IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 1, 2021, accepted September 19, 2021, date of publication October 8, 2021, date of current version October 19, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3118959

Information-Theoretically Secure String Commitments Based on Packet Reordering Channels

VINICIUS DE MORAIS ALVES[1], RAFAEL DOWSLEY[2], RAFAEL TIMÓTEO DE SOUSA, JR.[1], (Senior Member, IEEE), AND ANDERSON C. A. NASCIMENTO[3]

[1]Electrical Engineering Department, National Science and Technology Institute on Cybersecurity, University of Brasília (UnB), Brasília 70910-900, Brazil
[2]Department of Software Systems and Cybersecurity, Faculty of Information Technology, Monash University, Clayton, VIC 3800, Australia
[3]School of Engineering and Technology, University of Washington Tacoma, Tacoma, WA 98402, USA

Corresponding author: Vinicius de Morais Alves (vinicius.alves@redes.unb.br)

This work is supported in part by CNPq - Brazilian National Research Council (Grants 312180/2019-5 PQ-2 and 465741/2014-2 INCT on Cybersecurity), in part by the Brazilian Ministry of the Economy (Grant DIPLA 005/2016 and Grant ENAP 083/2016), in part by the Administrative Council for Economic Defense (Grant CADE 08700.000047/2019-14), in part by the General Attorney of the Union (Grant AGU 697.935/2019), in part by the National Auditing Department of the Brazilian Health System SUS (Grant DENASUS 23106.118410/2020-85), and in part by the General Attorney's Office for the National Treasure (Grant PGFN 23106.148934/2019-67).

ABSTRACT Realizing fundamental cryptographic primitives with unconditional security is a central topic in information-theoretic cryptography. These primitives can be realized based on physical assumptions, such as the existence of noisy channels, an upper bound on the storage capacity, or the laws of quantum mechanics. Palmieri and Pereira [1] demonstrated that delays in communication channels can be used as a reasonable and effective assumption to obtain an unconditionally secure oblivious transfer protocol against honest-but-curious adversaries. While any oblivious transfer protocol secure against malicious adversaries can be used to implement commitment, the reduction does not work if the oblivious transfer protocol is only secure against honest-but-curious adversaries. Thus, the question of obtaining a secure commitment protocol based on channel delays is still open. In this paper, we provide a concrete protocol for implementing string commitments based on packet reordering – a consequence of channel delays in packet networks.

INDEX TERMS Commitment schemes, packet reordering, unconditional security.

I. INTRODUCTION

Commitment schemes were introduced by Blum [2] and are fundamental cryptographic primitives, being building blocks of several cryptographic applications (e.g. zero-knowledge proofs [3], [4] and multi-party computation [5]–[7]).

A commitment scheme consists of two phases, *commit* and *reveal*, performed by two parties, a sender (or committer) and a receiver. We will denote these parties henceforth by Alice and Bob, respectively. In the commit phase, Alice commits to a value v and sends an evidence of her commitment to Bob. This evidence should unveil no information to Bob about the original value v. This is the security guarantee for Alice, also known as hiding. In the reveal phase, Alice sends some extra information to Bob, such that he can determine the value that was concealed by the commitment. In order to prevent Alice's malicious behavior, Bob may accept or reject the disclosed value after verifying its consistency with the evidence that was previously received. The protocol should guarantee that Alice is not able to reveal two different values, v and $\overline{v}$, successfully. This is the security guarantee for Bob, also known as binding. Commitment schemes are the digital equivalent of a sealed envelope. Alice puts the value v inside the envelope in the commit phase. If the protocol is hiding, Bob should not be able to read the value before the opening phase. During the opening phase, Alice should be able to open at most one value (the binding property).

A. RELATED WORK

Computational and unconditional security are two security notions usually considered in cryptography. Computational security makes use of unproven intractability assumptions on the hardness of certain computational problems and imposes an upper bound on the computing power available to an adversary in order to guarantee the security. Unconditional (or information-theoretic) security, on the other hand, neither requires computational intractability assumptions nor

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Ming Chen.

imposes any bounds on the adversary's computing power, whether in processing time, memory space, or technology available. In many scenarios, particularly when long term secrecy is required, it is desirable to achieve unconditional security.

Secure commitment schemes are known to be impossible to achieve from scratch: as a consequence of the so-called *symmetry condition* on what the parties know about each other's data [8], assumptions are needed to obtain a secure commitment scheme. According to this condition, after the realization of a two-party protocol over a noiseless channel and without further assumptions, Alice is able to determine exactly what Bob knows about her input, and vice-versa. Such impossibility result is known to hold even when the parties have access to a quantum channel [9] and [10]. A common assumption used to overcome the symmetry condition (while achieving unconditional security) is the existence of noisy channels.

The seminal work of Wyner [11] demonstrated that noisy channels can be useful for cryptographic purposes by showing that these channels can be used as a resource for obtaining secret key agreement. Numerous subsequent works extended this line of research to cover other types of noisy channels, protocols and applications. Crépeau and Kilian [12] proposed the first commitment and oblivious transfer protocols based on noisy channels. Crépeau [13] proposed an efficient unconditionally secure bit commitment protocol based on a binary symmetric channel. Since then, other physical assumptions have been used to obtain unconditionally secure commitment schemes, such as bounded storage capacity [14]–[16], the existence of tamper-proof hardware tokens [17]–[19], non-signaling correlations [20] and the impossibility of superluminal communications [21]. The universal composability of statistically secure protocols based on noisy channels has been investigated [22]–[24].

Winter *et al.* [8] introduced the concept of commitment capacity. They characterised the optimal rate at which a discrete memoryless channel can be used for obtaining commitment, calculated as the maximum equivocation of the channel after removing trivial redundancy (even when unlimited authenticated bidirectional noiseless side communication is allowed). Nascimento *et al.* [25] proved that the commitment capacity of a Gaussian channel is infinite. Crépeau *et al.* obtained the commitment capacity of unfair noisy channels [26]. Several papers also studied the related notions of secrecy key capacity (e.g., [11], [27]–[35]) and of oblivious transfer capacity (e.g., [36]–[40]).

Palmieri and Pereira [41] proposed a new channel, the Binary Discrete-time Delaying Channel (BDDC), and used it to obtain an oblivious transfer protocol that is unconditionally secure against honest-but-curious adversaries (this kind of adversary tries to obtain unauthorized information, but strictly follows the protocol instructions; while a malicious adversary, on the other hand, can cheat in an arbitrary way). Later, Palmieri and Pereira [42] demonstrated the practicality of their assumption by providing an implementation of an oblivious transfer protocol based on IP networks. They also claimed [1] that a BDDC is related to a Packet Reordering Noisy Channel (PRNC). In this work, we build a new scheme motivated by the model proposed in [1] and show that the existence of a transmission reordering effect in communication channels can also be leveraged to break the symmetry condition and obtain unconditionally secure commitment schemes.

The permutation concept behind the PRNC model is a powerful tool for constructing cryptographic protocols and has been similarly used in the controlled order rearrangement technique in Quantum Key Distribution (QKD) [43] and Quantum Secure Direct Communication (QSDC) [44]. We notice that the channel performs the permutation of the packets in the PRNC model, but the players perform the permutation of the particles in the quantum protocols.

It is known that oblivious transfer protocols secure against malicious adversaries imply secure commitment schemes [45]. However, this result does not hold in the case of oblivious transfer protocols secure solely against honest-but-curious adversaries. Therefore, the known oblivious transfer protocols cannot be used to directly argue that commitment is possible based on the assumption that time-delaying channels exist. Moreover, Palmieri and Pereira [42] argue that their result can be reduced via black-box combiners and/or compilers to a malicious adversarial security model, based on results of Haitner [46] and Ishai *et al.* [47]. However, these results make use of a commitment primitive that is still not defined neither proposed based on this specific model/channel. Finally, direct constructions of commitment schemes are often much more efficient than protocols derived from oblivious transfer.

B. OUR CONTRIBUTIONS

In this work we propose a novel protocol that implements a commitment scheme based on a packet reordering noisy channel. Our scheme has attractive features:

- It is unconditionally binding and hiding and, consequently, does not rely on any unproven intractability assumption;
- It is the first commitment scheme based on the reordering effect;
- It is a direct construction that does not use oblivious transfer as a building block;
- It introduces a new formal definition of reordering noisy channels. This definition captures the behavior of packet networks and makes it easy to compute entropic measures and conditional probabilities associated with the channel.

C. ORGANIZATION

Section II briefly reviews some information-theoretic measures and results that are used in this work. In Section III, we introduce the new definition of a packet reordering noisy channel. Section IV formally defines the security model that we consider. In Section V, we present our protocol. Finally,

we prove the correctness and the security of the proposed protocol in Section VI.

II. PRELIMINARIES

A. NOTATION

We use calligraphic letters $\mathcal{X}, \mathcal{Y}, \ldots$ to denote the domain of random variables, upper case letters $X, Y, \ldots$ to denote random variables, lower case letters $x, y, \ldots$ to denote realizations of random variables, and bold upper case letters $\mathbf{X}, \mathbf{Y}, \ldots$ to denote sets. The cardinality of a set $\mathbf{X}$ is denoted by $|\mathbf{X}|$. We use the notation $x \leftarrow X$ to denote a realization x of the random variable X. We also use the notation $x \in_R \mathbf{X}$ to denote sampling an element x uniformly from a set $\mathbf{X}$. We write U_r for a random variable uniformly distributed over $\{0,1\}^r$.

Except where stated otherwise, we work with discrete random variables. For a random variable X over the arbitrary alphabet $\mathcal{X}$, we denote its probability mass function by $P_X : \mathcal{X} \to [0,1]$ with $\sum_{x\in\mathcal{X}} P_X(x) = 1$. For a joint probability mass function $P_{XY} : \mathcal{X} \times \mathcal{Y} \to [0,1]$, let $P_X(x) := \sum_{y\in\mathcal{Y}} P_{XY}(x,y)$ denote the marginal probability mass function and let $P_{X|Y}(x|y) := P_{XY}(x,y)/P_Y(y)$ denote the conditional probability mass function when $P_Y(y) \neq 0$. The statistical distance between two probability distributions P_X and P_Y over the same domain $\mathcal{V}$ is given by

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

B. ENTROPY AND EXTRACTORS

The logarithms used in this paper are taken to the base 2 unless stated otherwise. The entropy of a random variable X is denoted by $H(X)$, the entropy of a random variable X conditioned on a random variable Y by $H(X|Y)$, and the joint entropy of two random variables X and Y by $H(X;Y)$. We denote the binary entropy function by $\mathsf{H}_b(\cdot)$. For random variables $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$ with finite alphabets, the min-entropy and its conditional version are defined as

$$H_\infty(X) = \min_x \log(1/P_X(x))$$
$$H_\infty(X|Y) = \min_y H_\infty(X|Y=y)$$

and the max-entropy and its conditional version as

$$H_0(X) = \log|\{x \in \mathcal{X} | P_X(x) > 0\}|$$
$$H_0(X|Y) = \max_y H_0(X|Y=y).$$

Strong extractors are algorithms that can extract nearly uniform bits from a source of correlated and biased bits, using as input a short seed of uniformly distributed bits:

Definition 1 (Strong Extractor [48]): A probabilistic polynomial time function $\mathsf{Ext} : \{0,1\}^u \times \{0,1\}^r \to \{0,1\}^k$ which uses r bits of randomness is an efficient (u, m, k, ϵ)-*strong extractor* if for all probability distributions P_X over $\{0,1\}^u$ with $H_\infty(X) \geq m$, and for random variables R and K independently and uniformly distributed in $\{0,1\}^r$ and $\{0,1\}^k$, respectively, it holds that $\mathsf{SD}\left(P_{\mathsf{Ext}(X,R),R}; P_{K,R}\right) \leq \epsilon$.

In this work we use a hash function from a family of universal hash functions as a strong extractor. A family of universal hash functions [49] is defined as follows:

Definition 2 (Universal Hash Function [49]): A family $\mathcal{G}$ of hash functions $g : \mathcal{X} \to \mathcal{Y}$ is *2-universal* if, for any distinct $x_1, x_2 \in \mathcal{X}$, the probability that $g(x_1) = g(x_2)$ is at most $|\mathcal{Y}|^{-1}$ when g is chosen uniformly at random from $\mathcal{G}$.

We will use the same statement of the Leftover-Hash Lemma [48], [50]–[55] (also known as the Privacy-Amplification Lemma) as Dodis *et al.* [48], which follows from the result of Håstad *et al.* [51].

Lemma 1 ([48], [51]): Let $\mathcal{G}$ be a 2-universal class of hash functions $g : \{0,1\}^u \to \{0,1\}^k$. Then for G uniformly distributed in $\mathcal{G}$, a random variable X with alphabet $\{0,1\}^u$, and a random variable K uniformly distributed in $\{0,1\}^k$, we have that

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

In particular, it is a $(u, \delta n, k, \epsilon)$ − strong extractor when $k \leq \delta n - 2\log(\epsilon^{-1}) + 2$, where δn is the min-entropy of X.

We also use the following lemma by Cachin *et al.* [56]. It bounds the remaining uncertainty on a random variable X given that a realization of an arbitrary random variable Z is known.

Lemma 2 ([56]): Let X be a random variable with alphabet $\mathcal{X}$, let Z be an arbitrary random variable defined over $\mathcal{Z}$ and let $s > 0$. Then, with probability at least $1 - 2^{-s}$, Z takes on a value z for which

$$H_\infty(X|Z=z) \geq H_\infty(X) - \log|\mathcal{Z}| - s.$$

III. PACKET REORDERING NOISY CHANNELS - A NEW DEFINITION

This work considers a noisy channel that models the packet reordering effect that is so common on the Internet nowadays. The Packet Reordering Noisy Channel (PRNC), as we denote it, models the effect of packet forwarding in high-speed, complex networks, which causes delays and, consequently, permutations in the order that the packets are received [57]. This packet reordering happens due to a number of factors, such as the physical distance between the nodes, number of intermediate hops in the network, transmission medium quality, speed of point-to-point links, traffic and congestion level on the network, multipath routing, route fluttering, packet size, inter-packet spacing and retransmissions.

Palmieri and Pereira [41] proposed the first cryptographic protocol based on the effects of packet forwarding in a network, but they focused on the delays that the packets suffer. They defined the Binary Discrete-time Delaying Channel (BDDC) that captures the probability that a packet is delayed by a given discrete amount of time. In their model, each packet admitted into the channel at input time $t_i \in T$ is output once by the channel, with probability of being output at time $u_j \in U$ given by $P(u_j) = p^{j-i} - p^{j-i+1}$.

Delay channels and reordering channels are related but distinct as the different delays of the packets might or might

not be enough to cause a reordering of the packets. We argue that for practical purposes reordering channels are a more natural choice than delay channels as the reordering effect is easier to quantify and measure in the Internet than the delay. Our definition of PRNC is based solely on the probability of the channel outputting a permutation of packets given an arbitrary sequence of packets as input. This definition captures the behavior of packet networks and makes it easy to compute entropic measures associated with the channel.

Before presenting a formal definition, we will try to give an intuition behind the behavior of our proposed channel. We model the collective behavior of routers, communication delays and multiple routes by a black box channel containing an input queue and an output queue. The sender transmits an arbitrarily ordered sequence of n distinct packets through the packet reordering noisy channel, modeled by the random variable X^n, and the channel outputs to the receiver a permuted version of the original sequence, modeled by Y^n.

To do so, the channel receives the sequence of n packets sent by Alice, forming an input queue $x^n = [x_1, x_2, \ldots, x_n]$. The channel then generates the output permutation moving packets from the input to the output queue - packet reordering potentially happening in the process.

The packet x_1 is placed directly in the output queue without permutation with probability 1. Each one of the packets x_i, with $i \in [2, n]$, in the input queue is either placed just behind all the other packets already moved to the output queue, from x_1 to x_{i-1} (and no permutation happens), or may perform pairwise adjacent data packet transpositions (swaps) with them, landing in one of the possible $i-1$ positions.

Let each K_i, for all $i \in [1, n]$, be the random variable that represents the amount of swaps performed by each packet x_i when moved by the channel from the input to the output queue, where $0 \leq K_i \leq i-1$. Notice that the random variables $\{K_1, \ldots, K_n\}$ are independent but not identically distributed.

In more details, if the packet x_i is placed in the output queue behind all others, then $K_i = 0$ and x_i becomes the last packet in the output queue. If the packet x_i swaps with the last packet already in the queue, then $K_i = 1$ and x_i becomes the second to last packet in the output queue by now. If it swaps with the last two packets already in the output queue, then $K_i = 2$ and x_i becomes the third from last packet in the output queue, and so on.

The procedure above is repeated by the channel until every packet is moved from the input to the output queue. Finally, the permutation formed in the output queue is represented by $y^n = [y_1, y_2, \ldots, y_n]$, where for some bijective mapping f, $x_i = y_{f(i)}$ for every i.

Define $K = \sum_{i=1}^{n} K_i$, which is the random variable representing the total amount of pairwise adjacent transpositions performed by the channel to generate the output permutation. Such distance is known as the Kendall tau distance.

Definition 3 (Kendall Tau Distance): Let x^n be a sequence of n distinct elements and y^n be a sequence obtained by a permutation of the elements of x^n. The Kendall tau distance $K(x^n, y^n)$ between x^n and y^n is defined as the minimum number of transpositions of pairwise adjacent elements that are necessary to change x^n into y^n.

For any such sequences x^n and y^n of n elements, the Kendall tau distance between them is at least 0 and at most

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

For a given sequence x^n, the Mahonian number $M(n, k)$ represents the amount of permutations y^n such that $K(x^n, y^n) = k$. The Mahonian triangle is defined as follows:

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

The first rows of the Mahonian triangle[1] are

$$\begin{aligned} n = 1 &: \ 1 \\ n = 2 &: \ 1\ 1 \\ n = 3 &: \ 1\ 2\ 2\ 1 \\ n = 4 &: \ 1\ 3\ 5\ 6\ 5\ 3\ 1 \\ n = 5 &: \ 1\ 4\ 9\ 15\ 20\ 22\ 20\ 15\ 9\ 4\ 1 \end{aligned}$$

In the Mahonian triangle, the sum of the elements of the n-th row is $n!$. There is no simple, general formula for the terms, mainly in case when $k > n$. Janjić [58] presented a complex closed form.

Now, let $S_i(\rho)$ denote the geometric series

$$\begin{aligned} S_i(\rho) &= \sum_{j=0}^{i-1} \rho^j \\ &= \frac{1-\rho^i}{1-\rho}. \end{aligned}$$

The probability mass function of each random variable K_i will be defined using a constant parameter $0 < \rho < 1$ that characterizes the channel. In practice, it is observed that the probability $\Pr[K_i = k_i]$ decreases exponentially with the number k_i of pairwise adjacent transpositions performed when a new packet is inserted in the output queue. Normalizing to get a probability mass function, we set

$$\begin{aligned} \Pr[K_i = k_i] &= \frac{\rho^{k_i}}{\sum_{k_i=0}^{i-1} \rho^{k_i}} \\ &= \frac{\rho^{k_i}}{S_i(\rho)}. \end{aligned}$$

[1]Note that "triangle" is a misnomer, as the amount of elements by row grows quadratically, rather than linearly like in Pascal triangle.

The conditional probability of the channel outputting Y^n given the input X^n is just the intersection of the probabilities of each packet x_i being reordered, thus $\Pr[Y^n = y^n | X^n = x^n] = \Pr[K_1 = k_1 \wedge K_2 = k_2 \wedge \cdots \wedge K_n = k_n]$, where k_i for $i \in \{1, \ldots, n\}$ is the number of pairwise adjacent transpositions that happened when x_i was moved from the input to the output queue and $[y_1, \ldots, y_n]$ is the final output. Since the random variables K_i are independent, we can further develop this conditional probability as follows:

$$\begin{aligned}\Pr[Y^n = y^n | X^n = x^n] &= \Pr[K_1 = k_1 \wedge K_2 = k_2 \wedge \cdots \wedge K_n = k_n] \\ &= \prod_{i=1}^{n} \Pr[K_i = k_i] \\ &= \prod_{i=1}^{n} \frac{\rho^{k_i}}{S_i(\rho)} \\ &= \frac{\rho^{\sum_{i=1}^{n} k_i}}{\prod_{i=1}^{n} S_i(\rho)} \\ &= \frac{\rho^{k}}{\prod_{i=1}^{n} S_i(\rho)},\end{aligned}$$

where k is a realization of the random variable $K(X^n, Y^n)$. We will henceforth use the shorthand $\sigma_n(\rho)$ for denoting $\prod_{i=1}^{n} S_i(\rho)$. Note that

$$\begin{aligned}\sigma_n(\rho) &= \frac{(1-\rho)(1-\rho^2)\cdots(1-\rho^n)}{(1-\rho)^n} \\ &= \left(\frac{1}{1-\rho}\right)^n \cdot \prod_{i=1}^{n}(1-\rho^i) \\ &= \sum_{k=0}^{\infty} M(n,k)\rho^k \\ &= \sum_{k=0}^{n(n-1)/2} M(n,k)\rho^k,\end{aligned}$$

where the penultimate equation follows from the well-known generating function for the numbers $M(n, k)$ [59] and the last equation from the fact that for a fixed n, the numbers $M(n, k)$ are non-zero only for $0 \leq k \leq \mathsf{N}$.

We define the Packet Reordering Noisy Channel as follows:

Definition 4 (Packet Reordering Noisy Channel): Let $0 < \rho < 1$ be a fixed parameter of the channel. The Packet Reordering Noisy Channel (PRNC) takes as input a sequence $x^n = (x_1, x_2, \ldots, x_n)$ of n distinct data packets distributed according to a random variable $X^n = \{X_1, X_2, \ldots, X_n\}$ with arbitrary probability distribution and where the data packets have domain $\mathcal{X}_i = \{0, 1\}^{\ell}$. It outputs a sequence $y^n = (y_1, y_2, \ldots, y_n)$ such that there exists a bijective function $f : \{1, \ldots n\} \to \{1, \ldots n\}$ with $x_i = y_{f(i)}$ for all $i \in \{1, \ldots n\}$, and the conditional probability mass function of Y^n is given by

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

IV. SECURITY MODEL

A commitment scheme based on a packet reordering noisy channel consists of two phases: the Commit and Reveal phases. In the Commit phase packets x^n are transmitted from Alice to Bob through the packet reordering noisy channel, who gets y^n. Alice and Bob can also exchange messages through an authenticated bidirectional noiseless channel. We will denote all messages exchanged by t. At the end of this phase, Alice should be committed to a value v. If the Reveal phase takes place, Alice sends x^n and v to Bob. After receiving the disclosed information, he performs a test using the variables $\{x^n, y^n, t, v\}$ and accepts or rejects the value v based on this test.

Let X^n, Y^n, T, V be the random variables corresponding to the respective values described above. We assume that V is a uniformly random bit-string of length m. Moreover, let View_A and View_B be random variables representing all the values (and randomness) known by Alice and Bob, respectively, at the end of the Commit phase. Let R be a uniformly random bit-string of length m that is independent from the parties' views. Let $\mathsf{Test} : \{0,1\}^{n\cdot\ell} \times \{0,1\}^{n\cdot\ell} \times \mathcal{T} \times \{0,1\}^m \to \{\text{ACC}, \text{REJ}\}$ be a public test function used by Bob to verify the validity of the value that Alice tries to open in the Reveal phase. The security of a commitment scheme is defined as follows.

Definition 5: A commitment scheme based on a PRNC is $(\varphi, \kappa, \theta)$-secure if, and only if, the following conditions are satisfied:

- φ-Correctness: If Alice and Bob are honest, then any value $v \in \{0,1\}^m$ committed to and then revealed by Alice will be accepted with probability
$$\Pr[\mathsf{Test}(X^n, Y^n, T, v) = \text{ACC}] \geq 1 - \varphi.$$
- κ-Concealing: If Alice is honest, then the amount of information about v leaked to Bob in the Commit phase is bounded:
$$\mathsf{SD}\left(P_{V,\mathsf{View}_B}; P_{R,\mathsf{View}_B}\right) \leq \kappa.$$
- θ-Binding: If Bob is honest, then for any $\widetilde{v}, \overline{v} \in \{0,1\}^m$ such $\widetilde{v} \neq \overline{v}$, and for any strategy of (a potentially malicious) Alice for choosing X^n that is sent through the PRNC during the Commit phase, and any random variables $\widetilde{X^n}$, $\overline{X^n}$ that Alice potentially presents during the Reveal phase, we have that:
$$\begin{aligned}\Pr[\mathsf{Test}(\widetilde{X^n}, Y^n, T, \widetilde{v}) &= \text{ACC} \wedge \mathsf{Test}(\overline{X^n}, Y^n, T, \overline{v}) \\ &= \text{ACC}] \leq \theta.\end{aligned}$$

The probabilities are taken over the private randomness of Alice and Bob, and the channel. A commitment scheme is said to be unconditionally secure when φ, κ and θ are negligible functions of n and s, security parameters previously agreed upon by both parties.

Note that our definition of security implicitly assumes that the committed value is uniformly distributed. While this assumptions simplifies our definitions and security proofs,

it does not affect the generality of our results, since random commitments can always be transformed into commitments to a specific value [60].

V. PROTOCOL

In this section, we present our commitment protocol. The parties have access to a PRNC with parameters ρ and n. The constant $0 < \varepsilon < 1$ and the length $\ell \geq \lceil \log(n) \rceil$ are parameters of the protocol. Our protocol works for PRNCs that have a parameter ρ such that $0 \leq \rho \leq 1/(5 + 8\varepsilon)$. Let $\mathcal{G}$ be a family of 2-universal hash functions $g : \{0,1\}^{n\ell} \to \{0,1\}^m$ and $\mathcal{F}$ be another family of 2-universal hash functions $f : \{0,1\}^{n\ell} \to \{0,1\}^\omega$.

COMMIT PHASE:

C.1. Alice creates a sequence of n distinct binary strings (data packets), each one with a fixed length ℓ. We define the random variable X^n as:

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

The data packets X_i's are chosen uniformly at random conditioned on being distinct, and are used both as content and identifier. We denote by $x^n \leftarrow X^n$ a realization of X^n:

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

C.2. Alice sends x^n to Bob through the PRNC.

C.3. Bob keeps listening the noisy channel until all packets are received. At the end of this process, Bob obtains the permutation

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

which consists of a permutation of the data packets in x^n and is a realization of the random variable Y^n.

C.4. Let F be a random variable uniformly distributed in the family of 2-universal hash functions $\mathcal{F}$. Bob samples a realization f of F and sends the description of f to Alice over the authenticated bidirectional noiseless channel.

C.5. Let G be a random variable uniformly distributed in the family of 2-universal hash functions $\mathcal{G}$. Alice samples a realization g of G. Alice also chooses a uniformly distributed binary string value $v \in \{0,1\}^m$.

C.6. Alice computes $\mathsf{hash} := f(x^n)$ and $\mathsf{commit} := g(x^n) \oplus v$ (where $\oplus$ denotes the bitwise exclusive-or).

C.7. Alice sends hash, commit and the description of g to Bob over the authenticated bidirectional noiseless channel.

REVEAL PHASE:

R.1. If the Reveal Phase takes place, Alice sends $\widetilde{v}$ and $\overline{x^n}$ to Bob over the authenticated bidirectional noiseless channel, where $\widetilde{v} = v$ and $\overline{x^n} = x^n$ if Alice is honest.

R.2. Bob executes the Test function, which performs the following checks:

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

(ii) If y^n consists of a permutation of the data packets in $\overline{x^n}$ and if

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

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

R.3. If all checks are satisfied, then return ACC; otherwise, return REJ.

VI. SECURITY

We prove the unconditional security of the scheme by showing that it is $(\varphi, \kappa, \theta)$-secure for φ, κ, and θ that are negligible in the security parameters.

A. CORRECTNESS

When the players are honest, the protocol fails if, and only if, the Kendall tau distance between the random variables X^n and Y^n falls outside the range around the expected distance. To prove the correctness of the protocol, we show that this case occurs only with negligible probability in the security parameter n.

Adopting the shorthand K for $K(X^n, Y^n)$, we have that

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

These tails probabilities can be bounded using Chernoff inequalities. Let

$$\beta = 1 - \frac{2\rho}{(n-1)(1-\rho)},$$

which goes to 1 when $n \to \infty$. It holds that

$$\begin{aligned}\Pr\big[K \geq (1+\varepsilon)E[K]\big] &\leq \min_{t>0} \frac{E[e^{tK}]}{e^{t(1+\varepsilon)E[K]}} \\ &\leq e^{-(n-1)[\varepsilon\rho\beta - \ln(1+\varepsilon\rho)]}, \\ \Pr\big[K \leq (1-\varepsilon)E[K]\big] &\leq \min_{t>0} \frac{E[e^{-tK}]}{e^{-t(1-\varepsilon)E[K]}} \\ &\leq e^{-(n-1)\rho\varepsilon^2\beta^2/2}.\end{aligned}$$

The computation of these inequalities is presented in Appendix A. Then,

$$\begin{aligned}\Pr\Big[\big|K - E[K]\big| \geq \varepsilon E[K]\Big] \\ \leq e^{-(n-1)[\varepsilon\rho\beta - \ln(1+\varepsilon\rho)]} + e^{-(n-1)\rho\varepsilon^2\beta^2/2}.\end{aligned}$$

For $\forall\, x \geq 0$ it holds that $\frac{x^2}{2} \geq x - \ln(1+x)$ and thus

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

Therefore we get that

$$\Pr\Big[\big|K - E[K]\big| \geq \varepsilon E[K]\Big] \leq 2e^{-(n-1)[\varepsilon\rho\beta - \ln(1+\varepsilon\rho)]}.$$

Finally, for honest Alice and Bob,

$$\begin{aligned}\Pr[\mathsf{Test}(x^n, y^n, t, v) &= \mathrm{ACC}] \\ &= 1 - \Pr\Big[\big|K - E[K]\big| \geq \varepsilon E[K]\Big] \\ &\geq 1 - 2e^{-(n-1)[\varepsilon\rho\beta - \ln(1+\varepsilon\rho)]} \\ &= 1 - \varphi.\end{aligned}$$

The protocol fails with probability at most $\varphi = 2\exp[-(n-1)(\varepsilon\rho\beta - \ln(1+\varepsilon\rho))]$, which is negligible in n. ■

B. BINDING CONDITION

When Bob is honest, Alice should not be able to successfully open two different commitments $\overline{v}$ and $\widetilde{v}$. Let x^n be the sequence of data packets that Alice sends through the noisy channel and y^n the permutation received by Bob. In our protocol, Bob can detect Alice's malicious behavior due to his knowledge of characteristics of the channel (the noisy parameter ρ) and the hash value $f(\cdot)$ received from Alice. A malicious Alice can open two distinct commitment values only if she can find distinct permutations $\overline{x^n} \neq \widetilde{x^n}$ of the data packets (possibly one of them is equal to x^n) such that

$$\begin{aligned} f(\overline{x^n}) &= f(\widetilde{x^n}), \\ \left|K(\overline{x^n}, y^n) - E[K]\right| &< \varepsilon E[K], \\ \left|K(\widetilde{x^n}, y^n) - E[K]\right| &< \varepsilon E[K]. \end{aligned}$$

We show that the probability of such permutations existing is negligible in the security parameters. There are two steps to be proved. In the first step, we show that for any permutation $\overline{x^n}$ with $K(\overline{x^n}, x^n) > \tau$ (for a certain threshold value τ to be determined later), we have that $|K(\overline{x^n}, y^n) - E[K]| \geq \varepsilon E[K]$ with overwhelming probability. Next, we show that the probability of existing permutations $\overline{x^n} \neq \widetilde{x^n}$ such that

$$\begin{aligned} f(\overline{x^n}) &= f(\widetilde{x^n}), \\ K(\overline{x^n}, x^n) &\leq \tau, \\ K(\widetilde{x^n}, x^n) &\leq \tau, \end{aligned}$$

is negligible. In the remaining of this proof, we assume that $\left|K(x^n, y^n) - E[K]\right| < \varepsilon E[K]$, which happens with probability at least $1 - \varphi$, for φ negligible in the security parameter n, as demonstrated in the previous subsection.

The probability of a malicious Alice being detected depends on the distance between $\overline{x^n}$ (the sequence announced to Bob during the opening phase) and y^n (the actual permutation Bob receives from the channel). This distance depends on the swaps performed by channel to map x^n (the sequence originally sent down the channel by Alice) into y^n and the swaps performed by Alice to map x^n into $\overline{x^n}$. We observe that there exists a threshold τ for the swaps that Alice introduces such that Bob can detect them. The check performed by Bob in step R.2 (ii) fails when

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

Some of the swaps introduced by Alice will increase the distance between $\overline{x^n}$ and y^n. However, it is possible that Alice chooses to introduce swaps that will reduce the distance between $\overline{x^n}$ and y^n. That happens when Alice and the channel swap the same pair of adjacent data packets. We call this event a *swap collision*. Let the random variable $C(\overline{x^n}, y^n)$ represent the number of swap collisions that happened. Adopting the shorthand C for $C(\overline{x^n}, y^n)$ and assuming that a malicious Alice introduces $q = K(\overline{x^n}, x^n)$ swaps to forge $\overline{x^n}$, then C swaps will favor her, reducing the Kendall tau distance between $\overline{x^n}$ and y^n, and $q - C$ will harm her, increasing the distance. Adopting the shorthand $E[K]$ for $E[K(x^n, y^n)]$, we have that

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

As by assumption $(1-\varepsilon)E[K] < K(x^n, y^n) < (1+\varepsilon)E[K]$, the check performed in step R.2 (ii) will detect a malicious Alice in the case

$$|q - 2C| \geq 2\varepsilon E[K].$$

We observe that C must always be a fraction of K since it is impossible to happen more collisions than the number of swaps performed by the channel. Given that $K < (1 + \varepsilon)E[K]$ with overwhelming probability, we obtain the following lower bound

$$\begin{aligned} q &\geq 2(1 + \varepsilon)E[K] + 2\varepsilon E[K] \\ &= 2(1 + 2\varepsilon)E[K] \end{aligned}$$

such that a malicious Alice is always detected whenever she performs more than $2(1 + 2\varepsilon)E[K]$ swaps.

Now, it is necessary take C into account to determine the appropriate value of the threshold τ. There are $\mathsf{N} = n(n-1)/2$ distinct possible pairwise adjacent transpositions (swaps), where $k = K(x^n, y^n)$ of them are performed by channel and $q = K(\overline{x^n}, x^n)$ by malicious Alice.

We define *the order of a swap* as the minimum number of pairwise adjacent transpositions that need to be performed toward implement it. In general, there are $n - j$ distinct order-j swaps in any permutation with n elements. Moreover, the order of a specific swap is relative to the original permutation. For example, let $\pi_n = [1, 2, 3, 4 \ldots, n]$ be the identity permutation of n elements and $\mu_{(i+1,i)} = [1, \ldots, i + 1, i, \ldots, n]$ be any order-1 swap operation over the identity permutation. when $n = 5$, there are 4 distinct order-1 swaps over the identity permutation $\pi_5 = [1, 2, 3, 4, 5]$:

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

Now, let the original permutation be $\zeta_5 = [3, 1, 5, 2, 4]$. Then, the 4 distinct order-1 swaps will be:

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

We note that the swaps above are not order-1 when the original permutation is the identity. Also, it is convenient to assume that $\mu_{(1,3)} = \mu_{(3,1)}$, since both are swap operations over the same elements. So, to avoid confusion, we agreed henceforth in relabeling the order of the packets in X^n as the identity permutation without loss of generality. Thereby, an order-j swap will always be of the form $\mu_{(i+j,i)}$. So, the 3 distinct order-2 swaps when $n = 5$ are $\mu_{(3,1)}$, $\mu_{(4,2)}$

and $\mu_{(5,3)}$; the 2 distinct order-3 swaps are $\mu_{(4,1)}$ and $\mu_{(5,2)}$; and the only order-4 swap is $\mu_{(5,1)}$.

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

The order of a swap does not depend of the relative position where the swap occurs. The permutations $\{\mu_{(3,2)}, \mu_{(3,1)}\} = [3, 1, 2, 4, 5]$ and $\{\mu_{(2,1)}, \mu_{(3,1)}, \mu_{(4,1)}\} = [2, 3, 4, 1, 5]$ both have the same order-2 swap $\mu_{(3,1)}$, which is the intersection of the sets and represents a swap collision between the permutations. This means that the permutations y^n and $\overline{x^n}$ can be represented by sets of swap operations over packets of x^n, treated as the identity permutation. We assume henceforth that $\overline{\mathbf{X}}$ and $\mathbf{Y}$ are the sets of swaps that constitute $\overline{x^n}$ and y^n respectively.

We assume that Alice only performs $\mu_{(i+1,i)}$ order-1 swaps to forge $\overline{X^n}$. Although the number of possible order-1 swaps is $n-1$, there are at most $(n-1)/2$ disjoint order-1 swaps that Alice can perform at once to map x^n into $\overline{x^n}$, which upper bounds q. In order not to restrict the capabilities of a malicious Alice, we need a bound over the noisy parameter to reach this condition. Combining the upper bound above and the lower bound on q derived previously, we show that ρ must be

$$\begin{aligned}\frac{n-1}{2} \geq q \geq 2(1+2\varepsilon)\frac{\rho}{1-\rho}(n-1)\\ 1-\rho \geq 4(1+2\varepsilon)\rho\\ \therefore \rho \leq \frac{1}{5+8\varepsilon}\end{aligned}$$

We choose the restriction above because order-1 swaps of disjoint pairs of elements are independent and identically distributed. Moreover, the probability of channel performing an order-1 swap in the output is greater, since the occurrence of any swap of higher order depends of some order-1 swap occurs first. Given Alice's malicious strategy of always perform the most probable swaps to forge $\overline{x^n}$, the restriction in ρ implies that Alice will just perform order-1 swaps.

As demonstrated in Appendix C, the probability of each order-1 swap occurs is equal to

$$\begin{aligned}p &= \Pr[\mu_{(i+1,i)} \in \mathbf{Y}]\\ &= \frac{\rho}{1+\rho}\end{aligned}$$

We note that $C = \sum_{i=1}^{n-1} C_{\mu_{(i+1,i)}}$ the swap collision random variable can be obtained as the summation of indicator random variables, where $C_{\mu_{(i+1,i)}} = 1$ when both Alice and the channel perform the swap $\mu_{(i+1,i)}$ and $C_{\mu_{(i+1,i)}} = 0$ otherwise. Furthermore, the swaps performed by Alice in $\overline{\mathbf{X}}$ and by channel in $\mathbf{Y}$ are also independent. Remembering that malicious Alice performs $|\overline{\mathbf{X}}| = q$ swaps arbitrarily, the expected number of swap collisions can be calculated as:

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

We can obtain a concentration bound for C. To do this, we first observe that:

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

where we set $\delta = (e^t - 1)$ above.

So, remembering that Alice performs arbitrarily independent order-1 swaps, it follows that:

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

Observing that $t = \ln(1+\delta)$, we bound $E[C]$ by means of the following Chernoff bound:

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

We remember that $q \geq \tau$. So, it follows that:

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

which goes to zero in τ.

Finally, we have:

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

As showed in Appendix A, $E[K] \leq (n-1)\rho/(1-\rho)$. Therefore, our threshold τ is set as:

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

such that for all $q \geq \tau$ Alice's malicious behavior is detected by Bob in the test performed during the Reveal Phase.

Now, to complete the proof, we show that when cheating Alice performs $q \leq \tau$ permutations, Bob detects her malicious behavior since she cannot find two distinct permutations having the same hash with overwhelming probability.

Lemma 3: Let $\mathcal{F}$ be a family of 2-universal hash functions $f : \{0,1\}^{n\ell} \to \{0,1\}^{\omega}$ and let

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

where s is the security parameter. Then the probability that there are two permutations of the data packets $\overline{x^n} \neq \widetilde{x^n}$ such that $f(\overline{x^n}) = f(\widetilde{x^n})$, $K(\overline{x^n}, x^n) \leq \tau$ and $K(\widetilde{x^n}, x^n) \leq \tau$ is at most 2^{-s}.

Proof of Lemma 3: Let $x^n \leftarrow X^n$ be a sequence as defined in step C.1 of the Commit Phase. Let $\mathbf{W}$ be the set of permutations of data packets with Kendall tau distance at most τ from x^n. We know that the number of sequences with Kendall tau distance k from x^n is given by the Mahonian triangle term $M(n,k)$. Then, we just need to add every Mahonian term for $0 \leq k \leq \tau$ to calculate the volume of the hypersphere with center in the arbitrary sequence x^n. A well-known property of the Mahonian triangle is

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

and as showed in Lemma 13 of [61]

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

Thus, we get that

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

We apply the Stirling's approximation and some other simplifications in the expression above, obtaining

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

Taking the logarithm of the cardinality of the set $\mathbf{W}$ we have

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

Using the definition of 2-universal hash functions and the union bound, the success probability of Alice finding a hash collision between two distinct permutations of the data packets $\overline{x^n}, \widetilde{x^n} \in \mathbf{W}$ is upper bounded by

$$\begin{aligned}|\mathbf{W}|^2 \cdot 2^{-\omega} &\leq 2^{2(n-1+\tau)\mathsf{H}_b(\tau/(n-1+\tau))} \\ &\quad \cdot 2^{-2(n-1+\tau)\mathsf{H}_b(\tau/(n-1+\tau))-s} \\ &= 2^{-s}\end{aligned}$$

which concludes the proof. ■

This means that Alice succeeds in cheating Bob only when one of the following cases occurs: the channel permutes less than $(1-\varepsilon)E[K]$ pairwise adjacent data packets of x^n; the number of swap collisions exceeds $(1+\delta)E[C]$ or the hashes $f(\overline{x^n}) = f(\widetilde{x^n})$ collide.

In light of the arguments above, when Bob follows the protocol, the probability of a malicious Alice successfully cheating is upper bounded by θ, which goes exponentially to zero in the security parameters n and s:

$$\begin{aligned}\Pr[\mathsf{Test}(\widetilde{x^n}, y^n, t, \widetilde{v}) = \mathrm{ACC} \wedge \mathsf{Test}(\overline{x^n}, y^n, t, \overline{v}) = \mathrm{ACC}] \\ \leq e^{-(n-1)\rho\varepsilon^2\beta^2/2} + e^{-\frac{\delta^2}{(2+\delta)}\frac{\rho\tau}{1+\rho}} + 2^{-s} \\ = \theta\end{aligned}$$

which concludes the proof. ■

C. HIDING CONDITION

The protocol is secure for Alice if, before the reveal phase, a dishonest Bob can obtain at most a negligible amount of information about the string v that Alice commits to in the commit phase.

Alice extracts an one-time pad key from her string x^n and uses it to encrypt the value v that she commits to. As evidence of the commitment, Bob has a random variable Y^n correlated with X^n (obtained through the noisy channel) and an output $f(x^n)$ of a universal hash function (based on a seed chosen by him) computed by Alice. To show that Bob has almost no knowledge on Alice's commitment v, we must show that the key extracted by Alice and used to one-time pad v is almost uniformly distributed given all information in possession of Bob - this result will follow from the Leftover Hash Lemma. In order to apply this lemma, we will need to bound the uncertainty Bob has on X^n. When Bob receives Y^n his uncertainty about X^n is given by the behavior of the noisy channel, which randomly permutes the data packets in X^n with the following conditional probability mass function

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

As $\rho^{K(x^n,y^n)}$ is maximized when $y^n = x^n$, the min-entropy of X^n given Y^n is such that:

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

The Taylor Series of $\ln(1+x)$ is given by

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

Replacing x by $-\rho^i$ in the expression above and making the substitution of the natural logarithm function, we have

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

Now, we get that

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

Applying Lemma 4 (see Appendix B), we have

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

It follows that

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

Using Lemma 2, we bound the reduction on the uncertainty of Bob about X^n due to the universal hash computed by Alice, whose size is given by $\omega = 2(n-1+\tau)\mathsf{H}_b\left(\frac{\tau}{n-1+\tau}\right) + s$. So, we have:

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

Lemma 1 establishes that 2-universal hash functions can extract $m \leq \delta n - 2\log(\epsilon^{-1}) + 2$ random bits, where δn is the min-entropy of the source. Letting $\epsilon = 2^{-s}$, in our case it is possible to extract

$$\begin{aligned}
m \leq\ & n \log\left(\frac{1}{1-\rho}\right) - 2(n-1+\tau)\mathsf{H}_b\left(\frac{\tau}{n-1+\tau}\right) \\
& -\frac{2\rho(1+\rho)}{(1-\rho)} - 4s + 2
\end{aligned}$$

random bits such that the statistical distance between the output of the hash function G applied by Alice over X^n and truly random bits is at most 2^{-s} in Bob's view, given that G is randomly chosen over a family $\mathcal{G}$ of 2-universal hash functions.

As Alice does the exclusive-or of her commitment v with $g(x^n)$, we get that

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

and the proof follows. ■

VII. CONCLUSION

In this work, we built upon the pioneering work of Palmieri and Pereira and proposed the first efficient string commitment protocol based on the packet reordering effect. Our commitment scheme is unconditionally hiding and binding. It has a restriction, since it works only when $0 \leq \rho \leq 1/(5+8\varepsilon)$. We have also introduced a new definition of packet reordering channels that naturally follows from the behavior of packet switching networks such as the Internet. There are several interesting sequels to this work:

- designing a protocol that works for all $0 < \rho < 1$;
- proposing protocols that are optimal in terms of commitment rate and failure probabilities;
- showing the possibility of obtaining commitment and oblivious transfer protocols when the channel parameters are influenced by the adversary, in the stronger adversarial model known as unfair noisy channel;
- extend our model to combine the packet reordering with other noisy channels, such as the binary symmetric and the erasure channels;
- investigating secret key agreement protocols based on packet reordering channels as defined in this work.

APPENDIX A. OBTAINING THE CONCENTRATION INEQUALITIES

In this section, we derive the bounds presented in Subsection VI-A. At first, we obtain the expected Kendall tau distance between X^n and Y^n. Adopting the shorthand of $E[K(X^n, Y^n)] = E[K]$ and $n(n-1)/2 = \mathsf{N}$, we have that

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

The first derivative of the generating function σ_n can be calculated as follows

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

Here, we are interested in the upper and lower bounds for the first derivative of the function $\sigma_n(\rho)$. First, we obtain the upper bound:

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

Now, we derive the lower bound. Let $u(\rho)$ be any function in ρ. Remembering that

$$\frac{d}{d\rho}\ln(u) = \frac{1}{u}\frac{du}{d\rho}$$

we have

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

In the last step above (as done in Subsection VI-C), we replaced the natural logarithm function by the Taylor series expansion. So,

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

where we use in the last step the fact that $\sum_{k=0}^{j}\rho^k = (1-\rho^{j+1})/(1-\rho)$.

Using Lemma 4 (presented in Appendix B) to bound the summation above, we have

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

$$= \sigma_n(\rho)\frac{n-1}{1-\rho}\left[1 - \frac{2\rho}{(n-1)(1-\rho)}\right]$$

Let $\beta = 1 - 2\rho/[(n-1)(1-\rho)]$, which goes to 1 when $n \to \infty$. Then, by the Squeeze Theorem, $\forall\, 0 < \rho < 1$, the first derivative of the function $\sigma_n(\rho)$ is such that

$$\sigma_n(\rho)\frac{n-1}{1-\rho}\beta \;\leq\; \frac{d\sigma_n}{d\rho} \;\leq\; \sigma_n(\rho)\frac{n-1}{1-\rho}$$
$$\therefore \lim_{n\to\infty}\frac{d\sigma_n}{d\rho} = \sigma_n(\rho)\frac{n-1}{1-\rho}$$

The expected Kendall tau distance between X^n and Y^n is given by

$$(n-1)\frac{\rho}{1-\rho}\beta \leq E[K] \leq (n-1)\frac{\rho}{1-\rho}$$
$$\therefore \lim_{n\to\infty} E[K] = (n-1)\left(\frac{\rho}{1-\rho}\right) \;\; \forall \;\; 0 \leq \rho < 1$$

A. UPPER TAIL

The Chernoff bound for an arbitrary random variable K is achieved by means of Markov's inequality applied to e^{tK}. For every $t > 0$, we have that

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

The inequality above can be minimized in t as follows:

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

Now, we observe that

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

For $n \to \infty$,

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

The goal is to choose a $t > 0$ such that

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

and $e^{-t} = \dfrac{1+\varepsilon\rho}{1+\varepsilon} = 1 - \dfrac{\varepsilon(1-\rho)}{1+\varepsilon}$

Now, we have

$$e^{-t(1+\varepsilon)E[K]} = \left(1 - \frac{\varepsilon(1-\rho)}{1+\varepsilon}\right)^{(1+\varepsilon)E[K]}$$
$$\leq \left[\left(1 - \frac{\varepsilon}{\left(\frac{1+\varepsilon}{1-\rho}\right)}\right)^{\frac{1+\varepsilon}{1-\rho}}\right]^{(n-1)\rho\beta}$$
$$\leq e^{-(n-1)\varepsilon\rho\beta}$$

Then,

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

Let $\alpha = \varepsilon(1-\rho)/(1+\varepsilon\rho)$ and let the notation $\sigma_n^{(i)}(\rho)$ denote the i-th derivative of the function $\sigma_n(\rho)$. Considering that $(1+\alpha)^k = \sum_{i=0}^{k}\binom{k}{i}\alpha^i$ we have

$$\Pr\left[K \geq (1+\varepsilon)E[K]\right]$$
$$\leq \frac{e^{-(n-1)\varepsilon\rho\beta}}{\sigma_n(\rho)}\sum_{k=0}^{\mathsf{N}} M(n,k)\rho^k\,(1+\alpha)^k$$
$$\leq \frac{e^{-(n-1)\varepsilon\rho\beta}}{\sigma_n(\rho)}\sum_{k=0}^{\mathsf{N}}\sum_{i=0}^{k}\binom{k}{i}M(n,k)\rho^k\alpha^i$$
$$\leq \frac{e^{-(n-1)\varepsilon\rho\beta}}{\sigma_n(\rho)}\left(\sigma_n(\rho) + \alpha\rho\sigma_n^{(1)}(\rho) + \frac{\alpha^2\rho^2}{2!}\sigma_n^{(2)}(\rho) + \cdots + \frac{\alpha^{\mathsf{N}}\rho^{\mathsf{N}}}{\mathsf{N}!}\sigma_n^{(\mathsf{N})}(\rho)\right)$$

where the last expansion above is just the Taylor series of $\sigma_n(\rho e^t) = \sigma_n(\rho + \alpha\rho)$.

Let $\langle n-1\rangle^i = (n-1)n(n+1)(n+2)\cdots(n-1+i-1)$ be the rising factorial. We obtain the upper bound for the derivatives of higher order of the function $\sigma_n(\rho)$ as follows:

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

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

$$\sigma_n^{(3)}(\rho) = \sigma_n^{(2)}(\rho)\left[\frac{n-1}{1-\rho} - \sum_{k=2}^{n}\frac{d}{d\rho}\sum_{j=1}^{\infty}\frac{(\rho^k)^j}{j}\right]$$
$$+2\sigma_n^{(1)}(\rho)\left[\frac{n-1}{(1-\rho)^2} - \sum_{k=2}^{n}\frac{d^2}{d\rho^2}\sum_{j=1}^{\infty}\frac{(\rho^k)^j}{j}\right]$$
$$+\sigma_n(\rho)\left[\frac{2(n-1)}{(1-\rho)^3} - \sum_{k=2}^{n}\frac{d^3}{d\rho^3}\sum_{j=1}^{\infty}\frac{(\rho^k)^j}{j}\right]$$
$$\leq \sigma_n(\rho)\frac{n(n-1)^2}{(1-\rho)^3} + \sigma_n(\rho)\frac{2(n-1)^2}{(1-\rho)^3}$$
$$+\sigma_n(\rho)\frac{2(n-1)}{(1-\rho)^3}$$
$$= \sigma_n(\rho)\frac{(n-1)n(n+1)}{(1-\rho)^3}$$

$$\sigma_n^{(4)}(\rho) = \sigma_n^{(3)}(\rho)\left[\frac{n-1}{1-\rho} - \sum_{k=2}^{n}\frac{d}{d\rho}\sum_{j=1}^{\infty}\frac{(\rho^k)^j}{j}\right]$$
$$+3\sigma_n^{(2)}(\rho)\left[\frac{n-1}{(1-\rho)^2} - \sum_{k=2}^{n}\frac{d^2}{d\rho^2}\sum_{j=1}^{\infty}\frac{(\rho^k)^j}{j}\right]$$
$$+3\sigma_n^{(1)}(\rho)\left[\frac{2(n-1)}{(1-\rho)^3} - \sum_{k=2}^{n}\frac{d^3}{d\rho^3}\sum_{j=1}^{\infty}\frac{(\rho^k)^j}{j}\right]$$
$$+\sigma_n(\rho)\left[\frac{6(n-1)}{(1-\rho)^4} - \sum_{k=2}^{n}\frac{d^4}{d\rho^4}\sum_{j=1}^{\infty}\frac{(\rho^k)^j}{j}\right]$$
$$\leq \sigma_n(\rho)\frac{(n-1)^2n(n+1)}{(1-\rho)^4} + \sigma_n(\rho)\frac{3(n-1)^2n}{(1-\rho)^4}$$
$$+\sigma_n(\rho)\frac{6(n-1)^2}{(1-\rho)^4} + \sigma_n(\rho)\frac{6(n-1)}{(1-\rho)^4}$$
$$= \sigma_n(\rho)\frac{\langle n-1\rangle^4}{(1-\rho)^4}$$
$$\vdots$$
$$\therefore \sigma_n^{(i)}(\rho) \leq \sigma_n(\rho)\frac{\langle n-1\rangle^i}{(1-\rho)^i}$$

Hence, by the principle of mathematical induction, having shown all the inequalities above, we need to demonstrate the validity for $i+1$ to prove that it holds for all $i \geq 1$. So,

$$\sigma_n^{(i+1)}(\rho) = \sum_{j=0}^{i}\binom{i}{j}\sigma_n^{(j)}(\rho)\left[(i-j)!\frac{n-1}{(1-\rho)^{i+1-j}}\right.$$
$$\left. - \sum_{k=2}^{n}\frac{d^{i+1-j}}{d\rho^{i+1-j}}\sum_{j=1}^{\infty}\frac{(\rho^k)^j}{j}\right]$$
$$\leq \sigma_n(\rho)\sum_{j=0}^{i}\frac{i!}{j!}\frac{\langle n-1\rangle^j}{(1-\rho)^j}\left[\frac{n-1}{(1-\rho)^{i+1-j}}\right]$$
$$= \frac{\sigma_n(\rho)}{(1-\rho)^{i+1}}i!(n-1)\sum_{j=0}^{i}\frac{\langle n-1\rangle^j}{j!}$$
$$= \frac{\sigma_n(\rho)}{(1-\rho)^{i+1}}i!(n-1)$$
$$\cdot\left[1 + (n-1) + \frac{(n-1)n}{2} + \cdots\right.$$
$$\left. + \frac{(n-1)n(n+1)\cdots(n-1+i-1)}{i!}\right]$$
$$= \frac{\sigma_n(\rho)}{(1-\rho)^{i+1}}i!(n-1)n$$
$$\cdot\left[1 + \frac{(n-1)}{2} + \cdots\right.$$
$$\left. + \frac{(n-1)(n+1)\cdots(n-1+i-1)}{i!}\right]$$
$$= \frac{\sigma_n(\rho)}{(1-\rho)^{i+1}}i!(n-1)n(n+1)$$
$$\cdot\left[\frac{1}{2} + \frac{(n-1)}{6} + \frac{(n-1)(n+2)}{24} + \cdots\right.$$
$$\left. + \frac{(n-1)\cdots(n-1+i-1)}{i!}\right]$$
$$\vdots$$
$$= \frac{\sigma_n(\rho)}{(1-\rho)^{i+1}}i!(n-1)n(n+1)\cdots$$
$$\cdots(n-1+i-1)\left[\frac{1}{(i-1)!} + \frac{(n-1)}{i!}\right]$$
$$= \sigma_n(\rho)\frac{\langle n-1\rangle^{i+1}}{(1-\rho)^{i+1}}$$

Replacing the derivatives above in the previous concentration bound inequality we have:

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

Using the identity (5.56) presented in [62], it follows that

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

$$= e^{-(n-1)\varepsilon\rho\beta}\,(1+\varepsilon\rho)^{n-1}$$
$$= e^{-(n-1)\varepsilon\rho\beta}\cdot e^{(n-1)\ln(1+\varepsilon\rho)}$$
$$= e^{-(n-1)[\varepsilon\rho\beta-\ln(1+\varepsilon\rho)]}$$

which goes exponentially to zero for n sufficiently large. ■

B. LOWER TAIL

The lower tail of the concentration inequality is given by

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

for $0 < \varepsilon < 1$.

Here, we use a different approach. Let $\psi_K(t)$ be defined as

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

It's easy to see that $\psi_K(0) = 0$. The first derivative of the function is

$$\psi_K'(t) = \frac{d\psi_K(t)}{dt} = \frac{E[-Ke^{-tK}]}{E[e^{-tK}]}$$
$$\therefore \psi_K'(0) = -E[K]$$

The second derivative is given by

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

Then,

$$\frac{E[Ke^{-tK}]}{E[e^{-tK}]} = \frac{\sigma_n^{-1}(\rho)\sum_{k=0}^{\mathsf{N}} ke^{-tk}M(n,k)\rho^k}{\sigma_n^{-1}(\rho)\sum_{k=0}^{\mathsf{N}} e^{-tk}M(n,k)\rho^k}$$
$$= \frac{\rho e^{-t}\sum_{k=0}^{\mathsf{N}} kM(n,k)(\rho e^{-t})^{k-1}}{\sum_{k=0}^{\mathsf{N}} M(n,k)(\rho e^{-t})^k}$$
$$= \frac{\rho e^{-t}}{\sigma_n(\rho e^{-t})}\left[\frac{d\sigma_n(\rho e^{-t})}{d(\rho e^{-t})}\right]$$
$$= \frac{\rho e^{-t}\sigma_n'(\rho e^{-t})}{\sigma_n(\rho e^{-t})}$$

and also

$$\frac{E[K^2e^{-tK}]}{E[e^{-tK}]} = \frac{\sigma_n^{-1}(\rho)\sum_{k=0}^{\mathsf{N}} k^2\,e^{-tk}M(n,k)\rho^k}{\sigma_n^{-1}(\rho)\sum_{k=0}^{\mathsf{N}} e^{-tk}M(n,k)\rho^k}$$
$$= \frac{(\rho e^{-t})^2\sum_{k=0}^{\mathsf{N}} k(k-1)M(n,k)(\rho e^{-t})^{k-2}}{\sum_{k=0}^{\mathsf{N}} M(n,k)(\rho e^{-t})^k}$$
$$+ \frac{\rho e^{-t}\sum_{k=0}^{\mathsf{N}} kM(n,k)(\rho e^{-t})^{k-1}}{\sum_{k=0}^{\mathsf{N}} M(n,k)(\rho e^{-t})^k}$$
$$= \frac{(\rho e^{-t})^2}{\sigma_n(\rho e^{-t})}\left[\frac{d^2\sigma_n(\rho e^{-t})}{d(\rho e^{-t})^2}\right]$$
$$+ \frac{\rho e^{-t}}{\sigma_n(\rho e^{-t})}\left[\frac{d\sigma_n(\rho e^{-t})}{d(\rho e^{-t})}\right]$$
$$= \frac{(\rho e^{-t})^2\sigma_n''(\rho e^{-t})}{\sigma_n(\rho e^{-t})} + \frac{\rho e^{-t}\sigma_n'(\rho e^{-t})}{\sigma_n(\rho e^{-t})}.$$

With this, we conclude that:

$$\psi_K''(t) = \frac{(\rho e^{-t})^2\sigma_n''(\rho e^{-t})}{\sigma_n(\rho e^{-t})} + \frac{\rho e^{-t}\sigma_n'(\rho e^{-t})}{\sigma_n(\rho e^{-t})} - \left(\frac{\rho e^{-t}\sigma_n'(\rho e^{-t})}{\sigma_n(\rho e^{-t})}\right)^2$$

The variance of K is defined as

$$Var_K(\rho) = E[(K - E[K])^2] = E[K^2] - E[K]^2$$

We observe that

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

Remembering that

$$E[K] = \frac{\rho\sigma_n'(\rho)}{\sigma_n(\rho)}$$

It follows:

$$Var_K(\rho) = \frac{\rho^2\sigma_n''(\rho)}{\sigma_n(\rho)} + \frac{\rho\sigma_n'(\rho)}{\sigma_n(\rho)} - \left(\frac{\rho\sigma_n'(\rho)}{\sigma_n(\rho)}\right)^2$$
$$= \rho\frac{d}{d\rho}E[K]$$
$$\le \frac{(n-1)\rho}{(1-\rho)^2}$$

Hence, we claim that

$$\psi_K''(t) = Var_K(\rho e^{-t})$$

Now, by the Taylor theorem, we have

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

for some c between 0 and t. We notice that,

$$\psi_K''(t) = Var_K(\rho e^{-t}) \le Var_K(\rho)\ \ \forall\ \ t \ge 0$$

Then,

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

We can bound the desired probability as

$$\Pr\left[K \le (1-\varepsilon)E[K]\right] \le \min_{t>0} \frac{E[e^{-tK}]}{e^{-t(1-\varepsilon)E[K]}}$$
$$= \min_{t>0} e^{-\varepsilon E[K]t + Var_K(\rho)\frac{t^2}{2}}$$

Since the exponential is monotonic, we just need minimize the function $\phi(t)$ defined as

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

So, it follows that

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

Now, we have

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

Finally, it follows that

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

which goes exponentially to zero when $n \to \infty$. ■

APPENDIX B AUXILIARY LEMMA

Lemma 4: For $0 \leq \rho \leq 1$ we have

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

Proof: Let be the following identity

$$\begin{aligned}&\frac{\rho^n}{1+\rho+\cdots+\rho^{n-1}} - \frac{\rho^{n+1}}{1+\rho+\cdots+\rho^n} \\ &\qquad = \frac{\rho^n}{1+\rho+\cdots+\rho^{n-1}}\frac{1}{1+\rho+\cdots+\rho^n}\end{aligned}$$

To prove it is true, we show it is valid for $n = 1$:

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

By the principle of mathematical induction, assuming the case for n, we show it is valid for $n+1$ as well

$$\begin{aligned}&\frac{\rho^{(n+1)}}{1+\rho+\cdots+\rho^{(n+1)-1}} - \frac{\rho^{(n+1)+1}}{1+\rho+\cdots+\rho^{(n+1)}} \\ &= \rho^{n+1}\left(\frac{1}{1+\rho+\cdots+\rho^n} - \frac{\rho}{1+\rho+\cdots+\rho^{n+1}}\right) \\ &= \rho^{n+1}\left(\frac{1+\rho+\cdots+\rho^{n+1}-\rho(1+\rho+\cdots+\rho^n)}{(1+\rho+\cdots+\rho^n)(1+\rho+\cdots+\rho^{n+1})}\right) \\ &= \frac{\rho^{(n+1)}}{1+\rho+\cdots+\rho^{(n+1)-1}}\cdot\frac{1}{1+\rho+\cdots+\rho^{(n+1)}}\end{aligned}$$

so, it is valid for all $n \geq 1$.

Now we observe that it is possible to develop the recurrence above for ρ as follows:

$$\begin{aligned}\rho &= \frac{\rho}{1+\rho} + \frac{\rho^2}{1+\rho} \\ &= \frac{\rho}{1+\rho} + \frac{\rho^2}{1+\rho}\cdot\frac{1}{1+\rho+\rho^2} + \frac{\rho^3}{1+\rho+\rho^2} \\ &= \frac{\rho}{1+\rho} + \frac{\rho^2}{1+\rho}\cdot\frac{1}{1+\rho+\rho^2} \\ &\quad + \frac{\rho^3}{1+\rho+\rho^2}\cdot\frac{1}{1+\rho+\rho^2+\rho^3} + \frac{\rho^4}{1+\rho+\rho^2+\rho^3} \\ &\quad \vdots\end{aligned}$$

We claim that each term in the expansion of ρ is greater than each term with the same numerator in the proposed series. It is easy to verify the correctness of the claim since the difference between the term of the expansion and the term of the series, both with the same numerator, is always positive:

$$\begin{aligned}&\frac{\rho}{1+\rho} - \frac{\rho}{(1+\rho)^2} = \frac{\rho^2}{(1+\rho)^2} \\ &\frac{\rho^2}{1+\rho}\cdot\frac{1}{1+\rho+\rho^2} - \frac{\rho^2}{(1+\rho+\rho^2)^2} \\ &= \frac{\rho^2}{1+\rho}\cdot\frac{\rho^2}{(1+\rho+\rho^2)^2} \\ &\frac{\rho^3}{1+\rho+\rho^2}\cdot\frac{1}{1+\rho+\rho^2+\rho^3} - \frac{\rho^3}{(1+\rho+\rho^2+\rho^3)^2} \\ &= \frac{\rho^3}{1+\rho+\rho^2}\cdot\frac{\rho^3}{(1+\rho+\rho^2+\rho^3)^2} \\ &\vdots\end{aligned}$$

which is a simple consequence of the fact that the denominator of the terms of the expansion are smaller than those of the terms of the series.

Finally, in light of argumentation above, we have that

$$\begin{aligned}\sum_{i=0}^{\infty}\frac{\rho^i}{(\sum_{j=0}^{i}\rho^j)^2} &= 1 + \frac{\rho}{(1+\rho)^2} + \frac{\rho^2}{(1+\rho+\rho^2)^2} + \cdots \\ &\leq 1 + \frac{\rho}{1+\rho} + \frac{\rho^2}{(1+\rho)(1+\rho+\rho^2)} + \cdots \\ &\leq 1+\rho\end{aligned}$$

■

APPENDIX C. SWAPS

Let $T(n,k)$ be the number of permutations containing any given $\mu_{(i+1,i)}$ order-1 swap between all possible $M(n,k)$ permutations at a Kendall tau distance k of the identity permutation.

We remember that a swap is a pairwise adjacent data packet transposition. Also, an order-1 swap is a pairwise adjacent data packet transposition that can be performed independent of any other swap occurs.

Trivially, no order-1 swap occurs when $k = 0$ and it is easy to see that, for $k = 1$, every order-1 swap appears only once between all $M(n, 1)$ possible permutations, so

$$T(n, 0) = 0$$

and

$$T(n, 1) = M(n, 0) = 1$$

for all $n \geq 2$.

When $k = 2$, every order-1 swap appears exactly $n - 2$ times. To see this, after performing any order-1 swap, there are $M(n, 1) = n - 1$ possible swaps, but $T(n, 1) = 1$ that undo the first one. So, we have:

$$T(n, 2) = M(n, 1) - T(n, 1) = M(n, 1) - M(n, 0) = n - 2.$$

Now, when $k = 3$, fixing any order-1 swap lasts $M(n, 2)$ possible swaps, but $T(n, 2)$ swaps that undo the previous fixed one. Then:

$$T(n, 3) = M(n, 2) - T(n, 2) = M(n, 2) - M(n, 1) + M(n, 0).$$

Therefore, the pattern generalizes as follows:

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

It is a simple corollary the following observation:

$$M(n, k) = T(n, k) + T(n, k + 1)$$

The numbers $T(n, k)$ form the following triangle:

$n = 2$: 0 1
$n = 3$: 0 1 1 1
$n = 4$: 0 1 2 3 3 2 1
$n = 5$: 0 1 3 6 9 11 11 9 6 3 1
$n = 6$: 0 1 4 10 19 30 41 49 52 49 41 $\cdots$

Above, we have the column for $k = 0$ always equal to 0 as there are no order-1 swap when no swap has been made. We notice that $T(n, k)$ forms the integer sequence A307429 with an offset of one in k. In other words, $T(n, k) = A307429(n, k - 1)$, for all $n \geq 2$.

To obtain the probability $p = \Pr[\mu_{(i+1,i)} \in \mathbf{Y}]$ of a given order-1 swap be in the set of swaps performed by channel to map x^n into y^n, we apply the law of total probability, calculating first $\Pr[\mu_{(i+1,i)} \in \mathbf{Y} : |\mathbf{Y}| = k]$, multiplying by the probability $\Pr[|\mathbf{Y}| = k]$ and sum over all possible k. For any fixed k, the probability of any order-1 swap occurs is given by the ratio between the number of permutations containing a given order-1 swap, i.e. $T(n, k)$, and the number of permutations at Kendall tau distance k, i.e. $M(n, k)$. The probability $\Pr[|\mathbf{Y}| = k]$ is given by the probability of y^n have Kendall tau distance k, $\rho^k/\sigma_n(\rho)$, multiplied by the total number of permutations with Kendall tau distance k. So, it follows that:

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

We claim that the polynomial $\sum_{k=0}^{\mathsf{N}} T(n, k)\rho^k$ can also be written as a product of polynomials, in the same way of $\sigma_n(\rho) = \prod_{i=1}^{n} S_i(\rho)$. We notice that there is no reason to limit the sum in the definition of the polynomials. Assuming that $\forall\, k < 0 \vee k > \mathsf{N},\ T(n, k) = M(n, k) = 0$, we have:

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

And now it is easy to check that the coefficients $T(n, k)$ of the polynomial above indeed form the triangle specified in the OEIS A307429 sequence and reproduced previously. Moreover, we can see that the product by ρ is the cause of the shift of one column to the right in this triangle when compared with the Mahonian triangle. Finally, we have:

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

REFERENCES

[1] P. Palmieri and O. Pereira, "Implementing information-theoretically secure oblivious transfer from packet reordering," in *Proc. ICISC*, 2011, pp. 332–345, doi: 10.1007/978-3-642-31912-9_22.

[2] M. Blum, "Coin flipping by telephone a protocol for solving impossible problems," *ACM SIGACT News*, vol. 15, no. 1, pp. 23–27, Jan. 1983.

[3] G. Brassard, D. Chaum, and C. Crépeau, "Minimum disclosure proofs of knowledge," *J. Comput. Syst. Sci.*, vol. 37, no. 2, pp. 156–189, 1988.

[4] O. Goldreich, S. Micali, and A. Wigderson, "Proofs that yield nothing but their validity and a methodology of cryptographic protocol design," in *Proc. 27th Annu. Symp. Found. Comput. Sci. (SFCS)*, Oct. 1986, pp. 174–187.
[5] O. Goldreich, S. Micali, and A. Wigderson, "How to play ANY mental game," in *Proc. 19th Annu. ACM Conf. Theory Comput. (STOC)*, 1987, pp. 218–229.
[6] D. Chaum, I. Damgård, and J. van de Graaf, "Multiparty computations ensuring privacy of each party's input and correctness of the result," in *Advances in Cryptology—CRYPTO'87* (Lecture Notes in Computer Science), vol. 293, C. Pomerance, Ed. Santa Barbara, CA, USA: Springer, 1988, pp. 87–119.
[7] D. Chaum, C. Crépeau, and I. Damgard, "Multiparty unconditionally secure protocols," in *Proc. 20th Annu. ACM Symp. Theory Comput. (STOC)*, 1988, pp. 11–19.
[8] A. Winter, A. Nascimento, and H. Imai, "Commitment capacity of discrete memoryless channels," in *Cryptography and Coding* (Lecture Notes in Computer Science), vol. 2898, K. Paterson, Ed. Berlin, Germany: Springer, 2003, pp. 35–51.
[9] D. Mayers, "Unconditionally secure quantum bit commitment is impossible," *Phys. Rev. Lett.*, vol. 78, pp. 3414–3417, Apr. 1997, doi: 10.1103/PhysRevLett.78.3414
[10] H.-K. Lo and H. F. Chau, "Why quantum bit commitment and ideal quantum coin tossing are impossible," *Phys. D*, vol. 120, nos. 1–2, pp. 177–187, Sep. 1998, doi: 10.1016/S0167-2789(98)00053-0.
[11] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
[12] C. Crepeau and J. Kilian, "Achieving oblivious transfer using weakened security assumptions," in *Proc. 29th Annu. Symp. Found. Comput. Sci.*, Oct. 1988, pp. 42–52.
[13] C. Crépeau, "Efficient cryptographic protocols based on noisy channels," in *Proc. EUROCRYPT*, 1997, pp. 306–317.
[14] V. M. Alves, "Protocolo de comprometimento de bit eficiente com segurança sequencial baseado no modelo de memória limitada," M.S. thesis, Dept. de Engenharia Elétrica, Faculdade de Tecnologia, Universidade de Brasília, Campus Anísio Teixeira, Asa Norte, Brasília-DF, Brasília, Brazil, Feb. 2010.
[15] J. Shikata and D. Yamanaka, "Bit commitment in the bounded storage model: Tight bound and simple optimal construction," in *Cryptography Coding* (Lecture Notes in Computer Science), vol. 7089, L. Chen, Ed. Berlin, Germany: Springer, 2011, pp. 112–131.
[16] R. Dowsley, F. Lacerda, and A. C. A. Nascimento, "Commitment and oblivious transfer in the bounded storage model with errors," *IEEE Trans. Inf. Theory*, vol. 64, no. 8, pp. 5970–5984, Aug. 2018.
[17] V. Goyal, Y. Ishai, M. Mahmoody, and A. Sahai, "Interactive locking, zero-knowledge PCPs, and unconditional cryptography," in *Proc. 30th Annual Cryptol. Conf.* in Lecture Notes in Computer Science, vol. 6223, T. Rabin, Ed. Santa Barbara, CA, USA: Springer, Aug. 2010, pp. 173–190.
[18] N. Döttling, D. Kraschewski, and J. Müller-Quade, "Unconditional and composable security using a single stateful tamper-proof hardware token," in *Proc. 8th Theory Cryptogr. Conf. Theory Cryptogr. (TCC)* in Lecture Notes in Computer Science, vol. 6597, Y. Ishai, Ed. Providence, RI, USA: Springer, Mar. 2011, pp. 164–181.
[19] R. Dowsley, J. Müller-Quade, and T. Nilges, "Weakening the isolation assumption of tamper-proof hardware tokens," in *Proc. 8th Int. Conf. Inf. Theoretic Secur. (ICITS)* in Lecture Notes in Computer Science, vol. 9063, A. Lehmann and S. Wolf, Eds. Lugano, Switzerland: Springer, May 2015, pp. 197–213.
[20] S. Winkler, J. Wullschleger, and S. Wolf, "Bit commitment from nonsignaling correlations," *IEEE Trans. Inf. Theory*, vol. 57, no. 3, pp. 1770–1779, Mar. 2011.
[21] A. Kent, "Unconditionally secure bit commitment," *Phys. Rev. Lett.*, vol. 83, no. 7, pp. 1447–1450, Aug. 1999.
[22] R. Dowsley, J. Müller-Quade, and A. C. A. Nascimento, "On the possibility of universally composable commitments based on noisy channels," in *Proc. Anais do 8th Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, (SBSEG)*, A. L. M. dos Santos and M. P. Barcellos, Eds. Gramado, Brazil: Sociedade Brasileira de Computação (SBC), Sep. 2008, pp. 103–114.
[23] R. Dowsley, J. van de Graaf, J. Müller-Quade, and A. C. A. Nascimento, "On the composability of statistically secure bit commitments," *J. Internet Technol.*, vol. 14, no. 3, pp. 509–516, 2013.
[24] R. Dowsley, J. Müller-Quade, and A. C. A. Nascimento, "On the composability of statistically secure random oblivious transfer," *Entropy*, vol. 22, no. 1, p. 107, Jan. 2020.
[25] A. C. A. Nascimento, J. Barros, S. Skludarek, and H. Imai, "The commitment capacity of the Gaussian channel is infinite," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2785–2789, Jun. 2008.
[26] C. Crepeau, R. Dowsley, and A. C. A. Nascimento, "On the commitment capacity of unfair noisy channels," *IEEE Trans. Inf. Theory*, vol. 66, no. 6, pp. 3745–3752, Jun. 2020.
[27] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.
[28] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.
[29] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.
[30] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, Dec. 2004.
[31] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
[32] I. Csiszar and P. Narayan, "Secrecy capacities for multiterminal channel models," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2437–2452, Jun. 2008.
[33] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y.-H. Kim, "Wiretap channel with secure rate-limited feedback," *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5353–5361, Dec. 2009.
[34] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, Apr. 2011.
[35] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.
[36] H. Imai, K. Morozov, and A. A. Nascimento, "On the oblivious transfer capacity of the erasure channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2006, pp. 1428–1431.
[37] R. Ahlswede and I. Csiszár, "On oblivious transfer capacity," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2007, pp. 2061–2064.
[38] A. C. A. Nascimento and A. Winter, "On the oblivious-transfer capacity of noisy resources," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2572–2581, Jun. 2008.
[39] A. C. B. Pinto, R. Dowsley, K. Morozov, and A. C. A. Nascimento, "Achieving oblivious transfer capacity of generalized erasure channels in the malicious model," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 5566–5571, Aug. 2011.
[40] R. Dowsley and A. C. A. Nascimento, "On the oblivious transfer capacity of generalized erasure channels against malicious adversaries: The case of low erasure probability," *IEEE Trans. Inf. Theory*, vol. 63, no. 10, pp. 6819–6826, Oct. 2017.
[41] P. Palmieri and O. Pereira, "Building oblivious transfer on channel delays," in *Information Security and Cryptology* (Lecture Notes in Computer Science), vol. 6584, X. Lai, M. Yung, and D. Lin, Eds. Berlin, Germany: Springer, 2011, pp. 125–138.
[42] P. Palmieri and O. Pereira, "Unconditionally secure oblivious transfer from real network behavior," in *Advances in Information and Computer Security* (Lecture Notes in Computer Science), vol. 8231, K. Sakiyama and M. Terada, Eds. Berlin, Germany: Springer, 2013, pp. 168–182.
[43] F.-G. Deng and G. L. Long, "Controlled order rearrangement encryption for quantum key distribution," *Phys. Rev. A, Gen. Phys., Gen. Phys.*, vol. 68, Oct. 2003, Art. no. 042315, doi: 10.1103/PhysRevA.68.042315.
[44] J. Wang, Q. Zhang, and C.-J. Tang, "Quantum secure direct communication based on order rearrangement of single photons," *Phys. Lett. A*, vol. 358, no. 4, pp. 256–258, Oct. 2006, doi: 10.1016/j.physleta.2006.05.035.
[45] J. Kilian, "Founding cryptography on oblivious transfer," in *Proc. STOC*. New York, NY, USA: ACM, 1988, pp. 20–31.
[46] I. Haitner, "Semi-honest to malicious oblivious transfer—The black-box way," in *Proc. TCC*, 2008, pp. 412–426.
[47] Y. Ishai, E. Kushilevitz, Y. Lindell, and E. Petrank, "Black-box constructions for secure computation," in *Proc. 38th Annu. ACM Symp. Theory Comput. (STOC)*, May 2006, pp. 99–108.
[48] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM J. Comput.*, vol. 38, no. 1, pp. 97–139, 2008.
[49] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *J. Comput. Syst. Sci.*, vol. 18, no. 2, pp. 143–154, Apr. 1979.

[50] R. Impagliazzo, L. A. Levin, and M. Luby, "Pseudo-random generation from one-way functions," in *Proc. 21st Annu. ACM Symp. Theory Comput. (STOC)*, Feb. 1989, pp. 12–24.
[51] J. HÅstad, R. Impagliazzo, L. A. Levin, and M. Luby, "A pseudorandom generator from any one-way function," *SIAM J. Comput.*, vol. 28, no. 4, pp. 1364–1396, 1999.
[52] C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy amplification by public discussion," *SIAM J. Comput.*, vol. 17, no. 2, pp. 210–229, Apr. 1988.
[53] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.
[54] K.-M. Chung and S. Vadhan, "Tight bounds for hashing block sources," in *Proc. 11th Int. Workshop, APPROX, 12th Int. Workshop, RANDOM Approximation, Randomization Combinat. Optim., Algorithms Techn.*, Boston, MA, USA. Berlin, Germany: Springer-Verlag, 2008, pp. 357–370, doi: 10.1007/978-3-540-85363-3_29.
[55] M. Tomamichel, R. Renner, C. Schaffner, and A. Smith, "Leftover hashing against quantum side information," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2010, pp. 2703–2707.
[56] C. Cachin, C. Crepeau, and J. Marcil, "Oblivious transfer with a memory-bounded receiver," in *Proc. 39th Annu. Symp. Found. Comput. Sci.*, Nov. 1998, pp. 493–502.
[57] J. Feng, Z. Ouyang, L. Xu, and B. Ramamurthy, "Packet reordering in high-speed networks and its impact on high-speed TCP variants," *Comput. Commun.*, vol. 32, no. 1, pp. 62–68, 2008.
[58] M. Janjić, "A generating function for numbers of insets," *J. Integer Sequences*, vol. 17, no. 14.9.7, pp. 1–9, Sep. 2014.
[59] J. Treadway and D. Rawlings, "Bernoulli trials and mahonian statistics: A tale of two q's," *Math. Mag.*, vol. 67, no. 5, pp. 345–354, Dec. 1994. [Online]. Available: http://www.jstor.org/stable/2690993
[60] R. L. Rivest, "Unconditionally secure commitment and oblivious transfer schemes using private channels and a trusted initializer," Dept. Elect. Eng. Comput. Sci., Lab. Comput. Sci., Massachusetts Inst. Technol., Cambridge, MA, USA, Tech. Rep., 1999.
[61] D. Wang, A. Mazumdar, and G. W. Wornell, "Compression in the space of permutations," *IEEE Trans. Inf. Theory*, vol. 61, no. 12, pp. 6417–6431, Dec. 2015.
[62] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics: A Foundation for Computer Science*, 2nd ed. Reading, MA, USA: Addison-Wesley, 1994.

VINICIUS DE MORAIS ALVES received the bachelor's and master's degrees from the University of Brasília (UnB), Brazil, where he is currently pursuing the Ph.D. degree with the Electrical Engineering Department. He is also a Public Servant working as a Cyber Security Team Leader in the Chamber of Deputies of Brazil.

RAFAEL DOWSLEY received the Ph.D. degree from Karlsruhe Institute of Technology, Germany. He is currently a Lecturer with the Department of Software Systems and Cybersecurity, Faculty of Information Technology, Monash University, Australia. His research interests include cryptography and its abundant intersections with fields, such as machine learning, security, privacy, and information theory.

RAFAEL TIMÓTEO DE SOUSA, JR. (Senior Member, IEEE) received the bachelor's degree in electrical engineering from the Federal University of Paraíba—UFPB, Campina Grande, Brazil, in 1984, the master's degree in computing and information systems from Ecole Supérieure d'Electricité—Supélec, Rennes, France, in 1985, and the Ph.D. degree in telecommunications and signal processing from the University of Rennes, Rennes, in 1988. He was a Visiting Researcher with the Group for Security of Information Systems and Networks (SSIR), Supélec, Rennes, from 2006 to 2007. He worked in the private sector, from 1988 to 1996. Since 1996, he has been a Network Engineering Associate Professor with the Electrical Engineering Department, University of Brasília—UnB, Brazil, where he is the Coordinator of the Professional Post-Graduate Program on Electrical Engineering (PPEE) and supervises the Decision Technologies Laboratory (LATITUDE). He is the Chair of the IEEE VTS Centro-Norte Brasil Chapter (IEEE VTS Chapter of the Year 2019) and IEEE Centro-Norte Brasil Blockchain Group. His professional experience includes research projects with Dell Computers, HP, IBM, Cisco, and Siemens. He has coordinated research, development, and technology transfer projects with the Brazilian Ministries of Planning, Economy, and Justice and with the Institutional Security Office of the Presidency of Brazil, the Administrative Council for Economic Defense, the General Attorney of the Union, and the Brazilian Union Public Defender. He has received research grants from the Brazilian research and innovation agencies CNPq, CAPES, FINEP, RNP, and FAPDF. He has developed research in cyber, information and network security, distributed data services and machine learning for intrusion and fraud detection, and signal processing, energy harvesting and security at the physical layer.

ANDERSON C. A. NASCIMENTO received the Ph.D. degree from the University of Tokyo, in 2004. He currently holds the endowed professorship in information systems and information security with the School of Engineering and Technology, University of Washington, Tacoma. Previously, he was a Professor with the University of Brasília, Brazil, and a Research Scientist with NTT Corporation, in Japan. He researches in cryptography and information security. He has edited four books, published over 100 papers in journals and conference proceedings. He has supervised over 20 master thesis and three Ph.D. thesis. He was an Editor of the *IET Information Security* journal and the Technical Program Chair or the General Chair of ISC 2016, ICITS 2016, SBSeg 2009, and SBSeg 2012. He was a Panelist and a Reviewer for the National Science Foundation, the European Science Foundation, CAPES, and CNPq.