

# On the Commitment Capacity of Unfair Noisy Channels

Claude Crépeau, Rafael Dowsley and Anderson C. A. Nascimento

**Abstract**—Noisy channels are a valuable resource from a cryptographic point of view. They can be used for exchanging secret-keys as well as realizing other cryptographic primitives such as commitment and oblivious transfer. To be really useful, noisy channels have to be considered in the scenario where a cheating party has some degree of control over the channel characteristics. Damgård et al. (EUROCRYPT 1999) proposed a more realistic model where such level of control is permitted to an adversary, the so called unfair noisy channels, and proved that they can be used to obtain commitment and oblivious transfer protocols. Given that noisy channels are a precious resource for cryptographic purposes, one important question is determining the optimal rate in which they can be used. The commitment capacity has already been determined for the cases of discrete memoryless channels and Gaussian channels. In this work we address the problem of determining the commitment capacity of unfair noisy channels. We compute a single-letter characterization of the commitment capacity of unfair noisy channels. In the case where an adversary has no control over the channel (the fair case) our capacity reduces to the well-known capacity of a discrete memoryless binary symmetric channel.

**Index Terms**—Commitment capacity, unconditionally secure cryptography, unfair noisy channels.

## I. INTRODUCTION

**Commitment protocols.** Consider the case of first-price sealed-bid auctions: the participants place their bids in sealed envelopes that are later on opened to determine the winner and how much he will pay. The sealed envelopes play a crucial role in this protocol since they protect the secrecy of each bid during the bidding process but at the same time they preclude the winner from changing his bid after the first phase. In the digital world, commitment protocols have a role similar to that of the sealed envelopes. They are cryptographic protocols involving two mutually distrustful parties, Alice and Bob. The idea of the protocol is very simple: in a first phase Alice commits to a value  $c$  by sending some information to Bob which commits her to  $c$  without revealing it. Later on, Alice can execute with Bob a second phase of the protocol in order to reveal the value  $c$ . From Alice's point of view the protocol should guarantee that after the first phase no information about  $c$  is leaked to Bob. From Bob's point of view the protocol

should guarantee that Alice cannot change her mind after the first phase, i.e., there is at most one value that Alice can successfully open in an eventual execution of the second phase.

Commitment was introduced by Blum [1] and is one of the most fundamental cryptographic protocols, widely used as sub-protocol in applications such as secure multi-party computation [2], [3], [4], contract signing [5] and zero-knowledge proofs [6], [7], [8]. In this work we are interested in commitment protocols that are information-theoretically secure, i.e., both security guarantees should hold even against (computationally) unbounded adversaries.

**Noise-based cryptography.** The potential of noisy channels for cryptographic purposes was first noticed by Wyner [9] who proposed a scheme for exchanging a secret-key in the presence of an eavesdropper (henceforth denote Eve). Wyner considered a model in which Eve receives the transmitted symbols over a degraded channel with respect to the legitimate receiver's channel. This possibility result was later extended to the class of general (non-degraded) broadcast channels by Csiszár and Körner [10]. Both models did not consider public communication. Maurer [11] proved that public communication can improve the parties' ability of generating a secret. Ahlswede and Csiszár [12] also improved the previous results.

In the case of commitment protocols, the first solution based on noisy channels was developed by Crépeau and Kilian [13]. The efficiency of the commitment protocols based on noisy channels was later improved by Crépeau [14].

In all these pioneering works, the case where an adversary can control the characteristics of the channel was not considered.

**Unfair noisy channels.** Damgård et al. [15] proposed a more realistic model, called unfair noisy channels (UNC), in which the error probability of the channel is not exactly known by the protocol participants and can be influenced by malicious parties. The honest parties only know that the crossover probability is between  $\gamma$  and  $\delta$  (for  $0 < \gamma < \delta < 1/2$ ), and an adversary can set the crossover probability to any value in this range. Damgård et al. [15] proved that using UNC with certain parameters it is possible to implement an information-theoretically secure commitment protocol.

Recently a variant of UNC known as elastic channel has been studied. On one hand, it has two restrictions with relation to UNC: (1) only a corrupt receiver can manipulate the crossover probability to any value in the range  $[\gamma; \delta]$ ; (2) when both parties are honest the crossover probability is always  $\delta$ . On the other hand, commitment (and even oblivious transfer) can be obtained for all parameters  $0 < \gamma < \delta < 1/2$  [16], [17].

Claude Crépeau is with the School of Computer Science, McGill University, Local 318, Pavillon McConnell, 3480 rue University Montréal (Québec), Canada H3A 2A7. Email: crepeau@cs.mcgill.ca

Rafael Dowsley is with the Department of Computer Science, Bar-Ilan University, Israel. Email: rafael@dowsley.net. He is supported by the BIU Center for Research in Applied Cryptography and Cyber Security in conjunction with the Israel National Cyber Bureau in the Prime Minister's Office.

Anderson C. A. Nascimento is with the Institute of Technology, University of Washington Tacoma, 1900 Commerce Street, Tacoma, WA 98402-3100, USA. E-mail: andclay@uw.edu.

**Commitment capacity.** Since noisy channels are valuable resources for cryptography, an important question is determining the optimal rate in which they can be used to implement the diverse cryptographic primitives. In the case of commitment this amounts to determining the optimal ratio between the length of the committed values and the number of uses of the noisy channel (i.e., the commitment capacity of the channel). This problem was first raised by Winter et al. [18], who also answered the question for the case of discrete memoryless channels. After that, the commitment capacity of Gaussian channels was obtained by Nascimento et al. [19]. The question of determining the optimal way of using noisy channels was also studied for other cryptographic tasks, for instance in the vast literature on secrecy capacity [9], [10], [20], [21], [11], [12], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33] and also in the works that deal with the oblivious transfer capacity [34], [35], [36], [37], [38].

Our contribution in this work is determining the commitment capacity of unfair noisy channels. The work is organized as follows. In section II we establish our notation and present some existing results that will be used thereafter. In section III, we introduce the model and the security definitions, and also state our main theorem. In section IV we prove the direct part of the theorem and in section V the converse. We finish with some concluding remarks in section VI.

## II. PRELIMINARIES

### A. Notation

We will denote by calligraphic letters the domains of random variables, by upper case letters the random variables and by lower case letters the realizations of the random variables. Other sets are also denoted by calligraphic letters and the cardinality of a set  $\mathcal{X}$  is denoted by  $|\mathcal{X}|$ . For a random variable  $X$  over  $\mathcal{X}$ , we denote its probability distribution by  $P_X : \mathcal{X} \rightarrow [0, 1]$  with  $\sum_{x \in \mathcal{X}} P_X(x) = 1$ . For a joint probability distribution  $P_{XY} : \mathcal{X} \times \mathcal{Y} \rightarrow [0, 1]$ , let  $P_X(x) := \sum_{y \in \mathcal{Y}} P_{XY}(x, y)$  denote the marginal probability distribution and let  $P_{X|Y}(x|y) := \frac{P_{XY}(x, y)}{P_Y(y)}$  denote the conditional probability distribution if  $P_Y(y) \neq 0$ . We write  $U_n$  for a random variable uniformly distributed over  $\{0, 1\}^n$ .

If an algorithm (or a function)  $f$  is randomized, we denote by  $f(x; r)$  the result of computing  $f$  on input  $x$  with randomness  $r$ . If  $a$  and  $b$  are two strings of bits of the same length, we denote by  $a \oplus b$  their bitwise XOR and by  $\text{HD}(a, b)$  their Hamming distance. The logarithm used in this paper are in base 2.

### B. Entropies

The binary entropy function of  $x$  is denoted by  $h(x) := -x \log x - (1 - x) \log(1 - x)$ . For finite alphabets  $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$  and random variables  $X \in \mathcal{X}, Y \in \mathcal{Y}, Z \in \mathcal{Z}$ , the entropy of  $X$  is denoted by  $H(X)$  and the mutual information between  $X$  and  $Y$  by  $I(X; Y)$ . The min-entropy is given by

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

Its conditional version is defined as

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

The max-entropy is defined as

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

and its conditional version is given by

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

The statistical distance between two probability distributions  $P_X$  and  $P_Y$  over the same domain  $\mathcal{V}$  is

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

For  $0 \leq \varepsilon < 1$  the  $\varepsilon$ -smooth versions of the above entropies are defined as

$$\begin{aligned} H_\infty^\varepsilon(X) &= \max_{X': \text{SD}(P_{X'}, P_X) \leq \varepsilon} H_\infty(X'), \\ H_\infty^\varepsilon(X|Y) &= \max_{X'Y': \text{SD}(P_{X'Y'}, P_{XY}) \leq \varepsilon} H_\infty(X'|Y'), \\ H_0^\varepsilon(X) &= \min_{X': \text{SD}(P_{X'}, P_X) \leq \varepsilon} H_0(X'), \\ H_0^\varepsilon(X|Y) &= \min_{X'Y': \text{SD}(P_{X'Y'}, P_{XY}) \leq \varepsilon} H_0(X'|Y'). \end{aligned}$$

We will need the chain rules for smooth entropies conditioned on an additional random variable  $Z$  [39]:

$$\begin{aligned} H_\infty^{\varepsilon+\varepsilon'}(XY|Z) - H_\infty^{\varepsilon'}(Y|Z) &\geq H_\infty^\varepsilon(X|YZ) \\ &\geq H_\infty^{\varepsilon_1}(XY|Z) - H_\infty^{\varepsilon_2}(Y|Z) - \log(1/(\varepsilon - \varepsilon_1 - \varepsilon_2)) \end{aligned}$$

and

$$\begin{aligned} H_0^{\varepsilon+\varepsilon'}(XY|Z) - H_0^{\varepsilon'}(Y|Z) &\leq H_0^\varepsilon(X|YZ) \\ &\leq H_0^{\varepsilon_1}(XY|Z) - H_0^{\varepsilon_2}(Y|Z) + \log(1/(\varepsilon - \varepsilon_1 - \varepsilon_2)). \end{aligned}$$

### C. Strong Extractors and the Leftover-Hash Lemma

In the direct part of our proof we will use strong randomness extractors, therefore we present here the relevant definitions and properties.

*Definition 2.1 (Strong Randomness Extractors [40], [41]):* Let  $\text{Ext} : \{0, 1\}^n \rightarrow \{0, 1\}^\ell$  be a probabilistic polynomial time function which uses  $r$  bits of randomness. We say that  $\text{Ext}$  is an efficient  $(n, m, \ell, \varepsilon)$ -strong extractor if for all probability distributions  $P_W$  with  $\mathcal{W} = \{0, 1\}^n$  and such that  $H_\infty(W) \geq m$ , for random variables  $R$  uniformly distributed in the bit-strings of length  $r$  and  $L$  uniformly distributed in the bit-strings of length  $\ell$ , we have that  $\text{SD}(P_{\text{Ext}(W; R), R}, P_{L, R}) \leq \varepsilon$ . Strong extractors can extract at most  $\ell = m - 2 \log(\varepsilon^{-1}) + O(1)$  bits of nearly random bits [42] and this optimal bound is achieved by universal hash functions [43].

*Definition 2.2 ( $t$ -Universal Hash Functions):* A class  $\mathcal{G}$  of functions  $\mathcal{A} \rightarrow \mathcal{B}$  is  $t$ -universal if, for any distinct  $x_1, \dots, x_t \in \mathcal{A}$ , when  $g$  is chosen uniformly at random from  $\mathcal{G}$ , the induced distribution on  $(g(x_1), \dots, g(x_t))$  is uniform over  $\mathcal{B}^t$ .

The leftover-hash lemma (similarly the privacy-amplification lemma) [44], [45], [46], [47], [41] guarantees

that universal hash functions can be used to extract  $\ell = m - 2 \log(\varepsilon^{-1}) + 2$  nearly random bits.

*Lemma 2.3 (Leftover-hash lemma):* Assume that a class  $\mathcal{G}$  of functions  $G : \{0, 1\}^n \rightarrow \{0, 1\}^\ell$  is 2-universal. Then for  $G$  selected uniformly at random from  $\mathcal{G}$  we have that

$$\text{SD}(P_{G(W), G}, P_{U_\ell, G}) \leq \frac{1}{2} \sqrt{2^{-H_\infty(W)} 2^\ell}.$$

In particular, universal hash functions are  $(n, m, \ell, \varepsilon)$ -strong extractors whenever  $\ell \leq m - 2 \log(\varepsilon^{-1}) + 2$ .

The following lemma by Rompel will be also useful.

*Lemma 2.4 ([48]):* Suppose  $t$  is a positive even integer,  $X_1, \dots, X_u$  are  $t$ -wise independent random variables taking values in the range  $[0, 1]$ ,  $X = \sum_{i=1}^u X_i$ ,  $\mu = E[X]$ , and  $A > 0$ . Then

$$\Pr[|X - \mu| > A] < O\left(\left(\frac{t\mu + t^2}{A^2}\right)^{t/2}\right).$$

### III. PROBLEM STATEMENT

#### A. Unfair Noisy Channels

Since commitment protocols that are information-theoretically secure cannot be implemented from scratch, the efforts were focused on obtaining such protocols based on physical assumptions. One of these assumptions is the existence of noisy channels that can be used by the parties. Binary symmetric channels are known to allow the implementation of commitment schemes [13], [14]. But these protocols have the disadvantage that they rely on the assumption that a malicious party do not interfere with the channel to try to modify its error probability.

Damgård et al. [15] introduced a more realistic assumption, namely unfair noisy channels, that is a modification of the binary symmetric channel. In this model, a channel is specified by two parameters:  $\gamma$  and  $\delta$  (with  $0 < \gamma < \delta < \frac{1}{2}$ ); and the channel is denoted as  $(\gamma, \delta)$ -UNC. The error probability of the channel is guaranteed to fall into the interval  $[\gamma, \delta]$ , but is not known by the honest parties. Therefore any protocol based on a  $(\gamma, \delta)$ -UNC should work for any error probability in the range  $[\gamma, \delta]$ . On the other hand, a malicious party can set the error probability to any value in the range  $[\gamma, \delta]$ .

*Definition 3.1 (Unfair Noisy Channels):* The  $(\gamma, \delta)$ -UNC receives as input a bit  $X$  and outputs a bit  $Y$ . The transition probability of the  $(\gamma, \delta)$ -UNC is determined by an auxiliary parameter  $T$  whose alphabet are the real numbers in the interval  $[\gamma, \delta]$ . If the transmitter or the receiver is malicious, he can choose the value of  $T$ ; otherwise it is randomly chosen and is not revealed to the parties. The transition probability is given by  $P_{Y|XT}(y, x, t) = 1 - t$  if  $y = x$  and  $P_{Y|XS}(y, x, t) = t$  if  $y \neq x$ .

Damgård et al. [15] proved that, on one hand, if  $\delta \geq 2\gamma(1 - \gamma)$  then the  $(\gamma, \delta)$ -UNC is trivial (i.e., secure commitment protocols cannot be based on this channel). On the other hand, if  $\delta < 2\gamma(1 - \gamma)$  then there is a commitment protocol based on the  $(\gamma, \delta)$ -UNC.

*Remark:* Note that a  $(\gamma, \delta)$ -UNC can equivalently be seen as the concatenation of two binary symmetric channels,  $W_f$  with error probability  $\gamma$  and  $W_v$  with error probability  $\theta$  for

$0 \leq \theta \leq \frac{\delta - \gamma}{1 - 2\gamma}$ . The error probability of the channel  $W_v$  can be controlled by a malicious party and it is unknown in the case that both parties are honest.

*Definition 3.2:* We say that two strings  $x^n$  and  $y^n$  are  $\epsilon$ -compatible with an  $(\gamma, \delta)$ -Unfair Noisy Channel if, for  $\epsilon > 0$ , the Hamming distance (HD) of  $x^n$  and  $y^n$  is at most  $\delta n + \epsilon$ . Similarly, two random variables  $X^n$  and  $Y^n$  are said to be compatible with an  $(\gamma, \delta)$ -Unfair Noisy Channel if  $\Pr[\text{HD}(X^n, Y^n) > \delta n]$  is negligible in  $n$ .

#### B. Commitment Capacity

Since  $(\gamma, \delta)$ -UNC are valuable resources, one would like to use them in the most efficient way. Hence the important question of determining the commitment capacity of these channels arises. Our goal in this work is to determine the commitment capacity of unfair noisy channels in the same way that Winter et al. [18] did for the discrete memoryless channels and Nascimento et al. [19] did for the Gaussian channels. Let us begin by defining the concept of commitment protocols and recalling its security notions.

A commitment protocol has two phases: called commitment and opening. There are two parties involved in the protocol: the committer (also denoted Alice) and the verifier (also denoted Bob). The protocol works as follows. In the commitment phase, Alice commits to a value  $c$ , but without revealing anything about it to Bob. Later on, Alice can execute the opening phase to disclose the value  $c$  to Bob. The security guarantee that Alice expects from the protocol is that nothing about  $c$  should be learned by Bob in the first phase, while the security guarantee that Bob expects is that Alice should not be able to change the value committed to after the first phase. We proceed with a more detailed description of these definitions and of the resources available to the parties in our model.

Alice and Bob have two channels available between them:

- a bidirectional authenticated noiseless channel, and
- $(\gamma, \delta)$ -UNC from Alice to Bob

Note that this model allows multiple uses of the  $(\gamma, \delta)$ -UNC within a protocol in an interactive manner. Let  $n$  denote the number of times that the parties use the  $(\gamma, \delta)$ -UNC channel.

*a) Commitment Protocol:* A commitment protocol is a family of protocols indexed by the security parameter  $n$ . Each protocol uses the  $(\gamma, \delta)$ -UNC  $n$  times and proceeds in two phases as described below. For the sake of simplicity in the notation we will not explicitly mention the dependence on the security parameter. Both parties have access to local randomness. Note that all the messages generated by Alice and Bob are well-defined random variables, depending on the value that Alice wants to commit to,  $c$ , and the local randomness of the parties. As usual, we assume that the noiseless messages exchanged by the players and their personal randomness are taken from  $\{0, 1\}^*$ .

*b) Commitment Phase:* Alice has an input  $c$  (from the message space  $\mathcal{C}$ ) that she wants to commit to. There are  $n$  rounds of communication through the  $(\gamma, \delta)$ -UNC and in each of these rounds Alice inputs a symbol  $x_i$  to the  $(\gamma, \delta)$ -UNC and an output  $y_i$  is delivered to Bob. Let  $X^n$  be the random variable denoting the bitstring sent through the  $(\gamma, \delta)$ -UNC

and  $Y^n$  the bitstring received through the  $(\gamma, \delta)$ -UNC. The parties can use the bidirectional authenticated noiseless channel at any time, with the messages possibly depending on  $X^n$ ,  $C$  and the local randomness. Let  $M$  be the random variable denoting all the noiseless messages exchanged between the players,

*c) Opening Phase:* The parties only exchange messages over the noiseless channel. Alice announces the value  $\hat{c}$  and the bitstring  $\hat{x}^n$  that she claims that she used during the first phase. Finally Bob executes a test  $\beta(\hat{x}^n, y^n, m, \hat{c})$  in order to decide if he accepts the value  $\hat{c}$  or not.

We call Bob's view all the data in his possession after the completion of the commitment phase and denote it by  $view_B$ .

A commitment protocol is  $\epsilon$ -*sound* if for honest Alice and Bob executing the protocol and for all  $c \in \mathcal{C}$  and for any  $X^n$  compatible with  $Y^n$  for the  $(\gamma, \delta)$ -UNC,

$$\Pr[\beta(X^n, Y^n, M, c) = \text{accept}] \geq 1 - \epsilon.$$

A commitment protocol is  $\epsilon$ -*concealing* if for any possible behavior of Bob in the commitment phase,

$$I(C; View_B) \leq \epsilon.$$

A protocol is  $\epsilon$ -*binding*, if for all  $\tilde{c}, \bar{c} \in \mathcal{C}$  such that  $\tilde{c} \neq \bar{c}$  and for any strategy of (a dishonest) Alice to pick the random variable  $X^n$  that is sent through the  $(\gamma, \delta)$ -UNC channel, and the random variables  $\tilde{X}^n$  and  $\bar{X}^n$  that are presented during the opening phase

$$\Pr \left[ \begin{array}{l} \beta(\tilde{X}^n, Y^n, M, \tilde{c}) = \text{accept} \ \& \ \\ \beta(\bar{X}^n, Y^n, M, \bar{c}) = \text{accept} \end{array} \right] \leq \epsilon.$$

We call a commitment protocol *secure* if there exists a function  $\epsilon$  that is negligible in the security parameter  $n$  and is such that the protocol is  $\epsilon$ -*sound*,  $\epsilon$ -*concealing* and  $\epsilon$ -*binding*.<sup>1</sup>

*Remark:* We restrict our model to protocols where the public conversation  $M$  does not depend on the channel output  $Y^n$  given  $X^n$ , that is  $I(M; Y^n | X^n) = 0$ . This is indeed the case for all the protocols in the literature. Moreover, the public communication is used solely to prevent Alice from cheating, thus we see no reason for a commitment protocol based on noisy channels to have its public communication depending on the channel output for a given input  $X^n$ .

The *commitment rate* of the protocol is given by

$$R_C = \frac{\log |\mathcal{C}|}{n}.$$

A commitment rate is said to be achievable if there exists a secure commitment protocol that achieves this rate. The *commitment capacity* of a  $(\gamma, \delta)$ -UNC is the supremum of the achievable rates.

Our main result is presented below and states the commitment capacity of the  $(\gamma, \delta)$ -UNC. The proof appears in sections IV and V.

<sup>1</sup>For easy of presentation the security of the constructions is argued in the stand-alone model (as usual in cryptography) in which case there is only one execution of the protocol. But the security of the commitment protocols based on noisy channels can be extended to the UC framework [49] in which the protocols can be composed and arbitrary protocols can be executed in parallel [50], [51].

*Theorem 3.3:* The commitment capacity of any non-trivial  $(\gamma, \delta)$ -Unfair Noisy Channel is given by

$$h(\gamma) - h(\theta), \text{ for } \theta = \frac{\delta - \gamma}{1 - 2\gamma}.$$

#### IV. PROTOCOL - DIRECT PART

We first prove the direct part of the theorem, i.e., we describe the protocol that achieves the commitment capacity and prove its security. The protocol follows the approach of Damgård et al. [15] and uses two rounds of hash challenge-response in order to guarantee the binding property: the intuition is that the first round reduces the number of inputs that Alice can successfully open to be polynomial in the security parameter. The second round then binds Alice to one specific input. The concealing condition is achieved using a 2-universal hash function Ext chosen by Alice that is used to generate a secure key which is then applied as a one-time pad to cipher  $c$ .

Let  $\theta = \frac{\delta - \gamma}{1 - 2\gamma}$  and let  $\nu > 0$  be a parameter of the protocol. Let  $\alpha_1, \alpha_2, \beta$  be parameters such that  $\alpha_1, \alpha_2 > 0$ ,  $\beta > \alpha_1 + \alpha_2$ , and  $n(h(\theta) + \alpha_1)$ ,  $n\alpha_2$  and  $n(h(\gamma) - h(\theta) - \beta)$  are integers. In the following commitment protocol the message space is  $\mathcal{C} = \{0, 1\}^{n(h(\gamma) - h(\theta) - \beta)}$ .

*Commitment Phase:* Alice wants to commit to the binary string  $c \in \mathcal{C}$ . The parties proceed as follows:

- 1) Alice chooses a random binary string  $x^n = (x_1, \dots, x_n)$  of dimension  $n$  and for  $1 \leq i \leq n$  sends the bit  $x_i$  to Bob over the  $(\gamma, \delta)$ -UNC.
- 2) Bob receives the string  $y^n = (y_1, \dots, y_n)$  sent over the  $(\gamma, \delta)$ -UNC, chooses uniformly at random a function  $g_1$  of the class of  $4n$ -universal hash functions  $\mathcal{G}_1 : \{0, 1\}^n \rightarrow \{0, 1\}^{n(h(\theta) + \alpha_1)}$ , and sends the description of  $g_1$  to Alice over the noiseless channel.
- 3) Alice computes  $e_1 = g_1(x^n)$  and sends it to Bob.
- 4) Bob chooses uniformly at random a function  $g_2$  of the class of 2-universal hash functions  $\mathcal{G}_2 : \{0, 1\}^n \rightarrow \{0, 1\}^{n\alpha_2}$ , and sends its description to Alice over the noiseless channel.
- 5) Alice chooses uniformly at random a function Ext :  $\{0, 1\}^n \rightarrow \{0, 1\}^{n(h(\gamma) - h(\theta) - \beta)}$  of the class of two-universal hash functions, computes  $d = c \oplus \text{Ext}(x^n)$  and  $e_2 = g_2(x^n)$ , and sends  $d$ ,  $e_2$  and the description of Ext to Bob over the noiseless channel.

*Opening Phase:* Alice wants to reveal the value of  $c$  to Bob. The parties proceed as follow:

- 1) Alice sends to Bob over the noiseless channel the values  $x^n$  and  $c$ .
- 2) Bob checks if  $\gamma n - \nu n \leq \text{HD}(x^n, y^n) \leq \delta n + \nu n$ , if  $g_1(x^n) = e_1$ ,  $g_2(x^n) = e_2$  and if  $c = \text{Ext}(x^n) \oplus d$ . Bob accepts if there are no problems in the tests.

*Theorem 4.1:* The protocol is secure and can achieve the commitment rate  $h(\gamma) - h(\theta) - \beta$  for any  $h(\gamma) - h(\theta) > \beta > 0$  and  $n$  sufficiently large.

**Proof:** We proof that the protocol is binding, concealing and sound, and furthermore achieves the desired commitment rate.

a) *Soundness*: The protocol fails for honest Alice and Bob only if  $\text{HD}(x^n, y^n) > \delta n + \nu n$  or  $\text{HD}(x^n, y^n) < \gamma n - \nu n$ . We have that the expectation of  $\text{HD}(x^n, y^n)$  is less than or equal to  $\delta n$ , because the  $(\gamma, \delta)$ -UNC has error probability less than or equal to  $\delta$ . So the Chernoff bound guarantees that the probability that  $\text{HD}(x^n, y^n) > \delta n + \nu n$  is a negligible function of  $n$ . Similarly we can prove that the probability that  $\text{HD}(x^n, y^n) < \gamma n - \nu n$  is a negligible function of  $n$ .

b) *Concealment*: For any  $\eta > 0$  and  $n$  sufficiently large, we have that

$$\begin{aligned}
& H_\infty^\varepsilon(X^n | G_1(X^n), G_2(X^n), Y^n, G_1, G_2) \geq \\
& \geq H_\infty(X^n, G_1(X^n), G_2(X^n) | Y^n, G_1, G_2) \\
& \quad - H_0(G_1(X^n), G_2(X^n) | Y^n, G_1, G_2) - \log(\varepsilon^{-1}) \\
& = H_\infty(X^n | Y^n, G_1, G_2) \\
& \quad - H_0(G_1(X^n), G_2(X^n) | Y^n, G_1, G_2) - \log(\varepsilon^{-1}) \\
& = H_\infty(X^n | Y^n) \\
& \quad - H_0(G_1(X^n), G_2(X^n) | Y^n, G_1, G_2) - \log(\varepsilon^{-1}) \\
& \geq n(h(\gamma) - \eta) - n(h(\theta) + \alpha_1 + \alpha_2) - \log(\varepsilon^{-1}) \\
& = n(h(\gamma) - h(\theta) - \eta - \alpha_1 - \alpha_2) - \log(\varepsilon^{-1})
\end{aligned}$$

where the first inequality follows from the chain rule for smooth entropy, the first equality from the fact that  $G_1(X^n), G_2(X^n)$  are functions of  $G_1, G_2$  and  $X^n$ , the second equality from the fact that  $X^n$  is independent of  $G_1, G_2$  given  $Y^n$  and the last inequality follows from the facts that the error probability of the channel is at least  $\gamma$ , the range of  $G_1$  has cardinality  $2^{n(h(\theta)+\alpha_1)}$  and the range of  $G_2$  has cardinality  $2^{n\alpha_2}$ .

Setting  $\varepsilon = 2^{-\kappa n}$  (with  $\kappa > 0$ ), for  $n$  sufficiently large, the security of the key obtained by applying the hash function  $\text{Ext} : \{0, 1\}^n \rightarrow \{0, 1\}^{n(h(\gamma)-h(\theta)-\beta)}$  to  $x$  follows from the leftover-hash lemma since  $\beta > \alpha_1 + \alpha_2$  and  $\kappa$  and  $\eta$  can be arbitrarily small for  $n$  sufficiently large. Note that having a negligible statistical distance is equivalent to having a negligible mutual information [52].

c) *Binding*: A dishonest Alice can cheat successfully only if she finds two different strings  $\bar{x}^n$  and  $\tilde{x}^n$  such that  $\gamma n - \nu n \leq \text{HD}(\bar{x}^n, y^n) \leq \delta n + \nu n$ ,  $\gamma n - \nu n \leq \text{HD}(\tilde{x}^n, y^n) \leq \delta n + \nu n$ , and both pass the sequentially performed hash challenge-response tests, for arbitrarily small  $\nu$  and sufficiently large  $n$ . We can assume without loss of generality that Alice sets the error probability of the channel to  $\gamma$  when she sends  $x^n$ . In the typicality test an honest Bob accepts any string that is jointly typical with  $y^n$  for any error probability  $\gamma \leq \rho \leq \delta$ . So Alice can cheat only if she finds two strings  $\bar{x}^n$  and  $\tilde{x}^n$  so that both pass the hash tests and are jointly typical with  $x^n$  for binary symmetric channels with error probabilities  $0 \leq \bar{\tau} \leq \theta$  and  $0 \leq \tilde{\tau} \leq \theta$ . The number of such jointly typical strings is upper bounded by  $2^{n(h(\theta)+\varepsilon')}$  for any  $\varepsilon' > 0$  and  $n$  sufficiently large. We fix  $\alpha_1 > \varepsilon'$ .

Let the viable set denote the channel inputs that Alice can possibly open to Bob and he would accept. If there were no

hash checks, the viable set would have at most  $2^{n(h(\theta)+\varepsilon')}$  elements. Lets consider this initial viable set. The goal of the first round of hash challenge-response is to, with overwhelming probability, reduce the number of elements of the viable set to at most  $8n + 1$ . In this first round, Alice has to commit to one arbitrary value  $e_1$  for the output of the hash function  $g_1$ . Considering the  $j$ -th viable string before this first round, we define  $I_j$  as 1 if that string is mapped to  $e_1$  by  $g_1$ ; and  $I_j = 0$  otherwise. Let  $I = \sum_j I_j$ . Clearly  $\mu = E[I] < 1$  as  $\alpha_1 > \varepsilon'$ . Let  $e_1$  be considered bad if  $I$  is bigger than  $8n + 1$ . Given that  $g_1$  is  $4n$ -wise independent, by applying Lemma 2.4 with  $t = 4n$  and  $A = 2t = 8n$ , we get

$$\begin{aligned}
\Pr[I > 8n + 1] & < O\left(\left(\frac{t\mu + t^2}{(2t)^2}\right)^{t/2}\right) \\
& < O\left(\left(\frac{1+t}{4t}\right)^{t/2}\right) \\
& < O\left(2^{-t/2}\right).
\end{aligned}$$

Then the probability that any  $e_1$  is bad is upper bounded by

$$O\left(2^{n(h(\theta)+\alpha_1)} 2^{-t/2}\right) < O\left(2^{-n}\right).$$

But if the viable set contains at most  $8n + 1$  elements after the first hash challenge-response round, the probability that some of those collide in the second hash challenge-response round is upper bounded by

$$(8n + 1)^2 2^{-\alpha_2 n},$$

which is negligible in  $n$ .

d) *Commitment Rate*: For  $n$  sufficiently large,  $\alpha_1$  and  $\alpha_2$  can be made arbitrarily small, and thus  $\beta$  can also be made arbitrarily small while preserving the security of the protocol. Therefore it is possible to achieve the commitment rate  $h(\gamma) - h(\theta) - \beta$  for any  $h(\gamma) - h(\theta) > \beta > 0$ . ■

## V. CONVERSE

For proving the converse, we will assume a specific cheating behavior for Alice. As we are interested in proving an upper bound in the commitment capacity, restricting Alice's behavior will only strength our result. Let  $k = \log|\mathcal{C}|$  and  $C$  be uniformly random over  $\mathcal{C}$ . Let  $X^n$  be a random variable representing the data Alice inputs into the unfair noisy channel. Assume, Alice sets the noise level of the unfair noisy channel connecting her to Bob to  $\gamma$ . Let  $Y^n$  be a random variable obtained by passing  $X^n$  through the unfair noisy channel (Channel 1). Let  $Z^n$  be a random variable obtained by passing  $X^n$  through a binary symmetric channel with error probability equal to  $\theta$  with  $0 \leq \theta \leq \frac{\delta-\gamma}{1-2\gamma}$  (Channel 2). Denote the conversation over the public authenticated and noiseless channel by  $M$ .

In the case of commitments based on fair noisy channels, it was proved in [18] that after the commit phase is finished, if Bob is presented with Alice's inputs to the channel,  $X^n$ , he is able to obtain almost complete knowledge on the committed

value  $C$ . Here we will prove that in the case of unfair noisy channels if Bob is presented with a noisy version of  $X^n$  he is still able to compute the committed value  $C$  with high probability.

*Lemma 5.1:*  $H(C|Z^n M) \leq 1 + kp$  for  $p$  negligible in  $n$ .

**Proof:** Let  $C, X^n, Y^n, Z^n$  and  $M$  be defined as above. We first give a procedure so that the commitment  $C$  can be estimated with high probability from  $Z^n, Y^n$  and  $M$ .

The procedure is as follows: given  $Z^n, Y^n$  and  $M$ , compute the value  $c$  that maximizes  $\Pr[\beta(Z^n, Y^n, M, c) = \text{accept}]$ , breaking ties in an arbitrary way. Because of the bindingness condition, we know that no two different values of  $c$  will be accepted with high probability

$$\Pr \left[ \begin{array}{l} \beta(\tilde{X}^n, Y^n, M, \tilde{c}) = \text{accept} \ \& \\ \beta(\bar{X}^n, Y^n, M, \bar{c}) = \text{accept} \end{array} \right] \leq \epsilon$$

for all  $\tilde{X}^n$  and  $\bar{X}^n$  compatible with  $Y^n$ .

Moreover, from the correctness property of the protocol and from the fact that  $Z^n$  and  $Y^n$  are compatible for the unfair noisy channel in question, we know that for the correct value  $c$  we have

$$\Pr[\beta(Z^n, Y^n, M, c) = \text{accept}] \geq 1 - \epsilon.$$

Thus, with high probability this procedure will give us the right committed value  $c$ . Let  $p$  be the probability that this procedure returns a wrong value. Using Fano's inequality we get

$$\begin{aligned} H(C|Z^n Y^n M) &\leq h(p) + p \log |C| \\ &\leq 1 + p \log |C| \\ &\leq 1 + kp. \end{aligned}$$

One can prove that the output of the channel  $Y^n$  is not needed in the above described procedure. The intuition is that  $Z^n$  is a "less noisy" version of  $X^n$  and thus can be used (instead of  $Y^n$ ) for retrieving the value of the commitment. In order to formalize this result, we need to use the assumed independence of the public conversation  $M$  and  $Y^n$  given  $X^n$ , i.e.,  $I(M; Y^n | X^n) = 0$ . First, we pass (or simulate the passing of)  $Z^n$  through a binary symmetric channel with error probability  $\gamma$ . Denote the output of the simulated channel by  $\tilde{Y}^n$ . Note that  $\tilde{Y}^n$  and  $X^n$  are compatible. Moreover, given the fact that the public conversation is independent of  $Y^n$  given  $X^n$ , we have that the public communication of the protocol using Channel 1 ( $M, C, X^n$  and  $\tilde{Y}^n$  are a valid transcript of a commitment protocol (the correctness, binding and concealing properties should apply). Thus, one has from the correctness property that

$$\Pr[\beta(Z^n, \tilde{Y}^n, M, c) = \text{accept}] \geq 1 - \epsilon.$$

From bindingness we have that

$$\Pr \left[ \begin{array}{l} \beta(\tilde{X}^n, \tilde{Y}^n, M, \tilde{c}) = \text{accept} \ \& \\ \beta(\bar{X}^n, \tilde{Y}^n, M, \bar{c}) = \text{accept} \end{array} \right] \leq \epsilon$$

for all  $\tilde{X}^n$  and  $\bar{X}^n$  compatible with  $\tilde{Y}^n$ .

Again, using Fano's inequality we get

$$\begin{aligned} H(C|Z^n \tilde{Y}^n M) &\leq h(p) + p \log |C| \\ &\leq 1 + p \log |C| \\ &\leq 1 + kp. \end{aligned}$$

Because the Markov chain  $CX^n \leftrightarrow Z^n \leftrightarrow \tilde{Y}^n$  holds, we have that  $H(C|Z^n \tilde{Y}^n M) = H(C|Z^n M)$ , which proves our result.

■

We have that

$$\begin{aligned} k &\leq H(C|Y^n M) + \epsilon & (1) \\ &= H(C|Y^n M) - H(C|Z^n M) + H(C|Z^n M) + \epsilon \\ &\leq H(C|Y^n M) - H(C|Z^n M) + 1 + kp + \epsilon & (2) \\ &= H(C|Y^n M) - H(C|Z^n M) - H(C|M) + H(C|M) \\ &\quad + 1 + kp + \epsilon \\ &= I(C; Z^n | M) - I(C; Y^n | M) + 1 + kp + \epsilon \end{aligned}$$

where inequality 1 comes from the  $\epsilon$ -concealing requirement and inequality 2 from the previous lemma.

Now we develop the expression  $I(C; Z^n | M) - I(C; Y^n | M)$  using the same steps used on the Section V of the seminal work of Csiszár and Körner [10]; the details are included for the sake of completeness. Let  $Z^i$  denote  $Z_1 \dots Z_i$  and  $\hat{Y}^i$  denote  $Y_i \dots Y_n$ . We expand  $I(C; Z^n | M)$  starting from  $I(C; Z_1 | M)$  and  $I(C; Y^n | M)$  starting from  $I(C; Y_n | M)$

$$\begin{aligned} I(C; Z^n | M) &= \sum_{i=1}^n I(C; Z_i | M Z^{i-1}) \\ &= \sum_{i=1}^n \left[ H(Z_i | M Z^{i-1}) - H(Z_i | M Z^{i-1} C) \right. \\ &\quad \left. - H(Z_i | M Z^{i-1} C \hat{Y}^{i+1}) \right. \\ &\quad \left. + H(Z_i | M Z^{i-1} C \hat{Y}^{i+1}) \right] \\ &= \sum_{i=1}^n \left[ I(C \hat{Y}^{i+1}; Z_i | M Z^{i-1}) \right. \\ &\quad \left. - I(\hat{Y}^{i+1}; Z_i | M Z^{i-1} C) \right] \\ &= \sum_{i=1}^n \left[ I(C; Z_i | M Z^{i-1} \hat{Y}^{i+1}) \right. \\ &\quad \left. + I(\hat{Y}^{i+1}; Z_i | M Z^{i-1}) \right. \\ &\quad \left. - I(\hat{Y}^{i+1}; Z_i | M Z^{i-1} C) \right]. \end{aligned}$$

Similarly we obtain

$$\begin{aligned} I(C; Y^n | M) &= \sum_{i=1}^n \left[ I(C; Y_i | MZ^{i-1} \hat{Y}^{i+1}) \right. \\ &\quad \left. + I(Z^{i-1}; Y_i | M\hat{Y}^{i+1}) \right. \\ &\quad \left. - I(Z^{i-1}; Y_i | M\hat{Y}^{i+1} C) \right]. \end{aligned}$$

We have that

$$\begin{aligned} \sum_{i=1}^n I(\hat{Y}^{i+1}; Z_i | MZ^{i-1}) &= \sum_{i=1}^n \sum_{j=i+1}^n I(Y_j; Z_i | MZ^{i-1} \hat{Y}^{j+1}) \\ &= \sum_{j=2}^n \sum_{i=1}^{j-1} I(Y_j; Z_i | MZ^{i-1} \hat{Y}^{j+1}) \\ &= \sum_{j=1}^n I(Z^{j-1}; Y_j | M\hat{Y}^{j+1}). \end{aligned}$$

Similarly we can get that

$$\sum_{i=1}^n I(\hat{Y}^{i+1}; Z_i | MZ^{i-1} C) = \sum_{j=1}^n I(Z^{j-1}; Y_j | M\hat{Y}^{j+1} C).$$

Therefore

$$\begin{aligned} I(C; Z^n | M) - I(C; Y^n | M) &= \sum_{i=1}^n \left[ I(C; Z_i | MZ^{i-1} \hat{Y}^{i+1}) \right. \\ &\quad \left. - I(C; Y_i | MZ^{i-1} \hat{Y}^{i+1}) \right]. \end{aligned}$$

Letting  $L$  be a random variable uniformly distributed in  $\{1, \dots, n\}$  and independent of  $CMX^nY^nZ^n$ , and setting  $U \triangleq MZ^{L-1}\hat{Y}^{L+1}L$ ,  $V \triangleq UC$ ,  $X \triangleq X_L$ ,  $Y \triangleq Y_L$  and  $Z \triangleq Z_L$  we get that  $U \leftrightarrow V \leftrightarrow X \leftrightarrow YZ$  form a Markov chain and

$$\begin{aligned} \frac{1}{n} \sum_{i=1}^n \left[ I(C; Z_i | MZ^{i-1} \hat{Y}^{i+1}) - I(C; Y_i | MZ^{i-1} \hat{Y}^{i+1}) \right] &= \\ &= I(C; Z | U) - I(C; Y | U) \\ &= I(V; Z | U) - I(V; Y | U). \end{aligned}$$

Putting everything together, for any secure commitment protocol, there are  $U \leftrightarrow V \leftrightarrow X \leftrightarrow YZ$  such that

$$\frac{k}{n} \leq I(V; Z | U) - I(V; Y | U) + \epsilon' \quad (3)$$

where  $\epsilon' = \frac{1+kp+\epsilon}{n}$  goes to 0 for  $n$  sufficiently large.

We now set  $\theta = \frac{\delta-\gamma}{1-2\gamma}$ . In our case channel 2 is less noisy than channel 1, therefore maximizing over all  $U \leftrightarrow V \leftrightarrow X \leftrightarrow YZ$  we get

$$\begin{aligned} I(V; Z | U) - I(V; Y | U) &= I(V; Z) - I(V; Y) \\ &\quad - [I(U; Z) - I(U; Y)] \\ &= I(X; Z) - I(X; Y) \\ &\quad - [I(X; Z | V) - I(X; Y | V)] \\ &\quad - [I(U; Z) - I(U; Y)] \\ &\leq I(X; Z) - I(X; Y) \quad (4) \\ &\leq h(\gamma) - h(\theta) \quad (5) \end{aligned}$$

where inequality 4 comes from the fact that both expressions in the brackets are non-negative since channel 2 is less noisy than channel 1 and inequality 5 follows taking the maximum over  $X$ . Hence

$$\frac{k}{n} \leq h(\gamma) - h(\theta) + \epsilon'$$

where  $\epsilon'$  goes to 0 for  $n$  sufficiently large. This completes the proof of the converse.

## VI. FINAL REMARKS

In this paper we obtained the commitment capacity of the unfair noisy channels. A similar notion of capacity for oblivious transfer was defined in [34]. We state as an open problem to obtain the oblivious transfer capacity of unfair noisy channels. Another open question is to derive the commitment capacity of weak channels [53]. In the case of elastic channels, for commitments from Alice to Bob, the channel is essentially degraded to a binary symmetric channel with crossover probability  $\gamma$  and therefore the commitment capacity is  $h(\gamma)$ . On the other hand, we conjecture that the commitment capacity for commitments from Bob to Alice is  $h(\delta) - h(\theta)$  for  $\theta = \frac{\delta-\gamma}{1-2\gamma}$ . However, if either of the two restrictions of the elastic channels in relation to unfair noisy channels is discarded (i.e., only the receiver being able to set the crossover probability; and the crossover probability being fixed to  $\delta$  when both parties are honest), then we get back to the same commitment capacity as for the unfair noisy channels.

Finally, we need in our proof to assume that  $I(M; Y^n | X^n) = 0$ , that is, the public communication and the channel outputs are independent given the channel inputs. While that is a natural condition respected by all the protocols that exist, we believe that, ultimately, a more general proof that does not depend on this restriction is possible. We leave such a proof as a future research problem.

## REFERENCES

- [1] M. Blum, "Coin flipping by telephone a protocol for solving impossible problems," *SIGACT News*, vol. 15, no. 1, pp. 23–27, Jan. 1983. [Online]. Available: <http://doi.acm.org/10.1145/1008908.1008911>
- [2] O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game or A completeness theorem for protocols with honest majority," in *19th Annual ACM Symposium on Theory of Computing*, A. Aho, Ed. New York City, NY, USA: ACM Press, May 25–27, 1987, pp. 218–229.
- [3] 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*, ser. Lecture Notes in Computer Science, C. Pomerance, Ed., vol. 293. Santa Barbara, CA, USA: Springer, Heidelberg, Germany, Aug. 16–20, 1988, pp. 87–119.
- [4] D. Chaum, C. Crépeau, and I. Damgård, "Multiparty unconditionally secure protocols (extended abstract)," in *20th Annual ACM Symposium on Theory of Computing*. Chicago, IL, USA: ACM Press, May 2–4, 1988, pp. 11–19.
- [5] S. Even, O. Goldreich, and A. Lempel, "A randomized protocol for signing contracts," *Commun. ACM*, vol. 28, no. 6, pp. 637–647, Jun. 1985. [Online]. Available: <http://doi.acm.org/10.1145/3812.3818>
- [6] O. Goldreich, S. Micali, and A. Wigderson, "Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems," *Journal of the ACM*, vol. 38, no. 3, pp. 691–729, 1991.
- [7] O. Goldreich, *Foundations of Cryptography: Basic Tools*. Cambridge, UK: Cambridge University Press, 2001, vol. 1.
- [8] G. Brassard, D. Chaum, and C. Crépeau, "Minimum disclosure proofs of knowledge," *J. Comput. Syst. Sci.*, vol. 37, no. 2, pp. 156–189, Oct. 1988. [Online]. Available: [http://dx.doi.org/10.1016/0022-0000\(88\)90005-0](http://dx.doi.org/10.1016/0022-0000(88)90005-0)

- [9] A. Wyner, "The wire-tap channel," *The Bell Systems Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [10] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *Information Theory, IEEE Transactions on*, vol. 24, no. 3, pp. 339–348, May 1978.
- [11] U. Maurer, "Secret key agreement by public discussion from common information," *Information Theory, IEEE Transactions on*, vol. 39, no. 3, pp. 733–742, May 1993.
- [12] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. i. secret sharing," *Information Theory, IEEE Transactions on*, vol. 39, no. 4, pp. 1121–1132, Jul 1993.
- [13] C. Crépeau and J. Kilian, "Achieving oblivious transfer using weakened security assumptions (extended abstract)," in *29th Annual Symposium on Foundations of Computer Science*. White Plains, New York: IEEE Computer Society Press, Oct. 24–26, 1988, pp. 42–52.
- [14] C. Crépeau, "Efficient cryptographic protocols based on noisy channels," in *Advances in Cryptology – EUROCRYPT'97*, ser. Lecture Notes in Computer Science, W. Fumy, Ed., vol. 1233. Konstanz, Germany: Springer, Heidelberg, Germany, May 11–15, 1997, pp. 306–317.
- [15] I. Damgård, J. Kilian, and L. Salvail, "On the (im)possibility of basing oblivious transfer and bit commitment on weakened security assumptions," in *Advances in Cryptology – EUROCRYPT'99*, ser. Lecture Notes in Computer Science, J. Stern, Ed., vol. 1592. Prague, Czech Republic: Springer, Heidelberg, Germany, May 2–6, 1999, pp. 56–73.
- [16] D. Khurana, H. K. Maji, and A. Sahai, "Secure computation on elastic noisy channels," in *Advances in Cryptology – EUROCRYPT 2016, Part II*, ser. Lecture Notes in Computer Science, M. Fischlin and J.-S. Coron, Eds., vol. 9666. Vienna, Austria: Springer, Heidelberg, Germany, May 8–12, 2016, pp. 184–212.
- [17] I. Cascudo, I. Damgård, F. Lacerda, and S. Ranellucci, "Oblivious transfer from any non-trivial elastic noisy channels via secret key agreement," Cryptology ePrint Archive, Report 2016/120. To appear on TCC 2016b, 2016, <http://eprint.iacr.org/2016/120>.
- [18] A. Winter, A. Nascimento, and H. Imai, "Commitment capacity of discrete memoryless channels," in *Cryptography and Coding*, ser. Lecture Notes in Computer Science, K. Paterson, Ed. Springer Berlin Heidelberg, 2003, vol. 2898, pp. 35–51. [Online]. Available: [http://dx.doi.org/10.1007/978-3-540-40974-8\\_4](http://dx.doi.org/10.1007/978-3-540-40974-8_4)
- [19] A. Nascimento, J. Barros, S. Skludarek, and H. Imai, "The commitment capacity of the gaussian channel is infinite," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2785–2789, June 2008.
- [20] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *Information Theory, IEEE Transactions on*, vol. 24, no. 4, pp. 451–456, Jul 1978.
- [21] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," in *Advances in Cryptology – EUROCRYPT'84*, ser. Lecture Notes in Computer Science, T. Beth, N. Cot, and I. Ingemarsson, Eds., vol. 209. Paris, France: Springer, Heidelberg, Germany, Apr. 9–11, 1985, pp. 33–50.
- [22] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *Information Theory, IEEE Transactions on*, vol. 50, no. 12, pp. 3047–3061, Dec 2004.
- [23] P. Parada and R. Blahut, "Secrecy capacity of simo and slow fading channels," in *Information Theory, 2005. ISIT 2005. Proceedings. International Symposium on*, Sept 2005, pp. 2152–2155.
- [24] J. Barros and M. Rodrigues, "Secrecy capacity of wireless channels," in *Information Theory, 2006 IEEE International Symposium on*, July 2006, pp. 356–360.
- [25] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Securing Wireless Communications at the Physical Layer*, R. Liu and W. Trappe, Eds. Springer US, 2010, pp. 1–18. [Online]. Available: [http://dx.doi.org/10.1007/978-1-4419-1385-2\\_1](http://dx.doi.org/10.1007/978-1-4419-1385-2_1)
- [26] Y. Liang, H. Poor, and S. Shamai, "Secrecy capacity region of fading broadcast channels," in *Information Theory, 2007. ISIT 2007. IEEE International Symposium on*, June 2007, pp. 1291–1295.
- [27] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *Information Theory, IEEE Transactions on*, vol. 54, no. 10, pp. 4687–4698, Oct 2008.
- [28] L. Lai, H. El Gamal, and H. V. Poor, "Secrecy capacity of the wiretap channel with noisy feedback," in *45th Annu. Allerton Conf. Communications, Control and Computing*, 2007.
- [29] I. Csiszár and P. Narayan, "Secrecy capacities for multiterminal channel models," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2437–2452, June 2008.
- [30] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y.-H. Kim, "Wiretap channel with secure rate-limited feedback," *Information Theory, IEEE Transactions on*, vol. 55, no. 12, pp. 5353–5361, Dec 2009.
- [31] G. Bagherikaram, A. Motahari, and A. Khandani, "Secrecy capacity region of gaussian broadcast channel," in *Information Sciences and Systems, 2009. CISS 2009. 43rd Annual Conference on*, March 2009, pp. 152–157.
- [32] E. Ekrem and S. Ulukus, "The secrecy capacity region of the gaussian mimo multi-receiver wiretap channel," *Information Theory, IEEE Transactions on*, vol. 57, no. 4, pp. 2083–2114, April 2011.
- [33] F. Oggier and B. Hassibi, "The secrecy capacity of the mimo wiretap channel," *Information Theory, IEEE Transactions on*, vol. 57, no. 8, pp. 4961–4972, Aug 2011.
- [34] A. Nascimento and A. Winter, "On the oblivious-transfer capacity of noisy resources," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2572–2581, June 2008.
- [35] H. Imai, K. Morozov, and A. Nascimento, "On the oblivious transfer capacity of the erasure channel," in *Information Theory, 2006 IEEE International Symposium on*, July 2006, pp. 1428–1431.
- [36] R. Ahlswede and I. Csiszár, "On oblivious transfer capacity," in *Information Theory, 2007. ISIT 2007. IEEE International Symposium on*, June 2007, pp. 2061–2064.
- [37] A. Pinto, R. Dowsley, K. Morozov, and A. Nascimento, "Achieving oblivious transfer capacity of generalized erasure channels in the malicious model," *Information Theory, IEEE Transactions on*, vol. 57, no. 8, pp. 5566–5571, Aug 2011.
- [38] 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 Transactions on Information Theory*, vol. 63, no. 10, pp. 6819–6826, Oct 2017.
- [39] R. Renner and S. Wolf, "Simple and tight bounds for information reconciliation and privacy amplification," in *Advances in Cryptology – ASIACRYPT 2005*, ser. Lecture Notes in Computer Science, B. K. Roy, Ed., vol. 3788. Chennai, India: Springer, Heidelberg, Germany, Dec. 4–8, 2005, pp. 199–216.
- [40] N. Nisan and D. Zuckerman, "Randomness is linear in space," *J. Comput. Syst. Sci.*, vol. 52, no. 1, pp. 43–52, Feb. 1996. [Online]. Available: <http://dx.doi.org/10.1006/jcss.1996.0004>
- [41] 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, Mar. 2008. [Online]. Available: <http://dx.doi.org/10.1137/060651380>
- [42] J. Radhakrishnan and A. Ta-Shma, "Bounds for dispersers, extractors, and depth-two superconcentrators," *SIAM J. Discret. Math.*, vol. 13, no. 1, pp. 2–24, Jan. 2000. [Online]. Available: <http://dx.doi.org/10.1137/S0895480197329508>
- [43] J. L. Carter and M. N. Wegman, "Universal classes of hash functions (extended abstract)," in *Proceedings of the Ninth Annual ACM Symposium on Theory of Computing*, ser. STOC '77. New York, NY, USA: ACM, 1977, pp. 106–112. [Online]. Available: <http://doi.acm.org/10.1145/800105.803400>
- [44] R. Impagliazzo, L. A. Levin, and M. Luby, "Pseudo-random generation from one-way functions (extended abstracts)," in *21st Annual ACM Symposium on Theory of Computing*. Seattle, WA, USA: ACM Press, May 15–17, 1989, pp. 12–24.
- [45] J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby, "A pseudorandom generator from any one-way function," *SIAM Journal on Computing*, vol. 28, no. 4, pp. 1364–1396, 1999.
- [46] 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. [Online]. Available: <http://dx.doi.org/10.1137/0217014>
- [47] C. Bennett, G. Brassard, C. Crépeau, and U. Maurer, "Generalized privacy amplification," *Information Theory, IEEE Transactions on*, vol. 41, no. 6, pp. 1915–1923, Nov 1995.
- [48] J. T. Rompel, "Techniques for computing with low-independence randomness," Ph.D. dissertation, Massachusetts Institute of Technology, Cambridge, MA, USA, 1990.
- [49] R. Canetti, "Universally composable security: A new paradigm for cryptographic protocols," in *42nd Annual Symposium on Foundations of Computer Science*. Las Vegas, NV, USA: IEEE Computer Society Press, Oct. 14–17, 2001, pp. 136–145.
- [50] R. Dowsley, J. van de Graaf, J. Müller-Quade, and A. C. A. Nascimento, "On the compossibility of statistically secure bit commitments," *Journal of Internet Technology*, vol. 14, no. 3, pp. 509–516, 2013.
- [51] R. Dowsley, J. Müller-Quade, and A. C. A. Nascimento, "On the possibility of universally composable commitments based on noisy channels," in *Anais do VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, SBSEG 2008*, A. L. M. dos Santos and M. P. Barcellos, Eds. Gramado, Brazil: Sociedade Brasileira de Computação (SBC), Sep. 1–5, 2008, pp. 103–114.



- [52] I. Damgård, T. Pedersen, and B. Pfitzmann, "Statistical secrecy and multibit commitments," *Information Theory, IEEE Transactions on*, vol. 44, no. 3, pp. 1143–1151, May 1998.
- [53] J. Wullschleger, "Oblivious transfer from weak noisy channels," in *TCC 2009: 6th Theory of Cryptography Conference*, ser. Lecture Notes in Computer Science, O. Reingold, Ed., vol. 5444. Springer, Heidelberg, Germany, Mar. 15–17, 2009, pp. 332–349.