de um canal completamente aleatório, com distribuição de probabilidade uniforme para todas as possíveis saídas. Logo, a faixa de interesse do parâmetro é $0 < \rho < 1$. A modelagem proposta para o canal assume que a probabilidade $\Pr[K_i = k_i]$ decresce exponencialmente a medida que o número de inversões k_i realizadas pelo canal ao adicionar o pacote x_i na fila de saída aumenta, o que se constata na prática a partir da observação experimental desses canais [92]. Normalizando para obtermos uma função massa de probabilidade, temos que:

$$\Pr[K_i = k_i] = \frac{\rho^{k_i}}{\sum_{k_i=0}^{i-1} \rho^{k_i}} \tag{5.7}$$

$$= \frac{\rho^{k_i}}{S_i(\rho)}. \tag{5.8}$$

A probabilidade condicional de a saída do canal apresentar $Y^n = y^n$ dado que a entrada é $X^n = x^n$ pode ser obtida simplesmente pela intersecção das probabilidades de cada pacote x_i ser reordenado. Ou seja, $\Pr[Y^n = y^n | X^n = x^n] = \Pr[K_1 = k_1 \wedge K_2 = k_2 \wedge \cdots \wedge K_n = k_n]$, onde k_i para

[1] Observe que "triângulo" é uma utilização imprópria do termo, uma vez que a quantidade de números de Mahonian por linha cresce de forma quadrática, ao invés de linearmente como no caso do triângulo de Pascal.

todo $i \in \{1, \ldots, n\}$ é o número de inversões que acontecem quando cada pacote x_i é movido da fila de entrada para a de saída, sendo $[y_1, \ldots, y_n]$ a resultado final na saída. Dado que as variáveis aleatórias K_i são independentes, podemos desenvolver ainda mais essa probabilidade condicional da seguinte forma:

$$\Pr[Y^n = y^n | X^n = x^n] = \Pr[K_1 = k_1 \wedge K_2 = k_2 \wedge \cdots \wedge K_n = k_n] \tag{5.9}$$

$$= \prod_{i=1}^{n} \Pr[K_i = k_i] \tag{5.10}$$

$$= \prod_{i=1}^{n} \frac{\rho^{k_i}}{S_i(\rho)} \tag{5.11}$$

$$= \frac{\rho^{\sum_{i=1}^{n} k_i}}{\prod_{i=1}^{n} S_i(\rho)} \tag{5.12}$$

$$= \frac{\rho^{k}}{\prod_{i=1}^{n} S_i(\rho)}, \tag{5.13}$$

onde k é uma realização da variável aleatória $K(X^n, Y^n)$. De agora em diante, usaremos a abreviação $\sigma_n(\rho)$ para denotar o produtório $\prod_{i=1}^{n} S_i(\rho)$. Assim, observe que

$$\sigma_n(\rho) = \prod_{i=1}^{n} S_i(\rho) \tag{5.14}$$

$$= \frac{(1-\rho)(1-\rho^2)\cdots(1-\rho^n)}{(1-\rho)^n} \tag{5.15}$$

$$= \left(\frac{1}{1-\rho}\right)^n \cdot \prod_{i=1}^{n}(1-\rho^i) \tag{5.16}$$

$$= \sum_{k=0}^{\infty} M(n,k)\rho^k \tag{5.17}$$

$$= \sum_{k=0}^{n(n-1)/2} M(n,k)\rho^k, \tag{5.18}$$

Onde a equação (5.17) é a função geradora dos números de Mahonian $M(n,k)$ [98] e a equação (5.18) segue do fato de que, para um n fixo, os números $M(n,k)$ são diferentes de zero apenas no intervalo $0 \leq k \leq \mathsf{N}$.

A nossa definição do canal está fundamentada na distribuição de probabilidade do canal, modelada com base em estatística de permutação de Mahonian [99]. Observe que a probabilidade de uma dada saída do canal diminui exponencialmente com o número de permutação de pares de pacotes efetuadas pelo canal; ou seja, a distância de Kendall tau entre X^n e Y^n. Note que $x^n = y^n$ é a única situação possível no caso em que se tem $\rho = 0$. Finalmente, quando $\rho = 1$, tem-se um caso trivial, simulável por uma caixa preta que entrega aleatoriamente com distribuição uniforme em sua saída uma entre todas as possíveis permutações do espaço amostral, independentemente da sequência de entrada, situação que não permite comunicação efetivamente, o que justifica a escolha do intervalo de funcionamento $0 < \rho < 1$ para o parâmetro característico do ruído do canal.

Enfim, após as considerações anteriores, definimos formalmente o Canal com Ruído de Reordenamento de Pacotes (PRNC) da seguinte forma:

Definição 5.2 (Canal com Ruído de Reordenamento de Pacotes). *Seja $0 < \rho < 1$ um parâmetro fixo que caracteriza o canal. O Canal com Ruído de Reordenamento de Pacotes (The Packet Reordering Noisy Channel - PRNC) recebe como entrada uma sequência $x^n = [x_1, x_2, \ldots, x_n]$ de n pacotes de dados distintos distribuídos de acordo com a variável aleatória $X^n = \{X_1, X_2, \ldots, X_n\}$ com distribuição de probabilidade arbitrária, onde os pacotes de dados têm domínio $\mathcal{X}_i = \{0,1\}^\ell$. O canal apresenta na saída uma sequência $y^n = [y_1, y_2, \ldots, y_n]$ que representa uma permutação da sequência de entrada, tal que exista uma função bijetiva $b : \{1, \ldots n\} \to \{1, \ldots n\}$ de forma que $x_{b(i)} = y_i$ para todo $i \in \{1, \ldots n\}$. A função massa de probabilidade condicional da saída Y^n do canal é dada por*

$$\Pr[Y^n = y^n | X^n = x^n] = \frac{\rho^{K(x^n, y^n)}}{\sigma_n(\rho)}. \tag{5.19}$$

5.3 Modelagem alternativa para o canal PRNC

Introduzimos agora uma forma alternativa de modelar o canal PRNC. Porém, vamos demonstrar que essa alternativa resulta na mesma definição obtida anteriormente. Trata-se apenas de uma outra maneira de olhar o comportamento do canal, sob a visão de um jogo.

Para isso, vamos modelar o comportamento do canal PRNC de forma que ao se apresentar X^n, uma sequência de n pacotes arbitrariamente ordenados, à entrada do canal este decide a sequência de saída Y^n com base no seguinte jogo:

1. O canal fixa um contador i com o valor igual a 1, que aponta para o pacote de posição relativa i na fila de entrada remanescente;
2. O canal toma uma decisão probabilística, executando uma dentre as duas alternativas a seguir:
   (a) com probabilidade $1 - \rho$, retira o pacote na posição i da fila de entrada remanescente, movendo-o para a próxima posição livre no final da fila de saída.
   (b) com probabilidade ρ, incrementa o contador i, pulando para o próximo pacote da fila de entrada e retorna ao passo 2;
3. o canal retoma a execução do passo 1 até que todos os pacotes presentes na fila de entrada do canal tenham sido movidos para a fila de saída, onde se forma a permutação de saída Y^n.

No algoritmo acima, assumimos que ρ é um parâmetro fixo e que a probabilidade de o canal tomar a decisão de mover um pacote da entrada para a saída é independente e identicamente distribuída (i.i.d) entre cada tomada de decisão realizada pelo jogo que emula o comportamento do canal PRNC. A seguir, apresentamos um detalhamento para os casos com dois e três pacotes, a fim de facilitar a generalização para o caso com n pacotes e demonstrar que equivale ao resultado da definição 5.2.

5.3.1 PRNC: O caso com dois pacotes

Partindo do caso mais simples, vamos supor a transmissão de dois pacotes $[x_1, x_2]$ por um canal PRNC modelado conforme a descrição do jogo supracitado. Neste caso, o canal tem duas saídas possíveis, a saber, $[x_1, x_2]$ e $[x_2, x_1]$. A primeira saída representa o caso sem reordenamento dos pacotes transmitidos e a segunda representa o caso no qual ocorre o único reordenamento possível.

A probabilidade de ocorrer a saída do canal PRNC sem reordenamento, $[x_1, x_2]$, dar-se-á quando o pacote x_1 for escolhido pelo canal na primeira rodada para aparecer na saída ou quando o pacote x_1 e o pacote x_2 não forem escolhidos na primeira rodada, tendo início a segunda rodada. Como a probabilidade de o canal tomar a decisão de apresentar os pacotes na saída é i.i.d, tem-se novamente a probabilidade inicial. Note que a probabilidade de o pacote x_2 ocupar a segunda posição da saída é 1 quando o pacote x_1 é escolhido logo na primeira rodada. Isso porque o pacote x_2 será escolhido logo na primeira rodada, ou será pulado na primeira rodada, mas escolhido na segunda, ou pulado na primeira e na segunda, mas escolhido na terceira etc. Em termos matemáticos:

$$\begin{aligned}
\Pr[x_2 \text{ ser escolhido na última rodada}] &= (1-\rho) + \rho(1-\rho) + \rho^2(1-\rho) + \cdots && (5.20)\\
&= (1-\rho)\left[1 + \rho + \rho^2 + \cdots\right] && (5.21)\\
&= (1-\rho)\left[\frac{1}{1-\rho}\right] && (5.22)\\
&= 1 && (5.23)
\end{aligned}$$

Assim, seja W_i a variável aleatória que representa a probabilidade de o canal pular um pacote. Ou seja, $\Pr(W_i = 1) = \rho$ e $\Pr(W_i = 0) = 1 - \rho$. Logo, com base na descrição do jogo acima que modela o comportamento do canal, temos:

$$\begin{aligned}
\Pr([x_1, x_2]) &= \Pr(W_1 = 0) + \Pr(W_1 = 1) \cdot \Pr(W_2 = 1) \cdot \Pr([x_1, x_2]) && (5.24)\\
&= (1-\rho) + \rho^2 \Pr([x_1, x_2]) && (5.25)\\
\Pr([x_1, x_2]) - \rho^2 \Pr([x_1, x_2]) &= 1 - \rho && (5.26)
\end{aligned}$$

Isolando no lado esquerdo da expressão (5.26) acima a probabilidade $\Pr([x_1, x_2])$, segue que:

$$\begin{aligned}
\therefore \Pr([x_1, x_2]) &= \frac{1-\rho}{(1-\rho)^2} && (5.27)\\
&= \frac{1-\rho}{(1-\rho)(1+\rho)} && (5.28)\\
&= \frac{1}{1+\rho} && (5.29)
\end{aligned}$$

Já a saída do canal PRNC será $[x_2, x_1]$, caso com reordenamento, sempre que o pacote x_1 não for escolhido de primeira, mas o pacote x_2 for, ou quando nenhum deles for escolhido na primeira rodada, com a probabilidade se repetindo na segunda rodada, por ser independente. Logo,

$$\Pr([x_2, x_1]) = \Pr(W_1 = 1) \cdot \Pr(W_2 = 0) + \Pr(W_1 = 1) \cdot \Pr(W_2 = 1) \cdot \Pr([x_2, x_1])$$

$$\therefore \Pr([x_2, x_1]) = \rho(1-\rho) + \rho^2 \Pr([x_2, x_1]) \quad (5.30)$$

$$= \frac{\rho(1-\rho)}{1-\rho^2} \quad (5.31)$$

$$= \frac{\rho}{1+\rho} \quad (5.32)$$

A probabilidade acima já era esperada, uma vez que há apenas duas saídas possíveis. Ou seja:

$$\Pr([x_1, x_2]) + \Pr([x_2, x_1)] = 1 \quad (5.33)$$

$$\Pr([x_2, x_1)] = 1 - \Pr([x_1, x_2]) \quad (5.34)$$

$$\Pr([x_2, x_1)] = 1 - \frac{1}{1+\rho} \quad (5.35)$$

$$\Pr([x_2, x_1)] = \frac{\rho}{1+\rho} \quad (5.36)$$

5.3.2 PRNC: O caso com três pacotes

Vamos tratar agora a transmissão de três pacotes pelo canal PRNC. Neste caso, ao se transmitir a sequência de pacotes $[x_1, x_2, x_3]$, as possíveis saídas do canal serão:

$$[x_1, x_2, x_3]; [x_1, x_3, x_2]; [x_2, x_1, x_3]; [x_2, x_3, x_1]; [x_3, x_1, x_2]; [x_3, x_2, x_1].$$

Começando pelo caso sem reordenamento e generalizando a lógica utilizada no caso mais simples, a saída $[x_1, x_2, x_3]$ será obtida quando uma das seguintes situações ocorrer:

- O pacote x_1 for escolhido pelo canal para a saída na primeira rodada. Neste caso, inicia-se uma nova rodada somente com os pacotes x_2 e x_3. Então, tem-se a probabilidade de os pacotes restantes não serem reordenados, ou seja, $\Pr([x_2, x_3])$;
- Os pacotes x_1, x_2 e x_3 não forem escolhidos na primeira rodada, retornando outra vez a probabilidade desses pacotes não serem reordenados na próxima rodada, ou seja, $\Pr([x_1, x_2, x_3])$;

Note que $\Pr([x_2, x_3]) = 1/(1+\rho)$ já foi calculada anteriormente, correspondendo a probabilidade de não haver reordenamento na transmissão de dois pacotes pelo canal PRNC. Além disso, a probabilidade original se repete na segunda rodada porque assumimos que ela é i.i.d. Logo, dada a recorrência das probabilidades nas situações descritas acima, podemos determinar a probabilidade da saída $[x_1, x_2, x_3]$ como sendo:

$$\Pr([x_1, x_2, x_3]) = \Pr(W_1 = 0) \cdot \Pr([x_2, x_3]) + \Pr(W_1 = 1, W_2 = 1, W_3 = 1) \cdot \Pr([x_1, x_2, x_3]) \quad (5.37)$$

$$= (1-\rho) \Pr([x_2, x_3]) + \rho^3 \Pr([x_1, x_2, x_3]) \quad (5.38)$$

$$= \frac{(1-\rho)}{(1+\rho)(1-\rho^3)} \quad (5.39)$$

$$\therefore \Pr([x_1, x_2, x_3]) = \frac{1}{(1+\rho)(1+\rho+\rho^2)} \quad (5.40)$$

Seguindo a mesma lógica, a saída $[x_1, x_3, x_2]$ será obtida quando uma das situações ocorrer:

- O canal escolher o pacote x_1 na primeira rodada, tomando vez a segunda rodada e a probabilidade $\Pr([x_3, x_2])$ de reordenamento dos pacotes restantes;
- O canal não escolher pacote algum na primeira rodada, tendo a segunda rodada novamente a probabilidade original $\Pr([x_1, x_3, x_2])$.

$$\begin{aligned}
\therefore \Pr([x_1, x_3, x_2]) &= \Pr(W_1 = 0) \cdot \Pr([x_3, x_2]) \\
&\quad + \Pr(W_1 = 1, W_2 = 1, W_3 = 1) \cdot \Pr([x_1, x_3, x_2]) && (5.41)\\
&= (1-\rho)\Pr([x_3, x_2]) + \rho^3 \Pr([x_1, x_3, x_2]) && (5.42)\\
&= \frac{(1-\rho)\rho}{(1+\rho)(1-\rho^3)} && (5.43)\\
&= \frac{\rho}{(1+\rho)(1+\rho+\rho^2)} && (5.44)
\end{aligned}$$

A saída $[x_2, x_1, x_3]$ será obtida quando o canal:

- Pular o pacote x_1 e escolher o pacote x_2. Nesse caso, o canal volta para o início da fila de entrada, onde se encontra o pacote x_1. Então, nesta segunda rodada, tem-se a probabilidade $\Pr([x_1, x_3]) = 1/(1+\rho)$ de o canal escolher os pacotes sem reordenamento;
- Pular os pacotes x_1, x_2 e x_3 na primeira rodada, tendo a segunda rodada a mesma probabilidade original $\Pr([x_2, x_1, x_3])$.

$$\begin{aligned}
\therefore \Pr([x_2, x_1, x_3]) &= \Pr(W_1 = 1) \cdot \Pr(W_2 = 0) \cdot \Pr([x_1, x_3]) \\
&\quad + \Pr(W_1 = 1) \cdot \Pr(W_2 = 1) \cdot \Pr(W_3 = 1) \cdot \Pr([x_2, x_1, x_3]) && (5.45)\\
&= (1-\rho)\rho \Pr([x_1, x_3]) + \rho^3 \Pr([x_1, x_2, x_3]) && (5.46)\\
&= \frac{(1-\rho)\rho}{(1+\rho)(1-\rho^3)} && (5.47)\\
&= \frac{\rho}{(1+\rho)(1+\rho+\rho^2)} && (5.48)
\end{aligned}$$

A saída $[x_2, x_3, x_1]$ irá ocorrer quando o canal:

- Pular o pacote x_1 e escolher o pacote x_2. Nesse caso, o canal volta para o início da fila de entrada, onde se encontra o pacote x_1. Então, nesta segunda rodada, tem-se a probabilidade de o canal escolher os pacotes x_1 e x_3 reordenados, ou seja, $\Pr([x_3, x_1])$;
- Pular os pacotes x_1, x_2 e x_3 na primeira rodada, tendo a segunda rodada a mesma probabilidade anterior.

$$\begin{aligned}
\Pr([x_2, x_3, x_1]) &= \Pr(W_1 = 1) \cdot \Pr(W_2 = 0) \cdot \Pr([x_3, x_1]) \\
&\quad + \Pr(W_1 = 1) \cdot \Pr(W_2 = 1) \cdot \Pr(W_3 = 1) \cdot \Pr([x_2, x_3, x_1]) && (5.49)\\
&= (1-\rho)\rho \Pr([x_3, x_1]) + \rho^3 \Pr([x_1, x_2, x_3]) && (5.50)
\end{aligned}$$

$$\therefore \Pr([x_2, x_3, x_1]) = \frac{(1-\rho)\rho^2}{(1+\rho)(1-\rho^3)} \tag{5.51}$$

$$= \frac{\rho^2}{(1+\rho)(1+\rho+\rho^2)} \tag{5.52}$$

A saída $[x_3, x_1, x_2]$ irá ocorrer quando o canal:

- Pular os pacotes x_1 e x_2 e escolher o pacote x_3. Nesse caso, o canal volta para o início da fila de entrada, onde se encontra o pacote x_1. Então, nesta segunda rodada, tem-se a probabilidade de o canal escolher os pacotes x_1 e x_2 sem reordenamento, ou seja, $\Pr([x_1, x_2])$;
- Pular os pacotes x_1, x_2 e x_3 na primeira rodada, tendo a segunda rodada a mesma probabilidade anterior.

$$\begin{aligned}
\therefore \Pr([x_3, x_1, x_2]) &= \Pr(W_1 = 1) \cdot \Pr(W_2 = 1) \cdot \Pr(W_3 = 0) \cdot \Pr([x_1, x_2]) \\
&\quad + \Pr(W_1 = 1) \cdot \Pr(W_2 = 1) \cdot \Pr(W_3 = 1) \cdot \Pr([x_3, x_1, x_2]) && (5.53) \\
&= (1-\rho)\rho^2 \Pr([x_1, x_2]) + \rho^3 \Pr([x_3, x_1, x_2]) && (5.54) \\
&= \frac{(1-\rho)\rho^2}{(1+\rho)(1-\rho^3)} && (5.55) \\
&= \frac{\rho^2}{(1+\rho)(1+\rho+\rho^2)} && (5.56)
\end{aligned}$$

Por fim, a saída $[x_3, x_2, x_1]$ irá ocorrer sempre que o canal:

- Pular os pacotes x_1 e x_2 e escolher o pacote x_3. Nesse caso, o canal volta para o início da fila de entrada, onde se encontra o pacote x_1. Então, nesta segunda rodada, tem-se a probabilidade de o canal escolher os pacotes x_1 e x_2 reordenados, ou seja, $\Pr([x_2, x_1])$;
- Pular os pacotes x_1, x_2 e x_3 na primeira rodada, tendo a segunda rodada a mesma probabilidade anterior.

$$\begin{aligned}
\therefore \Pr([x_3, x_2, x_1]) &= \Pr(W_1 = 1) \cdot \Pr(W_2 = 1) \cdot \Pr(W_3 = 0) \cdot \Pr([x_2, x_1]) \\
&\quad + \Pr(W_1 = 1) \cdot \Pr(W_2 = 1) \cdot \Pr(W_3 = 1) \cdot \Pr([x_3, x_2, x_1]) && (5.57) \\
&= (1-\rho)\rho^2 \Pr([x_2, x_1]) + \rho^3 \Pr([x_3, x_2, x_1]) && (5.58) \\
&= \frac{(1-\rho)\rho^3}{(1+\rho)(1-\rho^3)} && (5.59) \\
&= \frac{\rho^3}{(1+\rho)(1+\rho+\rho^2)} && (5.60)
\end{aligned}$$

As saídas do canal, que representam todas as permutações possíveis dos pacotes de entrada, foram particionadas em relação a função massa de probabilidade e estão relacionadas na tabela 5.2 abaixo:

Tabela 5.2: Probabilidades de ocorrência das permutações de saída do canal PRNC com 3 pacotes

$\frac{1}{(1+\rho)(1+\rho+\rho^2)}$	$[x_1, x_2, x_3]$
$\frac{\rho}{(1+\rho)(1+\rho+\rho^2)}$	$[x_1, x_3, x_2]; [x_2, x_1, x_3]$
$\frac{\rho^2}{(1+\rho)(1+\rho+\rho^2)}$	$[x_2, x_3, x_1]; [x_3, x_1, x_2]$
$\frac{\rho^3}{(1+\rho)(1+\rho+\rho^2)}$	$[x_3, x_2, x_1]$

5.3.3 Generalizando para mais pacotes

A partir do que foi mostrado acima, podemos constatar que a probabilidade de cada saída é dada pelo parâmetro ρ elevado a quantidade de inversões ocorridas na sequência de entrada para transformá-la na sequência de saída. Essa é justamente a definição da distância de Kendall tau. O denominador da probabilidade nada mais é do que uma função normalizadora, dada pelo somatório de todos os possíveis numeradores. Mais ainda, observe que o denominador é dado pela função geradora dos números de Mahonian, cujos coeficientes $M(n,k)$ representam a quantidade de permutações a uma distância k da permutação original. Portanto:

$$\Pr[Y^n = y^n | X^n = x^n] = \frac{\rho^{K(x^n, y^n)}}{\sigma_n(\rho)}. \tag{5.61}$$

Para podermos provar a validade da definição acima, precisamos demonstrar que a probabilidade deduzida realmente vale para todo n. Isso pode ser feito por indução. Dado que já mostramos os casos para dois e três pacotes, vamos assumir como válido o caso para $n-1$ pacotes e mostrar a validade para o caso n.

A estratégia para essa prova é utilizar a recorrência que identificamos no caso para três pacotes enviados pelo canal. Então, seja $[x_1, x_2, \ldots, x_n]$ uma sequência original de n pacotes transmitida pelo canal e $[x_{b(1)}, x_{b(2)}, \ldots, x_{b(n)}]$ a permutação produzida. Assim, a saída $[x_{b(1)}, x_{b(2)}, \ldots, x_{b(n)}]$ irá ocorrer sempre que o canal:

- Pular os pacotes da sequência de entrada em posições anteriores a de $x_{b(1)}$ e escolher mover $x_{b(1)}$ para a primeira posição da fila de saída na primeira rodada, tendo a segunda rodada a probabilidade $\Pr([x_{b(2)}, \ldots, x_{b(n)}])$;
- Pular todos os pacotes da sequência de entrada na primeira rodada, tendo a segunda rodada a mesma probabilidade original.

Uma observação importante agora é sobre a distância de Kendall tau da sequência remanescente na entrada. Note que se a sequência $[x_1, x_2, \ldots, x_n]$ com n pacotes tiver distância de Kendall tau igual a k, então a sequência remanescente na entrada com $n-1$ pacotes terá distância de Kendall

tau igual a $k - b(1) + 1$, já que a quantidade de inversões necessárias para que o pacote $x_{b(1)}$ seja movido de sua posicão $b(1)$ na fila de entrada para a primeira posição da fila de saída é $b(1) - 1$. Por exemplo, se $b(1) = 2$, significa que o pacote x_2 foi movido para a primeira posição da fila de saída, e para isso o canal PRNC precisa realizar apenas uma inversão, ou seja, pular o pacote x_1 e escolher o pacote x_2 na primeira rodada do jogo. Se $b(1) = 3$, significa que o pacote x_3 foi movido para a primeira posição da fila de saída, e para isso o canal PRNC precisa realizar duas inversões, ou seja, pular os pacotes x_1 e x_2, escolhendo o pacote x_3 e assim sucessivamente.

Lembramos que, por hipótese, $\Pr([x_{b(2)}, \ldots, x_{b(n)}]) = \rho^{k-b(1)+1}/\sigma_{n-1}(\rho)$ é conhecida, já que representa o caso para $n - 1$ pacotes. Isso implica dizer que:

$$\begin{aligned}
\Pr([x_{b(1)}, x_{b(2)}, \ldots, x_{b(n)}]) &= \prod_{i=1}^{b(1)-1} \Pr(W_i = 1) \cdot \Pr(W_{b(1)} = 0) \cdot \Pr([x_{b(2)}, \ldots, x_{b(n)}]) \\
&\quad + \prod_{i=1}^{n} \Pr(W_i = 1) \cdot \Pr([x_{b(1)}, x_{b(2)}, \ldots, x_{b(n)}]) && (5.62) \\
&= \rho^{b(1)-1}(1-\rho) \Pr([x_{b(2)}, \ldots, x_{b(n)}]) && (5.63) \\
&\quad + \rho^n \Pr([x_{b(1)}, x_{b(2)}, \ldots, x_{b(n)}]) && (5.64) \\
&= \frac{\rho^{b(1)-1}(1-\rho)}{(1-\rho^n)} \frac{\rho^{k-b(1)+1}}{\sigma_{n-1}(\rho)} && (5.65) \\
&= \frac{\rho^k}{\sigma_n(\rho)} && (5.66)
\end{aligned}$$

■

A demonstração acima mostra que as duas propostas de modelagem do canal PRNC são equivalentes. A primeira tem um caráter mais empírico, fornecendo uma melhor intuição sob a ótica da teoria da informação. A segunda é inspirada em [98], tendo um caráter mais construtivo, dando uma intuição maior sob a ótica da teoria de permutações. Cada uma delas permite intuições distintas, mas complementares ao entendimento do efeito de reordenamento capaz de produzir permutações aleatórias na saída de canais de comutação de alta velocidade.

Capítulo 6

Protocolo de Comprometimento

Apresentamos o protocolo de comprometimento construído com base no canal PRNC, sendo incondicionamente seguro para ambas as partes no modelo adversarial malicioso. As computações efetuadas por Alice e Bob no protocolo são todas de tempo polinomial, pois envolvem operações de ou-exclusivo (XOR) bit-a-bit, o cômputo da distância de Kendall tau, que pode ser realizado com complexidade $\mathcal{O}(n\sqrt{\ln n})$ [100], e o cálculo de funções de *hash* 2-universal, que podem ser efetuadas utilizando-se apenas operações modulares.

Outro aspecto positivo do protocolo é ser sucinto, pois utiliza o canal ruidoso apenas uma vez no sentido de Alice para Bob. Mais ainda, Bob envia para Alice apenas uma mensagem pelo canal sem ruído (com correção de erro), com a descrição da função de *hash* 2-universal. Alice também necessita enviar apenas uma mensagem no canal sem ruído durante a primeira fase do protocolo para se comprometer com um valor v. Caso necessite provar para Bob o seu comprometimento, Alice anuncia pelo canal sem ruído o valor v de seu comprometimento e a sequência x^n enviada pelo canal PRNC inicialmente.

6.1 Modelo Geral de um Esquema de Comprometimento

Todo esquema de comprometimento consiste de ao menos duas fases, *Commit* (fase de comprometimento) e *Reveal* (fase de abertura), executadas por dois participantes, um emissor, Alice, e um receptor, Bob. Na fase de comprometimento, Alice se compromete com um valor v, enviando informações contendo vestígios sobre v para Bob. No caso ideal, Bob não deve ser capaz de descobrir o valor v, por conta própria, a partir dos vestígios recebidos durante a execução da fase de comprometimento.

Posteriormente, Alice e Bob podem se engajar na fase de abertura. Nessa fase, Alice revelará para Bob um valor $\overline{v}$, permitindo-lhe conferir se as informações vestigiais recebidas durante a fase de comprometimento executada anteriormente de fato correspondem ao valor $\overline{v}$ declarado por Alice. Observe que, em princípio, a fase de abertura pode jamais vir a ser executada. Por fim, Alice não deve ser capaz de abrir um valor $\overline{v} \neq v$ válido na fase de abertura, impossibilitando que mude de ideia sobre o seu comprometimento.

6.2 Segurança de um Esquema de Comprometimento

Formalmente, um esquema de comprometimento deve satisfazer as seguintes condições para ser considerado seguro:

• *Correctness*: Se ambos os participantes forem honestos, então o destinatário sempre aceitará o valor revelado na abertura do comprometimento.

• *Concealing*: Se o remetente for honesto, então o destinatário não aprenderá informação alguma sobre o comprometimento antes dele ser revelado na fase de abertura pelo remetente.

• *Binding*: Se o destinatário for honesto, então o valor escolhido pelo remetente para se comprometer será o único que ele será capaz de revelar na fase de abertura.

6.3 Modelo de Comprometimento baseado no canal PRNC

Um esquema de comprometimento baseado no canal com ruído do tipo reordenamento de pacotes (PRNC) consiste da fase de comprometimento e da fase de abertura. A fase de comprometimento se inicia com a transmissão de pacotes x^n através do canal PRNC no sentido de Alice para Bob, que recebe y^n na saída do canal. Depois, Alice e Bob trocam mensagens através de um canal autenticado sem de ruído (com correção de erros). Seja t a variável que representa toda a informação trocada entre Alice e Bob durante a fase de comprometimento. Ao final dessa fase, Alice deve se comprometer com um valor v.

Se a fase de abertura vier a ocorrer, então Alice enviará x^n e v para Bob. Ao receber a informação aberta por Alice, ele executa uma função de teste sobre as variáveis $\{x^n, y^n, t, v\}$. Baseado no resultado desse teste, Bob pode aceitar ou rejeitar o comprometimento de Alice.

6.4 Definição de Segurança do Protocolo de Comprometimento

Sejam X^n, Y^n, T e V as variáveis aleatórias correspondentes aos valores mencionados na seção anterior. Seja x^n uma realização de X^n. Seja V a variável aleatória que representa o valor com o qual Alice se compromete, onde assumimos que V é uma *string* binária aleatória com distribuição uniforme e de comprimento m. Seja T a variável aleatória que corresponde a toda comunicação trocada entre Alice e Bob durante a fase de comprometimento e seja R uma *string* binária uniformemente distribuída de comprimento m e independente da visão das partes.

Mais ainda, sejam $View_A$ e $View_B$ as representações de toda as informações, computacões e aleatoriedades locais obtidas por Alice e Bob durante a execução da fase de comprometimento, respectivamente. É dado que os participantes do protocolo conhecem a função pública binária $\mathsf{Teste} : \{0,1\}^{n\cdot\ell} \times \{0,1\}^{n\cdot\ell} \times \mathcal{T} \times \{0,1\}^m \to \{\text{ACEITA}, \text{REJEITA}\}$ que permite a Bob verificar a validade do comprometimento de Alice. A segurança do protocolo de comprometimento baseado no canal PRNC proposto nesta tese é definida da seguinte forma:

Definição 6.1. *Um protocolo de comprometimento baseado em um canal com ruído de reordenamento de pacotes é $(\varphi, \theta, \epsilon)$-seguro se, e somente se, satifaz as seguintes condições:*

- φ-***Correctness***: *Se Alice e Bob são honestos, então qualquer valor $v \in \{0,1\}^m$ comprometido e revelado por Alice será aceito por Bob com probabililidade dada por*

$$\Pr[\mathsf{Teste}(X^n, Y^n, T, v) = \text{ACEITA}] \geq 1 - \varphi$$

- θ-***Binding***: *Se Bob é honesto, então para quaisquer $\widetilde{v}, \overline{v} \in \{0,1\}^m$ onde $\widetilde{v} \neq \overline{v}$, e para qualquer estratégia de Alice (potencialmente maliciosa) na escolha do X^n que será enviado através do canal PRNC durante a fase de Comprometimento ou quaisquer variáveis aleatórias $\widetilde{X^n} \neq \overline{X^n}$ que Alice possa apresentar durante a fase de Abertura, temos que:*

$$\Pr[\mathsf{Teste}(\widetilde{X^n}, Y^n, T, \widetilde{v}) = \text{ACEITA} \wedge \mathsf{Teste}(\overline{X^n}, Y^n, T, \overline{v}) = \text{ACEITA}] \leq \theta$$

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

$$\mathsf{SD}\left(P_{V,\mathsf{View}_B}; P_{R,\mathsf{View}_B}\right) \leq \epsilon.$$

As probabilidades acima estão baseadas nas aleatoriedades privadas de Alice, Bob e o canal PRNC. Um protocolo de comprometimento é dito incondicionalmente seguro se φ, θ e ϵ tornam-se tão próximos de zero quanto se queira para valores suficientemente grandes de n e s, parâmetros de segurança previamente acordados entre ambas as partes.

Observe que nossa definição de segurança assume que o valor v que Alice se compromete é aleatório com distribuição uniforme. Embora essa suposição simplifique nossa definição, ela não afeta a generalidade do resultado, uma vez que protocolos de comprometimento com valor aleatório sempre podem ser transformados em protocolos de comprometimento com valor específico, conforme demonstrado por Rivest em [101].

6.5 Descrição do Protocolo de Comprometimento

Nesta seção, apresentamos a descrição do nosso protocolo de comprometimento baseado no canal PRNC. Vamos assumir a existência de dois participantes computacionalmente ilimitados; a Alice, remetente do comprometimento; e o Bob, destinatário do comprometimento. Os participantes têm acesso a um canal PRNC, com parâmetros ρ, ε e δ, onde n, a quantidade de pacotes a ser enviada pelo canal, é acordado publica e previamente a execução do protocolo. Além disso, eles também têm acesso e fazem uso livremente de um canal de comunicação bidirecional, autenticado e sem ruído (com correção de erro). Esse canal é utilizado em toda a comunicação efetuada no protocolo após a utilização do canal PRNC. O recurso valioso, que representa custo em termos de eficiência do protocolo, é somente o canal PRNC, onde o efeito de reordenamento de pacotes é explorado como hipótese para o estabelecimento da assimetria de informação entre as partes. Conforme detalhamento apresentado no Capítulo 8, o canal PRNC pode ser emulado por transmissões

através da Internet utilizando o protocolo UDP (onde não há correção para o efeito de reordenamento dos pacotes), enquanto o canal sem ruído pode ser emulado por transmissões através da Internet utilizando o protocolo TCP.

Os participantes estabelecem publicamente pelo canal sem ruído os parâmetros de execução antes de iniciarem o protocolo. Seja $\mathcal{G}$ uma família de funções de *hash* 2-universal $g : \{0,1\}^{n\ell} \to \{0,1\}^m$ e $\mathcal{F}$ outra família de funções de *hash* 2-universal $f : \{0,1\}^{n\ell} \to \{0,1\}^\omega$. As ações tomadas pelos participantes engajados no protocolo de comprometimento estão descritas abaixo:

FASE DE COMPROMETIMENTO

C.1. Alice forma uma sequência de n pacotes de dados distintos (*strings* binárias), cada um com um comprimento fixo $\ell \geq \lceil \log(n) \rceil$, definida pela variável aleatória a seguir:

$$X^n = [X_1, X_2, \ldots, X_n], \text{ tal que } X_i \in \{0,1\}^\ell.$$

Os pacotes de dados X_i são escolhidos aleatoriamente com distribuição uniforme condicionada a serem distintos, sendo utilizados tanto como conteúdo, quanto identificador. Denotamos por $x^n \leftarrow X^n$ uma realização de X^n:

$$x^n = [x_1, x_2, \ldots, x_n]$$

C.2. Alice envia x^n para Bob através do canal PRNC.

C.3. Bob escuta a saída do canal PRNC até que todos os pacotes sejam recebidos. Ao final do processo, Bob obtém a permutação

$$y^n = [y_1, y_2, \ldots, y_n],$$

que consiste no reordenamento dos pacotes de dados de x^n realizado pelo canal PRNC, resultado de uma realização da variável aleatória Y^n, tal que exista uma função bijetiva $b : \{1, \ldots n\} \to \{1, \ldots n\}$ de forma que $x_{b(i)} = y_i$ para cada $i \in \{1, \ldots n\}$.

C.4. Seja F uma variável aleatória uniformemente distribuida sobre a família de funções de *hash* 2-universal $\mathcal{F}$. Bob amostra uma realização $f \leftarrow F$ e envia a descrição da função f para Alice através do canal autenticado bidirecional sem ruído.

C.5. Seja G uma variável aleatória uniformemente distribuida sobre a família de funções de *hash* 2-universal $\mathcal{G}$. Alice amostra uma realização $g \leftarrow G$. Alice também sorteia com distribuição uniforme uma *string* binária $v \in \{0,1\}^m$, que será o valor com o qual se comprometerá.

C.6. Alice computa $\mathsf{hash} := f(x^n)$ e $\mathsf{commit} := g\left(x^n\right) \oplus v$, onde $\oplus$ representa a função binária ou-exclusivo (XOR) bit-a-bit.

C.7. Alice envia hash; commit e a descrição de g para Bob através do canal autenticado bidirecional sem ruído.

FASE DE ABERTURA

R.1. Se a fase de abertura for realizada, então, Alice envia $\widetilde{v}$ e $\overline{x^n}$ para Bob através do canal sem ruído, onde $\widetilde{v} = v$ e $\overline{x^n} = x^n$ quando Alice é honesta.

R.2. Então, Bob executa a função $\mathsf{Teste}(X^n, Y^n, T, v)$, que realiza as seguintes verificações:

(i) Se $f(\overline{x^n}) = \mathsf{hash}$;

(ii) Se y^n consiste de uma permutação dos pacotes de dados em $\overline{x^n}$ e se

$$|K(\overline{x^n}, y^n) - E[K(X^n, Y^n)]| < \varepsilon E[K(X^n, Y^n)];$$

(iii) Se $g\left(\overline{x^n}\right) \oplus \mathsf{commit} = \widetilde{v}$.

R.3. Caso os testes sejam bem sucedidos, a função retorna ACEITA. Caso contrário, retorna REJEITA.

Capítulo 7

Prova de Segurança

Para provar que o protocolo apresentado na seção anterior é incondicionalmente seguro para ambas as partes, será necessário mostrar que ele atende as três condições de segurança definidas na seção 6.4. Importante destacar que o poder computacional dos participantes é ilimitado. Nenhuma hipótese é feita sobre as ações do adversário, que pode agir de forma irrestrita e maliciosa. A seguir, provamos que o protocolo proposto é $(\varphi, \theta, \epsilon)$-seguro e mostramos que os valores de φ, θ, e ϵ tendem a zero assintoticamente nos parâmetros de segurança do protocolo.

7.1 *Correctness*: Corretude do Protocolo

Quando os participantes são honestos, o protocolo falha se e somente se a distância de Kendall tau entre as variáveis aleatórias X^n e Y^n for maior que um determinado intervalo em torno da distância esperada, a margem de erro do canal. Para provar a condição de corretude do protocolo, demonstramos que a referida hipótese de falha ocorre apenas com probabilidade desprezível quando o parâmetro de segurança n é suficientemente grande, tendo por base o teste realizado por Bob no passo **R.2 (ii)** da fase de abertura do protocolo, conforme descrito no seção 6.5. Adotamos daqui em diante as abreviações $\mathsf{N} = n(n-1)/2$ e $K = K(X^n, Y^n)$ para a variável aleatória resultante da distância de Kendall tau entre as permutações de entrada e saída do canal PRNC. Assim, calculando a probabilidade de falha no teste realizado por Bob, temos que:

$$\Pr\Big[\Big|K - E[K]\Big| \geq \varepsilon E[K]\Big] = \Pr\big[K \geq (1+\varepsilon)E[K]\big] + \Pr\big[K \leq (1-\varepsilon)E[K]\big]. \tag{7.1}$$

Pode-se obter cotas superiores nas probabilidades do lado direito da expressão (7.1) acima se utilizando a desigualdade de Chernoff-Hoeffding apresentada na expressão (4.59):

$$\Pr\big[K \geq (1+\varepsilon)E[K]\big] \leq \min_{t>0} \frac{E[e^{tK}]}{e^{t(1+\varepsilon)E[K]}} \leq e^{-(n-1)[\varepsilon\rho\beta - \ln(1+\varepsilon\rho)]} \tag{7.2}$$

$$\Pr\big[K \leq (1-\varepsilon)E[K]\big] \leq \min_{t>0} \frac{E[e^{-tK}]}{e^{-t(1-\varepsilon)E[K]}} \leq e^{-(n-1)\rho\frac{\varepsilon^2\beta^2}{2}} \tag{7.3}$$

Por uma questão de rigor, derivamos cada uma das cotas acima nas subseções seguintes.

7.1.1 Esperança da Distância de Kendall tau

Primeiro, calcularemos a distância de Kendall tau esperada entre X^n e Y^n, conforme segue:

$$\begin{aligned} E[K(X^n, Y^n)] &= \sum_{k=0}^{\mathsf{N}} k \Pr[K = k] && (7.4)\\ &= \sum_{k=0}^{\mathsf{N}} kM(n,k)\frac{\rho^k}{\sigma_n(\rho)} && (7.5)\\ &= \frac{\rho}{\sigma_n(\rho)} \sum_{k=0}^{\mathsf{N}} kM(n,k)\rho^{k-1} && (7.6)\\ &= \frac{\rho}{\sigma_n(\rho)} \cdot \frac{d\sigma_n}{d\rho} && (7.7) \end{aligned}$$

A primeira derivada da função geradora $\sigma_n(\rho)$ pode ser obtida da seguinte forma:

$$\begin{aligned} \frac{d\sigma_n}{d\rho} &= \frac{d}{d\rho}\left[\left(\frac{1}{1-\rho}\right)^n \prod_{i=1}^{n}(1-\rho^i)\right] && (7.8)\\ &= \frac{n}{(1-\rho)^{n+1}} \prod_{i=1}^{n}(1-\rho^i) + \left(\frac{1}{1-\rho}\right)^n \prod_{i=1}^{n}(1-\rho^i)\left(\sum_{k=1}^{n}\frac{-k\rho^{k-1}}{1-\rho^k}\right) && (7.9)\\ &= \left[\left(\frac{1}{1-\rho}\right)^n \prod_{i=1}^{n}(1-\rho^i)\right]\left(\frac{n}{1-\rho} - \sum_{k=1}^{n}\frac{k\rho^{k-1}}{1-\rho^k}\right) && (7.10) \end{aligned}$$

Aqui, estamos interessados nos limites superior e inferior da primeira derivada da função $\sigma_n(\rho)$. Começamos pelo limite superior:

$$\begin{aligned} \frac{d\sigma_n}{d\rho} &= \sigma_n(\rho)\left(\frac{n}{1-\rho} - \sum_{k=1}^{n}\frac{k\rho^{k-1}}{1-\rho^k}\right) && (7.11)\\ &\leq \sigma_n(\rho)\left(\frac{n}{1-\rho} - \frac{1}{1-\rho}\right) && (7.12)\\ &\leq \sigma_n(\rho)\left(\frac{n-1}{1-\rho}\right) && (7.13) \end{aligned}$$

Agora, derivamos o limite inferior. Seja $u(\rho)$ uma função qualquer de ρ. Lembrando que $\frac{d}{d\rho}\ln(u) = \frac{1}{u}\frac{du}{d\rho}$, temos o seguinte:

$$\begin{aligned} \frac{d\sigma_n}{d\rho} &= \sigma_n(\rho)\left[\frac{n}{1-\rho} + \sum_{k=1}^{n}\frac{d}{d\rho}\ln(1-\rho^k)\right] && (7.14)\\ &= \sigma_n(\rho)\left[\frac{n}{1-\rho} + \sum_{k=1}^{n}\frac{d}{d\rho}\sum_{j=1}^{\infty}\frac{-(\rho^k)^j}{j}\right] && (7.15) \end{aligned}$$

No último passo acima, na expressão (7.15), substituímos a função logaritmo neperiano por

sua expansão em série de Taylor. Dessa forma:

$$\begin{aligned}
\frac{d\sigma_n}{d\rho} &\geq \sigma_n(\rho)\left[\frac{n}{1-\rho} - \sum_{j=1}^{\infty}\frac{1}{j}\frac{d}{d\rho}\sum_{k=1}^{\infty}(\rho^j)^k\right] && (7.16)\\
&= \sigma_n(\rho)\left[\frac{n}{1-\rho} - \sum_{j=1}^{\infty}\frac{1}{j}\frac{d}{d\rho}\left(\frac{\rho^j}{1-\rho^j}\right)\right] && (7.17)\\
&= \sigma_n(\rho)\left[\frac{n}{1-\rho} - \sum_{j=1}^{\infty}\frac{1}{j}\frac{j\rho^{j-1}}{(1-\rho^j)^2}\right] && (7.18)\\
&= \sigma_n(\rho)\left[\frac{n}{1-\rho} - \sum_{j=0}^{\infty}\frac{\rho^j}{(1-\rho^{j+1})^2}\right] && (7.19)\\
&= \sigma_n(\rho)\left[\frac{n}{1-\rho} - \frac{1}{(1-\rho)^2}\sum_{j=0}^{\infty}\frac{\rho^j}{(\sum_{k=0}^{j}\rho^k)^2}\right] && (7.20)
\end{aligned}$$

onde adotamos na expressão (7.20) o fato de que $\sum_{k=0}^{j}\rho^k = (1-\rho^{j+1})/(1-\rho)$.

Para limitar o somatório infinito na expressão (7.20), faremos uso do lema 4.3. Assim, o limite inferior da primeira derivada da função $\sigma_n(\rho)$ é dada por:

$$\begin{aligned}
\frac{d\sigma_n}{d\rho} &\geq \sigma_n(\rho)\left[\frac{n}{1-\rho} - \frac{1+\rho}{(1-\rho)^2}\right] && (7.21)\\
&= \sigma_n(\rho)\left[\frac{n-1}{1-\rho} + \frac{1}{1-\rho} - \frac{1+\rho}{(1-\rho)^2}\right] && (7.22)\\
&= \sigma_n(\rho)\left[\frac{n-1}{1-\rho} + \frac{1-\rho}{(1-\rho)^2} - \frac{1+\rho}{(1-\rho)^2}\right] && (7.23)\\
&= \sigma_n(\rho)\left[\frac{n-1}{1-\rho} - \frac{2\rho}{(1-\rho)^2}\right] && (7.24)\\
&= \sigma_n(\rho)\frac{n-1}{1-\rho}\left[1 - \frac{2\rho}{(n-1)(1-\rho)}\right] && (7.25)
\end{aligned}$$

Seja $\beta = 1 - 2\rho/[(n-1)(1-\rho)]$, que vai para 1 quando $n \to \infty$. Então, pelo Teorema do Confronto (*Squeeze theorem*), $\forall\ 0 < \rho < 1$, a primeira derivada da função $\sigma_n(\rho)$ é tal que

$$\sigma_n(\rho)\frac{n-1}{1-\rho}\beta \ \leq\ \frac{d\sigma_n}{d\rho} \ \leq\ \sigma_n(\rho)\frac{n-1}{1-\rho} \tag{7.26}$$

$$\therefore \lim_{n\to\infty}\frac{d\sigma_n}{d\rho} = \sigma_n(\rho)\frac{n-1}{1-\rho} \tag{7.27}$$

Logo, $\forall\ \ 0 < \rho < 1$, A distância de Kendall tau esperada entre X^n e Y^n é dada por:

$$(n-1)\frac{\rho}{1-\rho}\beta \leq E[K(X^n, Y^n)] \leq (n-1)\frac{\rho}{1-\rho} \tag{7.28}$$

$$\therefore \lim_{n\to\infty} E[K(X^n, Y^n)] = (n-1)\left(\frac{\rho}{1-\rho}\right) \tag{7.29}$$

7.1.2 Limite Superior

Começamos com a desigualdade do limite superior. A desigualdade de Chernoff-Hoeffding para uma variável aleatória arbitrária K pode ser obtida por meio da desigualdade de Markov aplicada para e^{tK}. Para todo $t > 0$, temos que:

$$\Pr\left[K \geq (1+\varepsilon)E[K]\right] \leq \min_{t>0} \frac{E[e^{tK}]}{e^{t(1+\varepsilon)E[K]}} \tag{7.30}$$

Observe que a desigualdade (7.30) acima pode ser minimizada em t da seguinte forma:

$$\frac{\partial}{\partial t}\frac{E[e^{tK}]}{e^{t(1+\varepsilon)E[K]}} = -(1+\varepsilon)E[K]e^{-t(1+\varepsilon)E[K]}E[e^{tK}] + e^{-t(1+\varepsilon)E[K]}E[Ke^{tK}] = 0 \tag{7.31}$$

$$\therefore \frac{E[Ke^{tK}]}{E[e^{tK}]} = (1+\varepsilon)E[K] \tag{7.32}$$

Segue que:

$$\begin{aligned}
\frac{E[Ke^{tK}]}{E[e^{tK}]} &= \frac{\sigma_n^{-1}(\rho)\sum_{k=0}^{\mathsf{N}} ke^{tk}M(n,k)\rho^k}{\sigma_n^{-1}(\rho)\sum_{k=0}^{\mathsf{N}} e^{tk}M(n,k)\rho^k} && (7.33)\\
&= \frac{\rho e^t \sum_{k=0}^{\mathsf{N}} kM(n,k)(\rho e^t)^{k-1}}{\sum_{k=0}^{\mathsf{N}} M(n,k)(\rho e^t)^k} && (7.34)\\
&= \frac{\rho e^t}{\sigma_n(\rho e^t)}\left[\frac{d\left(\sigma_n(\rho e^t)\right)}{d(\rho e^t)}\right]. && (7.35)
\end{aligned}$$

Observe que a expressão entre colchetes em (7.35) é a primeira derivada da função σ_n quando o parâmetro do canal é ρe^t. Assim, para $n \to \infty$, temos que:

$$\begin{aligned}
\lim_{n\to\infty}\frac{E[Ke^{tK}]}{E[e^{tK}]} &= \frac{\rho e^t}{\sigma_n(\rho e^t)}\sigma_n(\rho e^t)\left(\frac{n-1}{1-\rho e^t}\right) && (7.36)\\
&= (n-1)\left(\frac{\rho e^t}{1-\rho e^t}\right). && (7.37)
\end{aligned}$$

Uma vez que o objetivo é escolher qualquer $t > 0$ que minimize a desigualdade (7.30), temos:

$$(n-1)\left(\frac{\rho e^t}{1-\rho e^t}\right) = (1+\varepsilon)(n-1)\left(\frac{\rho}{1-\rho}\right) \tag{7.38}$$

$$\frac{e^t}{1-\rho e^t} = \frac{1+\varepsilon}{1-\rho} \tag{7.39}$$

$$\therefore e^t = \frac{1+\varepsilon}{1+\varepsilon\rho} = 1 + \frac{\varepsilon(1-\rho)}{1+\varepsilon\rho} \tag{7.40}$$

$$\text{ou } e^{-t} = \frac{1+\varepsilon\rho}{1+\varepsilon} = 1 - \frac{\varepsilon(1-\rho)}{1+\varepsilon} \tag{7.41}$$

Agora, podemos mostrar que:

$$\begin{aligned}
e^{-t(1+\varepsilon)E[K]} &= \left(\frac{1+\varepsilon\rho}{1+\varepsilon}\right)^{(1+\varepsilon)(n-1)\beta\rho/(1-\rho)} && (7.42)\\
&\leq \left[\left(1-\frac{\varepsilon(1-\rho)}{1+\varepsilon}\right)^{\frac{1+\varepsilon}{1-\rho}}\right]^{\rho(n-1)\beta} && (7.43)\\
&\leq e^{-(n-1)\varepsilon\rho\beta} && (7.44)
\end{aligned}$$

Aplicando o resultado obtido em (7.44) na desigualdade (7.30), temos que:

$$\Pr\left[K \geq (1+\varepsilon)E[K]\right] \leq \min_{t>0} e^{-t(1+\varepsilon)E[K]} E\left[e^{tK}\right] \tag{7.45}$$

$$\leq \min_{t>0} e^{-t(1+\varepsilon)E[K]} \sum_{k=0}^{\mathsf{N}} M(n,k)\frac{\rho^k}{\sigma_n(\rho)} e^{tk} \tag{7.46}$$

$$\leq \frac{e^{-(n-1)\varepsilon\rho\beta}}{\sigma_n(\rho)} \sum_{k=0}^{\mathsf{N}} M(n,k)\rho^k \left(1+\frac{\varepsilon(1-\rho)}{1+\varepsilon\rho}\right)^k \tag{7.47}$$

Seja $\alpha = \varepsilon(1-\rho)/(1+\varepsilon\rho)$ e assuma que a notação $\sigma_n^{(i)}(\rho)$ denota a i-ésima derivada da função $\sigma_n(\rho)$. Considerando que $(1+\alpha)^k = \sum_{i=0}^{k}\binom{k}{i}\alpha^i$, segue que:

$$\Pr\left[K \geq (1+\varepsilon)E[K]\right] \leq \frac{e^{-(n-1)\varepsilon\rho\beta}}{\sigma_n(\rho)} \sum_{k=0}^{\mathsf{N}} M(n,k)\rho^k (1+\alpha)^k \tag{7.48}$$

$$\leq \frac{e^{-(n-1)\varepsilon\rho\beta}}{\sigma_n(\rho)} \sum_{k=0}^{\mathsf{N}} \sum_{i=0}^{k} \binom{k}{i} M(n,k)\rho^k\alpha^i \tag{7.49}$$

$$\leq \frac{e^{-(n-1)\varepsilon\rho\beta}}{\sigma_n(\rho)} \left(\sigma_n(\rho) + \alpha\rho\sigma_n^{(1)}(\rho) + \frac{\alpha^2\rho^2}{2!}\sigma_n^{(2)}(\rho) + \cdots \right.$$
$$\left. \cdots + \frac{\alpha^{\mathsf{N}}\rho^{\mathsf{N}}}{\mathsf{N}!}\sigma_n^{(\mathsf{N})}(\rho)\right) \tag{7.50}$$

onde a expressão entre parênteses em (7.50) representa a série de Taylor da seguinte função:

$$\sigma_n(\rho e^t) = \sigma_n(\rho + \alpha\rho). \tag{7.51}$$

Seja $\langle n-1\rangle^i = (n-1)n(n+1)(n+2)\cdots(n-1+i-1)$ o fatorial crescente. Para se limitar superiormente as derivadas de diversas ordens da função $\sigma_n(\rho)$, procedemos da seguinte forma:

$$\sigma_n^{(1)}(\rho) = \sigma_n(\rho)\left[\frac{n-1}{1-\rho} - \sum_{k=2}^{n}\frac{d}{d\rho}\sum_{j=1}^{\infty}\frac{(\rho^k)^j}{j}\right] \tag{7.52}$$

$$\leq \sigma_n(\rho)\frac{n-1}{1-\rho} \tag{7.53}$$

$$\sigma_n^{(2)}(\rho) = \sigma_n^{(1)}(\rho)\left[\frac{n-1}{1-\rho} - \sum_{k=2}^{n}\frac{d}{d\rho}\sum_{j=1}^{\infty}\frac{(\rho^k)^j}{j}\right]$$
$$+ \sigma_n(\rho)\left[\frac{n-1}{(1-\rho)^2} - \sum_{k=2}^{n}\frac{d^2}{d\rho^2}\sum_{j=1}^{\infty}\frac{(\rho^k)^j}{j}\right] \tag{7.54}$$

$$\leq \sigma_n(\rho)\left(\frac{n-1}{1-\rho}\right)^2$$
$$+ \sigma_n(\rho)\frac{n-1}{(1-\rho)^2} \tag{7.55}$$

$$= \sigma_n(\rho)\frac{(n-1)n}{(1-\rho)^2} \tag{7.56}$$

$$
\begin{aligned}
\sigma_n^{(3)}(\rho) &= \sigma_n^{(2)}(\rho)\left[\frac{n-1}{1-\rho} - \sum_{k=2}^{n}\frac{d}{d\rho}\sum_{j=1}^{\infty}\frac{(\rho^k)^j}{j}\right] \\
&\quad + 2\sigma_n^{(1)}(\rho)\left[\frac{n-1}{(1-\rho)^2} - \sum_{k=2}^{n}\frac{d^2}{d\rho^2}\sum_{j=1}^{\infty}\frac{(\rho^k)^j}{j}\right] \\
&\quad + \sigma_n(\rho)\left[\frac{2(n-1)}{(1-\rho)^3} - \sum_{k=2}^{n}\frac{d^3}{d\rho^3}\sum_{j=1}^{\infty}\frac{(\rho^k)^j}{j}\right] && (7.57) \\
&\leq \sigma_n(\rho)\frac{n(n-1)^2}{(1-\rho)^3} \\
&\quad + \sigma_n(\rho)\frac{2(n-1)^2}{(1-\rho)^3} \\
&\quad + \sigma_n(\rho)\frac{2(n-1)}{(1-\rho)^3} && (7.58) \\
&= \sigma_n(\rho)\frac{(n-1)n(n+1)}{(1-\rho)^3} && (7.59) \\
\sigma_n^{(4)}(\rho) &= \sigma_n^{(3)}(\rho)\left[\frac{n-1}{1-\rho} - \sum_{k=2}^{n}\frac{d}{d\rho}\sum_{j=1}^{\infty}\frac{(\rho^k)^j}{j}\right] \\
&\quad + 3\sigma_n^{(2)}(\rho)\left[\frac{n-1}{(1-\rho)^2} - \sum_{k=2}^{n}\frac{d^2}{d\rho^2}\sum_{j=1}^{\infty}\frac{(\rho^k)^j}{j}\right] \\
&\quad + 3\sigma_n^{(1)}(\rho)\left[\frac{2(n-1)}{(1-\rho)^3} - \sum_{k=2}^{n}\frac{d^3}{d\rho^3}\sum_{j=1}^{\infty}\frac{(\rho^k)^j}{j}\right] \\
&\quad + \sigma_n(\rho)\left[\frac{6(n-1)}{(1-\rho)^4} - \sum_{k=2}^{n}\frac{d^4}{d\rho^4}\sum_{j=1}^{\infty}\frac{(\rho^k)^j}{j}\right] && (7.60) \\
&\leq \sigma_n(\rho)\frac{(n-1)^2n(n+1)}{(1-\rho)^4} \\
&\quad + \sigma_n(\rho)\frac{3(n-1)^2n}{(1-\rho)^4} \\
&\quad + \sigma_n(\rho)\frac{6(n-1)^2}{(1-\rho)^4} \\
&\quad + \sigma_n(\rho)\frac{6(n-1)}{(1-\rho)^4} && (7.61) \\
&= \sigma_n(\rho)\frac{\langle n-1\rangle^4}{(1-\rho)^4} && (7.62) \\
&\vdots \\
\therefore \sigma_n^{(i)}(\rho) &\leq \sigma_n(\rho)\frac{\langle n-1\rangle^i}{(1-\rho)^i} && (7.63)
\end{aligned}
$$

Portanto, pelo princípio da indução matemática, tendo mostrado todas as desigualdades acima, nós assumimos como válidos todos os casos de 1 até i e demonstramos a validade para o caso $i+1$, a fim de provar que a desigualdade obtida para as derivadas de ordens superiores da função σ_n

valem para todas as ordens $i \geq 1$. Logo:

$$\begin{aligned}
\sigma_n^{(i+1)}(\rho) &= \sum_{j=0}^{i} \binom{i}{j} \sigma_n^{(j)}(\rho) \left[(i-j)! \frac{n-1}{(1-\rho)^{i+1-j}} - \sum_{k=2}^{n} \frac{d^{i+1-j}}{d\rho^{i+1-j}} \sum_{j=1}^{\infty} \frac{(\rho^k)^j}{j} \right] && (7.64)\\
&\leq \sigma_n(\rho) \sum_{j=0}^{i} \frac{i!}{j!} \frac{\langle n-1 \rangle^j}{(1-\rho)^j} \left[\frac{n-1}{(1-\rho)^{i+1-j}} \right] && (7.65)\\
&= \frac{\sigma_n(\rho)}{(1-\rho)^{i+1}} i!(n-1) \sum_{j=0}^{i} \frac{\langle n-1 \rangle^j}{j!} && (7.66)\\
&= \frac{\sigma_n(\rho)}{(1-\rho)^{i+1}} i!(n-1) \\
&\quad \cdot \left[1 + (n-1) + \frac{(n-1)n}{2} + \cdots + \frac{(n-1)n \cdots (n-1+i-1)}{i!} \right] && (7.67)\\
&= \frac{\sigma_n(\rho)}{(1-\rho)^{i+1}} i!(n-1)n \\
&\quad \cdot \left[1 + \frac{(n-1)}{2} + \cdots + \frac{(n-1)(n+1) \cdots (n-1+i-1)}{i!} \right] && (7.68)\\
&= \frac{\sigma_n(\rho)}{(1-\rho)^{i+1}} i!(n-1)n(n+1) \\
&\quad \cdot \left[\frac{1}{2} + \frac{(n-1)}{6} + \frac{(n-1)(n+2)}{24} + \right. \\
&\qquad \left. \cdots + \frac{(n-1)(n+2) \cdots (n-1+i-1)}{i!} \right] && (7.69)\\
&\vdots \\
&= \frac{\sigma_n(\rho)}{(1-\rho)^{i+1}} i!(n-1)n(n+1) \cdots (n-1+i-1) \left[\frac{1}{(i-1)!} + \frac{(n-1)}{i!} \right] && (7.70)\\
&= \sigma_n(\rho) \frac{\langle n-1 \rangle^{i+1}}{(1-\rho)^{i+1}} && (7.71)
\end{aligned}$$

Substituindo as derivadas de ordens superiores obtidas acima na desigualdade do limite superior de concentração (7.50), temos:

$$\begin{aligned}
\Pr\left[K \geq (1+\varepsilon)E[K]\right] &\leq e^{-(n-1)\varepsilon\rho\beta} \left(1 + \alpha\rho \frac{n-1}{1-\rho} + \frac{\alpha^2\rho^2}{2!} \frac{n(n-1)}{(1-\rho)^2} + \right. \\
&\qquad \left. \cdots + \frac{\alpha^{\mathsf{N}}\rho^{\mathsf{N}}}{\mathsf{N}!} \frac{\langle n-1 \rangle^{\mathsf{N}}}{(1-\rho)^{\mathsf{N}}} \right) && (7.72)\\
&= e^{-(n-1)\varepsilon\rho\beta} \sum_{k=0}^{\mathsf{N}} \binom{n+k-2}{k} \left(\frac{\rho}{1-\rho} \right)^k \alpha^k && (7.73)\\
&= e^{-(n-1)\varepsilon\rho\beta} \sum_{k=0}^{\mathsf{N}} \binom{n-2+k}{k} \left(\frac{\rho}{1-\rho} \right)^k \left(\frac{\varepsilon(1-\rho)}{1+\varepsilon\rho} \right)^k && (7.74)\\
&\leq e^{-(n-1)\varepsilon\rho\beta} \sum_{k=0}^{\infty} \binom{n-2+k}{n-2} \left(\frac{\varepsilon\rho}{1+\varepsilon\rho} \right)^k && (7.75)
\end{aligned}$$

Para resolver o somatório em (7.75), vamos mostrar que ele é uma versão disfarçada do Teorema

Binomial Generalizado, definido como:

$$(x+y)^r = \sum_{k=0}^{\infty} \binom{r}{k} x^{r-k} y^k \tag{7.76}$$

onde x, y e $r \in \mathbb{C}$.

Para a identidade que desejamos mostrar, vamos assumir que $x = 1$, $r = -(n-1)$ e $y = -z$:

$$(1-z)^{-(n-1)} = \sum_{k=0}^{\infty} \binom{-(n-1)}{k} (-z)^k \tag{7.77}$$

Observe que o coeficiente binomial acima pode ser reescrito como:

$$\begin{aligned}
\binom{-(n-1)}{k} &= \frac{(-n+1)(-n)(-n-1)(-n-2)\cdots(-n-k+2)}{k!} && (7.78)\\
&= (-1)^k \frac{(n+k-2)(n+k-3)(n+k-4)\cdots n(n-1)}{k!} && (7.79)\\
&= (-1)^k \binom{n+k-2}{k} && (7.80)\\
&= (-1)^k \binom{n-2+k}{n-2} && (7.81)
\end{aligned}$$

Assim, temos que:

$$\begin{aligned}
\left(\frac{1}{1-z}\right)^{n-1} &= \sum_{k=0}^{\infty} (-1)^k \binom{n-2+k}{n-2} (-1)^k z^k && (7.82)\\
&= \sum_{k=0}^{\infty} \binom{n-2+k}{n-2} z^k && (7.83)
\end{aligned}$$

Aplicando a identidade (7.83) acima em (7.75), segue que:

$$\begin{aligned}
\Pr\left[K \geq (1+\varepsilon)E[K]\right] &\leq e^{-(n-1)\varepsilon\rho\beta} \left(1 - \frac{\varepsilon\rho}{1+\varepsilon\rho}\right)^{-(n-1)} && (7.84)\\
&= e^{-(n-1)\varepsilon\rho\beta} \left(1+\varepsilon\rho\right)^{n-1} && (7.85)\\
&= e^{-(n-1)\varepsilon\rho\beta} \cdot e^{(n-1)\ln(1+\varepsilon\rho)} && (7.86)\\
&= e^{-(n-1)[\varepsilon\rho\beta - \ln(1+\varepsilon\rho)]} && (7.87)
\end{aligned}$$

que vai exponencialmente para zero dado que n seja suficientemente grande. ■

7.1.3 Limite Inferior

A cauda inferior da desigualdade de concentração de Chernoff-Hoeffding é obtida se aplicando a desigualdade de Markov, conforme mostrado em (4.61), pela seguinte expressão:

$$\Pr\left[K \leq (1-\varepsilon)E[K]\right] \leq \min_{t>0} \frac{E[e^{-tK}]}{e^{-t(1-\varepsilon)E[K]}} \tag{7.88}$$

para $0 < \varepsilon < 1$.

Usamos uma abordagem distinta para obtenção do limite inferior. Seja a seguinte função geradora:

$$\psi_K(t) = \ln E[e^{-tK}] \tag{7.89}$$

É fácil ver que $\psi_K(0) = 0$. A primeira derivada da função (7.89) é dada por:

$$\psi'_K(t) = \frac{d\psi_K(t)}{dt} = \frac{E[-Ke^{-tK}]}{E[e^{-tK}]} \tag{7.90}$$

$$\therefore \psi'_K(0) = -E[K] \tag{7.91}$$

A segunda derivada da função geradora de Cramer (7.89) é dada por:

$$\psi''_K(t) = \frac{d^2\psi_K(t)}{dt^2} = \frac{E[K^2e^{-tK}]}{E[e^{-tK}]} - \left(\frac{E[Ke^{-tK}]}{E[e^{-tK}]}\right)^2 \tag{7.92}$$

Vamos obter cada um dos termos da expressão (7.92). Assim, o termo de primeira ordem é dado por:

$$\frac{E[Ke^{-tK}]}{E[e^{-tK}]} = \frac{\sigma_n^{-1}(\rho)\sum_{k=0}^{\mathsf{N}} ke^{-tk}M(n,k)\rho^k}{\sigma_n^{-1}(\rho)\sum_{k=0}^{\mathsf{N}} e^{-tk}M(n,k)\rho^k} \tag{7.93}$$

$$= \frac{\rho e^{-t}\sum_{k=0}^{\mathsf{N}} kM(n,k)(\rho e^{-t})^{k-1}}{\sum_{k=0}^{\mathsf{N}} M(n,k)(\rho e^{-t})^k} \tag{7.94}$$

$$= \frac{\rho e^{-t}}{\sigma_n(\rho e^{-t})}\left[\frac{d\sigma_n(\rho e^{-t})}{d(\rho e^{-t})}\right] \tag{7.95}$$

E o de segunda ordem é dado por:

$$\frac{E[K^2e^{-tK}]}{E[e^{-tK}]} = \frac{\sigma_n^{-1}(\rho)\sum_{k=0}^{\mathsf{N}} k^2e^{-tk}M(n,k)\rho^k}{\sigma_n^{-1}(\rho)\sum_{k=0}^{\mathsf{N}} e^{-tk}M(n,k)\rho^k} \tag{7.96}$$

$$= \frac{(\rho e^{-t})^2\sum_{k=0}^{\mathsf{N}} k(k-1)M(n,k)(\rho e^{-t})^{k-2}}{\sum_{k=0}^{\mathsf{N}} M(n,k)(\rho e^{-t})^k} + \frac{\rho e^{-t}\sum_{k=0}^{\mathsf{N}} kM(n,k)(\rho e^{-t})^{k-1}}{\sum_{k=0}^{\mathsf{N}} M(n,k)(\rho e^{-t})^k} \tag{7.97}$$

$$= \frac{(\rho e^{-t})^2}{\sigma_n(\rho e^{-t})}\left[\frac{d^2\sigma_n(\rho e^{-t})}{d(\rho e^{-t})^2}\right] + \frac{\rho e^{-t}}{\sigma_n(\rho e^{-t})}\left[\frac{d\sigma_n(\rho e^{-t})}{d(\rho e^{-t})}\right] \tag{7.98}$$

Substituindo os resultados obtidos em (7.95) e (7.98) acima para os dois termos na segunda derivada da função geradora Cramer (7.92), concluímos que:

$$\psi''_K(t) = \frac{(\rho e^{-t})^2\sigma''_n(\rho e^{-t})}{\sigma_n(\rho e^{-t})} + \frac{\rho e^{-t}\sigma'_n(\rho e^{-t})}{\sigma_n(\rho e^{-t})} - \left(\frac{\rho e^{-t}\sigma'_n(\rho e^{-t})}{\sigma_n(\rho e^{-t})}\right)^2. \tag{7.99}$$

A variância da variável aleatória K é definida como:

$$Var_K(\rho) = E[(K - E[K])^2] \tag{7.100}$$

$$= E[K^2] - E[K]^2 \tag{7.101}$$

Vamos obter uma expressão para cada um dos termos em (7.101) acima. Logo:

$$E[K^2] = \sigma_n^{-1}(\rho)\sum_{k=0}^{\mathsf{N}} k^2 M(n,k)\rho^k \tag{7.102}$$

$$= \frac{\rho^2}{\sigma_n(\rho)}\sum_{k=0}^{\mathsf{N}} k(k-1)M(n,k)\rho^{k-2} + \frac{\rho}{\sigma_n(\rho)}\sum_{k=0}^{\mathsf{N}} kM(n,k)\rho^{k-1} \tag{7.103}$$

$$= \frac{\rho^2}{\sigma_n(\rho)}\frac{d^2\sigma_n}{d\rho^2} + \frac{\rho}{\sigma_n(\rho)}\frac{d\sigma_n}{d\rho} \tag{7.104}$$

Lembrando que:

$$E[K] = \frac{\rho}{\sigma_n(\rho)}\frac{d\sigma_n}{d\rho} \tag{7.105}$$

Temos:

$$Var_K(\rho) = \frac{\rho^2}{\sigma_n(\rho)}\frac{d^2\sigma_n}{d\rho^2} + \frac{\rho}{\sigma_n(\rho)}\frac{d\sigma_n}{d\rho} - \left(\frac{\rho}{\sigma_n(\rho)}\frac{d\sigma_n}{d\rho}\right)^2 \tag{7.106}$$

$$= \rho\frac{d}{d\rho}E[K] \tag{7.107}$$

$$\leq \frac{(n-1)\rho}{(1-\rho)^2} \tag{7.108}$$

Portanto, podemos afirmar o seguinte:

$$\psi''_K(t) = Var_K(\rho e^{-t}) \tag{7.109}$$

Agora, pelo teorema de Taylor, temos que:

$$\psi_K(t) = \psi_K(0) + \psi'_K(0)t + \psi''_K(c)\frac{t^2}{2} \tag{7.110}$$

Para algum valor c entre 0 e t. Observe que:

$$\psi''_K(t) = Var_K(\rho e^{-t}) \leq Var_K(\rho) \quad \forall \quad t \geq 0 \tag{7.111}$$

Finalmente, concluímos que:

$$\psi_K(t) \leq -E[K]t + Var_K(\rho)\frac{t^2}{2} \tag{7.112}$$

$$\therefore E[e^{-tK}] \leq e^{-E[K]t + Var_K(\rho)\frac{t^2}{2}} \tag{7.113}$$

Podemos, então, obter a cota inferior desejada na probabilidade (7.88) com a aplicação do resultado em (7.113) da seguinte forma:

$$\Pr\left[K \leq (1-\varepsilon)E[K]\right] \leq \min_{t>0}\frac{E[e^{-tK}]}{e^{-t(1-\varepsilon)E[K]}} \tag{7.114}$$

$$= \min_{t>0} e^{-\varepsilon E[K]t + Var_K(\rho)\frac{t^2}{2}} \tag{7.115}$$

Como a exponencial é uma função monotônica, para obter um t que minimiza a função em (7.115) , podemos trabalhar apenas com a função $\phi(t)$ no expoente, dada por:

$$\phi(t) = -\varepsilon E[K]t + Var_K(\rho)\frac{t^2}{2} \tag{7.116}$$

Assim, dado que $\phi(t)$ é um polinômio quadrático em t, derivamos e igualamos a zero para encontrar o mínimo global:

$$\frac{d\phi(t)}{dt} = -\varepsilon E[K] + Var_K(\rho)t = 0 \tag{7.117}$$

$$\therefore t_{min} = \frac{\varepsilon E[K]}{Var_K(\rho)} \tag{7.118}$$

Segue que:

$$\begin{aligned}
\phi(t_{min}) &= -\varepsilon E[K]\left(\frac{\varepsilon E[K]}{Var_K(\rho)}\right) + \frac{Var_K(\rho)}{2}\left(\frac{\varepsilon E[K]}{Var_K(\rho)}\right)^2 && (7.119)\\
&= -\frac{(\varepsilon E[K])^2}{2Var_K(\rho)} && (7.120)\\
&\leq -\frac{\varepsilon^2(n-1)^2\rho^2\beta^2(1-\rho)^2}{2(1-\rho)^2(n-1)\rho} && (7.121)\\
&= -(n-1)\rho\frac{\varepsilon^2\beta^2}{2} && (7.122)
\end{aligned}$$

Finalmente, a cauda inferior da desigualdade de concentração (7.88) é cotada por:

$$\begin{aligned}
\Pr\left[K \leq (1-\varepsilon)E[K]\right] &\leq e^{\phi(t_{min})} && (7.123)\\
&\leq e^{-(n-1)\rho\frac{\varepsilon^2\beta^2}{2}} && (7.124)
\end{aligned}$$

que vai exponencialmente para zero quando o parâmetro de segurança $n \to \infty$. ■

7.1.4 Limite de Concentração Resultante

Somando ambas as caudas da desigualdade, a probabilidade de falha fica limitada a

$$\begin{aligned}
\Pr\left[|K - E[K]| \geq \varepsilon E[K]\right] &= \Pr\left[K \geq (1+\varepsilon)E[K]\right] + \Pr\left[K \leq (1-\varepsilon)E[K]\right] && (7.125)\\
&\leq e^{-(n-1)[\varepsilon\rho\beta - \ln(1+\varepsilon\rho)]} + e^{-(n-1)\rho\frac{\varepsilon^2\beta^2}{2}} && (7.126)
\end{aligned}$$

Como $\forall\ x \geq 0$ é verdade que $\frac{x^2}{2} \geq x - \ln(1+x)$, temos então:

$$\frac{\varepsilon^2\rho\beta^2}{2} \geq \frac{(\varepsilon\rho\beta)^2}{2} \geq \varepsilon\rho\beta - \ln(1+\varepsilon\rho\beta) \geq \varepsilon\rho\beta - \ln(1+\varepsilon\rho) \tag{7.127}$$

Isso implica no seguinte:

$$\Pr\left[\left|K - E[K]\right| \geq \varepsilon E[K]\right] \leq 2e^{-(n-1)[\varepsilon\rho\beta - \ln(1+\varepsilon\rho)]} \tag{7.128}$$

Por fim, quando Alice e Bob são honestos,

$$\Pr[\mathsf{Test}(x^n, y^n, t, v) = \text{ACC}] = 1 - \Pr\left[\left|K - E[K]\right| \geq \varepsilon E[K]\right] \tag{7.129}$$

$$\geq 1 - 2e^{-(n-1)[\varepsilon\rho\beta - \ln(1+\varepsilon\rho)]} \tag{7.130}$$

$$= 1 - \varphi. \tag{7.131}$$

A probabilidade de falha do protocolo é no máximo $\varphi = 2\exp\left[-(n-1)(\varepsilon\rho\beta - \ln(1+\varepsilon\rho))\right]$, sendo desprezível quando n é suficientemente grande. ■

7.2 *Binding*: Condição de Segurança para o Destinatário

Quando Bob é honesto, Alice não deve ser capaz de abrir dois comprometimentos distintos $\overline{v}$ e $\widetilde{v}$ com sucesso. Seja x^n a sequência de pacotes de dados que Alice envia através do canal PRNC e y^n a permutação recebida por Bob. Em nosso protocolo, Bob consegue detectar o comportamento malicioso de Alice devido ao seu conhecimento da característica do canal (o parâmetro de ruído ρ) e do valor da função de *hash* $f(\cdot)$ recebida de Alice. Uma Alice maliciosa consegue abrir dois valores de comprometimento distintos somente se ela puder encontrar permutações distintas $\overline{x^n} \neq \widetilde{x^n}$ dos pacotes de dados (possivelmente uma delas sendo igual a x^n) tal que:

$$f(\overline{x^n}) = f(\widetilde{x^n}), \tag{7.132}$$

$$\left|K(\overline{x^n}, y^n) - E[K]\right| < \varepsilon E[K], \tag{7.133}$$

$$\left|K(\widetilde{x^n}, y^n) - E[K]\right| < \varepsilon E[K]. \tag{7.134}$$

Vamos mostrar que a probabilidade de tais permutações existirem é desprezível dado os parâmetros de segurança. Há duas etapas a serem provadas. Na primeira, demonstramos que para qualquer permutação $\overline{x^n}$ com $K(\overline{x^n}, x^n) > \tau$ (para um certo valor limiar τ a ser determinado posteriormente), tem-se que $|K(\overline{x^n}, y^n) - E[K]| \geq \varepsilon E[K]$ com probabilidade tendendo a 1. Na segunda, demonstramos que a probabilidade de existirem permutações distintas $\overline{x^n} \neq \widetilde{x^n}$ com o mesmo valor de *hash* tal que

$$f(\overline{x^n}) = f(\widetilde{x^n}), \tag{7.135}$$

$$K(\overline{x^n}, x^n) \leq \tau, \tag{7.136}$$

$$K(\widetilde{x^n}, x^n) \leq \tau, \tag{7.137}$$

é desprezível nos parâmetros de segurança.

No restante dessa prova, assumimos que $\left|K(x^n, y^n) - E[K]\right| < \varepsilon E[K]$, o que ocorre com probabilidade pelo menos $1 - \varphi$, onde φ tende a zero, como demonstrado na seção 7.1.4.

A probabilidade de uma Alice maliciosa ser detectada depende da distância de Kendall tau entre $\overline{x^n}$ (a sequência anunciada para Bob durante a fase de Abertura) e y^n (a permutação que Bob de fato recebe da saída do canal PRNC). Essa distância depende da quantidade de inversões realizadas pelo canal para mapear x^n (a sequência originalmente enviada pelo canal PRNC por

Alice) em y^n e as inversões realizadas por Alice para mapear x^n em $\overline{x^n}$. Observe que existe um limiar τ para o número de inversões que Alice introduz de modo que Bob consiga detectá-la. A verificação realizada por Bob no passo R.2 (ii) do protocolo falha se

$$K(\overline{x^n}, y^n) \geq (1+\varepsilon)E[K] \qquad \text{ou} \qquad K(\overline{x^n}, y^n) \leq (1-\varepsilon)E[K].$$

Algumas das inversões introduzidas por Alice aumentam a distância de Kendall tau entre $\overline{x^n}$ e y^n. Entretanto, é possível que Alice realize inversões que reduzam a distância entre $\overline{x^n}$ and y^n. Isso acontece quando Alice e o canal PRNC invertem o mesmo par de pacotes de dados. Chamamos esse evento de *colisão de inversão*. Seja $C(\overline{x^n}, y^n)$ a variável aleatória que representa a quantidade de colisões de inversão ocorridas. Considerando a abreviação C para $C(\overline{x^n}, y^n)$ e assumindo que uma Alice maliciosa realiza $q = K(\overline{x^n}, x^n)$ inversões para forjar $\overline{x^n}$, então C inversões irão favorecê-la, reduzindo a distância de Kendall tau entre $\overline{x^n}$ e y^n, enquanto $q - C$ irão prejudicá-la, aumentando a distância. Ou seja:

$$K(\overline{x^n}, y^n) = K(x^n, y^n) + (q - C) - C \tag{7.138}$$

Uma vez que $(1-\varepsilon)E[K] < K(x^n, y^n) < (1+\varepsilon)E[K]$, onde $E[K]$ é a abreviação para $E[K(x^n, y^n)]$, temos que:

$$\begin{aligned}
K(\overline{x^n}, y^n) &= K(x^n, y^n) + (q - C) - C && (7.139)\\
&> (1-\varepsilon)E[K] + q - 2C && (7.140)\\
&\geq (1+\varepsilon)E[K] && (7.141)\\
\therefore q - 2C &\geq 2\varepsilon E[K] && (7.142)
\end{aligned}$$

ou

$$\begin{aligned}
K(\overline{x^n}, y^n) &= K(x^n, y^n) + (q - C) - C && (7.143)\\
&< (1+\varepsilon)E[K] + q - 2C && (7.144)\\
&\leq (1-\varepsilon)E[K] && (7.145)\\
\therefore q - 2C &\leq -2\varepsilon E[K] && (7.146)
\end{aligned}$$

Assim, a verificação realizada no passo R.2 (ii) do protocolo vai detectar o comportamento malicioso de Alice sempre que:

$$|q - 2C| \geq 2\varepsilon E[K]. \tag{7.147}$$

Importante observar que a variável aleatória C sempre será uma fração da variável aleatória K, uma vez que é impossível termos mais colisões de inverão do que a quantidade de inversões realizadas pelo canal. Com isso, podemos impor o seguinte limite inferior em q:

$$\begin{aligned}
q - 2C &\geq q - 2K && (7.148)\\
&\geq q - 2(1+\varepsilon)E[K] && (7.149)\\
&\geq 2\varepsilon E[K] && (7.150)
\end{aligned}$$

$$\therefore q \geq 2(1+2\varepsilon)E[K] \tag{7.151}$$

de forma que uma Alice maliciosa será sempre detectada pelo teste realizado por Bob caso ela realize mais do que $2(1+2\varepsilon)E[K]$ inversões sobre x^n para forjar $\overline{x^n}$. Agora, é necessário levar em conta a variável aleatória C para determinar o valor apropriado do limiar τ. Há ao todo $\mathsf{N} = n(n-1)/2$ inversões distintas possíveis, onde $k = K(x^n, y^n)$ delas são realizadas pelo canal PRNC e $q = K(\overline{x^n}, x^n)$, por uma Alice maliciosa.

Definimos *a ordem de uma inversão* como o menor número de transposições de pares vizinhos de pacotes de dados necessário para efetivar a inversão. No geral, existem $n-j$ inversões distintas de ordem-j em qualquer permutação com n elementos. Além disso, a ordem de uma inversão específica é sempre dada em relação à permutação original. Por exemplo, seja $\pi_n = [1, 2, 3, 4..., n]$ a permutação identidade de n elementos e $\mu_{(i+1,i)} = [1, ..., i+1, i, .., n]$ alguma operação de inversão de ordem-1 sobre a permutação identidade. Quando $n = 5$, existem 4 inversões distintas de ordem-1 sobre a permutação identidade $\pi_5 = [1, 2, 3, 4, 5]$:

$$\begin{aligned}
\mu_{(2,1)} &= [\mathbf{2}, \mathbf{1}, 3, 4, 5], \\
\mu_{(3,2)} &= [1, \mathbf{3}, \mathbf{2}, 4, 5], \\
\mu_{(4,3)} &= [1, 2, \mathbf{4}, \mathbf{3}, 5], \\
\mu_{(5,4)} &= [1, 2, 3, \mathbf{5}, \mathbf{4}].
\end{aligned}$$

Por outro lado, seja uma permutação originária dada por $\zeta_5 = [3, 1, 5, 2, 4]$. Então, as 4 inversões distintas de ordem-1 são as seguintes:

$$\begin{aligned}
\mu_{(1,3)} &= [\mathbf{1}, \mathbf{3}, 5, 2, 4], \\
\mu_{(5,1)} &= [3, \mathbf{5}, \mathbf{1}, 2, 4], \\
\mu_{(2,5)} &= [3, 1, \mathbf{2}, \mathbf{5}, 4], \\
\mu_{(4,2)} &= [3, 1, 5, \mathbf{4}, \mathbf{2}].
\end{aligned}$$

Observe que as inversões acima não seriam de ordem-1 caso a permutação originária fosse a identidade. Além disso, é conveniente assumirmos que $\mu_{(1,3)} = \mu_{(3,1)}$, dado que ambas se tratam de operações de inversão sobre os mesmos elementos da permutação. Então, para tornar mais clara a definição e evitar confusão, daqui em diante, convencionamos se tratar o ordenamento dos pacotes em X^n como sendo a permutação identidade, sem perda de generalidade. Sendo assim, uma inversão de ordem-j é bem definida da forma $\mu_{(i+j,i)}$. Logo, as três inversões distintas de ordem-2 quando $n = 5$ são $\mu_{(3,1)}$, $\mu_{(4,2)}$ e $\mu_{(5,3)}$; as duas inversões distintas de ordem-3 são $\mu_{(4,1)}$ e $\mu_{(5,2)}$; e a única inversão de ordem-4 é $\mu_{(5,1)}$. Isso está esquematizado na tabela 7.1 a seguir:

Tabela 7.1: Ordem de uma inversão

Ordem-1	Ordem-2	Ordem-3	Ordem-4
$\{\mu_{(2,1)}\}$	$\{\mu_{(3,1)}\}$	$\{\mu_{(4,1)}\}$	$\{\mu_{(5,1)}\}$
$\{\mu_{(3,2)}\}$	$\{\mu_{(4,2)}\}$	$\{\mu_{(5,2)}\}$	
$\{\mu_{(4,3)}\}$	$\{\mu_{(5,3)}\}$		
$\{\mu_{(5,4)}\}$			

A ordem de uma inversão não depende da posição relativa onde ela ocorre. As permutações $\{\mu_{(3,2)}, \mu_{(3,1)}\} = [3,1,2,4,5]$ e $\{\mu_{(2,1)}, \mu_{(3,1)}, \mu_{(4,1)}\} = [2,3,4,1,5]$ possuem ambas a mesma inversão de ordem-2, i.e. $\mu_{(3,1)}$, que representa a colisão de inversão entre as duas permutações, sendo a intersecção entre os dois conjuntos de inversões. Isso significa que as permutações y^n e $\overline{x^n}$ podem ser representadas por conjuntos de inversões aplicadas sobre os pacotes de dados de x^n, tratado como a permutação identidade. Convencionamos daqui em diante que $\overline{\mathbf{X}}$ e $\mathbf{Y}$ são os conjuntos de inversões realizadas para mapear x^n em $\overline{x^n}$ e x^n em y^n, respectivamente.

Uma Alice maliciosa sempre irá realizar as inversões mais prováveis de ocorrer na saída do canal, a fim de maximizar a probabilidade de uma colisão de inversão acontecer. Vamos considerar que Alice realiza apenas inversões de ordem-1 $\mu_{(i+1,i)}$ para forjar $\overline{X^n}$. Embora existam $n-1$ inversões de ordem-1, há no máximo $(n-1)/2$ inversões de ordem-1 disjuntas que Alice consegue realizar de uma vez para mapear x^n em $\overline{x^n}$, o que limita superiormente a quantidade q de inversões maliciosas que ela pode introduzir.

Com o intuito de não restringir as capacidades maliciosas do adversário, precisamos impor uma restrição ao canal PRNC para atender essa condição. Ou seja, se Alice realizar menos de $(n-1)/2$ inversões, todas serão de ordem-1, já que são as mais prováveis. Caso ela realize $(n-1)/2$ ou mais inversões, vamos assumir que essa quantidade de inversões terá superado o limite inferior que derivamos em (7.151) para q, garantindo que o comportamento malicioso de Alice seja detectado. Assim, o parâmetro de ruído ρ do canal PRNC deve ser tal que:

$$2(1+2\varepsilon)\frac{\rho}{1-\rho}(n-1) \leq q \leq \frac{n-1}{2} \tag{7.152}$$

$$1-\rho \geq 4(1+2\varepsilon)\rho \tag{7.153}$$

$$\therefore \rho \leq \frac{1}{5+8\varepsilon} \tag{7.154}$$

Escolhemos impor a restrição acima porque inversões de ordem-1 de pares de elementos disjuntos são independentes e identicamente distribuídas. Além disso, a probabilidade de o canal PRNC realizar inversões de ordem-1 é sempre maior do que a probabilidade de realizar inversões de outras ordens, já que a ocorrência de qualquer inversão de ordem-j, $\forall\ j > 1$, depende da ocorrência de ao menos uma inversão de ordem-1 anteriormente.

Vamos calcular a probabilidade de ocorrer qualquer inversão de ordem-1 na saída do canal PRNC. Seja $T(n,k)$ o número de permutações contendo uma dada inversão $\mu_{(i+1,i)}$ de ordem-1 dentre todas as possíveis permutações $M(n,k)$ a uma distância de Kendall tau k da permutação identidade. Trivialmente, nenhuma inversão de ordem-1 ocorre quando $k=0$ e não é difícil notar que, para $k=1$, cada inversão de ordem-1 aparece apenas uma vez entre todas as possíveis permutações $M(n,1)$. Logo:

$$T(n,0) = 0 \tag{7.155}$$

e

$$T(n,1) = M(n,0) = 1 \quad \forall\ n \geq 2. \tag{7.156}$$

Quando $k=2$, cada inversão de ordem-1 ocorre exatamente $n-2$ vezes dentre todas as $M(n,2)$ permutações possíveis. Para ver isso, após se efetuar qualquer inversão de ordem-1, restam

$M(n,1) = n-1$ inversões que poderiam ser realizadas em seguida, menos $T(n,1) = 1$ que desfaria a inversão feita anteriormente. Assim, segue que:

$$T(n,2) = M(n,1) - T(n,1) = M(n,1) - M(n,0) = n-2. \tag{7.157}$$

Agora, quando $k = 3$, ao se fixar qualquer inversão de ordem-1 restarão $M(n,2)$ inversões possíveis, exceto as $T(n,2)$ inversões capazes de desfazer a inversão fixada inicialmente. Então:

$$T(n,3) = M(n,2) - T(n,2) = M(n,2) - M(n,1) + M(n,0). \tag{7.158}$$

Dessa forma, já é possível identificar o padrão, que se generaliza como segue:

$$T(n,k) = \sum_{j=0}^{k-1} (-1)^j M(n, k-1-j) \tag{7.159}$$

O seguinte fato é um simples corolário do resultado acima:

$$M(n,k) = T(n,k) + T(n,k+1) \tag{7.160}$$

Os números $T(n,k)$ formam um triângulo cujas primeiras linhas são apresentadas na tabela 7.2 abaixo. Nela os valores na coluna para $k = 0$ são sempre iguais a zero, uma vez que não há inversões de ordem-1 sem que haja a realização de ao menos uma inversão pelo canal. Destaca-se que $T(n,k)$ constitui a sequência de números inteiros catalogada na Enciclopédia On-line de Sequências de Números Inteiros (*On-line Encyclopedia of Integer Sequences* - OEIS) sob a numeração A307429 com um deslocamento de uma coluna em k. Ou seja, $T(n,k) = A307429(n, k-1)$, $\forall\ n \geq 2$.

Tabela 7.2: Triângulo $T(n,k)$

n \ k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	0															
2	0	1														
3	0	1	1	1												
4	0	1	2	3	3	2	1									
5	0	1	3	6	9	11	11	9	6	3	1					
6	0	1	4	10	19	30	41	49	52	49	41	30	19	10	4	1

Para se obter a probabilidade $p = \Pr[\mu_{(i+1,i)} \in \mathbf{Y}]$ de uma dada inversão de ordem-1 estar no conjunto de inversões realizadas pelo canal PRNC para mapear a entrada x^n na saída y^n, aplicamos a lei da probabilidade total, calculando em primeiro lugar a probabilidade condicional $\Pr[\mu_{(i+1,i)} \in \mathbf{Y} : |\mathbf{Y}| = k]$, multiplicando pela probabilidade $\Pr[|\mathbf{Y}| = k]$ e somando sobre todos os possíveis valores de k. Para cada valor de k, a probabilidade de qualquer inversão de ordem-1 ocorrer na saída é dada pela razão entre o número de permutações contendo a inversão de ordem-1 fixada, i.e. $T(n,k)$, e o número total de permutações com distância k, ou seja, $M(n,k)$. A probabilidade

$\Pr[|\mathbf{Y}| = k]$ é dada pelo produto entre a probabilidade condicional $\Pr[Y^n = y^n | X^n = x^n]$ quando a distância de Kendall tau entre y^n e x^n é k e o número total de permutações com distância de Kendall tau igual a k, uma vez que estas são todas equiprováveis. Assim, temos que:

$$
\begin{aligned}
p &= \Pr[\mu_{(i+1,i)} \in \mathbf{Y}] && (7.161)\\
&= \sum_{k=0}^{\mathsf{N}} \Pr[\mu_{(i+1,i)} \in \mathbf{Y} : |\mathbf{Y}| = k] \cdot \Pr[|\mathbf{Y}| = k] && (7.162)\\
&= \sum_{k=0}^{\mathsf{N}} \Pr[\mu_{(i+1,i)} \in \mathbf{Y} : |\mathbf{Y}| = k] \cdot M(n,k) \Pr[Y^n = y^n | X^n = x^n] && (7.163)\\
&= \sum_{k=0}^{\mathsf{N}} \frac{T(n,k)}{M(n,k)} \cdot \frac{M(n,k)\rho^k}{\sigma_n(\rho)} && (7.164)\\
&= \frac{\sum_{k=0}^{\mathsf{N}} T(n,k)\rho^k}{\sigma_n(\rho)} && (7.165)
\end{aligned}
$$

Vamos mostrar que o polinômio $\sum_{k=0}^{\mathsf{N}} T(n,k)\rho^k$ também pode ser escrito como um produto de polinômios, da mesma forma que o polinômio $\sigma_n(\rho) = \prod_{i=1}^{n} S_i(\rho)$. Observe que os somatórios dos referidos polinômios não precisam se limitar aos intervalos propostos, uma vez que $\forall\ k < 0 \vee k > \mathsf{N},\ T(n,k) = M(n,k) = 0$. Logo:

$$
\begin{aligned}
\sum_{k=0}^{\mathsf{N}} T(n,k)\rho^k &= \sum_{k=0}^{\mathsf{N}} \sum_{j=0}^{k-1} (-1)^j M(n,k-1-j)\rho^k && (7.166)\\
&= \sum_{j=0}^{\infty} (-1)^j \sum_{k=0}^{\infty} M(n,k-1-j)\rho^k && (7.167)\\
&= \sum_{j=0}^{\infty} (-1)^j \rho^{j+1} \sum_{k=-(j+1)}^{\infty} M(n,k)\rho^k && (7.168)\\
&= \sum_{j=0}^{\infty} (-1)^j \rho^{j+1} \sum_{k=0}^{\mathsf{N}} M(n,k)\rho^k && (7.169)\\
&= \rho\sigma_n(\rho) \sum_{j=0}^{\infty} (-\rho)^j && (7.170)\\
&= \left(\frac{\rho}{1+\rho}\right) \sigma_n(\rho) && (7.171)
\end{aligned}
$$

É fácil verificar que os coeficientes $T(n,k)$ do polinômio acima de fato formam o triângulo catalogado pela sequência de números inteiros OEIS A307429 citada anteriormente. Além disso, podemos observar que o produto por ρ é a causa do deslocamento para a direita na coluna do triângulo formado pelos números $T(n,k)$ quando comparado ao triângulo de Mahonian. Logo:

$$
\begin{aligned}
p &= \frac{\sum_{k=0}^{\mathsf{N}} T(n,k)\rho^k}{\sigma_n(\rho)} && (7.172)\\
&= \frac{\left(\frac{\rho}{1+\rho}\right) \sigma_n(\rho)}{\sigma_n(\rho)} && (7.173)\\
&= \frac{\rho}{1+\rho} && (7.174)
\end{aligned}
$$

Tendo obtido a probabilidade de ocorrer uma inversão de ordem-1 na saída do canal PRNC, vamos partir agora para a obtenção do valor esperado da variável aleatória C. Destaca-se que a variável aleatória que representa a quantidade de colisões de inversão pode ser obtida a partir da soma de variáveis aleatórias indicadoras $C = \sum_{i=1}^{n-1} C_{\mu_{(i+1,i)}}$, onde $C_{\mu_{(i+1,i)}} = 1$ quando tanto Alice quanto o canal PRNC realizam a inversão $\mu_{(i+1,i)}$ e $C_{\mu_{(i+1,i)}} = 0$ caso contrário. Importante também destacar que as inversões efetuadas por Alice em $\overline{\mathbf{X}}$ e pelo canal em $\mathbf{Y}$ são independentes. Lembrando que uma Alice maliciosa efetua $|\overline{\mathbf{X}}| = q$ inversões arbitrariamente, o número esperado de colisões de inversão será:

$$
\begin{aligned}
E[C] &= E\left[\sum_{i=1}^{n-1} C_{\mu_{(i+1,i)}}\right] && (7.175)\\
&= \sum_{i=1}^{n-1} E[C_{\mu_{(i+1,i)}}] && (7.176)\\
&= \sum_{i=1}^{n-1} \Pr[C_{\mu_{(i+1,i)}} = 1] && (7.177)\\
&= \sum_{i=1}^{n-1} \Pr[\mu_{(i+1,i)} \in \mathbf{Y} \wedge \mu_{(i+1,i)} \in \overline{\mathbf{X}}] && (7.178)\\
&= \sum_{i=1}^{n-1} \Pr[\mu_{(i+1,i)} \in \mathbf{Y}] \cdot \Pr[\mu_{(i+1,i)} \in \overline{\mathbf{X}}] && (7.179)\\
&= \sum_{\mu \in \overline{\mathbf{X}}} p && (7.180)\\
&= |\overline{\mathbf{X}}| \cdot p && (7.181)\\
&= \frac{q\rho}{1+\rho} && (7.182)
\end{aligned}
$$

Podemos mostrar que o valor esperado obtido em (7.182) acima tem dispersão limitada, estando concentrado em torno da média. Para isso, primeiro observamos que:

$$
\begin{aligned}
E\left[e^{tC_{\mu_{(i+1,i)}}}\right] &= \Pr[C_{\mu_{(i+1,i)}} = 0] + e^t \cdot \Pr[C_{\mu_{(i+1,i)}} = 1] && (7.183)\\
&= \Big(1 - \Pr[C_{\mu_{(i+1,i)}} = 1]\Big) + e^t \cdot \Pr[C_{\mu_{(i+1,i)}} = 1] && (7.184)\\
&= 1 + (e^t - 1) \cdot \Pr[C_{\mu_{(i+1,i)}} = 1] && (7.185)\\
&= 1 + \delta p \Pr[\mu_{(i+1,i)} \in \overline{\mathbf{X}}] && (7.186)
\end{aligned}
$$

onde fixamos $\delta = (e^t - 1)$ no último passo acima.

Como Alice adota a melhor estratégia adversarial para forjar $\overline{x^n}$, ela irá escolher deterministica e arbitrariamente as inversões de ordem-1 independentes, ou seja, aquelas que ocorrem com maior probabilidade na saída no canal PRNC. Assim, temos que:

$$
\begin{aligned}
E\left[e^{tC}\right] &= E\left[e^{t\sum_{i=1}^{n-1} C_{\mu_{(i+1,i)}}}\right] && (7.187)\\
&= E\left[\prod_{i=1}^{n-1} e^{tC_{\mu_{(i+1,i)}}}\right] && (7.188)
\end{aligned}
$$

$$
\begin{aligned}
&= \prod_{i=1}^{n-1} E\left[e^{tC_{\mu_{(i+1,i)}}}\right] && (7.189)\\
&= \prod_{i=1}^{n-1} \left(1+\delta p \cdot \Pr[\mu_{(i+1,i)} \in \overline{\mathbf{X}}]\right) && (7.190)\\
&= \prod_{\mu\in\overline{\mathbf{X}}} (1+\delta p) && (7.191)\\
&= (1+\delta p)^q && (7.192)\\
&\leq e^{\delta qp} && (7.193)\\
&= e^{\delta E[C]} && (7.194)
\end{aligned}
$$

Lembrando que $t = \ln(1+\delta)$ e aplicando a desigualdade de Chernoff-Hoeffding em (4.57):

$$
\begin{aligned}
\Pr[C \geq (1+\delta)E[C]] &\leq \min_{t>0} \frac{E[e^{tC}]}{e^{t(1+\delta)E[C]}} && (7.195)\\
&\leq e^{\delta E[C]-(1+\delta)\ln(1+\delta)E[C]} && (7.196)\\
&= e^{\left(\delta-(1+\delta)\ln(1+\delta)\right)E[C]} && (7.197)\\
&\leq e^{-\frac{\delta^2}{2+\delta}E[C]} && (7.198)
\end{aligned}
$$

Para se determinar o limiar τ, lembramos que nesse passo da prova, por hipótese, $q \geq \tau$. Logo:

$$
\Pr[C \geq (1+\delta)E[C]] \leq e^{-\frac{\delta^2}{2+\delta}\frac{\rho\tau}{1+\rho}} \quad (7.199)
$$

sendo desprezível para τ suficientemente grande.

Finalmente, podemos mostrar que:

$$
\begin{aligned}
q - 2C &\geq q - 2(1+\delta)E[C] && (7.200)\\
&= q - 2(1+\delta)qp && (7.201)\\
&\geq 2\varepsilon E[K] && (7.202)
\end{aligned}
$$

$$
\therefore q \geq \frac{2\varepsilon E[K]}{1-2(1+\delta)p} \quad (7.203)
$$

Como mostrado na subseção 7.1.1, $E[K] \leq (n-1)\rho/(1-\rho)$. Consequentemente, podemos fixar o limiar τ como:

$$
\tau = \left(\frac{2\varepsilon}{1-2(1+\delta)p}\right)\left(\frac{\rho}{1-\rho}\right)(n-1) \quad (7.204)
$$

de modo que, para todo $q \geq \tau$, Bob detecta o comportamento malicioso de Alice através do teste que realiza no passo **R.2** da fase de abertura do protocolo, conforme descrito no seção 6.5.

Agora, para completar a prova de segurança para Bob, vamos demonstrar que, se uma Alice maliciosa efetuar $q \leq \tau$ permutações para forjar $\overline{x^n}$, então Bob detecta a tentativa de trapaça, uma vez que é desprezível a probabilidade de Alice encontrar duas permutações distintas que apresentam o mesmo valor de *hash* 2-universal.

Lema 7.1. *Seja $\mathcal{F}$ uma família de funções de hash 2-universal $f : \{0,1\}^{n\ell} \to \{0,1\}^{\omega}$ e seja*

$$\omega = 2(n-1+\tau)\mathsf{H}_b\left(\frac{\tau}{n-1+\tau}\right) + s, \tag{7.205}$$

onde s é o parâmetro de segurança. Então, a probabilidade de existirem duas permutações $\overline{x^n} \neq \widetilde{x^n}$ tal que $f(\overline{x^n}) = f(\widetilde{x^n})$, $K(\overline{x^n}, x^n) \leq \tau$ e $K(\widetilde{x^n}, x^n) \leq \tau$ é no máximo 2^{-s}.

Prova do Lema 7.1: Seja $x^n \leftarrow X^n$ uma sequência do tipo definido no passo **C.1** da fase de comprometimento do protocolo, conforme descrito no seção 6.5. Seja $\mathbf{W}$ um conjunto de permutações de pacotes de dados como distância de Kendall tau no máximo τ de x^n. Uma vez que o número de sequências com distância de Kendall tau k de x^n é dado pelo termo $M(n,k)$ do triângulo de Mahonian, para se obter a cardinalidade de $\mathbf{W}$ precisamos apenas somar cada um dos termos $M(n,k)$ para todo $0 \leq k \leq \tau$. Da definição do triângulo de Mahonian derivamos que:

$$\sum_{k=0}^{\tau} M(n,k) = M(n+1,\tau), \qquad \forall\ \tau \leq n, \tag{7.206}$$

Usando o seguinte resultado demonstrado no Lema 13 em [102]:

$$M(n+1,\tau) \leq \binom{n-1+\tau}{\tau}, \tag{7.207}$$

podemos obter a cardinalidade de $\mathbf{W}$:

$$\begin{aligned}
|\mathbf{W}| &= \sum_{k=0}^{\tau} M(n,k) && (7.208)\\
&= M(n+1,\tau) && (7.209)\\
&\leq \binom{n-1+\tau}{\tau} && (7.210)\\
&= \frac{(n-1+\tau)!}{(n-1)!\cdot\tau!}. && (7.211)
\end{aligned}$$

Aplicando a aproximação de Stirling e algumas outras simplificações na expressão acima, temos:

$$\begin{aligned}
|\mathbf{W}| &\leq \frac{e\sqrt{n-1+\tau}\left(\frac{n-1+\tau}{e}\right)^{n-1+\tau}}{\sqrt{2\pi(n-1)}\left(\frac{n-1}{e}\right)^{n-1}\sqrt{2\pi\tau}\left(\frac{\tau}{e}\right)^{\tau}} && (7.212)\\
&\leq \frac{e}{2\pi}\sqrt{\frac{n-1+\tau}{(n-1)\cdot\tau}}\left(\frac{n-1+\tau}{n-1}\right)^{n-1}\left(\frac{n-1+\tau}{\tau}\right)^{\tau}. && (7.213)
\end{aligned}$$

Estamos interessado no logaritmo da cardinalidade de $\mathbf{W}$, de forma que:

$$\begin{aligned}
\log|\mathbf{W}| &\leq (n-1)\log\left(\frac{n-1+\tau}{n-1}\right) + \tau\log\left(\frac{n-1+\tau}{\tau}\right)\\
&\quad - \frac{1}{2}\log\frac{(n-1)\cdot\tau}{n-1+\tau} - \log\frac{2\pi}{e} && (7.214)\\
&\leq (n-1+\tau)\left[\frac{n-1}{n-1+\tau}\log\left(\frac{n-1+\tau}{n-1}\right)\right.\\
&\quad \left. + \frac{\tau}{n-1+\tau}\log\left(\frac{n-1+\tau}{\tau}\right)\right] && (7.215)\\
&\leq (n-1+\tau)\mathsf{H}_b\left(\frac{\tau}{n-1+\tau}\right). && (7.216)
\end{aligned}$$

Usando a definição de funções de *hash* 2-universal em [79], obtemos a probabilidade de colisão:

$$\Pr[f(\overline{x^n}) = f(\widetilde{x^n}) \mid \overline{x^n} \neq \widetilde{x^n}] = \frac{1}{|F|} \tag{7.217}$$

Alice não pode ser capaz de encontrar qualquer par de permutações em $\mathbf{W}$ cujos os valores dos *hashes* colidam, a fim de que não obtenha sucesso em sua tentativa de trapacear. Pelo paradoxo do aniversário e a desigualdade de Boole (*Union Bound*), a probabilidade de Alice encontrar uma colisão entre os *hashes* de duas permutações distintas $\overline{x^n}, \widetilde{x^n} \in \mathbf{W}$ é cotada superiormente por:

$$\begin{aligned}
\Pr[f(\overline{x^n}) = f(\widetilde{x^n}) \;\forall\; \overline{x^n} \neq \widetilde{x^n} \in \mathbf{W}] &\leq \sum_{\overline{x^n} \in \mathbf{W}} \sum_{\widetilde{x^n} \in \mathbf{W}} \frac{1}{|F|} && (7.218)\\
&= |\mathbf{W}|^2 \cdot 2^{-\omega} && (7.219)\\
&\leq 2^{2(n-1+\tau)\mathsf{H}_b(\tau/(n-1+\tau))} \\
&\quad \cdot\, 2^{-2(n-1+\tau)\mathsf{H}_b(\tau/(n-1+\tau))-s} && (7.220)\\
&= 2^{-s}, && (7.221)
\end{aligned}$$

o que conclui a prova do lema. ■

Isso significa que Alice terá sucesso em trapacear Bob somente se ao menos uma das seguintes condições ocorrer: o canal inverter menos que $(1-\varepsilon)E[K]$ pares de pacotes de dados adjacentes da permutação de entrada x^n; o número de colisões de inversão exceder a quantidade $(1+\delta)E[C]$ ou uma colisão de *hashes* $f(\overline{x^n}) = f(\widetilde{x^n})$ for encontrada.

À luz dos argumentos acima, quando Bob segue o protocolo, a probabilidade de uma Alice maliciosa ter sucesso em trapacer é limitada superiormente por θ:

$$\begin{aligned}
&\Pr[\mathsf{Test}(\widetilde{X^n}, Y^n, T, \widetilde{v}) = \text{ACC} \wedge \mathsf{Test}(\overline{X^n}, Y^n, T, \overline{v}) = \text{ACC}] \\
&\qquad \leq e^{-(n-1)\rho\varepsilon^2\beta^2/2} + e^{-(n-1)\frac{\delta^2}{(2+\delta)}\frac{2\varepsilon\rho^2}{1-2\rho+(1+2\delta)\rho^2}} + 2^{-s} \\
&\qquad = \theta && (7.222)
\end{aligned}$$

que vai exponencialmente para zero nos parâmetros de segurança n e s. ■

7.3 *Hiding*: Condição de Segurança para o Remetente

Quando Alice é honesta, o protocolo precisa garantir que nenhuma informação sobre o seu comprometimento irá vazar para Bob, mesmo que ele aja de forma deliberadamente maliciosa para tentar obter alguma informação indevida. Vamos demonstrar que o protocolo é seguro para Alice se, antes da fase de abertura, um Bob malicioso consegue obter apenas uma quantidade ínfima de informação sobre o valor v com o qual Alice se compromete.

Em um protocolo ideal, Alice cifraria seu comprometimento usando uma chave perfeitamente aleatória e do mesmo tamanho de v utilizando uma operação XOR bit-a-bit, o chamado *One-Time Pad*. Porém, em um protocolo real, é necessário que Bob tenha evidências sobre a chave utilizada

por Alice para cifrar seu comprometimento, a fim de se evitar que ela consiga trapacear sem que seu comportamento malicioso seja detectado por Bob.

Para atender essa condição, Alice extrai uma chave a partir de X^n usando uma técnica conhecida como *Privacy Amplification*. A chave é usada para cifrar por meio de *One-Time Pad* o valor v com o qual Alice se compromete. Como evidência desse comprometimento, Bob possui a variável aleatória Y^n (obtida através do canal PRNC) correlacionada a X^n e o resultado de $f(x^n)$ uma função de *hash* 2-universal (baseada em uma semente escolhida por ele) computada por Alice. Para demonstrar que Bob possui um conhecimento ínfimo sobre o comprometimento v de Alice, vamos demonstrar que a chave extraída por Alice e usada para cifrar o comprometimento é ϵ-próximo de uma distribuição uniforme de probabilidade dada toda informação disponível na visão de Bob, modelada pela variável aleatória $View_B$, sendo esse resultado obtido com base no Lema do *Leftover-Hash*, tratado na seção 4.1.

A fim de aplicar esse lema, vamos precisar limitar a incerteza de Bob sobre X^n, a entrada de Alice no canal PRNC. Assim, quando Bob recebe Y^n sua incerteza sobre X^n se deve ao comportamento ruidoso do canal PRNC, que produz uma permutação aleatória de X^n com a seguinte função massa de probabilidade:

$$p(x^n|y^n) = \frac{\rho^{K(x^n,y^n)}}{\sigma_n(\rho)}. \tag{7.223}$$

Observe que $p(x^n|y^n) = p(y^n|x^n)$ se deve ao fato de a matriz de transição do canal PRNC ser simétrica, da mesma forma que outros canais ruidosos típicos. Como $\rho^{K(x^n,y^n)}$ é maximizado quando $y^n = x^n$, já que nesse caso $K(x^n, y^n) = K(x^n, x^n) = 0$, a min-entropia de X^n dado que Bob conhece Y^n pode ser obtida da seguinte forma:

$$\begin{aligned}
H_\infty(X^n|Y^n) &= \min_{y^n} H_\infty(X^n|Y^n = y^n) && (7.224)\\
&= -\log \max_{y^n} \left[p(x^n|y^n)\right] && (7.225)\\
&= -\log \max_{y^n} \left[\left(\frac{\rho^{K(x^n,y^n)}}{\sigma_n(\rho)}\right)\right] && (7.226)\\
&= \log \sigma_n(\rho) && (7.227)\\
&= \log \left[\left(\frac{1}{1-\rho}\right)^n \prod_{i=1}^{n}(1-\rho^i)\right] && (7.228)\\
&= n \log \left(\frac{1}{1-\rho}\right) + \sum_{i=1}^{n} \log\left(1-\rho^i\right). && (7.229)
\end{aligned}$$

Lembramos que a série de Taylor de $\ln(1+x)$ é dada por:

$$\ln(1+x) = \sum_{j=1}^{\infty} (-1)^{j+1} \frac{x^j}{j} \tag{7.230}$$

Então, substituindo x por $-\rho^i$ na expressão (7.230) e realizando a substituição da base do logaritmo de e para 2, temos:

$$\log(1-\rho^i) = \frac{-1}{\ln(2)} \sum_{j=1}^{\infty} \frac{\rho^{ij}}{j}. \tag{7.231}$$

Logo,

$$
\begin{aligned}
H_\infty(X^n|Y^n) &= n\log\left(\frac{1}{1-\rho}\right) - \frac{1}{\ln(2)}\sum_{i=1}^{n}\sum_{j=1}^{\infty}\frac{\rho^{ij}}{j} && (7.232)\\
&\geq n\log\left(\frac{1}{1-\rho}\right) - \frac{1}{\ln(2)}\sum_{i=1}^{\infty}\sum_{j=1}^{\infty}\frac{\rho^{ij}}{j} && (7.233)\\
&\geq n\log\left(\frac{1}{1-\rho}\right) - 2\sum_{j=1}^{\infty}\frac{1}{j}\sum_{i=1}^{\infty}(\rho^j)^i && (7.234)\\
&= n\log\left(\frac{1}{1-\rho}\right) - 2\sum_{j=1}^{\infty}\frac{1}{j}\frac{\rho^j}{1-\rho^j} && (7.235)\\
&= n\log\left(\frac{1}{1-\rho}\right) - \frac{2\rho}{1-\rho}\sum_{j=1}^{\infty}\frac{\rho^{j-1}}{j\sum_{k=0}^{j-1}\rho^k} && (7.236)
\end{aligned}
$$

Utilizando o lema 4.3 para obter uma cota superior para o somatório acima, temos:

$$
\sum_{j=1}^{\infty}\frac{\rho^{j-1}}{j\sum_{k=0}^{j-1}\rho^k} \leq \sum_{j=0}^{\infty}\frac{\rho^j}{(\sum_{k=0}^{j}\rho^k)^2} \leq 1+\rho \qquad (7.237)
$$

Logo,

$$
H_\infty(X^n|Y^n) \geq n\log\left(\frac{1}{1-\rho}\right) - \frac{2\rho(1+\rho)}{(1-\rho)}. \qquad (7.238)
$$

Aplicando agora o lema 4.2, vamos limitar a redução na incerteza de Bob sobre X^n devido ao seu conhecimento da função de *hash* 2-universal computada por Alice, cujo tamanho é dado por $\omega = 2(n-1+\tau)\mathsf{H}_b\left(\frac{\tau}{n-1+\tau}\right) + s$. Assim, segue que:

$$
\begin{aligned}
H_\infty(X^n|\mathsf{View_B}) &:= H_\infty(X^n|Y^n, \mathsf{Hash}) && (7.239)\\
&\geq H_\infty(X^n|Y^n) - \log 2^\omega - s && (7.240)\\
&\geq n\log\left(\frac{1}{1-\rho}\right) - \frac{2\rho(1+\rho)}{(1-\rho)}\\
&\quad - 2(n-1+\tau)\mathsf{H}_b\left(\frac{\tau}{n-1+\tau}\right) - 2s. && (7.241)
\end{aligned}
$$

O lema 4.1 (*Leftover-Hash*) estabelece que funções de *hash* 2-universal usadas como *Extratores de Aleatoriedade* conseguem extrair $m \leq \delta n - 2\log(\epsilon^{-1}) + 2$ bits de aleatoriedade, onde δn representa a min-entropia da fonte. Denotando $\epsilon = 2^{-s}$, no caso do protocolo proposto neste trabalho será possível extrair no máximo

$$
m = n\log\left(\frac{1}{1-\rho}\right) - 2(n-1+\tau)\mathsf{H}_b\left(\frac{\tau}{n-1+\tau}\right) - \frac{2\rho(1+\rho)}{(1-\rho)} - 4s + 2 \qquad (7.242)
$$

bits de aleatoriedade tal que a distância estatística entre a saída da função de *hash* G aplicada por Alice sobre X^n para se obter a chave $g(x^n)$ usada para cifrar a mensagem v e uma sequência realmente aleatória com distribuição uniforme é no máximo 2^{-s} na visão de Bob, dado que G é

escolhida também com distribuição de probabilidade uniforme sobre a família $\mathcal{G}$ de funções de *hash* 2-universal.

Uma vez que Alice efetua o *One-Time Pad* entre o seu comprometimento v e o resultado da função de *hash* 2-universal $g(x^n)$, concluímos que:

$$\begin{aligned} \mathsf{SD}\left(P_{V,\mathsf{View_B}}; P_{U_m,\mathsf{View_B}}\right) &\leq \mathsf{SD}\left(P_{G(X^n),G}; P_{U_m,G}\right) && (7.243)\\ &\leq 2^{-s} && (7.244)\\ &= \epsilon && (7.245) \end{aligned}$$

e a prova segue. ■

7.4 Limites teóricos sobre o adversário

Apresentamos alguns resultados anteriores sobre os limites teóricos na capacidade de adversário trapacear em um protocolo de comprometimento em canais discretos sem memória para efeito de comparação com os resultados das provas de segurança obtidos neste Capítulo.

O primeiro resultado vem de trabalhos anteriores sobre a viabilidade de protocolos de comprometimento baseados em dados pré-distribuídos [101], [103].

Lema 7.2. *A probabilidade média de trapaça de Alice $\bar{\theta}$ é limitada inferiormente por $2^{-H(Y|X)}$.*

Prova: A idéia da prova desse lema está no fato de a segurança do protocolo vir do sigilo de X e Y, deixando claro que se Alice for capaz de adivinhar corretamente os dados guardados por Bob ela será capaz de trapacear com sucesso. A probabilidade média de Alice errar ao tentar chutar o valor de Y é cotada inferiormente por

$$\bar{\theta} \geq 2^{-H(Y|X)} \tag{7.246}$$

■

A função de teste computada por Bob na fase de abertura pode ser compreendida como um problema de teste de hipóteses. No caso, o destinatário do comprometimento deseja distinguir entre duas situações:

- O remetente se comportou honestamente. (hipótese Λ_0)
- O remetente trapaceou (hipótese Λ_1).

Para demonstrar o próximo resultado, restringiremos a análise aos protocolos onde a troca de mensagens durante a fase de comprometimento do protocolo proposto não revelam informação alguma sobre Y que Bob recebe através do canal. Essa pode ser considerada uma restrição natural, já que não há absolutamente ganho algum em se revelar qualquer informação sobre os dados secretos que Bob possui, o que iria meramente melhorar as chances de Alice trapacear, conforme demonstrado no lema anterior. Além disso, todos os protocolos de comprometimento incondicionalmente seguros presentes atualmente na literatura atendem a essa restrição.

Considere que a hipótese Λ_0 representa a distribuição de probabilidade que realmente gera os dados que Alice e Bob possuem, dada a comunicação trocada entre eles, $(X^n, Y^n|T^n)$. Seja a distribuição de probabilidade realmente especificada pelas instruções do protocolo denotada aqui por $C_{(X^n,Y^n|T^n)}$. Considere que a hipótese Λ_1 tem a representação da informação trocada entre os participantes $(X_a, X_b|T)$ gerada por outra distribuição de probabilidade, $E_{(X',Y|T)}$, onde E representa uma estratégia de trapaça adotada por Alice.

Lema 7.3. *Em um protocolo de comprometimento baseado em canais distretos sem memória, o remetente sempre pode trapacear com probabilidade média maior ou igual a* $\bar{\theta} \geq 2^{-I(X;Y)}$

Prova: Em primeiro lugar, lembramos que η representa a probabilidade de Bob rejeitar um um comprometimento verdadeiro de Alice e θ representa a probabilidade de Bob aceitar um comprometimento falso enviado por uma Alice desonesta, conforme definido na seção 6.4. Fazendo a substituição das variáveis $C_{X|V=v}(x) = P_{X,Y|T}$ e $E_{X|V=v}(x) = P_X P_{Y|T}$ no Teorema 4.2 temos que:

$$\mathsf{d}(\bar{\eta}||1-\bar{\theta}) \leq \sum_{t\in\mathcal{T}} P_T(t) \sum_{x,y\in\mathcal{X}} P_{(X,Y|T=t)}(x,y) \log \frac{P_{(X,Y|T=t)}(x,y)}{P_{X'}(x')P_{Y|T=t}(y)} \tag{7.247}$$

$$\mathsf{d}(\bar{\eta}||1-\bar{\theta}) \leq I(X;Y|T) \tag{7.248}$$

Entretanto, assumimos que a comunicação sem ruído T não fornece para Alice informação sobre os dados privados de Bob. Logo:

$$I(X;Y|T) = I(X;Y) \tag{7.249}$$

Fazendo uso da definição $\mathsf{d}(\bar{\eta}, 1-\bar{\theta})$ e da condição de corretude de um protocolo de comprometimento no qual $\lim_{n\to\infty} \eta \to 0$, para o limite do parâmetro de segurança θ, segue que:

$$\bar{\eta} \log \frac{\bar{\eta}}{1-\bar{\theta}} + (1-\bar{\eta}) \log \frac{1-\bar{\eta}}{\bar{\theta}} \leq I(X;Y) \tag{7.250}$$

$$\log \frac{1}{\bar{\theta}} \leq I(X;Y) \tag{7.251}$$

$$\therefore \bar{\theta} \geq 2^{-I(X;Y)} \tag{7.252}$$

■

Por fim, como Alice escolhe X^n aleatoriamente, para o canal PRNC que é utilizado apenas uma vez, temos que:

$$\begin{aligned} I(X^n;Y^n) &= H(X^n) - H(X^n|Y^n) && (7.253)\\ &\leq \log(n!) - H_\infty(X^n|Y^n) && (7.254)\\ &\leq n\log(n) - n + O(1) - n\log\left(\frac{1}{1-\rho}\right) + \frac{2\rho(1+\rho)}{(1-\rho)} && (7.255) \end{aligned}$$

Com isso, o valor de $\bar{\theta}$ é cotado inferiormente por:

$$\bar{\theta} \geq 2^{-n(\log n - (1-\log(1-\rho))} \tag{7.256}$$

A partir da análise das proposições anteriores, comparando os valores obtidos para θ em (7.222) e em (7.256) acima, podemos concluir que o canal PRNC atende as cotas inferiores nas probabilidades de trapaça do adversário, podendo ser tratado também como um canal discreto sem memória.

Por fim, se o canal PRNC não realizar reordenamento algum, então não haverá equivocação e, assim, comprometimento será impossível. Da mesma forma, se o canal reordenar os pacotes com distribuição uniforme sobre todas as possíveis permutações de saída, os dados de Alice e Bob não serão correlacionados, sendo igualmente impossível obter comprometimentos com taxas diferentes de zero.

Capítulo 8

Análise de Desempenho

Neste capítulo é realizada uma análise sobre o desempenho do protocolo, de modo a demonstrar a existência de escolhas interessantes para o caso de uma implementação. Além disso, apresentamos um caso de estudo, com o intuito de deixar mais claro os cálculos realizados com os diversos parâmetros do protocolo e questões relativas as escolhas de valores adequados para os parâmetros em condições reais de funcionamento.

O protocolo de comprometimento baseado no efeito de reordenamento construído na presente tese tem um apelo prático, uma vez que todos os requisitos para sua implementação, sejam esses computacionais, tecnológicos ou físicos, estão disponíveis de modo acessível. Em outros termos, as computações que necessitam ser efetuadas no protocolo podem ser realizadas por computadores pessoais comumente utilizados desde os anos 2000. A largura de banda necessária para que a transmissão dos pacotes ocorra em poucos segundos já está disponível para a comercialização em países como o Japão e os Estados Unidos há mais de uma década e, mais recentemente, também em países como o Brasil.

O efeito de reordenamento de pacotes é corriqueiro na Internet, onde todo o roteamento de pacotes é feito com base no Protocolo de Internet (*Internet Protocol* - IP) com auxílio de um conjunto de protocolos de comunicação de computadores em rede pertencentes a pilha de protocolos TCP/IP, ilustrados na figura 8.1. O principal protocolo de roteamento utilizado no *backbone* da Internet é o *Border Gateway Protocol* (BGP), ou protocolo de roteador de borda em português.

A diversidade na publicação de rotas, quedas de links, uso de processadores dedicados (ASICs - *Application Specific Integrated Circuits*) para computação paralela em roteadores e possibilidades de pacotes percorrerem rotas distintas são alguns fatores que favorecem o reordenamento dos pacotes no tráfego entre dois pontos quaisquer na internet. Vamos assumir como modelo do caso de uso que Alice e Bob estão se comunicando através da Internet e estão em locais remotos, de modo que a comunicação entre eles trafegue para fora de suas redes locais, passando pelo *backbone* de ao menos uma operadora.

Figura 8.1: Pilha de Protocolos TCP/IP

(adaptada de `https://pt.wikipedia.org/wiki/Protocolo_de_controle_de_transmissão`)

O canal PRNC proposto pode ser emulado com a utilização do protocolo UDP (*User Datagram Protocol*) na transmissão dos pacotes, utilizando-se o campo de dados do segmento UDP para numerar os pacotes, intencionalmente de modo aleatório. O UDP é um protocolo simples da camada de transporte da pilha TCP/IP. O seguinte esquema ilustra a arquitetura TCP/IP:

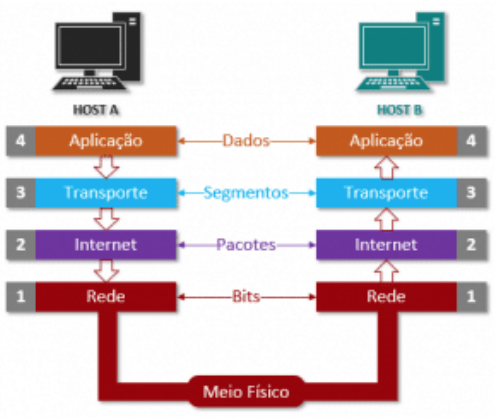

Figura 8.2: Modelo de Comunicação TCP/IP

(adaptada de `https://www.datarain.com.br/blog/tecnologia-e-inovacao/o-que-e-o-protocolo-tcpip/`)

O UDP está descrito na RFC 768 e permite que a aplicação envie um datagrama encapsulado num pacote IPv4 ou IPv6 a um destino, porém sem qualquer tipo de garantia quanto a entrega, especialmente quanto ao seu ordenamento original. O canal autenticado e livre de ruído utilizado no protocolo de comprometimento proposto pode ser emulado utilizando o protocolo TCP.

O TCP (*Transmission Control Protocol*), Protocolo de Controle de Transmissão em português, é um importante protocolo de rede que, assim como os protocolos IP e UDP, possibilita a duas máquinas se conectarem através da Internet, mas com garantia da entrega dos dados na mesma ordem que foram enviados. Portanto, o cenário físico delineado pelo canal PRNC no protocolo de comprometimento pode ser completamente emulado em uma transmissão através da Internet.

As RFCs 4737 e 5236 estabelecem um padrão com diversas métricas de medição do efeito de reordenamento de pacotes na Internet. Contudo, a medida efetuada por Bob não necessita ser realizada assim que os pacotes chegam, como preconizado nas RFCs, embora sejam interessantes e ilustrativas da relevância do efeito de reordenamento na comunicação através da Internet.

8.1 Eficiência dos parâmetros

Considerando a tecnologia atual, uma escolha razoável para a quantidade de pacotes n que Alice transmite para Bob através do canal PRNC emulado pelo uso de UDP em uma transmissão pela Internet seria de 16.777.216 pacotes, ou seja, $n = 2^{24}$. Com isso, cada pacote transmitido precisaria ter tamanho ao menos $\ell \geq \log(n) = 24$ bits. Essa quantidade de dados é pequena, sendo menor que o tamanho mínimo de carga de um pacote IP. Lembrando, porém, que uma transmissão de pacotes por uma rede ethernet tem um quadro (*frame*) com tamanho mínimo de 64 bytes, a quantidade de dados trafegados entre Alice e Bob seria de 1 GB. Apresentamos a representação de um quadro ethernet a seguir:

Figura 8.3: *Formato de um quadro (**frame**) Ethernet*
(adaptada de `https://pplware.sapo.pt/tutoriais/networking/`)

A parte dos dados do usuário (*user data*) é onde está encapsulado o pacote IP. O cabeçalho de um pacote IP é onde se encontra as informações para roteamento na Internet. A seguir, apresentamos um esquema ilustrativo de um cabeçalho IP:

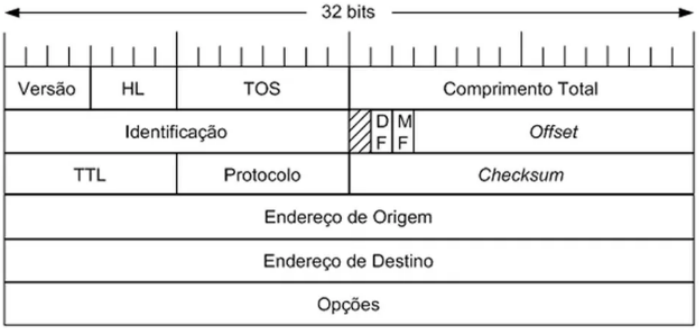

Figura 8.4: *Cabeçalho do protocolo IP*
(adaptada de `https://www.techtudo.com.br/noticias/2012/05/o-que-e-ip.ghtml`)

Em uma conexão caseira via fibra (*Fiber To The Home - FTTH*) de 512 Mbps, comum atualmente, essa transmissão levaria algo em torno de 30 segundos para ser realizada, dado um cenário conservador, onde apenas 50% da banda nominal estivesse disponível no momento da transmissão.

Em um caso de estudo teórico, vamos assumir para o parâmetro característico do canal PRNC o valor $\rho = 0,1$, para a margem de erro do canal o valor $\varepsilon = 1/40 = 2,5\%$ e para a margem superior de colisão de inversão o valor de $\delta = 1/12 = 8,\overline{3}\%$. Consideramos razoáveis os valores escolhidos para os parâmetros do canal por estarem dentro da faixa de restrição imposta sobre o canal para que seu funcionamento ocorra com garantia de segurança, $0 < \rho < 1/(5 + 8\varepsilon) = 5/26$. Além disso, essa escolha implica que um percentual máximo de 20% dos pacotes estarão fora de suas posições originais.

Estudos realizados [104, 105, 106] sugerem que comunicações através da Internet têm tipicamente um percentual médio em torno de 11% dos pacotes fora de suas posições originais e, aparentemente, uma concentração em torno da média que estabelece uma margem de erro próxima de 3% como realista. Até o presente momento, a medida da margem de erro δ para as colisões de inversões não existe na literatura, no melhor do nosso conhecimento. Contudo, entendemos ser razoável a escolha feita para o valor de δ por não representar uma margem muito apertada, comparada com a margem de erro ε do valor esperado de inversões realizadas pelo canal PRNC.

Agora, calculamos os valores dos demais parâmetros do protocolo. Com o intuito de manter a uniformidade entre as medidas e a precisão adequada para se estabelecer a sensibilidade dos parâmetros envolvidos, trabalhamos com 12 casas decimais de precisão para as medidas e consequentemente para os cálculos de propagação de erros. Assim, para se obter o valor esperado de inversões realizadas pelo canal PRNC, temos que:

$$\beta = 1 - \frac{2\rho}{(n-1)(1-\rho)} = 0,999999986755 \tag{8.1}$$

Ou seja,

$$1.864.134,975308640000 \leq (n-1)\frac{\rho}{1-\rho}\beta \leq E[K(X^n, Y^n)] \leq (n-1)\frac{\rho}{1-\rho} \leq 1.864.135 \tag{8.2}$$

$$\therefore E[K] = 1.864.135 \tag{8.3}$$

Lembrando que a margem de erro do canal é de $\varepsilon = 1/40 = 2,5\%$, segue que:

$$|K(\overline{x^n}, y^n) - E[K(X^n, Y^n)]| < \varepsilon E[K(X^n, Y^n)] \tag{8.4}$$

$$(1-\varepsilon)E[K] < K < (1+\varepsilon)E[K] \tag{8.5}$$

$$1.817.531 < K < 1.910.739 \tag{8.6}$$

com probabilidade de pelo menos $1 - \varphi = 1 - 2e^{-(n-1)[\varepsilon\rho\beta - \ln(1+\varepsilon\rho)]} = 1 - 2e^{-52,341} \to 1$.

Portanto, durante a fase de abertura, Bob espera que a distância entre a sequência $\overline{x^n}$ enviada por Alice e a sequência y^n recebida através do canal PRNC esteja dentro do intervalo obtido acima para K. Além disso, Bob também confere se a informação vestigial que recebeu de Alice na fase de comprometimento do protocolo proposto equivale ao valor da função de hash 2-universal computada sobre a sequência recebida de Alice, ou seja, se $\mathsf{hash} = f(\overline{x^n})$.

Para se obter ω, o tamanho da função de hash 2-universal $f(\cdot)$ que Bob amostra e envia para Alice, precisamos determinar o valor do limiar τ. Observe que o limiar depende apenas dos parâmetros do canal:

$$\tau = \left(\frac{2\varepsilon}{1-2(1+\delta)p}\right)\left(\frac{\rho}{1-\rho}\right)(n-1) \tag{8.7}$$

onde $p = \rho/(1+\rho)$ é a probabilidade de ocorrer uma inversão de ordem-1 na saída do canal.

Daqui em diante será conveniente definir a seguinte variável:

$$\Delta \stackrel{def}{=} \frac{\tau}{n-1} = \left(\frac{2\varepsilon}{1-2(1+\delta)p}\right)\left(\frac{\rho}{1-\rho}\right) \tag{8.8}$$

$$\therefore \Delta = 0,006918238994 \tag{8.9}$$

Vamos fixar o parâmetro de segurança $s = 64$ bits. Logo, o tamanho da saída da função de hash calculada por Alice como forma de evidência para Bob deve ser:

$$\begin{aligned}
\omega &= 2(n-1+\tau)\mathsf{H}_b\left(\frac{\tau}{n-1+\tau}\right) + s && (8.10)\\
&= 2(n-1)\left[(1+\Delta)\mathsf{H}_b\left(\frac{1}{1+\Delta}\right)\right] + s && (8.11)\\
&= 2(n-1)\left[(1+\Delta)\log(1+\Delta) - \Delta\log\Delta\right] + s && (8.12)\\
&= 2.001.799\ \textit{bits} && (8.13)
\end{aligned}$$

A probabilidade de que exista uma colisão entre duas sequências para uma função de hash 2-universal com o tamanho obtido acima é no máximo 2^{-64}, mesmo valor para a distância estatística na visão de Bob entre o extrator utilizado por Alice para cifrar seu comprometimento e uma sequência aleatória com distribuição uniforme. Ou seja, Alice consegue trapacear com probabilidade limitada superiormente por:

$$\begin{aligned}
\theta &= e^{-(n-1)\rho\varepsilon^2\beta^2/2} + e^{-(n-1)\frac{\delta^2}{2+\delta}\frac{\rho}{1+\rho}\Delta} + 2^{-s} && (8.14)\\
&= e^{-524,287954861111} + e^{-35,172358490566} + 2^{-64} && (8.15)\\
&= 5,31\cdot 10^{-16} && (8.16)
\end{aligned}$$

Portanto, o tamanho máximo em *bits* da sequência que Alice poderá se comprometer de forma segura no protocolo é dado por:

$$\begin{aligned}
m &= n\log\left(\frac{1}{1-\rho}\right) - 2(n-1+\tau)\mathsf{H}_b\left(\frac{\tau}{n-1+\tau}\right) - \frac{2\rho(1+\rho)}{(1-\rho)} - 4s + 2 && (8.17)\\
&= (n-1)\left\{\log\left(\frac{1}{1-\rho}\right) - 2\left[(1+\Delta)\log(1+\Delta) - \Delta\log\Delta\right]\right\}\\
&\quad + \log\left(\frac{1}{1-\rho}\right) - \frac{2\rho(1+\rho)}{(1-\rho)} - 4s + 2 && (8.18)\\
&\therefore m = 548.200\ \textit{bits} && (8.19)
\end{aligned}$$

Há ainda que se levar em conta as computações locais, principalmente de aleatoriedade para a amostragem das funções de hash 2-universal utilizadas na computação da evidência para Bob e do comprometimento de Alice. Produzir essa quantidade de aleatoriedade não é trivial. Contudo, há viabilidade prática nessa área. Há resultados na literatura [107, 108] tratando desse tema que, contudo, excede o escopo deste trabalho.

8.2 Análise de sensibilidade dos parâmetros do canal

Nos cálculos efetuados na seção anterior, a parte relevante na obtenção do tamanho do comprometimento de Alice está destacada na expressão entre colchetes na computação de m. É necessário que a referida expressão seja positiva para que haja comprometimento útil. Assim sendo:

$$\log\left(\frac{1}{1-\rho}\right) - 2\left[(1+\Delta)\log(1+\Delta) - \Delta\log\Delta\right] > 0 \tag{8.20}$$

Observe que Δ é uma função de ρ, ε e δ. Logo, fixado o valor do parâmetro característico do canal ρ, gostaríamos de saber para quais valores de ε e δ é possível estabelecer o comprometimento. Visto que a margem de erro do canal ε tende a ser o parâmetro mais sensível na análise, já que uma margem muito dilatada torna inviável o teste feito por Bob para detectar a tentativa de trapaça de Alice, faremos nossa análise de sensibilidade sobre esse parâmetro. Iremos realizá-la, contudo, para uma faixa de valores de δ, a fim de evidenciar a sua elasticidade. O primeiro passo para realizarmos essa análise é perceber que a variável Δ é diretamente proporcional a ε. Ou seja, podemos reescrevê-la como sendo $\Delta = z_\delta(\rho)\cdot\varepsilon$, tal que:

$$z_\delta(\rho) = \frac{2\rho(1+\rho)}{[1-\rho(1+2\delta)](1-\rho)} \tag{8.21}$$

Determinaremos a sensibilidade do parâmetro ε da margem de erro do canal PRNC considerando uma faixa entre valores mínimo e máximo do parâmetro de margem de erro das colisões entre inversões. Assim, quando $\delta = 0$ e $\delta = 1/2$ temos:

$$z_0(\rho) = \frac{2\rho(1+\rho)}{(1-\rho)^2} \tag{8.22}$$

$$z_{1/2}(\rho) = \frac{2\rho(1+\rho)}{(1-2\rho)(1-\rho)} \tag{8.23}$$

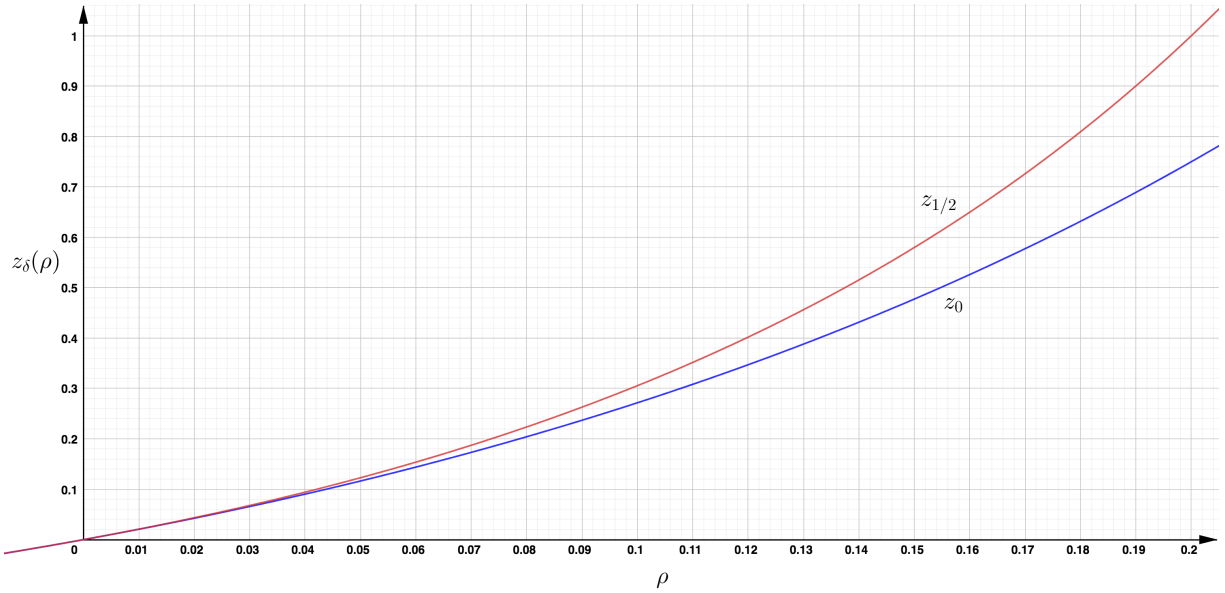

Figura 8.5: Comportamento das funções $z_0(\rho)$ e $z_{1/2}(\rho)$

O gráfico ilustrado na figura 8.5 acima mostra o comportamento das funções em (8.22) e (8.23) quando o parâmetro característico do canal varia no intervalo de $0 \leq \rho \leq 0,2$.

A tabela a seguir contém os valores calculados para as funções $z_\delta(\rho)$ e demais parâmetros estabelecidos acima na faixa de $0 < \rho \leq 0,2$ com variações de $0,005$. Esses dados permitem concluir que o comportamento dos parâmetros ε_{max_0} e $\varepsilon_{max_{1/2}}$, supremo do parâmetro da margem de erro do canal para os casos onde $\delta = 0$ e $\delta = 1/2$, respectivamente, é relativamente constante para toda a faixa útil de ρ. Além disso, é possível constatar que δ tem restrita influência sobre o valor máximo da margem de erro, sendo ε mais sensível a δ quanto maior o valor do parâmetro ρ.

Tabela 8.1: Cálculo de valores dos parâmetros do canal PRNC

ρ	$z_0(\rho)$	$z_{1/2}(\rho)$	$\varepsilon_{\max(\delta=0)}$	$\varepsilon_{\max(\delta=1/2)}$	Δ	$\frac{1}{2}\log_2\left(\frac{1}{1-\rho}\right)$
0,001	0,002006010014	0,002008020044	0,022674327606	0,022651630581	0,000045484928	0,000721708435
0,005	0,010151258807	0,010202527790	0,026809024068	0,026674305361	0,000272145342	0,003615784616
0,010	0,020610141822	0,020820449392	0,028940864590	0,028648532620	0,000596475324	0,007249784848
0,015	0,031384472674	0,031869799571	0,030248100211	0,029787469244	0,000949320675	0,010902185159
0,020	0,042482299042	0,043367346939	0,031173734630	0,030537535950	0,001324331917	0,014573172830
0,025	0,053911900066	0,055330634278	0,031871522875	0,031054304339	0,001718254356	0,018262938013
0,030	0,065681794027	0,067778021496	0,032415119300	0,031412589840	0,002129083189	0,021971673794
0,035	0,077800746329	0,080728731406	0,032846190976	0,031654878351	0,002555458172	0,025699576253
0,040	0,090277777778	0,094202898551	0,033190889710	0,031800388829	0,002996399765	0,029446844527
0,045	0,103122173186	0,108221621311	0,033466847964	0,031889876070	0,003451174092	0,033213680869
0,050	0,116343490305	0,122807017544	0,033686595372	0,031913616898	0,003919216082	0,037000290722
0,055	0,129951569105	0,137982284050	0,033859400703	0,031888747752	0,004400082250	0,040806882777
0,060	0,143956541421	0,153771760155	0,033992342710	0,031822618693	0,004893420091	0,044633669049
0,065	0,158368840973	0,170200995759	0,034090968308	0,031721007944	0,005398947139	0,048480864944
0,070	0,173199213782	0,187296824206	0,034159718026	0,031588556458	0,005916436305	0,052348689333
0,075	0,188458728999	0,205087440382	0,034202210892	0,031429058657	0,006445705194	0,056237364629
0,080	0,204158790170	0,223602484472	0,034221441727	0,031245664186	0,006986608141	0,060147116859
0,085	0,220311146944	0,242873131872	0,034219921666	0,031041021840	0,007539030191	0,064078175745
0,090	0,236927907258	0,262932189761	0,034199780420	0,030817384555	0,008102882404	0,068030774788
0,095	0,254021550014	0,283814200941	0,034162842477	0,030576687742	0,008678098199	0,072005151346
0,100	0,271604938272	0,305555555556	0,034110684697	0,030320608618	0,009264630412	0,076001546723
0,105	0,289691332980	0,328194611414	0,034044680775	0,030050612080	0,009862448954	0,080020206255
0,110	0,308294407272	0,351771823682	0,033966035813	0,029767986444	0,010471538878	0,084061379404
0,115	0,327428261355	0,376329884804	0,033875813817	0,029473871908	0,011091898820	0,088125319846
0,120	0,347107438017	0,401913875598	0,033774959547	0,029169283244	0,011723539677	0,092212285569
0,125	0,367346938776	0,428571428571	0,033664316297	0,028855128255	0,012366483538	0,096322538971
0,130	0,388162240719	0,456352904629	0,033544640383	0,028532222855	0,013020762775	0,100456346963
0,135	0,409569314043	0,485311584448	0,033416612963	0,028201303425	0,013686419249	0,104613981069
0,140	0,431584640346	0,515503875969	0,033280850104	0,027863037292	0,014363503723	0,108795717536
0,145	0,454225231695	0,546989539577	0,033137910942	0,027518031309	0,015052075276	0,113001837444
0,150	0,477508650519	0,579831932773	0,032988304628	0,027166839103	0,015752200826	0,117232626819
0,155	0,501453030356	0,614098276306	0,032832496350	0,026809967434	0,016463954789	0,121488376746
0,160	0,526077097506	0,649859943978	0,032670912270	0,026447881500	0,017187418700	0,125769383498
0,165	0,551400193625	0,687192778622	0,032503943899	0,026081008877	0,017922680960	0,130075948650
0,170	0,577442299318	0,726177437021	0,032331951801	0,025709744805	0,018669836589	0,134408379214
0,175	0,604224058770	0,766899766900	0,032155268826	0,025334454226	0,019428987041	0,138766987764
0,180	0,631766805473	0,809451219512	0,031974202894	0,024955475500	0,020200240020	0,143152092578
0,185	0,660092589108	0,853929301782	0,031789039451	0,024573122520	0,020983709356	0,147564017772
0,190	0,689224203627	0,900438072481	0,031600043637	0,024187687700	0,021779514910	0,152003093445
0,195	0,719185216620	0,949088687506	0,031407462189	0,023799443398	0,022587782498	0,156469655830
0,200	0,750000000000	1,000000000000	0,031211525016	0,023408643750	0,023408643762	0,160964047444

Para uma melhor visualização do comportamento dos parâmetros ε_{max_0} e $\varepsilon_{max_{1/2}}$ em relação ao parâmetro ρ, plotamos o gráfico a seguir:

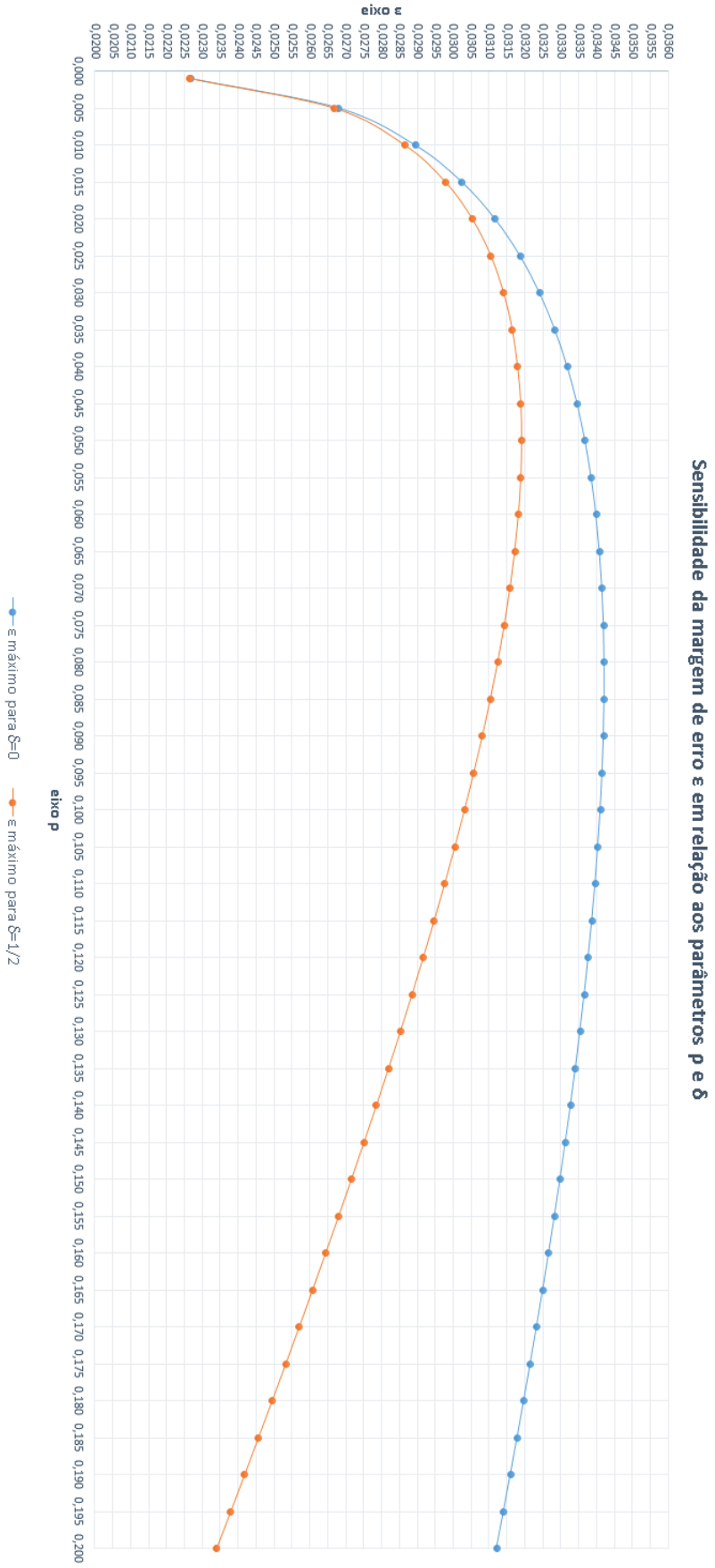

Figura 8.6: Gráfico de sensibilidade da margem de erro ε em relação aos parâmetros ρ e δ.

Realizamos os cálculos dos parâmetros com o objetivo de avaliar para quais valores o protocolo funciona efetivamente. Esse estudo fornece uma visão mais clara sobre os requisitos para se implementar na prática o protocolo de BC. É possível observar que a escolha dos valores para os parâmetros do canal é realística e há uma faixa de valores para cada parâmetro do canal PRNC para a qual o protocolo funciona com segurança demonstrada. O interessante é perceber que a margem de erro do canal fica limitada superiormente por valores que jamais excedem os $3,5\%$. Essa é uma característica intrínseca do protocolo proposto que pode limitar a viabilidade da implementação em alguns casos reais.

Observa-se que a escolha da margem de erro ε do canal PRNC em $2,5\%$ é adequada para praticamente toda a faixa de operação do parâmetro característico ρ. Por outro lado, observa-se que o tamanho de n não influencia nessa escolha, sendo imperativo que o canal possua uma margem de erro relativamente pequena para o funcionamento adequado do protocolo em um caso prático. De toda forma, estudos sugerem [104, 105, 106, 109, 110, 111] que esse é o caso em muitos canais reais, para uma vasta quantidade de situações consideradas.

Por fim, o estudo de caso realizado é apenas uma sinalização da viabilidade de uma implementação em *software* do protocolo proposto, considerados valores factíveis para os parâmetros de um canal PRNC emulado por meio da Internet. Para situações reais, há complicações não endereçadas no presente modelo que carecem de mais análise, pesquisa e desenvolvimento. Um exemplo de complicação é quando alguns pacotes não chegam ao destinatário, efeito comum em transmissões se utilizando segmentos UDP.

Capítulo 9

Conclusão e Trabalhos Futuros

Neste trabalho apresentamos uma nova formalização para canais com ruído do tipo reordenamento de pacotes, um efeito típico em canais de comunicação de comutação de pacotes, a exemplo da Internet. Apresentamos uma nova definição com rigor matemático para o canal PRNC, a qual facilita a obtenção das medidas estatísticas e entrópicas do canal. Introduzimos o primeiro protocolo de comprometimento incondicionalmente seguro para ambos os participantes baseado no canal PRNC, sem depender de forma alguma de hipóteses sobre dificuldade computacional baseadas em conjecturas matemáticas não comprovadas.

Outra contribuição deste trabalho está na construção de um protocolo de comprometimento de "*string*", sendo assim eficiente, pois a razão entre o tamanho do comprometimento v de Alice e a quantidade de pacotes que necessitam trafegar pelo canal para implementar o protocolo não tende assintoticamento a zero. Contudo, ainda não está formalmente definido para canais PRNC o conceito de Capacidade de Comprometimento, não sendo possível tratar sobre a questão de otimalidade do protocolo em termos de Capacidade, sendo essa uma linha de pesquisa futura relevante para a literatura da área.

A matriz de probabilidades do canal foi baseada apenas no resultado obtido em sua saída, para uma dada entrada, assim como é feito usualmente na maioria dos modelos de canais em teoria da informação, mas diferente da modelagem existente para esse tipo de canal no trabalho de Palmieri e Pereira [34]. Além disso, a construção do protocolo é concisa, realizando o menor número possível de interações entre as partes para sua execução.

O protocolo de comprometimento apresentado é resistente às ameaças de um comportamento mais geral de um participante trapaceiro, modelo tratado na literatura como seguro contra adversários maliciosos. Apresentamos, também, uma implementação direta do protocolo de comprometimento, sem utilizar reduções caixa preta baseadas na primitiva de OT. A redução por meio de OT é geralmente ineficiente, o que torna sempre preferível uma implementação direta.

O protocolo proposto apresenta como limitação uma restrição na faixa de valores que o parâmetro característico do canal ρ pode assumir, a fim de se obter a prova de segurança do protocolo. Essa limitação imposta, $0 < \rho < 1/(5 + 8\varepsilon)$, tem como finalidade garantir que a escolha feita por Alice da melhor estratégia para tentar trapacear será detectada por Bob em qualquer situação.

Tecnicamente, a restrição garante uma análise matemática baseada em eventos com probabilidade independente e identicamente distribuída.

É um problema em aberto demonstrar que o protocolo é incondicionalmente seguro para ambos os participantes para todo $0 < \rho < 1$, embora já tenha sido demonstrado nesta tese o seu funcionamento para $0 < \rho < 1$ quando os participantes são honestos. Essa extensão demanda um ferramental matemático mais robusto, a fim de possibilitar a demonstração de que eventos com um determinado tipo de dependendência estatística ainda permanencem concentrados em torno do valor esperado em casos assintóticos.

Outro ponto a ser atacado em trabalhos futuros é a possibilidade de o adversário ter controle parcial dos parâmetros do canal, em um modelo conhecido na literatura como *Unfair Noisy Channels* [42]. Isso implica na possibilidade de o adversário ter um controle limitado sobre o ruído do canal, de forma que tenha conhecimento exato do valor do parâmetro característico do canal ρ, enquanto a outra parte tem conhecimento apenas de uma faixa de valores dentre os quais ρ pode estar. Ou seja, a parte honesta sabe apenas que a quantidade de permutações está em uma faixa de probabilidade, enquanto o adversário tem noção mais precisa do nível de ruído do canal a cada utilização. Esse cenário é mais realista e torna de grande interesse o protocolo, devido ao apelo prático. É também um desafio em aberto e interessante definir e calcular a Capacidade de Comprometimento para um canal *unfair* com ruído do tipo reordenamento de pacotes.

Há várias possibilidades de trabalhos futuros que seguem desta tese. A possibilidade de implementação do protocolo de OT incondicionalmente seguro contra adversários maliciosos de forma direta baseado no canal PRNC é mais interessante do que as propostas em [33, 34], por não fazer uso de compiladores para construção da prova de segurança contra adversários maliciosos, sendo ainda mais eficiente em geral.

A construção de um protocolo de acordo de chave secreta incondicionalmente seguro com base em canais com ruído de reordenamento de pacotes talvez seja o caso de maior interesse dentre as possíveis continuações da presente tese. Isso porque esse tipo de protocolo é usado em casos reais para a implementação de canais seguros na Internet. Na atualidade, virtualmente todas as implementações de canais seguros comerciais são feitas com base em protocolos com segurança computacional, como o RSA e curvas elípticas.

Embora a parte de autenticação dificilmente se dará de forma distinta, vislumbra-se a possibilidade de se implementar em software protocolos de estabelecimento de chave secreta incondicionalmente seguros para geração de chaves a serem utilizadas em cifras de bloco e de fluxo para estabelecimento da chave de sessão, ao invés do procedimento atual. Ainda nesse contexto, estabelecer as Capacidades de Sigilo e de Chave Secreta de um canal PRNC seria de grande interesse teórico, tanto no caso padrão quanto para o caso de canais *unfair*.

Implementações em software das primitivas de BC e OT baseadas no canal PRNC também são uma interessante frente de trabalhos futuros, visto a escassez de trabalhos na literatura nesse sentido, muito provavelmente devido a ineficiência da maioria dos protocolos teóricos existentes na área de segurança incondicional com base em canais ruidosos. Uma implementação eficiente seria capaz de confirmar experimentalmente o apelo prático que apresentam.

Uma linha de pesquisa importante em criptografia é sobre composabilidade universal (*Universal Composability - UC*). Essa frente trata sobre a segurança de protocolos criptográficos construídos a partir da composição ou combinação de diversos outros protocolos ou primitivas, seja de modo sequencial ou não. Demonstrar a segurança sequencial e UC do nosso protocolo, além de estabelecer uma funcionalidade ideal e demais conceitos relacionados apresentam apelo teórico relevante para a pesquisa na área.

Caso fôssemos estabelecer uma ordem de prioridade no desenvolvimento de uma aplicação que implemente uma das primitivas supracitadas, o protocolo mais interessante para se implementar primeiro seria o acordo de chave secreta, já que esse é um problema sensível em criptografia e apenas protocolos computacionalmente seguros estão disponíveis no mercado. Levando-se em conta os recentes incidentes de segurança noticiados em todo o mundo envolvendo governos e grandes corporações, a existência de um novo protocolo com segurança incondicional e eficiente nessa área é extremamente desejável.

Por fim, a maior relevância em se aprofundar na discussão de protocolos incondicionalmente seguros e eficientes, a ponto de serem passíveis de implementação, talvez esteja nos rápidos avanços do poder computacional disponível, seja por meio de processamento mundialmente distribuído, seja pelo desenvolvimento de computadores quânticos. Todos esses avanços ameaçam gravemente as principais soluções criptográficas em uso atualmente. Contar com protocolos criptográficos cuja segurança não dependa do poder computacional disponível certamente alçará a segurança cibernética global a outro patamar de robustez.

Referências Bibliográficas

[1] SINGH, S. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. [S.l.]: Anchor Books, a division of Random House, Inc., 1999. ISBN 0-385-49532-3.

[2] BROEMELING, L. D. An account of early statistical inference in arab cryptology. *The American Statistician*, Taylor & Francis, v. 65, n. 4, p. 255–257, 2011.

[3] COPELAND, B. J. *Turing: Pioneer of the Information Age*. [S.l.]: Oxford University Press, 2012.

[4] COHEN, F. B. *A Short History of Cryptography*. http://all.net/edu/curr/ip/Chap2-1.html: [s.n.], 1995.

[5] SHANNON, C. E. Communication theory of secrecy systems. *Bell System Technical Journal*, v. 28, n. 4, p. 656–715, oct 1949. ISSN 0005-8580. A footnote on the initial page says: "The material in this paper appeared in a confidential report, 'A Mathematical Theory of Cryptography', dated Sept. 1, 1945 , which has now been declassified.". Disponível em: <http://bstj.bell-labs.com/BSTJ/images/Vol28/bstj28-4-656.pdf>.

[6] BLOCH, M.; BARROS, J. *Physical-Layer Security: From Information Theory to Security Engineering*. [S.l.]: Cambridge University Press, 2011.

[7] SHOR, P. W. Algorithms for quantum computation: Discrete logarithms and factoring. In: *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*. USA: IEEE Computer Society, 1994. (SFCS '94), p. 124–134. ISBN 0818665807. Disponível em: <https://doi.org/10.1109/SFCS.1994.365700>.

[8] DIFFIE, W.; HELLMAN, M. New directions in cryptography. *Information Theory, IEEE Transactions on*, v. 22, n. 6, p. 644–654, Nov 1976. ISSN 0018-9448.

[9] RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, ACM, New York, NY, USA, v. 21, n. 2, p. 120–126, fev. 1978. ISSN 0001-0782. Disponível em: <http://doi.acm.org/10.1145/359340.359342>.

[10] GOLDWASSER, S.; MICALI, S. Probabilistic encryption and how to play mental poker keeping secret all partial information. In: LEWIS, H. R. et al. (Ed.). *Proceedings of the 14th Annual ACM Symposium on Theory of Computing, May 5-7, 1982, San*

Francisco, California, USA. ACM, 1982. p. 365–377. ISBN 0-89791-067-2. Disponível em: <https://doi.org/10.1145/800070.802212>.

[11] SAWER, P. *The unsung genius who secured Britain's computer defences and paved the way for safe online shopping*. Mar 2016. Disponível em: <https://www.telegraph.co.uk/history/12191473/The-unsung-genius-who-secured-Britains-computer-defences-and-paved-the-way-for-safe-online-shopping.html>.

[12] WYNER, A. D. The Wire-tap Channel. *Bell Systems Technical Journal*, v. 54, n. 8, p. 1355–1387, jan. 1975.

[13] CSISZAR, I.; KORNER, J. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theor.*, IEEE Press, Piscataway, NJ, USA, v. 24, n. 3, p. 339–348, set. 2006. ISSN 0018-9448. Disponível em: <http://dx.doi.org/10.1109/TIT.1978.1055892>.

[14] MAURER, U. M. Perfect cryptographic security from partially independent channels. In: *Proc. 23rd ACM Symposium on Theory of Computing*. [S.l.: s.n.], 1991. p. 561–571.

[15] YAO, A. C. Protocols for secure computations. In: *Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science*. Washington, DC, USA: IEEE Computer Society, 1982. p. 160–164.

[16] YAO, A. C.-C. How to generate and exchange secrets. In: *Proceedings of the 27th Annual Symposium on Foundations of Computer Science*. Washington, DC, USA: IEEE Computer Society, 1986. (SFCS '86), p. 162–167. ISBN 0-8186-0740-8. Disponível em: <http://dx.doi.org/10.1109/SFCS.1986.25>.

[17] GOLDREICH, O.; MICALI, S.; WIGDERSON, A. How to play any mental game. In: *STOC '87: Proceedings of the nineteenth annual ACM symposium on Theory of computing*. New York, NY, USA: ACM, 1987. p. 218–229. ISBN 0-89791-221-7.

[18] MAYERS, D. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.*, American Physical Society, v. 78, p. 3414–3417, Apr 1997. Disponível em: <https://link.aps.org/doi/10.1103/PhysRevLett.78.3414>.

[19] LO, H.-K.; CHAU, H. F. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Phys. D*, Elsevier Science Publishers B. V., NLD, v. 120, n. 1–2, p. 177–187, set. 1998. ISSN 0167-2789. Disponível em: <https://doi.org/10.1016/S0167-2789(98)00053-0>.

[20] CRÉPEAU, C.; KILIAN, J. Achieving oblivious transfer using weakened security assumptions (extended abstract). In: *FOCS*. [S.l.]: IEEE, 1988. p. 42–52.

[21] LEUNG-YAN-CHEONG, S.; HELLMAN, M. The gaussian wire-tap channel. *Information Theory, IEEE Transactions on*, v. 24, n. 4, p. 451–456, Jul 1978. ISSN 0018-9448.

[22] OZAROW, L. H.; WYNER, A. D. Wire-tap channel ii. In: *Proc. Of the EUROCRYPT 84 Workshop on Advances in Cryptology: Theory and Application of Cryptographic Techniques*.

New York, NY, USA: Springer-Verlag New York, Inc., 1985. p. 33–51. ISBN 0-387-16076-0. Disponível em: <http://dl.acm.org/citation.cfm?id=20177.20182>.

[23] MAURER, U. M. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, v. 39, n. 3, p. 733–742, 1993.

[24] SUBRAMANIAN, A. et al. Strong secrecy on the binary erasure wiretap channel using large-girth ldpc codes. *Trans. Info. For. Sec.*, IEEE Press, Piscataway, NJ, USA, v. 6, n. 3, p. 585–594, set. 2011. ISSN 1556-6013. Disponível em: <http://dx.doi.org/10.1109/TIFS.2011.2148715>.

[25] THANGARAJ, A. et al. Applications of ldpc codes to the wiretap channel. *Information Theory, IEEE Transactions on*, v. 53, n. 8, p. 2933–2945, Aug 2007. ISSN 0018-9448.

[26] SUBRAMANIAN, A.; MCLAUGHLIN, S. W. Mds codes on the erasure-erasure wiretap channel. *CoRR*, abs/0902.3286, 2009.

[27] CHERAGHCHI, M.; DIDIER, F.; SHOKROLLAHI, A. Invertible extractors and wiretap protocols. *CoRR*, abs/0901.2120, 2009.

[28] WIESNER, S. Conjugate coding. *SIGACT News*, ACM, New York, NY, USA, v. 15, n. 1, p. 78–88, jan. 1983. ISSN 0163-5700. Disponível em: <http://doi.acm.org/10.1145/1008908.1008920>.

[29] RABIN, M. O. *How to Exchange Secrets with Oblivious Transfer*. East Lansing, Michigan, May 20 1981.

[30] EVEN, S.; GOLDREICH, O.; LEMPEL, A. A randomized protocol for signing contracts. *Commun. ACM*, ACM, New York, NY, USA, v. 28, n. 6, p. 637–647, jun. 1985. ISSN 0001-0782. Disponível em: <http://doi.acm.org/10.1145/3812.3818>.

[31] CRÉPEAU, C. Equivalence between two flavours of oblivious transfers. In: *A Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology*. London, UK, UK: Springer-Verlag, 1988. (CRYPTO '87), p. 350–354. ISBN 3-540-18796-0. Disponível em: <http://dl.acm.org/citation.cfm?id=646752.704744>.

[32] KILIAN, J. Founding cryptography on oblivious transfer. In: *STOC*. [S.l.]: ACM, 1988. p. 20–31.

[33] PALMIERI, P.; PEREIRA, O. Building oblivious transfer on channel delays. In: LAI, X.; YUNG, M.; LIN, D. (Ed.). *Information Security and Cryptology*. Springer Berlin Heidelberg, 2011, (Lecture Notes in Computer Science, v. 6584). p. 125–138. ISBN 978-3-642-21517-9. Disponível em: <http://dx.doi.org/10.1007/978-3-642-21518-6-10>.

[34] PALMIERI, P.; PEREIRA, O. Implementing information-theoretically secure oblivious transfer from packet reordering. In: KIM, H. (Ed.). *ICISC*. [S.l.]: Springer, 2011. (Lecture Notes in Computer Science, v. 7259), p. 332–345. ISBN 978-3-642-31911-2.

[35] BLUM, M. Coin flipping by telephone a protocol for solving impossible problems. *SIGACT News*, ACM, New York, NY, USA, v. 15, n. 4, p. 23–27, 1983.

[36] BRASSARD, G.; CHAUM, D.; CRéPEAU, C. Minimum disclosure proofs of knowledge. *J. Comput. Syst. Sci.*, Academic Press, Inc., Orlando, FL, USA, v. 37, n. 2, p. 156–189, 1988. ISSN 0022-0000.

[37] GOLDREICH, O.; MICALI, S.; WIGDERSON, A. Proofs that yield nothing but their validity and a methodology of cryptographic protocol design (extended abstract). In: *FOCS*. [S.l.]: IEEE, 1986. p. 174–187.

[38] DAMGÅRD, I.; PEDERSEN, T.; PFITZMANN, B. On the existence of statistically hiding bit commitment schemes and fail-stop signatures. *Journal of Cryptology*, v. 10, n. 3, p. 163–19, Jun 1997.

[39] CHAUM, D.; DAMGÅRD, I.; GRAAF, J. van de. Multiparty computations ensuring privacy of each party's input and correctness of the result. In: POMERANCE, C. (Ed.). *CRYPTO*. [S.l.]: Springer, 1987. (Lecture Notes in Computer Science, v. 293), p. 87–119. ISBN 3-540-18796-0.

[40] CHAUM, D.; CRÉPEAU, C.; DAMGARD, I. Multiparty unconditionally secure protocols. In: *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*. New York, NY, USA: ACM, 1988. (STOC '88), p. 11–19. ISBN 0-89791-264-0.

[41] DAMGÅRD, I. Commitment schemes and zero-knowledge protocols. In: *Lectures on Data Security, Modern Cryptology in Theory and Practice, Summer School, Aarhus, Denmark, July 1998*. London, UK: Springer-Verlag, 1999. p. 63–86. ISBN 3-540-65757-6.

[42] DAMGÅRD, I. B.; KILIAN, J.; SALVAIL, L. On the (im)possibility of basing oblivious transfer and bit commitment on weakened security assumptions. In: *Advances in Cryptology EUROCRYPT 99*. [S.l.]: Springer Berlin / Heidelberg, 1999. v. 1592, p. 56–73. ISBN 978-3-540-65889-4.

[43] KILIAN, J. A general completeness theorem for two-party games. In: KOUTSOUGERAS, C.; VITTER, J. S. (Ed.). *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, May 5-8, 1991, New Orleans, Louisiana, USA*. ACM, 1991. p. 553–560. ISBN 0-89791-397-3. Disponível em: <https://doi.org/10.1145/103418.103475>.

[44] NAOR, M. Bit commitment using pseudo-randomness. In: *CRYPTO '89: Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology*. London, UK: Springer-Verlag, 1990. p. 128–136. ISBN 3-540-97317-6.

[45] KENT, A. Unconditionally secure bit commitment. *Physical Review Letters*, APS, USA, v. 83, n. 7, p. 1447–1450, July 1998.

[46] CACHIN, C.; MAURER, U. M. Unconditional security against memory-bounded adversaries. In: JR., B. S. K. (Ed.). *CRYPTO*. [S.l.]: Springer, 1997. (Lecture Notes in Computer Science, v. 1294), p. 292–306. ISBN 3-540-63384-7.

[47] ALVES, V. M. *Protocolo de comprometimento de bit eficiente com segurança sequencial baseado no modelo de memória limitada*. Dissertação (Master Thesis) — Universidade de Brasília, Campus Anísio Teixeira, Asa Norte, Brasília-DF, feb 2010.

[48] SHIKATA, J.; YAMANAKA, D. Bit commitment in the bounded storage model: Tight bound and simple optimal construction. In: CHEN, L. (Ed.). *Cryptography and Coding*. [S.l.]: Springer Berlin Heidelberg, 2011, (Lecture Notes in Computer Science, v. 7089). p. 112–131. ISBN 978-3-642-25515-1.

[49] DOWSLEY, R.; LACERDA, F.; NASCIMENTO, A. C. A. Commitment and oblivious transfer in the bounded storage model with errors. *IEEE Transactions on Information Theory*, v. 64, n. 8, p. 5970–5984, Aug 2018. ISSN 0018-9448.

[50] GOYAL, V. et al. Interactive locking, zero-knowledge pcps, and unconditional cryptography. In: RABIN, T. (Ed.). *Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings*. [S.l.]: Springer, 2010. (Lecture Notes in Computer Science, v. 6223), p. 173–190.

[51] DÖTTLING, N.; KRASCHEWSKI, D.; MÜLLER-QUADE, J. Unconditional and composable security using a single stateful tamper-proof hardware token. In: ISHAI, Y. (Ed.). *Theory of Cryptography - 8th Theory of Cryptography Conference, TCC 2011, Providence, RI, USA, March 28-30, 2011. Proceedings*. [S.l.]: Springer, 2011. (Lecture Notes in Computer Science, v. 6597), p. 164–181.

[52] DOWSLEY, R.; MÜLLER-QUADE, J.; NILGES, T. Weakening the isolation assumption of tamper-proof hardware tokens. In: LEHMANN, A.; WOLF, S. (Ed.). *Information Theoretic Security - 8th International Conference, ICITS 2015, Lugano, Switzerland, May 2-5, 2015. Proceedings*. [S.l.]: Springer, 2015. (Lecture Notes in Computer Science, v. 9063), p. 197–213.

[53] WINKLER, S.; WULLSCHLEGER, J.; WOLF, S. Bit commitment from non-signaling correlations. *Information Theory, IEEE Transactions on*, v. 57, n. 3, p. 1770–1779, March 2011. ISSN 0018-9448.

[54] DOWSLEY, R.; MÜLLER-QUADE, J.; NASCIMENTO, A. C. A. On the possibility of universally composable commitments based on noisy channels. In: SANTOS, A. L. M. dos; BARCELLOS, M. P. (Ed.). *Anais do VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, SBSEG 2008*. Gramado, Brazil: Sociedade Brasileira de Computação (SBC), 2008. p. 103–114.

[55] DOWSLEY, R. et al. On the composability of statistically secure bit commitments. *Journal of Internet Technology*, v. 14, n. 3, p. 509–516, 2013.

[56] DOWSLEY, R.; MÜLLER-QUADE, J.; NASCIMENTO, A. C. A. On the composability of statistically secure random oblivious transfer. *Entropy*, v. 22, n. 1, p. 107, 2020.

[57] CRÉPEAU, C. Efficient cryptographic protocols based on noisy channels. In: *EUROCRYPT*. [S.l.: s.n.], 1997. p. 306–317.

[58] WULLSCHLEGER, J. Oblivious transfer from weak noisy channels. In: REINGOLD, O. (Ed.). *Theory of Cryptography, 6th Theory of Cryptography Conference, TCC 2009,*

San Francisco, CA, USA, March 15-17, 2009. Proceedings. Springer, 2009. (Lecture Notes in Computer Science, v. 5444), p. 332–349. ISBN 978-3-642-00456-8. Disponível em: <https://doi.org/10.1007/978-3-642-00457-5_20>.

[59] SHANNON, C. A mathematical theory of communication. *Bell System Technical Journal*, v. 27, p. 379–423, 623–656, July, October 1948. Disponível em: <http://cm.bell-labs.com/cm/ms/what/shannonday/shannon1948.pdf>.

[60] MAURER, U.; WOLF, S. Unconditionally secure key agreement and the intrinsic conditional information. *Information Theory, IEEE Transactions on*, v. 45, n. 2, p. 499–514, Mar 1999. ISSN 0018-9448.

[61] AHLSWEDE, R.; CSISZÁR, I. Common randomness in information theory and cryptography. i. secret sharing. *Information Theory, IEEE Transactions on*, v. 39, n. 4, p. 1121–1132, Jul 1993. ISSN 0018-9448.

[62] CSISZÁR, I.; NARAYAN, P. Secrecy capacities for multiple terminals. *Information Theory, IEEE Transactions on*, v. 50, n. 12, p. 3047–3061, Dec 2004. ISSN 0018-9448.

[63] CSISZÁR, I.; NARAYAN, P. Secrecy capacities for multiterminal channel models. *Information Theory, IEEE Transactions on*, v. 54, n. 6, p. 2437–2452, June 2008. ISSN 0018-9448.

[64] EKREM, E.; ULUKUS, S. The secrecy capacity region of the gaussian mimo multi-receiver wiretap channel. *Information Theory, IEEE Transactions on*, v. 57, n. 4, p. 2083–2114, April 2011. ISSN 0018-9448.

[65] OGGIER, F.; HASSIBI, B. The secrecy capacity of the mimo wiretap channel. *Information Theory, IEEE Transactions on*, v. 57, n. 8, p. 4961–4972, Aug 2011. ISSN 0018-9448.

[66] GOPALA, P. K.; LAI, L.; GAMAL, H. E. On the secrecy capacity of fading channels. *Information Theory, IEEE Transactions on*, v. 54, n. 10, p. 4687–4698, Oct 2008. ISSN 0018-9448.

[67] ARDESTANIZADEH, E. et al. Wiretap channel with secure rate-limited feedback. *Information Theory, IEEE Transactions on*, v. 55, n. 12, p. 5353–5361, Dec 2009. ISSN 0018-9448.

[68] NASCIMENTO, A. C. A.; WINTER, A. On the oblivious-transfer capacity of noisy resources. *IEEE Transactions on Information Theory*, v. 54, n. 6, p. 2572–2581, 2008.

[69] IMAI, H.; MOROZOV, K.; NASCIMENTO, A. C. On the oblivious transfer capacity of the erasure channel. In: IEEE. *Information Theory, 2006 IEEE International Symposium on*. [S.l.], 2006. p. 1428–1431.

[70] PINTO, A. C. B. et al. Achieving oblivious transfer capacity of generalized erasure channel in the malicious model. *IEEE Transactions on Information Theory*, v. 57, n. 8, p. 5566–71, 2011.

[71] DOWSLEY, R.; NASCIMENTO, A. C. A. On the oblivious transfer capacity of generalized erasure channels against malicious adversaries: The case of low erasure probability. *IEEE Transactions on Information Theory*, v. 63, n. 10, p. 6819–6826, Oct 2017. ISSN 0018-9448.

[72] WINTER, A.; NASCIMENTO, A. C. A.; IMAI, H. Commitment capacity of discrete memoryless channels. *CoRR*, cs.CR/0304014, 2003.

[73] NASCIMENTO, A. et al. The commitment capacity of the gaussian channel is infinite. *Information Theory, IEEE Transactions on*, v. 54, n. 6, p. 2785–2789, June 2008. ISSN 0018-9448.

[74] CRÉPEAU, C.; DOWSLEY, R.; NASCIMENTO, A. C. A. On the commitment capacity of unfair noisy channels. *IEEE Transactions on Information Theory*, v. 66, n. 6, p. 3745–3752, 2020.

[75] HAITNER, I. Semi-honest to malicious oblivious transfer - the black-box way. In: CANETTI, R. (Ed.). *TCC*. [S.l.]: Springer, 2008. (Lecture Notes in Computer Science, v. 4948), p. 412–426. ISBN 978-3-540-78523-1.

[76] ISHAI, Y. et al. Black-box constructions for secure computation. In: KLEINBERG, J. M. (Ed.). *STOC*. ACM, 2006. p. 99–108. ISBN 1-59593-134-1. Disponível em: <http://dblp.uni-trier.de/db/conf/stoc/stoc2006.html>.

[77] YAO, A. C.-C. Some complexity questions related to distributive computing(preliminary report). In: *Proceedings of the Eleventh Annual ACM Symposium on Theory of Computing*. New York, NY, USA: Association for Computing Machinery, 1979. (STOC '79), p. 209–213. ISBN 9781450374385. Disponível em: <https://doi.org/10.1145/800135.804414>.

[78] RENNER, R.; WOLF, S. Simple and tight bounds for information reconciliation and privacy amplification. In: ROY, B. K. (Ed.). *ASIACRYPT*. [S.l.]: Springer, 2005. (Lecture Notes in Computer Science, v. 3788), p. 199–216. ISBN 3-540-30684-6.

[79] CARTER, L.; WEGMAN, M. N. Universal classes of hash functions. *J. Comput. Syst. Sci.*, v. 18, n. 2, p. 143–154, 1979.

[80] DODIS, Y. et al. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM J. Comput.*, v. 38, n. 1, p. 97–139, 2008.

[81] BENNETT, C. H.; BRASSARD, G.; ROBERT, J.-M. Privacy amplification by public discussion. *SIAM J. Comput.*, Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, v. 17, p. 210–229, 1988.

[82] CHOR, B.; GOLDREICH, O. Unbiased bits from sources of weak randomness and probabilistic communication complexity. *SIAM J. Comput.*, Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, v. 17, n. 2, p. 230–261, 1988. ISSN 0097-5397.

[83] IMPAGLIAZZO, R.; LEVIN, L. A.; LUBY, M. Pseudo-random generation from one-way functions (extended abstracts). In: *STOC*. [S.l.]: ACM, 1989. p. 12–24.

[84] HÅSTAD, J. et al. A pseudorandom generator from any one-way function. *SIAM J. Comput.*, v. 28, n. 4, p. 1364–1396, 1999.

[85] BENNETT, C. H. et al. Generalized privacy amplification. *IEEE Transactions on Information Theory*, v. 41, n. 6, p. 1915–1923, 1995.

[86] CHUNG, K.-M.; VADHAN, S. P. Tight bounds for hashing block sources. In: GOEL, A. et al. (Ed.). *APPROX-RANDOM*. [S.l.]: Springer, 2008. (Lecture Notes in Computer Science, v. 5171), p. 357–370. ISBN 978-3-540-85362-6.

[87] TOMAMICHEL, M. et al. Leftover hashing against quantum side information. In: *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*. [S.l.: s.n.], 2010. p. 2703–2707.

[88] CACHIN, C.; CRÉPEAU, C.; MARCIL, J. Oblivious transfer with a memory-bounded receiver. In: *FOCS*. [S.l.: s.n.], 1998. p. 493–502.

[89] GUBNER, J. A. *Probability and Random Processes for Electrical and Computer Engineers*. USA: Cambridge University Press, 2006. ISBN 0521864704.

[90] NEYMAN, J.; PEARSON, E. S. 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*, v. 231, n. 694-706, p. 289–337, 1933. Disponível em: <http://rsta.royalsocietypublishing.org/content/231/694-706/289.short>.

[91] BLAHUT, R. E. Hypothesis testing and information theory. *Information Theory, IEEE Transactions on*, v. 20, n. 4, p. 405 – 417, July 1974. ISSN 0018-9448.

[92] FENG, J. et al. Packet reordering in high-speed networks and its impact on high-speed tcp variants. *Computer Communications*, v. 32, n. 1, p. 62–68, 2009. ISSN 0140-3664. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0140366408005100>.

[93] DENG, F.-G.; LONG, G. L. Controlled order rearrangement encryption for quantum key distribution. *Phys. Rev. A*, American Physical Society, v. 68, p. 042315, Oct 2003. Disponível em: <https://link.aps.org/doi/10.1103/PhysRevA.68.042315>.

[94] WANG, J.; ZHANG, Q.; TANG, C.-j. Quantum secure direct communication based on order rearrangement of single photons. *Physics Letters A*, Elsevier BV, v. 358, n. 4, p. 256–258, Oct 2006. ISSN 0375-9601. Disponível em: <http://dx.doi.org/10.1016/j.physleta.2006.05.035>.

[95] KENDALL, M. G. A new measure of rank correlation. *Biometrika*, Biometrika Trust, v. 30, n. 1/2, p. 81–93, 1938. ISSN 00063444. Disponível em: <http://www.jstor.org/stable/2332226>.

[96] KNUTH, D. *The Art of Computer Programming, Volume 3: Sorting and Searching*. Pearson Education, 1973. ISBN 9788131709832. Disponível em: <https://books.google.com.br/books?id=RlQqhEcLruUC>.

[97] JANJIĆ, M. A generating function for numbers of insets. *Journal of Integer Sequences*, v. 17, n. 14.9.7, p. 1–9, Sep 2014. ISSN 1530-7638.

[98] TREADWAY, J.; RAWLINGS, D. Bernoulli trials and mahonian statistics: A tale of two q's. *Mathematics Magazine*, Mathematical Association of America, v. 67, n. 5, p. 345–354, 1994. ISSN 0025570X, 19300980. Disponível em: <http://www.jstor.org/stable/2690993>.

[99] BABSON, E. Generalized permutation patterns and a classification of the mahonian statistics. *Sém. Lothar. Combin.*, v. 44, p. ?, 06 2000.

[100] CHAN, T. M.; PĂTRAŞCU, M. Counting inversions, offline orthogonal range counting, and related problems. In: *Proceedings of the Twenty-First Annual ACM-SIAM Symposium on Discrete Algorithms*. USA: Society for Industrial and Applied Mathematics, 2010. (SODA '10), p. 161–173. ISBN 9780898716986.

[101] RIVEST, R. L. *Unconditionally Secure Commitment and Oblivious Transfer Schemes Using Private Channels and a Trusted Initializer*. [S.l.], 1999.

[102] Wang, D.; Mazumdar, A.; Wornell, G. W. Compression in the space of permutations. *IEEE Transactions on Information Theory*, v. 61, n. 12, p. 6417–6431, 2015.

[103] NASCIMENTO, A. C. A. et al. Unconditionally secure homomorphic pre-distributed bit commitment and secure two-party computations. In: BOYD, C.; MAO, W. (Ed.). *Information Security, 6th International Conference, ISC 2003, Bristol, UK, October 1-3, 2003, Proceedings*. Springer, 2003. (Lecture Notes in Computer Science, v. 2851), p. 151–164. ISBN 3-540-20176-9. Disponível em: <https://doi.org/10.1007/10958513_12>.

[104] YE, B.; JAYASUMANA, A.; PIRATLA, N. On monitoring of end-to-end packet reordering over the internet. In: . [S.l.: s.n.], 2006. p. 3 – 3.

[105] Laghari, A. A.; He, H.; Channa, M. I. Measuring Effect of Packet Reordering on Quality of Experience (QoE) in Video Streaming. *3D Research*, v. 9, n. 3, p. 30, set. 2018.

[106] FUKUDA, Y.; NOBAYASHI, D.; IKENAGA, T. Performance evaluation of tcp variants with packet reordering. In: . Athens, Greece: Copyright (c) IARIA, 2018, 2018. (ICN 2018), p. 12–16. ISBN 978-1-61208-625-5. Disponível em: <`http://personales.upv.es/thinkmind/ICN/ICN_2018/icn_2018_1_30_30036.html`>.

[107] IVANCHYKHIN, D.; IGNATCHENKO, S.; LEMIRE, D. Regular and almost universal hashing: an efficient implementation. *Software: Practice and Experience*, Wiley, v. 47, n. 10, p. 1299–1323, Nov 2016. ISSN 0038-0644. Disponível em: <http://dx.doi.org/10.1002/spe.2461>.

[108] LEMIRE, D.; KASER, O. Strongly universal string hashing is fast. *The Computer Journal*, Oxford University Press (OUP), v. 57, n. 11, p. 1624–1638, Jul 2013. ISSN 1460-2067. Disponível em: <http://dx.doi.org/10.1093/comjnl/bxt070>.

[109] PAXSON, V. End-to-end internet packet dynamics. *IEEE/ACM Transactions on Networking*, v. 7, n. 3, p. 277–292, 1999.

[110] BELLARDO, J.; SAVAGE, S. Measuring packet reordering. 07 2003.

[111] BENNETT, J. C. R.; PARTRIDGE, C.; SHECTMAN, N. Packet reordering is not pathological network behavior. *IEEE/ACM Trans. Netw.*, IEEE Press, v. 7, n. 6, p. 789–798, dec 1999. ISSN 1063-6692. Disponível em: <https://doi.org/10.1109/90.811445>.