Wiretapped Commitment over Binary Channels

Anuj Kumar Yadav*, Manideep Mamindlapally†, and Amitalok J. Budkuley ‡.

*School of Computer and Communication Sciences, EPFL, Switzerland.
†CWI and University of Amsterdam, The Netherlands.
‡Department of Electronics and Electrical Communication Engg., IIT Kharagpur, India.

***Abstract*—We propose the problem of *wiretapped commitment*, where two parties, say *committer* Alice and *receiver* Bob, engage in a commitment protocol using a noisy channel as a resource, in the presence of a *eavesdropper*, say Eve. Noisy versions of Alice's transmission over the wiretap channel are received at both Bob and Eve. We seek to determine the maximum commitment throughput in the presence of a eavesdropper, i.e., *wiretapped commitment capacity*, where in addition to the standard security requirements for two-party commitment, one seeks to ensure that Eve doesn't learn about the commit string.**

A key interest in this work is to explore the effect of collusion (or lack of it) between the *eavesdropper* Eve and either Alice or Bob. Toward the same, we present results on the wiretapped commitment capacity under the so-called 1-*private regime* (when Alice or Bob cannot collude with Eve) and the 2-*private regime* (when Alice or Bob may possibly collude with Eve).

I. Introduction

A classic *two-party* primitive that finds wide application in cryptographic applications is *commitment* introduced by Blum [1]. In this work, we study a *three-party variation* of this problem, viz., *wiretapped commitment*, involving *committer* Alice, *receiver* Bob and an *eavesdropper* Eve. Imagine Alice and Bob engaging in a high-stakes business transaction, exchanging digital contract details over a communication channel that may be susceptible to wiretapping by an eavesdropper Eve. In this scenario, there's a concern that either Alice or Bob, individually or in possible collusion with Eve, may interact with the aim of either revealing the contract terms prematurely or altering them without detection at the time of finalization. We seek to devise *eavesdropper-resilient* commitment schemes, also called *wiretapped commitment schemes* henceforth, such that Alice and Bob can establish a secure and tamper-evident commitment protocol, mitigating the risks associated with wiretapping and possible collusion. Such a scheme would not only safeguard the confidentiality of the contract terms but also maintain the integrity of the agreement in the face of potential adversarial collaboration.

While Blum's classic work introduced commitment, it also brought to the fore the limitation that information-theoretically secure schemes were impossible under entirely noiseless interactions between two-parties.[1] Wyner's foundational work on *wiretap channels* [2] first demonstrated the use of *noisy channels* to devise schemes with information-theoretic security (albeit in the 'weak' sense). Through a series of subsequent works [3], [4], positive rate unconditionally secure commitment was shown to be possible over binary memoryless channels. Winter *et al.* [5] characterized the commitment capacity over any *non-redundant* discrete memoryless channel (DMC); this result was subsequently extended to DMCs with 'costs' in [6]. Commitment has also been explored for other channel models like the unfair noisy channels [7]–[9], elastic channels and their cousins [10], [11], quantum channels [12], etc. Several other variants of commitment too have been studied (see [13]–[15]).

Closer to the theme of this work, and a key motivation for our study, is the work by Mishra *et al.* [16], [17] on *wiretapped oblivious transfer*, where the authors studied another related cryptographic primitive called the *oblivious transfer* [18]–[20] in the presence of an eavesdropper. The presence of the eavesdropper necessitated additional security requirement (w.r.t. the classical problem). Here the authors focused on certain sub-classes of binary wiretap channels with erasures and studied their capacity (with potentially *honest-but-curious* users) under two versions of security guarantees: (i) the 1-*privacy* setting which precludes collusion with the eavesdropper, and (ii) 2-*privacy* setting where collusion is possible. Inspired by their work, in our problem we study wiretap channels under similarly inspired notions of privacy (with and without colluding parties); see Section III for their formal definitions.

Our work formalizes the wiretapped commitment problem and presents new results on their commitment capacity. In the following, we summarize our key contributions:

- We initiate a systematic study of wiretapped commitment in this work. For the 1-privacy setting, we completely characterize the commitment capacity for the binary symmetric broadcast (BS-BC) wiretap channels in Theorem 1. Here we present a converse (upper bound) for general alphabet wiretap channels, and then specialize it for the BS-BC class of such channels, followed by a matching lower bound using a scheme tailored for the BS-BC channels.
- Next, we present capacity results under the more challenging 2-privacy setting where Alice or Bob may collude with Eve. Using a general wiretap channel converse, and

A short version of this work has been accepted for publication at the 2024 IEEE International Symposium on Information Theory (ISIT), Athens, Greece. This extended version includes detailed proofs of theorems, discussion and open questions.

[1] Blum's work established the possibility of *conditionally-secure* commitment schemes under computationally-limited parties.

constructing a specialized achievability scheme matching that bound, we completely characterize the 2-private commitment capacity for the *independent* BS-BC wiretap channel (see Def. 5).

Organization of the paper: In the following, we briefly present the basic notation in Section II. Following which we present our problem setup in Section III. The main results of this work are presented in Section IV. We present some details of the converse proof and achievability in Section V. Finally, we make concluding remarks in Section VI.

II. Notation and Preliminaries:

We denote random variables by upper case letters (eg. X), their values by lower case letters (eg., x), and their alphabets by calligraphic letters (eg. $\mathcal{X}$). Random vectors and their accompanying values are denoted by boldface letters. For natural number $a \in \mathbb{N}$, let $[a] := \{1, 2, \cdots, a\}$. Let P_X denote the distribution of $X \in \mathcal{X}$. Distributions for multiple random variables are similarly defined. $P_{X|Y}$ and $[P_{X,Y}]_X$ denote the conditional distribution of X (conditioned on Y) and the marginal distribution of X (under the $P_{X,Y}$ joint distribution). Given $P_X, Q_X \in \mathcal{P}(\mathcal{X})$, $||P_X - Q_X||$ denotes their statistical distance.

Let random variables $X, Y \in \mathcal{X} \times \mathcal{Y}$, where $(X, Y) \sim P_{X,Y}$. The *min-entropy* of X is denoted by $H_\infty(X) := \min_{x \in \mathcal{X}} (-\log(P_X(x)))$; the conditional version is given by $H_\infty(X|Y) := \min_y H_\infty(X|Y = y)$. For $\epsilon \in [0, 1)$, the ϵ-*smooth min entropy* and its conditional version is given by: $H^\epsilon_\infty(X) := \max_{X':||P_{X'}-P_X|| \leq \epsilon} H_\infty(X')$ and $H^\epsilon_\infty(X|Y) := \max_{X',Y':||P_{X',Y'}-P_{X,Y}|| \leq \epsilon} H_\infty(X'|Y')$ respectively.

We also need universal hash functions and strong randomness extractors for our commitment scheme; see [21]–[23] for detailed definitions.

Definition 1 (ξ-Universal hash functions). *Let $\mathcal{H}$ be a class of functions from $\mathcal{X}$ to $\mathcal{Y}$. $\mathcal{H}$ is said to be $\xi-$universal hash function, where $\xi \in \mathbb{N}$, if when $h \in \mathcal{H}$ is chosen uniformly at random, then $(h(x_1), h(x_2), ...h(x_\xi))$ is uniformly distributed over $\mathcal{Y}^\xi$, $\forall x_1, x_2, ...x_\xi \in \mathcal{X}$.*

Definition 2 (Strong randomness extractors). *A probabilistic polynomial time function of the form Ext: $\{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is an (n, k, m, ϵ)-strong extractor if for every probability distribution P_Z on $\mathcal{Z} = \{0,1\}^n$, and $H_\infty(Z) \geq k$, for random variables D (called 'seed') and M, distributed uniformly in $\{0,1\}^d$ and $\{0,1\}^m$ respectively, we have $||P_{Ext(Z;D),D} - P_{M,D}|| \leq \epsilon$.*

III. System Model and Problem Description

Our problem (refer Fig. 1) comprises three parties: *committer* Alice, *receiver* Bob and *eavesdropper* Eve. Alice and Bob are mutually distrustful parties and employ a noisy wiretap channel (where potentially different noisy versions of Alice's transmission are broadcast to Bob and Eve) to realize commitment in the presence of Eve. The commit string C is chosen uniformly at random by Alice, where $C \in [2^{nR}]$, and she transmits her encrypted data or *codeword* $\mathbf{X}$ over a one-way wiretap channel where channel outputs $\mathbf{Y}$ and $\mathbf{Z}$ are received at Bob and Eve, respectively. We formally define the wiretap channel below:

Definition 3 (Wiretap channel [24], [25]). *A wiretap channel is a memoryless broadcast channel with Alice's input $X \in \mathcal{X}$, and outputs $Y \in \mathcal{Y}$ and $Z \in \mathcal{Z}$ at Bob and Eve, respectively. The memoryless channel law is given by $W_{Y,Z|X} : \mathcal{X} \to \mathcal{Y} \times \mathcal{Z}$ and is known to all parties.*

In this work, we specifically focus on the following class of binary wiretap channels.

Definition 4 (BS-BC wiretap channels [25]). *A binary input binary output (BIBO) memoryless broadcast channel $W_{Y,Z|X}$, where $\mathcal{X} = \mathcal{Y} = \mathcal{Z} = \{0,1\}$, and the* marginal *channel laws $W_{Y|X} := [W_{Y,Z|X}]_{Y|X}$ and $W_{Z|X} = [W_{Y,Z|X}]_{Z|X}$ are binary symmetric channels (BSCs), say BSC(p) and BSC(q), where $0 < p, q < 1/2$, is called a binary symmetric broadcast (BS-BC) wiretap channel and denoted by BS-BC(p, q). Note that the two BSCs may exhibit correlated behaviour.* [2]

Remark 1. *For given $0 < p, q < 1/2$, BS-BC(p, q) is not a unique channel but a class of channels.*

Next, we define two sub-classes of binary symmetric broadcast (BS-BC) wiretap channels which are relevant for this work.

Definition 5 (I-BS-BC wiretap channel [25]). *An independent binary symmetric broadcast (I-BS-BC(p, q)) wiretap channel is a BS-BC(p, q) wiretap channel where the channel law $W_{Y,Z|X}$ can be decomposed in the following manner: $W_{Y,Z|X} = W_{Y|X}W_{Z|X}$ i.e., the Markov chain $Y - X - Z$ holds. In other words, the binary symmetric channels BSC(p) and BSC(q) have independent channel noise.*

Definition 6 (D-BS-BC wiretap channel [25]). *A degraded binary symmetric broadcast (D-BS-BC(p, q)) wiretap channel is a BS-BC(p, q) wiretap channel where the channel law $W_{YZ|X}$ can be decomposed in the following manner: $W_{YZ|X} = W_{Y|X}W_{Z|Y}$, i.e., the Markov chain $X - Y - Z$ holds. In other words, the binary symmetric channel from Alice to Eve, i.e., BSC(q) is a physically degraded version of the binary symmetric channel from Alice to Bob, i.e., BSC(p).*

In addition to the noisy channel resource, as is common in such cryptographic primitives, we also assume that Alice and Bob can interact over a two-way link that is noiseless and where the interaction is public and fully authenticates the transmitting party.[3] The *eavesdropper* Eve is assumed to also have access to the interactions over the noiseless link.

To commit to her random string C, Alice uses the BS-BC wiretap channel $W_{Y,Z|X}$, n times and transmits over it

[2] Note that both p and q are strictly in the interior of the set $[0, 1/2]$. We include this restriction since (information-theoretic) the commitment capacity can be easily characterized when either (or both) of p and q equal 0 or 1.

[3] Recall from earlier that under unconditionally-secure commitment, even single-bit commitment is impossible to realize under purely noiseless interactions [7].

her encrypted string $\mathbf{X} = (X_1, X_2, \cdots, X_n) \in \{0,1\}^n$. Bob and Eve, respectively, receive noisy versions $\mathbf{Y} \in \{0,1\}^n$ and $\mathbf{Z} \in \{0,1\}^n$ of $\mathbf{X}$. Alice and Bob can both privately randomize their transmissions (over the noisy and noiseless links) via their respective keys $K_A \in \mathcal{K_A}$ and $K_B \in \mathcal{K_B}$. At any point in time, say instant $i \in [n]$, Alice and Bob can also exchange messages over the public, noiseless link prior to transmitting X_i; let M denote the entire collection of messages exchanged over the noiseless link. We call M the *transcript* of the protocol. We assume that at any point in time during the protocol, the transmissions of Alice and/or Bob can depend *causally* on the information previously available to them.

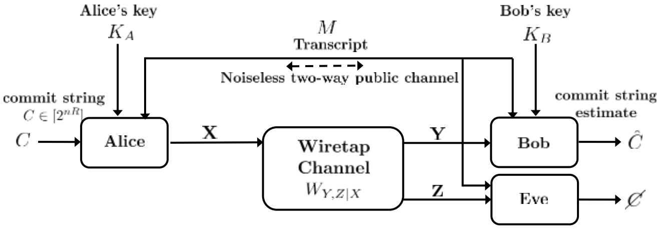

Fig. 1. The problem setup: commitment over a wiretap channel

We now formally introduce an (n, R)-commitment protocol for the above setup.

Definition 7 (Commitment protocol)**.** *An $(n, R)-$commitment protocol $\mathscr{P}$ is a message-exchange procedure between Alice and Bob (in the presence of Eve) to realize commitment over the random bit string $C \in [2^{nR}]$. Here R is called the* rate *of the above (n, R)-commitment protocol $\mathscr{P}$. There are two phases to $\mathscr{P}$:* commit phase *followed by the* reveal phase.

(a) Commit phase: Given $C \in [2^{nR}]$, Alice uses the BS-BC (p, q), n times to transmit $\mathbf{X}$ over it. Correspondingly, Bob receives $\mathbf{Y}$, and Eve receives $\mathbf{Z}$ over this channel. The two parties (Alice and Bob) may also exchange messages over the noiseless link during the transmission of $\mathbf{X}$. Let M denote this transcript (over the noiseless link) of protocol $\mathscr{P}$ at the end of Commit phase.[4] *Let $V_A = (C, K_A, \mathbf{X}, M), V_B = (K_B, \mathbf{Y}, M)$ and $V_E = (\mathbf{Z}, M)$ denote,* Alice's view, Bob's view *and* Eve's view *respectively which includes all the random variables and vectors known to the respective users at the end of the commit phase.*

(b) Reveal phase: In this phase, Alice and Bob communicate only over the noiseless public link and do not use the BS-BC wiretap channel[5]*. Alice announces the commit string $\tilde{c} \in [2^{nR}]$ and $\tilde{\mathbf{X}} \in \{0,1\}^n$. Bob then performs a test $T(\tilde{c}, \tilde{\mathbf{X}}, V_B)$ and either accepts (by setting $T = 1$) the commit string $\tilde{c}$ or reject it (by setting $T = 0$).*

In this work, we study *achievability* of rate R (defined later) with respect to two different notions of security metrics, viz., the $1-$privacy (where none of the legitimate parties i.e., Alice and Bob are allowed to collude with the *eavesdropper* Eve) and the $2-$privacy (where the collusion between 'a *malicious* Alice and Eve' or 'a *malicious* Bob and Eve' is possible). Toward defining the same, we first introduce the security metrics for any $(n, R)-$commitment protocol $\mathscr{P}$.

Definition 8 ($\epsilon-$sound)**.** *A protocol $\mathscr{P}$ is $\epsilon-$sound if for an honest Alice and an honest Bob, $\mathbb{P}\left(T(C, \mathbf{X}, V_B) \neq 1\right) \leq \epsilon$.*

Definition 9 ($\epsilon - 1-$concealing)**.** *A protocol $\mathscr{P}$ is $\epsilon - 1-$concealing if for an honest Alice and under any strategy of a malicious Bob, $I(C; V_B) \leq \epsilon$.*

Definition 10 ($\epsilon-1-$ binding)**.** *A protocol $\mathscr{P}$ is $\epsilon-1-$binding if for an honest Bob and under any cheating function $\mathcal{A}$ of a malicious Alice,*

$$\mathbb{P}\Big(T(\bar{c}, \bar{\mathbf{x}}, V_B) = 1 \quad \& \quad T(\hat{c}, \hat{\mathbf{x}}, V_B) = 1\Big) \leq \epsilon$$

for any two pairs $(\bar{c}, \bar{\mathbf{x}}), (\hat{c}, \hat{\mathbf{x}}) = \mathcal{A}(V_A)$ where $\bar{c} \neq \hat{c}$, and $\bar{\mathbf{x}}, \hat{\mathbf{x}} \in \{0,1\}^n$.

Definition 11 ($\epsilon-$secure)**.** *A protocol $\mathscr{P}$ is $\epsilon-$secure if for any strategy of the eavesdropper Eve, $I(C; V_E) \leq \epsilon$.*

Definition 12 ($\epsilon - 2-$concealing)**.** *A protocol $\mathscr{P}$ is $\epsilon - 2-$concealing if for an honest Alice and under any strategy of a malicious Bob possibly in collusion with Eve, $I(C; V_B, V_E) \leq \epsilon$.*

It might be of interest to note here that under the $2-$privacy caase, $\epsilon - 2-$concealing condition directly implies that the protocol is $\epsilon-$secure as well (due to the chain rule of mutual information and the fact that mutual information is non-negative). Alternatively, we could have also defined $\epsilon - 2-$secure condition which would be exactly similar to $\epsilon - 2-$concealing beacause the collusion between Bob and Eve leads to both having the same view i.e., (V_B, V_E).

Definition 13 ($\epsilon-2-$binding)**.** *A protocol $\mathscr{P}$ is $\epsilon-2-$binding if for an honest Bob and under any cheating function $\mathcal{A}$ of a malicious Alice possibly in collusion with Eve,*

$$\mathbb{P}\Big(T(\bar{c}, \bar{\mathbf{x}}, V_B) = 1 \quad \& \quad T(\hat{c}, \hat{\mathbf{x}}, V_B) = 1\Big) \leq \epsilon$$

for any two pairs $(\bar{c}, \bar{\mathbf{x}}), (\hat{c}, \hat{\mathbf{x}}) = \mathcal{A}(V_A, V_E)$ where $\bar{c} \neq \hat{c}$, and $\bar{\mathbf{x}}, \hat{\mathbf{x}} \in \{0,1\}^n$.

A rate R is said to be *achievable under* 1*-privacy* (resp. *achievable under* 2*-privacy*) if for every $\epsilon > 0$ arbitrarily small and n sufficiently large, there exists a commitment protocol $\mathscr{P}$ such that $\mathscr{P}$ is $\epsilon-$sound, $\epsilon - 1-$concealing (resp. $\epsilon - 2-$concealing) and $\epsilon - 1-$binding (resp. $\epsilon - 2-$binding) and $\epsilon-$secure.

The supremum of all achievable $1-$private rates (resp. $2-$private rates) is called the $1-$*private commitment capacity* (resp. $2-$*private commitment capacity*), and the commitment capacity capacity is denoted by $\mathbb{C}_1$ (resp. $\mathbb{C}_2$).

[4] We assume that the transcript may contain arbitrarily large, though finite, messages.

[5] We point that in some works, unlike in this work, the noisy channel may be used to also realize the bidirectional noiseless link, and the rate calculation is, subsequently, normalized also over such channel uses. We do not study such a definition of rate in this work.

IV. Our Main Results

We now state our key results in this section.

Theorem 1 (Capacity of BS-BC under $1-$privacy)**.** *Consider a channel $W_{Y,Z|X} \in$ BS-BC(p,q), where $0 < p, q < 1/2$. Then, the commitment capacity $\mathbb{C}_1$ of such a BS-BC(p,q) under $1-$privacy is*

$$\mathbb{C}_1 = \min\{H(p), H(q)\}. \tag{1}$$

We present the full proof in Section V-A and Section V-D.

We first a present a converse for a general (finite) alphabet wiretap channel and then specialize the same for the BS-BC(p,q) wiretap channel. Our achievability (inspired from [7], [8], [26]) is tailored for the BS-BC wiretap channels and utilizes random hash exchange challenge and a strong randomness extractor based on 2-universal hash function. However, unlike any of the previous works, our scheme just requires *one round* of random hash challenge essentially to guarantee bindingness.

For the I-BS-BC(p,q) the capacity expression remain unchanged from that in (1) since that expression depends entirely on the marginal channel laws $W_{Y|X}$ and $W_{Z|X}$ (which are specified via general parameters p and q). For the Degraded-BS-BC, however, we have the following immediate corollary.

Corollary 1 (Capacity of D-BS-BC under $1-$privacy)**.** *The commitment capacity for the degraded binary symmetric broadacst wiretap channel, D-BS-BC(p,q), under $1-$privacy is $H(p)$.*

The result follows by noting that for the D-BS-BC(p,q), we can express $q = p * \theta$, for some $\theta \in [0, 1/2)$. Hence, $q \geq p$, and the minimum in (1) evaluates to $H(p)$.

Next, we state our results for capacity under 2-privacy. For this setting, we completely characterize the 2-private commitment capacity for the I-BS-BCO(p,q). We state the following theorem:

Theorem 2 (Capacity of I-BS-BC under $2-$privacy)**.** *Consider an I-BS-BC(p,q) where $0 < p, q < 1/2$. Then, the commitment capacity $\mathbb{C}_2$ of such I-BS-BC(p,q) under $2-$privacy is*

$$\mathbb{C}_2 = H(p) + H(q) - H(p \circledast q). \tag{2}$$

where $p \circledast q$ denotes the binary convolution of p and q i.e., $p \circledast q := p(1-q) + q(1-p)$.

We present the proof in Section V. For the converse, we present a rate upper bound, viz., $R \leq H(X|Y,Z)$, for any general wiretap channel. This bound is then specialized to the binary setting (for I-BS-BC(p,q)) and evaluates to the expression given in Eq (2). It is pertinent to note that the above bound holds for *any* wiretap channel. For the I-BS-BC specifically, we present a matching lower bound through an achievable scheme. It has similarities to the scheme in the 1-private setting but crucially differs in the choice of the hash families and the randomness extractor.

V. Proofs

A. 1-privacy converse analysis for the wiretap channel $W_{Y,Z|X}$

In this subsection, we will first derive an upper bound on the rate of any commitment protocol for a general wiretap channel $W_{Y,Z|X}$ under 1-privacy. Then, we specialize the result to get a tight upper bound for the binary symmetric broadcast (BS-BC(p,q)) wiretap channel. Additionally, we *strengthen* our converse by proving that our upper bound on the commitment rate holds even under a *weaker* notion of ϵ-1-concealment and ϵ-secrecy against Eve, which are defined below:[6]

Definition 14 (ϵ-weakly-1-concealing)**.** *An (n,R)-commitment protocol is said to be ϵ-weakly-1-concealing if for an honest Alice and under* any *strategy of Bob,*

$$\frac{1}{n} I(C; V_B) \leq \epsilon. \tag{3}$$

Definition 15 (ϵ-weakly-secure)**.** *An (n,R)-commitment protocol is said to be ϵ-weakly-1-secure against the eavesdropper Eve if under* any *strategy of Eve,*

$$\frac{1}{n} I(C; V_E) \leq \epsilon. \tag{4}$$

Now, consider any sequence of commitment protocols $(\mathscr{P}_n)_{n \geq 1}$, such that $\forall n$, $\mathscr{P}_n$ is ϵ_n-sound, ϵ_n-weakly-1-concealing, ϵ_n-1-binding, and ϵ-weakly-secure, such that $\epsilon_n \geq 0$ and $\epsilon_n \to 0$ as $n \to \infty$.

For these sequence of protocols, we state the following lemma which upper bounds the conditional entropy $\frac{1}{n} H(C|\mathbf{X}, V_B)$ using Fano's inequality; we will use this lemma later to upper bound the commitment rate.

Lemma 1. *For every commitment protocol $\mathscr{P}_n$ satisfying all the security guarantees under $1-$privacy, we have $\frac{1}{n} H(C|\mathbf{X}, V_B) \leq \epsilon''_n$, where $\epsilon''_n \to 0$ as $n \to \infty$.*

The proof appears in Appendix A, and follows from the fact that each protocol $\mathscr{P}_n$ satisfies ϵ_n-soundness and ϵ_n-bindingness.

[6] This is a security notion directly inspired from the weak secrecy metric originally studied by Wyner [2] for wiretap channels.

Let us now bound the commitment rate R as follows:

$$\begin{aligned}
R &= \frac{1}{n}H(C)\\
&\overset{(a)}{=} \frac{1}{n}H(C|V_B) + \frac{1}{n}I(C;V_B)\\
&\overset{(b)}{\leq} \frac{1}{n}H(C|V_B) + \epsilon_n\\
&\overset{(c)}{=} \frac{1}{n}H(C|\mathbf{Y},K_B,M) + \epsilon_n\\
&\overset{(d)}{\leq} \frac{1}{n}H(C,\mathbf{X}|\mathbf{Y},K_B,M) + \epsilon_n\\
&\overset{(e)}{=} \frac{1}{n}H(\mathbf{X}|\mathbf{Y},K_B,M) + \frac{1}{n}H(C|\mathbf{X},\mathbf{Y},K_B,M) + \epsilon_n\\
&= \frac{1}{n}H(\mathbf{X}|\mathbf{Y},K_B,M) + \frac{1}{n}H(C|\mathbf{X},V_B) + \epsilon_n\\
&\overset{(f)}{\leq} \frac{1}{n}H(\mathbf{X}|\mathbf{Y}) + \epsilon''_n + \epsilon_n\\
&\leq \frac{1}{n}\sum_{i=1}^{n} H(X_i|Y_i) + \epsilon''_n + \epsilon_n\\
&\leq \max_{P_X} H(X|Y) + \epsilon''_n + \epsilon_n
\end{aligned} \tag{5}$$

Here,

(a) follows from the definition of mutual information.
(b) follows from the fact that every commitment protocol in the sequence $\mathscr{P}_n$ is ϵ_n-weakly-1-concealing.
(c) follows from noting that Bob's view $V_B = (\mathbf{Y}, M, K_B)$, where $\mathbf{Y}$ denotes the output of the wiretap channel.
(d) follows from property of joint entropy.
(e) follows from the chain rule of joint entropy.
(f) follows from lemma 1 and noting that conditioning reduces entropy.

Therefore, finally we have:

$$R \leq \max_{P_X} H(X|Y) \tag{6}$$

Let $W_{Y|X} := [W_{Y,Z|X}]_{Y|X}$ and $W_{Z|X} := [W_{Y,Z|X}]_{Z|X}$ denote the effective channels from Alice to Bob and Alice to Eve, respectively. Suppose there exists a channel $U_{\tilde{Y}|Z} : \mathcal{Z} \to \mathcal{Y}$ s.t.

$$W_{Y|X} = W_{Z|X}U_{\tilde{Y}|Z}, \tag{7}$$

[7] This happens when the channel from Alice to Bob is a *stochastically degraded* version of the channel from Alice to Eve. Consider a *cheating strategy* adopted by the *eavesdropper* Eve to learn about the commit string c. The eavesdropper Eve passes the received vector $\mathbf{Z}$ *locally* through the simulated *private channel* $U_{\tilde{Y}|Z}$ to generate a $\tilde{\mathbf{Y}}$ which is a candidate $\mathbf{Y}$ i.e., $P_{X,\tilde{Y}} = P_X W_{Y|X} = P_{XY}$. Note that the view of Eve here is $V_E = (\mathbf{Z}, \tilde{\mathbf{Y}}, M)$.

Suppose such a $U_{\tilde{Y}|Z}$ exists. Then, from Lemma 1, we have that

$$\begin{aligned}
H(C|\mathbf{X},\mathbf{Y},K_B,M) &\leq \epsilon''_n\\
H(C|\mathbf{X},\mathbf{Y},M) &\overset{(a)}{\leq} \epsilon''_n\\
H(C|\mathbf{X},\tilde{\mathbf{Y}},M) &\overset{(b)}{\leq} \epsilon''_n\\
H(C|\mathbf{X},Z,\tilde{\mathbf{Y}},M) &\overset{(c)}{\leq} \epsilon''_n\\
H(C|\mathbf{X},V_E) &\leq \epsilon''_n
\end{aligned} \tag{8}$$

where,

(a) follows from noting that K_B just models local randomness at Bob which is independent.
(b) follows from the assumption of the markov chain $M - \mathbf{X} - \mathbf{Y}$ (see Remark 2), and thus noting that the joint distributions of $(C, \mathbf{X}, \mathbf{Y}, M)$ and $(C, \mathbf{X}, \tilde{\mathbf{Y}}, M)$ are equal.
(c) follows from the fact that conditioning reduces entropy.

Now, we can also upper bound the commitment rate as follows:

$$\begin{aligned}
R &= \frac{1}{n}H(C)\\
&= \frac{1}{n}H(C|V_E) + \frac{1}{n}I(C;V_E)\\
&\overset{(a)}{\leq} \frac{1}{n}H(C|V_E) + \epsilon_n\\
&\overset{(b)}{\leq} \frac{1}{n}H(C,\mathbf{X}|V_E) + \epsilon_n\\
&\overset{(c)}{=} \frac{1}{n}H(\mathbf{X}|\mathbf{Z},\tilde{\mathbf{Y}},M) + \frac{1}{n}H(C|\mathbf{X},\mathbf{Z},\tilde{\mathbf{Y}},M) + \epsilon_n\\
&= \frac{1}{n}H(\mathbf{X}|\mathbf{Z},\tilde{\mathbf{Y}},M) + \frac{1}{n}H(C|\mathbf{X},V_E) + \epsilon_n\\
&\overset{(d)}{\leq} \frac{1}{n}H(\mathbf{X}|\mathbf{Z}) + \epsilon''_n + \epsilon_n\\
&\leq \frac{1}{n}\sum_{i=1}^{n} H(X_i|Z_i) + \epsilon''_n + \epsilon_n\\
&\leq \max_{P_X} H(X|Z) + \epsilon''_n + \epsilon_n
\end{aligned} \tag{9}$$

Here,

(a) follows from the fact that every commitment protocol in the sequence $\mathscr{P}_n$ is ϵ_n-weakly-secure against any statregy of Eve.
(b) follows from the chain rule of joint entropy.
(c) follows from noting that Eve's view $V_E = (\mathbf{Z}, \tilde{\mathbf{Y}}, M)$.
(d) follows from the fact that conditioning reduces entropy and from Eq. (8).

Finally, we also have:

$$R \leq \max_{P_X} H(X|Z) \tag{10}$$

The above upper bound holds only if a $U_{\tilde{Y}|Z}$ satisfying Eq. (7) exists.

Remark 2. *Note that the above approach includes a natural valid assuption of $M - \mathbf{X} - \mathbf{Y}$ i.e., the transcript of the public*

[7]Remember that $W_{Z|X}U_{\tilde{Y}|Z}$ represents composition of $W_{Z|X}$ and $U_{\tilde{Y}|Z}$. (c.f. definition 3).

communication M and $\mathbf{Y}$ are independent given $\mathbf{X}$. Most of the commitment protocols including the one presented below in our Achievability subsection follows this markov chain. This assumption was aslo made by Crepeau et.al [8] for proving the upper bound on the commitment rate for unfair noisy channels. As of now, it seems challenging to come up with a general converse approach without the above markov chain assumption, and is an interesting open problem. (see Lemma 5.1 *and Final remarks in [8], for details).*

From Eq. (6) and Eq. (10), we have the following upper bound on the commitment rate.

$$R \leq \min\left\{\max_{P_X} H(X|Y), \max_{P_X} H(X|Z)\right\} \tag{11}$$

Thus, we have the following upper bounds on the commitment rate for a wiretap channel $W_{Y,Z|X}$:

(i) If Alice to Bob channel i.e., $W_{Y|X}$ is a *stochastically degraded* version of the channel from Alice to Eve i.e., $W_{Z|X}$, then

$$R \leq \min\left\{\max_{P_X} H(X|Y), \max_{P_X} H(X|Z)\right\} \tag{12}$$

(ii) Else,

$$R \leq \max_{P_X} H(X|Y) \tag{13}$$

On solving the Eq. (11) or collectively solving the Eqs. (12) and (13) for the binary symmetric broadcast (BS-BC(p,q)) wiretap channels, we have the similar following upper bound on the commitment rate for BS-BC(p,q) under 1−privacy:

$$R \leq \min\left\{H(p), H(q)\right\} \tag{14}$$

where we observe that the optimizing the input distribution is $X \sim$ Bernoulli$(1/2)$.

Here, we have the following: when Alice to Bob channel is *stochastically degraded* version of Alice to Eve channel (i.e., $q < p$), the Eq. (12) evalautes to $R \leq H(q)$. Otherwise (i.e., $q \geq p$), the Eq. (13) evalautes to $R \leq H(p)$. Together, these reduce to the expression in the Eq. (14).

This completes our converse analysis for BS-BC(p,q) wiretap channels under 1−privacy.

B. 2*-privacy converse analysis for the wiretap channel* $W_{Y,Z|X}$.

In this subsection, we will first derive an upper bound on the rate of any commitment protocol for a general wiretap channel $W_{Y,Z|X}$ under 2-privacy. Then, we specialize the result to get an upper bound for the Independent binary symmetric broadcast (I-BS-BC(p,q)) wiretap channel.

Additionally, similar to the previous case we *strengthen* our converse by proving that our upper bound on the commitment rate holds even under a *weaker* notion of ϵ-2-concealment (defined below) and ϵ-secrecy against Eve.

Definition 16 (ϵ-weakly-2-concealing). *An (n,R)-commitment protocol is said to be ϵ-weakly-2-concealing if for an honest Alice and under* any *strategy of colluding Bob and Eve,*

$$\frac{1}{n}I(C;V_B,V_E) \leq \epsilon. \tag{15}$$

Now, consider any sequence of commitment protocols $(\mathscr{P}_n)_{n\geq 1}$, such that $\forall n$, $\mathscr{P}_n$ is ϵ_n-sound, ϵ_n-weakly-2-concealing, ϵ_n-2-binding, and ϵ-weakly-secure, such that $\epsilon_n \geq 0$ and $\epsilon_n \to 0$ as $n \to \infty$.

For these sequence of protocols, we state the following lemma which upper bounds the conditional entropy $\frac{1}{n}H(C|\mathbf{X},V_B,V_E)$ using Fano's inequality; similar to the 1-privacy case, we will use this lemma later to upper bound the commitment rate.

Lemma 2. *For every commitment protocol $\mathscr{P}_n$ satisfying all the security guarantees under 2−privacy, we have $\frac{1}{n}H(C|\mathbf{X},V_B,V_E) \leq \epsilon_n''$, where $\epsilon_n'' \to 0$ as $n \to \infty$.*

The proof appears in Appendix A, and follows from the fact that each protocol $\mathscr{P}_n$ satisfies ϵ_n−soundness and ϵ_n−2−bindingness.

Let us now bound the commitment rate R as follows:

$$\begin{aligned}
R &= \frac{1}{n}H(C) \\
&\overset{(a)}{=} \frac{1}{n}H(C|V_B,V_E) + \frac{1}{n}I(C;V_B,V_E) \\
&\overset{(b)}{\leq} \frac{1}{n}H(C|V_B,V_E) + \epsilon_n \\
&\overset{(c)}{=} \frac{1}{n}H(C|\mathbf{Y},\mathbf{Z},K_B,K_E,M) + \epsilon_n \\
&\overset{(d)}{\leq} \frac{1}{n}H(C,\mathbf{X}|\mathbf{Y},\mathbf{Z},K_B,K_E,M) + \epsilon_n \\
&\overset{(e)}{=} \frac{1}{n}H(\mathbf{X}|\mathbf{Y},\mathbf{Z},K_B,K_E,M) \\
&\qquad + \frac{1}{n}H(C|\mathbf{X},\mathbf{Y},\mathbf{Z},K_B,K_E,M) + \epsilon_n \\
&= \frac{1}{n}H(\mathbf{X}|\mathbf{Y},\mathbf{Z},K_B,K_E,M) + \frac{1}{n}H(C|\mathbf{X},V_B,V_E) + \epsilon_n \\
&\overset{(f)}{\leq} \frac{1}{n}H(\mathbf{X}|\mathbf{Y},\mathbf{Z}) + \epsilon_n'' + \epsilon_n \\
&\leq \frac{1}{n}\sum_{i=1}^{n} H(X_i|Y_i,Z_i) + \epsilon_n'' + \epsilon_n \\
&\leq \max_{P_X} H(X|Y,Z) + \epsilon_n'' + \epsilon_n
\end{aligned} \tag{16}$$

Here,

(a) follows from the definition of mutual information.
(b) follows from the fact that every commitment protocol in the sequence $\mathscr{P}_n$ is ϵ_n-weakly-2-concealing.
(c) follows from noting that the collective view of colluding Bob and Eve is $(V_B,V_E) = (\mathbf{Y},\mathbf{Z},K_B,K_E,M)$.
(d) follows from property of joint entropy.
(e) follows from the chain rule of joint entropy.
(f) follows from lemma 2 and noting that conditioning reduces entropy.

Therefore, finally we have the following upper bpund on the commitment rate for a wiretapped broadcast channel $W_{Y,Z|X}$ under $2-$privacy:

$$R \leq \max_{P_X} H(X|YZ) \tag{17}$$

On solving Eq. (17) for the independent binary symmetric broadcast (I-BS-BC(p,q)) wiretap channels, we have the following upper bound on the commitment rate for I-BS-BC(p,q) under $2-$privacy:

$$R \leq H(p) + H(q) - H(p \circledast q) \tag{18}$$

where $p \circledast q := p(1-q) + (1-p)q$, $\forall p,q \in [0,1]$ is the binary convolution between p and q, and we observe that the optimizing the input distribution is $X \sim$ Bernoulli$(1/2)$. This completes our converse analysis.

C. Achievability for the BS-BC(p,q) wiretap channel under $1-$privacy.

Our achievability protocol is inspired by works in [7], [8], [26] which utilize random hash exchange challenges and a strong randomness extractor based on 2-universal hash functions. However, unlike previous works, our scheme just requires *one round of random hash challenge* essentially to *bind* Alice to her choice in the commit phase thereby ensuring Bob's test T can detect any cheating attempt by a malicious Alice during the reveal phase. The strong randomness extractor 'Ext' extracts a secret key Ext$(\mathbf{X})$ with nR nearly random bits from $\mathbf{X}$. (note that the leftover hash lemma [27] allows us to quantify the size of this key). This secret key is then XOR-ed with the commit string c to realize a *one-time pad* scheme, which *conceals* the committed string against a malicious Bob and the wiretapper Eve in the commit phase.

Here are the details of our protocol. The rate $R := \min\{H(p), H(q)\} - \beta_2$, where the choice of $\beta_2 > 0$ is specified later. Let $\mathcal{G} := \{g : \{0,1\}^n \to \{0,1\}^{n\beta_1}\}$ be a $2-$universal hash family, where $\beta_2 > \beta_1 > 0$ is a small enough constant. Further, let $\mathcal{E} := \{\text{ext} : \{0,1\}^n \to \{0,1\}^{nR}\}$ be a $2-$universal hash family. [8]

We now describe the commit and reveal phases:

- *Commit Phase:* To commit string $c \in [2^{nR}]$, the protocol proceeds as follows:

(C1). Given c, Alice sends $\mathbf{X} \sim$ Bernoulli$(1/2)$ independent and identically distributed (i.i.d.) over the BS-BC(p,q) wiretap channel; Bob receives $\mathbf{Y}$ while Eve receives $\mathbf{Z}$.

(C2). Bob chooses a hash function $G \sim$ Unif$(\mathcal{G})$, and sends the description of G to Alice over the noiseless channel.

(C3). Alice computes $G(\mathbf{X})$ and sends it to Bob over the noiseless channel.

(C4). Alice chooses an extractor function Ext $\sim$ Unif$(\mathcal{E})$ and sends $Q = c \oplus \text{Ext}(\mathbf{X})$ and the description of Ext to Bob i.e., (Q, Ext) over the noiseless link.[9]

- *Reveal Phase:* Alice proceeds as follows:

(R1). Having received $\mathbf{Y} = \mathbf{y}$, Bob creates list $\mathcal{L}(\mathbf{y})$ of vectors given by:[10]

$$\mathcal{L}(\mathbf{y}) := \{\mathbf{x} \in \{0,1\}^n : n(p - \alpha_1) \leq d_H(\mathbf{x}, \mathbf{y}) \leq n(p + \alpha_1)\}.$$

(R2). Alice announces $(\tilde{c}, \tilde{\mathbf{x}})$ to Bob over the noiseless link.

(R3). Bob accepts $\tilde{c}$ if all the following three conditions are satisfied: (i) $\tilde{\mathbf{x}} \in \mathcal{L}(\mathbf{y})$, (ii) $g(\tilde{\mathbf{x}}) = g(\mathbf{x})$, and (iii) $\tilde{c} = q \ \oplus \text{ext}(\tilde{\mathbf{x}})$. Else, he rejects $\tilde{c}$ and outputs '0'.

Note that the wiretapper Eve also has the access to the noiseless channel so it observes everything shared between Alice and Bob over the noiseless channel during the commit as well as the reveal phase.

We now analyse and prove the security guarantees under $1-$privacy in detail for the (n,R)-commitment scheme, defined above:

[1] $\underline{\epsilon-\textit{sound:}}$ For our protocol to be ϵ-sound, it is sufficient to show that $\mathbb{P}(\mathbf{X} \notin \mathcal{L}(\mathbf{Y})) \leq \epsilon$ when both the parties, Alice and Bob, are honest; the proof for the same follows from classic Chernoff bounds.

[2] $\underline{\epsilon - 1-\textit{concealing \& } \epsilon-\textit{secure:}}$ It is known that a positive rate commitment protocol is $\epsilon - 1-$concealing and $\epsilon-$secure [11] if it satisfies the notion of *capacity-based secrecy* (cf. [28, Def. 3.2]) i.e., $I(C; V_B) \leq \epsilon$ and $I(C; V_E) \leq \epsilon$, respectively and vice versa. We use a well established equivalence relation between *capacity-based secrecy* and the *bias-based secrecy* (cf. [28, Th. 4.1]) to prove that our protocol is ϵ-concealing.

To begin, we prove that our protocol satisfies bias-based secrecy by essentially proving the perfect secrecy of the key Ext$(\mathbf{X})$; here we crucially use the *leftover hash* lemma. Several versions of this lemma exists (cf. [27], [29] for instance); we use the following (without proof):

Lemma 3 (Leftover hash lemma)**.** *Let $\mathcal{G} = \{G : \{0,1\}^n \to \{0,1\}^l\}$ be a family of universal hash functions. Then, for any hash function G chosen uniformly at random from $\mathcal{G}$, and W*

$$||(P_{G(W),G} - P_{U_l,G})|| \leq \frac{1}{2}\sqrt{2^{-H_\infty(W)}2^l}$$

where $U_l \sim$ Unif$\big(\{0,1\}^l\big)$.

[8] Note that R can be made arbitrarily close to $\mathbb{C}$.

[9] In the following expression, operator $\oplus$ denotes component-wise XOR.

[10] Here the parameter $\alpha_1 > 0$ is chosen appropriately small.

[11] where $\epsilon > 0$ is *exponentially decreasing* in blocklength n.

We begin by establishing the following lower bounds in Lemma 4 and Lemma 5 which quantify the left-over uncertainity in $\mathbf{X}$, after the information about $\mathbf{X}$ is lost to Bob and Eve due to the access of $(\mathbf{Y}, G, G(\mathbf{X}))$ and $(\mathbf{Z}, G, G(\mathbf{X}))$, respectively:

Lemma 4. *For any $\epsilon_1 > 0, \zeta_1 > 0$ and n sufficiently large,*

$$\begin{aligned} &H_\infty^{\epsilon_1}(\mathbf{X}|\mathbf{Y}, G, G(\mathbf{X})) \\ &\qquad \geq n(H(p) - \zeta_1 - \beta_1) - \log(\epsilon_1^{-1}) \end{aligned} \tag{19}$$

The proof appears in Appendix B.

Lemma 5. *For any $\epsilon_1 > 0, \zeta_2 > 0$ and n sufficiently large,*

$$\begin{aligned} &H_\infty^{\epsilon_1}(\mathbf{X}|\mathbf{Z}, G, G(\mathbf{X})) \\ &\qquad \geq n(H(q) - \zeta_2 - \beta_1) - \log(\epsilon_1^{-1}) \end{aligned} \tag{20}$$

The proof appears in Appendix B.

From Lemma 4 and Lemma 5, we have:

$$\begin{aligned} H_\infty(\mathbf{X}) &\geq \min\{H_\infty(\mathbf{X}|\mathbf{Y}, G, G(\mathbf{X})), H_\infty(\mathbf{X}|\mathbf{Z}, G, G(\mathbf{X}))\} \\ &\geq n\left\{\min\{H(p), H(q)\} - \max\{\zeta_1, \zeta_2\} - \beta_1\right\} \\ &\qquad - \log(\epsilon_1^{-1}) \end{aligned} \tag{21}$$

Now, we crucially use leftover hash lemma (Lemma 3) to show that nR nearly random bits can be extracted from $\mathbf{X}$ in the form of Ext($\mathbf{X}$) using the $2-$Universal hash function Ext (the key Ext($\mathbf{X}$) has nearly uniform distribution). This shows that the protocol satisfies *bias-based secrecy*.

Let us fix $\epsilon_1 := 2^{-n\alpha_2}$, where $\alpha_2 > 0$ is an arbitrary small constant. We make the following correspondence in Lemma 3: $G \leftrightarrow$ Ext, $W \leftrightarrow \mathbf{X}$ and $l \leftrightarrow nR$ to get the following:

$$\begin{aligned} &||P_{\text{Ext}(\mathbf{X}),\text{Ext}} - P_{U_l,\text{Ext}}|| \\ &\overset{(a)}{\leq} \frac{1}{2}\sqrt{2^{-H_\infty(\mathbf{X})}2^{nR}} \\ &\overset{(b)}{\leq} \frac{1}{2}\sqrt{2^{-n(\min\{H(p),H(q)\}-\max\{\zeta_1,\zeta_2\}-\beta_1-\alpha_2)}} \\ &\qquad\qquad . \sqrt{2^{n(\min\{H(p),H(q)\}-\beta_2)}} \\ &= \frac{1}{2}\sqrt{2^{n(\max\{\zeta_1,\zeta_2\}+\beta_1+\alpha_2-\beta_2))}} \\ &\overset{(c)}{\leq} 2^{-n\alpha_3} \end{aligned} \tag{22}$$

where, $\alpha_3 > 0$ and n is sufficiently large. Here,

(a) follows directly from Lemma 3.
(b) follows from (21) and noting that the choice of Ext is random and uniform from $\mathcal{E} : \{0,1\}^n \to \{0,1\}^{nR}$ where $R := \min\{H(p), H(q)\} - \beta_2$.
(c) follows from noting that β_2 is chosen such that $\max\{\zeta_1, \zeta_2\} + \beta_1 + \alpha_2 - \beta_2 < 0$; here, we note that α_2 is an arbitrarily chosen (small enough) constant, and $\zeta_1, \zeta_2 > 0$ can be made arbitrarily small for sufficiently large n. Thus, a choice of $\beta_2 > \beta_1$ is sufficient.

Thus, this proves that our commitment protocol satisfies bias-based secrecy (cf. [28, Def. 3.1]). Recall from our discussion earlier (see also [28, Th. 4.1]) that bias-based secrecy under *exponentially decaying* statistical distance, as in (22), implies capacity-based secrecy; hence, it follows that for n sufficiently large, we have $\max\{I(C;V_B), I(C;V_E)\} \leq \epsilon$ and our protocol is $\epsilon - 1-$concealing as well as $\epsilon-$secure.

[3] *$\epsilon - 1-$binding:* A commitment protocol satisfies $\epsilon - 1-$bindingness if under *any* behaviour of a malicicous Alice (without colluding with Eve), Bob can verify (with high probability) if Alice's revelation in the reveal phase $(\tilde{c}, \tilde{\mathbf{x}})$ are similar or different to it's choices in the commit phase.

Note that here in the $1-$privacy case, we only need to guarantee bindingness only between a malicious Alice (who *does not* colludes with the wiretapper Eve) and a honest Bob. Therefore, the $1-$bindingess analysis is almost similar to the case in which the wiretapper Eve is absent and there is a one-way *BSC(p)* from Alice to Bob.

Thus, let $\mathbf{X} = \mathbf{x}$ be the transmitted bit string and $\mathbf{Y} = \mathbf{y}$ be the bit string received by Bob's over the I-BS-BC(p, q). Alice can cheat successfully by confusing Bob in the reveal phase only if she can find two distinct bit strings $\mathbf{x}'$ and $\tilde{\mathbf{x}}$ such that (i) $\mathbf{x}', \tilde{\mathbf{x}} \in \mathcal{L}(\mathbf{y})$, and (ii) $\mathbf{x}'$, $\tilde{\mathbf{x}}$ pass the random hash exchange challenge (w.r.t hash functon $G(\cdot)$). The number of such strings that Alice can use to confuse Bob and that can pass the Bob's first test in the reveal phase are exponentially many in n; in particular, if $\mathcal{A}$ denotes this set of strings that Alice can choose to reveal in the reveal phase. Then, we have

$$|\mathcal{A}| \leq 2^{n\eta} \tag{23}$$

where $\eta > 0$.

Next, we show that the probability of hash collision for any two bit strings $\mathbf{x}$ and $\mathbf{x}'$ in $\mathcal{A}$ is exponentially decaying in n, i,e., the hash challenge prevents any malicious action of Alice.

Claim 1. *For n sufficiently large,*

$$\mathbb{P}\left(\exists \mathbf{x} \neq \mathbf{x}' \in \mathcal{A} : G(\mathbf{x}) = G(\mathbf{x}')\right) \leq 2^{-n\beta'} \tag{24}$$

The proof of the Claim appears in the Appendix C.

The fact that the secuirty parameter $\beta' > 0$, shows that our commitment protocol is $\epsilon-$binding.

D. Achievability for I-BS-BC(p, q) wiretap channel under $2-$privacy.

Similar to the previous case, this achievability protocol is also inspired by works in [7], [8], [26] and just requires *one round of random hash challenge* essentially to *bind* Alice to her choice in the commit phase.

Here are the details of our protocol. The rate $R := \min\{H(p) + H(q) - H(p \circledast q)\} - \beta_2$, where the choice of $\beta_2 > 0$ is specified later. Let $\mathcal{G} := \{g : \{0,1\}^n \to \{0,1\}^{n\beta_1}\}$ be a $2-$universal hash family, where $\beta_2 > \beta_1 > 0$ is a small enough constant. Further, let $\mathcal{E} := \{\text{ext} : \{0,1\}^n \to \{0,1\}^{nR}\}$

be a 2−universal hash family. [12]

We now describe the commit and reveal phases:

• *Commit Phase:* To commit string $c \in [2^{nR}]$, the protocol proceeds as follows:

(C1). Given c, Alice sends $\mathbf{X} \sim \text{Bernoulli}(1/2)$ independent and identically distributed (i.i.d.) over the I-BS-BC(p, q) wiretap channel; Bob receives $\mathbf{Y}$ and Eve receives $\mathbf{Z}$.

(C2). Bob chooses a hash function $G \sim \text{Unif}\,(\mathcal{G})$, and sends the description of G to Alice over the noiseless channel.

(C3). Alice computes $G(\mathbf{X})$ and sends it to Bob over the noiseless channel.

(C4). Alice chooses an extractor function $\text{Ext} \sim \text{Unif}\,(\mathcal{E})$ and sends $Q = c \oplus \text{Ext}(\mathbf{X})$ and the description of Ext to Bob i.e., (Q, Ext) over the noiseless link.[13]

• *Reveal Phase:* Alice proceeds as follows:

(R1). Having received $\mathbf{Y} = \mathbf{y}$, Bob creates list $\mathcal{L}(\mathbf{y})$ of vectors given by:[14]

$$\mathcal{L}(\mathbf{y}) := \{\mathbf{x} \in \{0,1\}^n : n(p - \alpha_1) \leq d_H(\mathbf{x}, \mathbf{y}) \leq n(p + \alpha_1)\}.$$

(R2). Alice announces $(\tilde{c}, \tilde{\mathbf{x}})$ to Bob over the noiseless link.

(R3). Bob accepts $\tilde{c}$ if all the following three conditions are satisfied:
(i) $\tilde{\mathbf{x}} \in \mathcal{L}(\mathbf{y})$,
(ii) $g(\tilde{\mathbf{x}}) = g(\mathbf{x})$, and
(iii) $\tilde{c} = q \ \oplus \text{ext}(\tilde{\mathbf{x}})$.
Else, he rejects $\tilde{c}$ and outputs '0'.

Note that the *eavesdropper* Eve also has the access to the noiseless channel so it observes everything shared between Alice and Bob over the noiseless channel during the commit as well as the reveal phase.

We now analyse and prove the security guarantees under 2−privacy in detail for the (n, R)-commitment scheme, defined above:

[1] *ϵ−sound:* This is similar to proving the ϵ−soundness for the case of 1−privacy. For our protocol to be ϵ-sound, it is sufficient to show that $\mathbb{P}\left(\mathbf{X} \notin \mathcal{L}(\mathbf{Y})\right) \leq \epsilon$ when both the parties, Alice and Bob, are honest; the proof for the same follows from classic Chernoff bounds.

[2] *$\epsilon - 2$−concealing:* It is known that a positive rate commitment protocol is $\epsilon - 2$−concealing if it satisfies the notion of *capacity-based secrecy* (cf. [28, Def. 3.2]) i.e., $I(C; V_B, V_E) \leq \epsilon$, and vice versa. We use a well established relation between *capacity-based secrecy* and the *bias-based secrecy* (cf. [28, Th. 4.1]) to prove that our protocol is $\epsilon - 2$−concealing.

We begin by establishing the following lower bound in Lemma 6 and Lemma 5 which quantify the left-over uncertainity in $\mathbf{X}$, after the information about $\mathbf{X}$ is lost to colluding Bob and Eve due to the collective access of $(\mathbf{Y}, \mathbf{Z}, G, G(\mathbf{X}))$:

Lemma 6. *For any $\epsilon_1 > 0, \zeta_1 > 0$ and n sufficiently large,*

$$\begin{aligned} &H_\infty^{\epsilon_1}(\mathbf{X}|\mathbf{Y}, \mathbf{Z}, G, G(\mathbf{X})) \\ &\qquad \geq n(H(p) + H(q) - H(p \circledast q) - \zeta_1 - \beta_1) - \log(\epsilon_1^{-1}) \end{aligned} \tag{25}$$

The proof appears in Appendix D.

Now, we crucially use leftover hash lemma (Lemma 3) to show that nR nearly random bits can be extracted from $\mathbf{X}$ in the form of $\text{Ext}(\mathbf{X})$ using the 2−Universal hash function Ext (the key $\text{Ext}(\mathbf{X})$ has nearly uniform distribution). This shows that the protocol satisfies *bias-based secrecy*.

Let us fix $\epsilon_1 := 2^{-n\alpha_2}$, where $\alpha_2 > 0$ is an arbitrary small constant. We make the following correspondence in Lemma 3: $G \leftrightarrow \text{Ext}$, $W \leftrightarrow \mathbf{X}$ and $l \leftrightarrow nR$ to get the following:

$$\begin{aligned} &\|(P_{\text{Ext}(\mathbf{X}),\text{Ext}} - P_{U_l,\text{Ext}})\| \\ &\overset{(a)}{\leq} \frac{1}{2}\sqrt{2^{-H_\infty(\mathbf{X})}2^l} \\ &\overset{(b)}{\leq} \frac{1}{2}\sqrt{2^{-H_\infty(\mathbf{X}|\mathbf{Y},\mathbf{Z},G(\mathbf{X}),G)}2^l} \\ &\overset{(c)}{\leq} \frac{1}{2}\sqrt{2^{-n(H(p)+H(q)-H(p\circledast q)-\zeta-\beta_1-\alpha_2)}} \\ &\qquad\qquad .\sqrt{2^{n(H(p)+H(q)-H(p\circledast q)-\beta_2)}} \\ &= \frac{1}{2}\sqrt{2^{n(\zeta+\beta_1-\beta_2+\alpha_2))}} \\ &\overset{(d)}{\leq} 2^{-n\alpha_3} \end{aligned} \tag{26}$$

where, $\alpha_3 > 0$ and n is sufficiently large. Here,

(a) follows from Lemma 3.
(b) follows from noting that min-entropy upper bounds conditional min-entropy.
(c) follows from Lemma 4 and noting that $R := H(p) + H(q) - H(p \circledast q) - \beta_2$ for arbitrarily small β_2.
(d) follows from noting that β_2 is chosen such that $\zeta + \beta_1 + \alpha_2 - \beta_2 < 0$; here, we note that ζ and α_2 can be made arbitrarily small for sufficiently large n, therefore, a choice of $\beta_2 > \beta_1$ is sufficient.

From (26) and Lemma 3, it follows that the specified commitment protocol satisfies biased-based secrecy which further implies capacity-based secrecy. Thus, our protocol satisfies ϵ-concealment for sufficiently large n.

[3] *$\epsilon - 2$−binding:* A commitment protocol satisfies ϵ-bindingness if under *any* behaviour of colluding Alice and Eve, Bob is able to verify (with high probability) if Alice's revelation in the reveal phase $(\tilde{c}, \tilde{\mathbf{x}})$ are similar to it's choices

[12] Note that R can be made arbitrarily close to $\mathbb{C}$.

[13] In the following expression, operator $\oplus$ denotes component-wise XOR.

[14] Here the parameter $\alpha_1 > 0$ is chosen appropriately small.

in the commit phase or are different.

Note that for the independent broadcast wiretap channel $W_{Y,Z|X}$, we have the following decomposition $W_{Y,Z|X} = W_{Y|X}W_{Z|X}$, and thus the following markov chain $Y - X - Z$ holds.

It implies that eventually Alice colluding with Eve doesn't helps Alice in extracting any extra information about the vector $\mathbf{Y}$ received by Bob i.e., $H(\mathbf{Y}|\mathbf{X},\mathbf{Z}) = H(\mathbf{Y}|\mathbf{X})$. Thus, the sender Alice in the $2-$privacy case is only as powerful as in the $1-$privacy case without colluding with Eve. Thus, our bindingness analysis for the $2-$privacy case is similar to the analysis for the $1-$privacy case, in the previous subsection. This completes our analysis for $\epsilon-2-$bindingness.

[4] $\underline{\epsilon-secure:}$ A commitment protocol is $\epsilon-$secure if for any behaviour of the wiretapper Eve, we have $I(C;V_E) \leq \epsilon$.

This directly holds due to the fact that our commitment protocol satisfies $\epsilon - 2-$concealment. As a result, we have

$$\begin{aligned} I(C;V_E) &\leq I(C;V_E,V_B) \\ &\leq \epsilon \end{aligned} \tag{27}$$

where ϵ is exponentially decaying in the blocklength n. Therefore, our commitment protocol is $\epsilon-$secure against Eve.

VI. Concluding Remarks and Discussion

We initiated the study of *wiretapped commitment* in the presence of an eavesdropper in this work. We studied the maximum commitment throughput *a.k.a commitment capacity* of certain subclasses of wiretap channels by providing security guarantees under two regimes i.e., $1-$privacy - where the eavesdropper *cannot* collude with any of the legitimate parties of the commitment protocol, and $2-$privacy - in which the eavesdropper can collude with (atmost) one of the legitimate (malicious) parties to affect the protocol.

Our converse bounds under the $1-$privacy regime as well as under the $2-$privacy regime hold for any wiretap channel. Then, under $1-$privacy we provided a matching achievability for BS-BC wiretap channels and completely characterized their $1-$privacy commitment capacity. In the $2-$privacy regime, we provided a matching achievability for I-BS-BC wiretap channel (which form a sub-class of the BS-BC wiretap channels) and thus, also completely characterized the $2-$privacy commitment capacity of the I-BS-BC wiretap channel. Also, it is important to note that our $1-$privacy converse proof for $R \leq \max_{P_X} H(X|Z)$ assumes the independence of the public communication and the channel output, given the channel input. While, it seems a fairly natural assumption in commitment protocols, we believe there might exist a more general converse proof which bypasses this asumption of the markov chain.

The degraded binary symmetric broadcast (D-BS-BC) wiretap channel presents an interesting challenge in the $2-$privacy regime. While the upper bound in Eq. (2) holds, it can be shown that the bound is quite weak (we conjecture that the capacity in this case will be strictly lower than in Eq. (2) for meaningful values of p, q). The key challenge for this setup resides in analysing the effect of collusion between Alice and Eve (and the accompanying commitment rate penalty).

VII. Acknowledgements

A. K. Yadav was partially supported by the Swiss National Science Foundation (SNSF) grant N$^{\text{o}}$ 211337. M. Mamindlapally was partially supported by the Dutch Research Council (NWO) as part of the project Divide and Quantum 'D&Q' NWA.1389.20.241 of the program 'NWA-ORC'. A. J. Budkuley was partially supported by Dept. of Science and Technology, Govt. of India, through grant MTR/2023/001412.

References

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

[2] A. D. Wyner, "The wire-tap channel," *Bell system technical journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[3] C. Crépeau and J. Kilian, "Achieving oblivious transfer using weakened security assumptions," in *[Proceedings 1988] 29th Annual Symposium on Foundations of Computer Science*. IEEE Computer Society, 1988, pp. 42–52.

[4] C. Crépeau, "Efficient cryptographic protocols based on noisy channels," in *Proceedings of the 16th annual international conference on Theory and application of cryptographic techniques*, ser. EUROCRYPT'97. Berlin, Heidelberg: Springer-Verlag, May 1997, pp. 306–317.

[5] A. Winter, A. C. A. Nascimento, and H. Imai, "Commitment capacity of discrete memoryless channels," in *IMA International Conference on Cryptography and Coding*. Springer, 2003, pp. 35–51.

[6] M. Mamindlapally, A. K. Yadav, M. Mishra, and A. J. Budkuley, "Commitment capacity under cost constraints," in *2021 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2021, pp. 3208–3213.

[7] I. Damgård, J. Kilian, and L. Salvail, "On the (im) possibility of basing oblivious transfer and bit commitment on weakened security assumptions," in *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 1999, pp. 56–73.

[8] C. Crépeau, R. Dowsley, and A. C. A. Nascimento, "On the commitment capacity of unfair noisy channels," *IEEE Transactions on Information Theory*, vol. 66, no. 6, pp. 3745–3752, 2020.

[9] A. Budkuley, P. Joshi, M. Mamindlapally, and A. K. Yadav, "On the (im) possibility of commitment over gaussian unfair noisy channels," in *2023 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2023, pp. 483–488.

[10] D. Khurana, H. K. Maji, and A. Sahai, "Secure computation from elastic noisy channels," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2016, pp. 184–212.

[11] A. J. Budkuley, P. Joshi, M. Mamindlapally, and A. K. Yadav, "On reverse elastic channels and the asymmetry of commitment capacity under channel elasticity," *IEEE Journal on Selected Areas in Communications*, 2022.

[12] H.-K. Lo and H. F. Chau, "Why quantum bit commitment and ideal quantum coin tossing are impossible," *Physica D: Nonlinear Phenomena*, vol. 120, no. 1-2, pp. 177–187, 1998.

[13] M. Fischlin, "Trapdoor commitment schemes and their applications," Ph.D. dissertation, Frankfurt (Main), Univ., Diss., 2001, 2001.

[14] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proceedings of the 6th ACM conference on Computer and communications security*, 1999, pp. 28–36.

[15] R. Chou and M. R. Bloch, "Commitment over multiple-access channels," in *2022 58th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2022, pp. 1–6.

[16] M. Mishra, B. K. Dey, V. M. Prabhakaran, and S. N. Diggavi, "Wiretapped oblivious transfer," *IEEE Transactions on Information Theory*, vol. 63, no. 4, pp. 2560–2595, 2017.

[17] M. Mishra, B. K. Dey, V. M. Prabhakaran, and S. Diggavi, "The oblivious transfer capacity of the wiretapped binary erasure channel," in *2014 IEEE International Symposium on Information Theory*, 2014, pp. 1539–1543.

[18] H. Imai, K. Morozov, A. C. A. Nascimento, and A. Winter, "Efficient protocols achieving the commitment capacity of noisy correlations," in *2006 IEEE International Symposium on Information Theory*, 2006, pp. 1432–1436.

[19] 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 Transactions on Information Theory*, vol. 57, no. 8, pp. 5566–5571, 2011.

[20] A. K. Yadav and P. Kumar, "Oblivious transfer over compound binary erasure channels," *IEEE Communications Letters*, vol. 26, no. 5, pp. 979–983, 2022.

[21] N. Nisan and D. Zuckerman, "Randomness is linear in space," *Journal of Computer and System Sciences*, vol. 52, no. 1, pp. 43–52, 1996.

[22] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *International conference on the theory and applications of cryptographic techniques*. Springer, 2004, pp. 523–540.

[23] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge: Cambridge University Press, 2011.

[24] A. D. Wyner, "The rate-distortion function for source coding with side information at the decoder-ii: General source," *Information and Control*, vol. 38, pp. 60–80, 1978.

[25] A. E. Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge University Press, 2011.

[26] A. K. Yadav, M. Mamindlapally, A. J. Budkuley, and M. Mishra, "Commitment over compound binary symmetric channels," in *2021 National Conference on Communications (NCC)*. IEEE, 2021, pp. 1–6.

[27] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *International conference on the theory and applications of cryptographic techniques*. Springer, 2004, pp. 523–540.

[28] I. B. Damgard, T. P. Pedersen, and B. Pfitzmann, "Statistical secrecy and multibit commitments," *IEEE Transactions on Information Theory*, vol. 44, no. 3, pp. 1143–1151, 1998.

[29] R. Impagliazzo, L. A. Levin, and M. Luby, "Pseudo-random generation from one-way functions," in *Proceedings of the twenty-first annual ACM symposium on Theory of computing*, 1989, pp. 12–24.

[30] A. Vitanov, F. Dupuis, M. Tomamichel, and R. Renner, "Chain rules for smooth min- and max-entropies," *IEEE Transactions on Information Theory*, vol. 59, no. 5, pp. 2603–2612, 2013.

[31] R. Renner and S. Wolf, "Simple and tight bounds for information reconciliation and privacy amplification," in *Advances in Cryptology - ASIACRYPT 2005*, B. Roy, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 199–216.

[32] A. C. A. Nascimento, J. Barros, S. Skludarek, and H. Imai, "The Commitment Capacity of the Gaussian Channel Is Infinite," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2785–2789, Jun. 2008.

Appendix

A. Proof of Lemma 1 and Lemma 2

Recall that V_B denotes the view of Bob at the end of commit phase.

Let's define[15] $\tilde{c} := \arg\max_{c\in[2^{nR}]} T(\tilde{c}, \mathbf{X}, V_B)$. Now, we will bound from above $\mathbb{P}(\hat{C} \neq C)$, where $\hat{C} = \hat{C}(V_B, \mathbf{X}) = \tilde{c}$. As the commitment scheme is $\epsilon_n - 2-$binding for the $2-$privacy case (similarly, $1-$binding for the $1-$privacy case), we know that,

$$\mathbb{P}\left(T(\bar{c}, \bar{\mathbf{X}}, V_B) = 1 \quad \& \quad T(\hat{c}, \hat{\mathbf{X}}, V_B) = 1\right) \le \epsilon_n \tag{28}$$

for any two distinct $(\bar{c}, \bar{\mathbf{X}})$ and $(\hat{c}, \hat{\mathbf{X}})$ under *any* behaviour of Alice under possible collusion with Eve (*any* behaviour of Alice under no collusion with Eve, in the $1-$privacy case). Thus, for the given decoder, we have

$$\begin{aligned}\mathbb{P}(\hat{C} \neq C) &= \mathbb{P}(\hat{C} = 0) + \mathbb{P}(\hat{C} \neq C | C \neq 0)\\ &\le \epsilon_n + \epsilon_n\\ &= 2\epsilon_n.\end{aligned} \tag{29}$$

where in the penultimate inequality, the first part follows from noting that $\mathscr{P}_n$ is $\epsilon_n - 2-$binding, and the second part follows from the fact that conditioned on $\mathscr{P}_n$ being $\epsilon_n - 2-$binding, the probability that $\hat{C}$ is different from C is at most ϵ_n due to $\mathscr{P}_n$ being ϵ_n-sound.

We now use Fano's inequality (cf. [25]) to upper bound the following conditional entropy.

$$\begin{aligned}H(C|\mathbf{X}, V_B, V_E) &\overset{(a)}{\le} H(C|\mathbf{X}, V_B)\\ &\overset{(b)}{\le} 1 + \mathbb{P}(\hat{C} \neq C) nR\\ &\overset{(c)}{\le} n\left(\frac{1}{n} + 2\epsilon_n R\right)\\ &\le n\epsilon_n'\end{aligned} \tag{30}$$

where $\epsilon_n' \to 0$ as $n \to \infty$, and

(a) follows from noting that conditioning reduces entropy.
(b) follows from the Fano's inequality (cf. [25]).
(c) follows from Eq. (29).

This completes the proof of the Lemma 1 as well as Lemma 2.

B. Proof of Lemma 4 and Lemmma 5

Before we start with the proof, we recap a few well known results (without proof) which will be needed in our proof.

Claim 2 (Min-entropy [30], [31]). *For any* $0 \le \mu, \mu', \mu_1, \mu_2 < 1$ *and any set of jointly distributed random variables* (X, Y, W)*, we have*

$$\begin{aligned}&H_\infty^{\mu+\mu'}(X, Y|W) - H_\infty^{\mu'}(Y|W)\\ &\ge H_\infty^{\mu}(X|Y, W) &(31)\\ &\ge H_\infty^{\mu_1}(X, Y|W) - H_0^{\mu_2}(Y|W) - \log\left[\frac{1}{\mu - \mu_1 - \mu_2}\right] &(32)\end{aligned}$$

Claim 3 (Max-entropy [30], [31]). *For any* $0 \le \mu, \mu', \mu_1, \mu_2 < 1$ *and any set of jointly distributed random variables* (X, Y, W)*, we have*

$$\begin{aligned}&H_0^{\mu+\mu'}(X, Y|W) - H_0^{\mu'}(Y|W)\\ &\le H_0^{\mu}(X|Y, W) &(33)\\ &\le H_0^{\mu_1}(X, Y|W) - H_\infty^{\mu_2}(Y|W) + \log\left[\frac{1}{\mu - \mu_1 - \mu_2}\right] &(34)\end{aligned}$$

Using the above two claims establishing a lower bound on the following smooth-min-entropy:

$$\begin{aligned}&H_\infty^{\epsilon_1}(\mathbf{X}|\mathbf{Y}, G(\mathbf{X}), G)\\ &\overset{(a)}{\ge} H_\infty(\mathbf{X}, G(\mathbf{X}), |\mathbf{Y}, G)\\ &\qquad - H_0(G(\mathbf{X})|\mathbf{Y}, G) - \log(\epsilon_1^{-1})\\ &\overset{(b)}{\ge} H_\infty(\mathbf{X}|\mathbf{Y}, G) + H_\infty(G(\mathbf{X})|\mathbf{Y}, G, \mathbf{X})\\ &\qquad - H_0(G(\mathbf{X})|\mathbf{Y}, G) - \log(\epsilon_1^{-1})\\ &\overset{(c)}{\ge} H_\infty(\mathbf{X}|\mathbf{Y}, G)\\ &\qquad - H_0(G(\mathbf{X})|\mathbf{Y}, G) - \log(\epsilon_1^{-1})\\ &\overset{(d)}{=} H_\infty(\mathbf{X}|\mathbf{Y}) - H_0(G(\mathbf{X})|\mathbf{Y}, G) - \log(\epsilon_1^{-1})\\ &\overset{(e)}{\ge} (H(\mathbf{X}|\mathbf{Y}) - \zeta_1) - H_0(G(\mathbf{X})|\mathbf{Y}, G) - \log(\epsilon_1^{-1})\\ &\overset{(f)}{\ge} n(H(p) - \zeta_1) - n\beta_1 - \log(\epsilon_1^{-1})\\ &= n(H(p) - \zeta_1 - \beta_1) - \log(\epsilon_1^{-1})\end{aligned} \tag{35}$$

where we have

(a) from the chain rule for smooth min-entropy; see Claim 2 and substitute $\mu = \epsilon_1$, $\mu_1 = 0$ and $\mu_2 = 0$ in Eq. (32).
(b) from the chain rule for min-entropy; see Claim 2 and and substitute $\mu = 0$ and $\mu' = 0$ in Eq. (31).
(c) from the fact that $G(\mathbf{X})$ is a deterministic function of G and $\mathbf{X}$.
(d) by the Markov chain $\mathbf{X} - \mathbf{Y} - G$.
(e) from [32, Th. 1] which allows us to lower bound $H_\infty(\mathbf{X}|\mathbf{Y})$ in terms of $H(\mathbf{X}|\mathbf{Y})$
(f) by noting that the effective channel from Alice to Bob is a *BSC(p)*, and from definition of max-entropy (also noting that the range of G is $\{0, 1\}^{n\beta_1}$).

Remark 3. *The proof for Lemma 5 follows similarly. Note that in this case, the following markov chain* $\mathbf{X} - \mathbf{Z} - G$ *exists. Additionally, we have* $H_\infty(\mathbf{X}|\mathbf{Z}) \ge H(\mathbf{X}|\mathbf{Z}) - \zeta_2 = H(q) - \zeta_2$*, for arbitrarily small constant* $\zeta_2 > 0$.

[15] Although Bob's test T is a randomized test, it can be shown that one can construct from T a deterministic test with essentially the same soundness and bindingness performance. Hence, for the rest of the converse, we consider that Bob's test is a deterministic function; as such, $\tilde{c}$ is well defined for such a deterministic test.

C. Proof of Claim 1

Recall that $G \sim \text{Unif}(\mathcal{G})$, where $\mathcal{G} = \{g : \{0,1\}^n \to \{0,1\}^{n\beta_1}\}$. Therefore for any $\mathbf{x}, \mathbf{x}' \in \{0,1\}^n$, we have

$$\mathbb{P}\Bigg(G(\mathbf{x}) = G(\mathbf{x}')\Bigg) \leq \frac{1}{2^{n\beta_1}} \tag{36}$$

Now,

$$\begin{aligned}
&\mathbb{P}\Bigg(\exists \mathbf{x} \neq \mathbf{x}' \in \mathcal{A} : G(\mathbf{x}) = G(\mathbf{x}')\Bigg) \\
&\overset{(a)}{\leq} \binom{|\mathcal{A}|}{2} \mathbb{P}\left(G(\mathbf{x}) = G(\mathbf{x}')\right) \\
&\overset{(b)}{\leq} \binom{2^{n\eta}}{2} 2^{-n\beta_2} \\
&< 2^{2n\eta} 2^{-n\beta_1} \\
&\overset{(c)}{\leq} 2^{-n\beta'}
\end{aligned} \tag{37}$$

where (a) follows from the definition of $\mathcal{A}$, and using the union bound (on distinct pairs of vectors in $\mathcal{A}$); we get (b) from the definition of $\mathcal{G}$. Further, (c) follows from the fact that β_1 is chosen such that $\beta' := \beta_1 - 2\eta > 0$. This completes the proof of the claim.

D. Proof of Lemma 6

Using the Claim 2 and Claim 3, we establish a lower bound on the following smooth-min-entropy:

$$\begin{aligned}
&H_\infty^{\epsilon_1}(\mathbf{X}|\mathbf{Y}, \mathbf{Z}, G, G(\mathbf{X})) \\
&\quad \overset{(a)}{\geq} H_\infty(\mathbf{X}, G(\mathbf{X}), |\mathbf{Y}, \mathbf{Z}, G) \\
&\qquad\quad - H_0(G(\mathbf{X})|\mathbf{Y}, \mathbf{Z}, G) - \log(\epsilon_1^{-1}) \\
&\quad \overset{(b)}{\geq} H_\infty(\mathbf{X}|\mathbf{Y}, \mathbf{Z}, G) + H_\infty(G(\mathbf{X})|\mathbf{Y}, \mathbf{Z}, G, \mathbf{X}) \\
&\qquad\quad - H_0(G(\mathbf{X})|\mathbf{Y}, \mathbf{Z}, G) - \log(\epsilon_1^{-1}) \\
&\quad \overset{(c)}{\geq} H_\infty(\mathbf{X}|\mathbf{Y}, \mathbf{Z}, G) \\
&\qquad\quad - H_0(G(\mathbf{X})|\mathbf{Y}, G) - \log(\epsilon_1^{-1}) \\
&\quad \overset{(d)}{=} H_\infty(\mathbf{X}|\mathbf{Y}, \mathbf{Z}) - H_0(G(\mathbf{X})|\mathbf{Y}, \mathbf{Z}, G) - \log(\epsilon_1^{-1}) \\
&\quad \overset{(e)}{\geq} (H(\mathbf{X}|\mathbf{Y}, \mathbf{Z}) - \zeta_1) - H_0(G(\mathbf{X})|\mathbf{Y}, \mathbf{Z}, G) - \log(\epsilon_1^{-1}) \\
&\quad \overset{(f)}{\geq} n(H(p) + H(q) - H(p \circledast q) - \zeta_1) - n\beta_1 - \log(\epsilon_1^{-1}) \\
&\quad = n(H(p) + H(q) - H(p \circledast q) - \zeta_1 - \beta_1) - \log(\epsilon_1^{-1})
\end{aligned} \tag{38}$$

where we have

(a) from the chain rule for smooth min-entropy; see Claim 2 and substitute $\mu = \epsilon_1$, $\mu_1 = 0$ and $\mu_2 = 0$ in Eq. (32).
(b) from the chain rule for min-entropy; see Claim 2 and and substitute $\mu = 0$ and $\mu' = 0$ in Eq. (31).
(c) from the fact that $G(\mathbf{X})$ is a deterministic function of G and $\mathbf{X}$.
(d) by the Markov chain $\mathbf{X} - (\mathbf{Y}, \mathbf{Z}) - G$.
(e) from [32, Th. 1] which allows us to lower bound $H_\infty(\mathbf{X}|\mathbf{Y}, \mathbf{Z})$ in terms of $H(\mathbf{X}|\mathbf{Y}, \mathbf{Z})$.
(f) by noting that $H(\mathbf{X}|\mathbf{Y}, \mathbf{Z}) = H(p) + H(q) - H(p \circledast q)$, and from definition of max-entropy (also noting that the range of G is $\{0,1\}^{n\beta_1}$).