Retractable Commitment over Noisy Channels

Rémi A. Chou
Department of Electrical Engineering and Computer Science
Wichita State University
Email: remi.chou@wichita.edu

Matthieu R. Bloch
School of Electrical and Computer Engineering
Georgia Institute of Technology
Email: matthieu.bloch@ece.gatech.edu

2023 IEEE Information Theory Workshop (ITW) | 979-8-3503-0149-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/ITW55543.2023.10161683

***Abstract*—Consider a commitment protocol between two parties, Alice and Bob, in which Alice may (i) commit to a message using a non-redundant discrete memoryless channel whose outputs are observed by Bob; and (ii) later reveal her committed message to Bob who must decide whether Alice is revealing the message she actually committed to. A commitment protocol should meet three standard requirements: concealment, bindingness, and soundness, to ensure that no party may act dishonestly. Our objective is to study whether one can enforce a fourth requirement that would allow Alice to retract a commitment before the reveal phase starts without Bob detecting that she ever participated in the commit phase of the protocol. We positively answer this question and characterize the commitment capacity for such a setting by relying on tools developed for covert communication.**

A full version of the paper is available at https://bloch.ece.gatech.edu/ITWretractablecommitment.pdf.

I. Introduction

A commitment protocol is a cryptographic protocol in which a player, Alice, commits a message to another player, Bob, hiding the value of the message until she chooses to reveal it but without being able to change its value. Specifically, in a commitment protocol, one wants to ensure that the protocol is i) *concealing*, i.e., Alice's message remains concealed from Bob until revealed; ii) *binding*, i.e., Alice cannot alter her message after committing to it; and, iii) *sound*, i.e., Alice's commitment is accepted as truthful when both players behave honestly. Commitment protocols may be used as primitives in a broad range of cryptographic applications, from online auctions [1] to zero-knowledge proofs [2], [3] or secure computations [4]. In the information-theoretic setting, in which players have unlimited computational power, commitment protocols can be constructed if the two players have access to noisy resources, e.g., in the form of a noisy channel between Alice and Bob [5], [6], [7]. Such commitment protocols leverage the information-theoretic mechanisms related to secure communication over wiretap channels [8] and secret-key generation from correlated sources [9], [10].

The commitment capacity of a non-redundant Discrete Memoryless Channel (DMC), defined as the supremum of message rates at which Alice can run a concealing, binding, and sound protocol using the DMC, has been fully characterized in [6]. The commitment capacity has also been derived for classical-quantum channels over finite-dimensional Hilbert spaces [11] and for Gaussian channels, in which case it is infinite [12]. A partial characterization of the commitment capacity region is also known when commitment involves multiple users connected with a single receiver through a multiple-access channel [13]. Finally, there has been renewed interest in studying commitment protocols over more adversarial models in which one or more players partially control the DMC between them [14], [15], [16], [17], [18].

In this paper, we study whether additional requirements can be imposed on a commitment protocol. Specifically, we study whether a commitment protocol can be *retractable*, in the sense that Alice would be able to retract her commitment *before the reveal phase starts* without Bob detecting that she ever participated in the commit phase of the protocol. Of course, the ability to retract should not compromise the concealing, binding, and sound nature of a protocol. Our main contribution is to show how to formulate the problem of retractable commitment and to characterize the commitment capacity by building upon concepts and tools developed for the study of covert communications [19], [20], [21]. In particular, we show that the number of commitment bits scales as $O(\sqrt{n}\log n)$. For ease of exposition, we focus on binary-input channels.

The remaining of the paper is organized as follows. After a brief review of notation in Section II, the retractable commitment model is introduced in Section III. Our main result, the characterization of the retractable commitment capacity, is given in Section IV, while proofs are deferred to Section V.

II. Notation

We denote random variables and their realizations by upper and lower case, respectively, e.g, X and x. Unless otherwise specified, a random variable X takes value in a generic finite alphabet $\mathcal{X}$, denoted in calligraphic case, and has distribution P_X. The cardinality of $\mathcal{X}$ is $|\mathcal{X}|$. The n-fold product distribution constructed from P_X is denoted by $P_X^{\otimes n}$. A length $n \in \mathbb{N}$ sequence is denoted by $\mathbf{x}$, where the value of n is given by the context, and the n components are denoted by $\{x_i\}_{i=1}^n$. Throughout the paper, $\log$ and $\exp$ are understood to the base e. For $x \in \mathcal{X}$ and a sequence $\mathbf{x} \in \mathcal{X}^n$, we define $N(x;\mathbf{x}) \triangleq \sum_{i=1}^n \mathbf{1}\{x_i = x\}$, where $\mathbf{1}\{\cdot\}$ denotes the indicator function. The Hamming distance $d_H(\mathbf{x},\mathbf{x}')$ between two sequences $\mathbf{x}$ and $\mathbf{x}'$ is the number of positions in which they differ. For $\mathcal{X} \triangleq \{x_0, x_1\}$, the weight of a sequence $\mathbf{x}$ is $\mathrm{wt}(\mathbf{x}) \triangleq d_H(\mathbf{x}, \mathbf{x}_0)$, where $\mathbf{x}_0$ is the all-x_0 sequence.

R. Chou was supported in part by NSF grant CCF-2047913. M. R. Bloch was supported in part by NSF grant CCF-1955401

For two random variables X, Y with joint distribution $P_X W_{Y|X}$, the mutual information is denoted by $\mathbb{I}\big(P_X; W_{Y|X}\big)$ or $\mathbb{I}(X;Y)$ depending on the context. We also let $P_X \circ W_{Y|X}$ denote the marginal on Y of $P_X W_{Y|X}$. For two distributions P and Q, $\|P-Q\|_1$ and $\mathbb{D}(P\,\|\,Q)$ denote the norm 1 distance and the relative entropy between them, respectively. We also use the chi-squared distance $\chi_2(P\|Q) \triangleq \sum_x \frac{(P(x)-Q(x))^2}{Q(x)}$. The binary entropy function with parameter $p \in [0;1]$ is denoted by $h_b(p)$.

III. Retractable Commitment Model

We assume that Alice and Bob have access to a DMC $(\mathcal{X}, W_{Y|X}, \mathcal{Y})$ with $\mathcal{X} = \{x_0, x_1\}$, whose input is controlled by Alice and whose output is observed by Bob. We set $Q_0 \triangleq W_{Y|X=x_0}$ and $Q_1 \triangleq W_{Y|X=x_1}$. Similar to [6], we assume that the DMC is non-redundant, i.e.,

$$Q_1 \neq Q_0. \tag{1}$$

We also assume that Q_1 is absolutely continuous with respect to Q_0. The DMC itself is outside the control of all parties and we assume that the input symbol x_0 is an *innocent* input symbol, that corresponds to the resting state of the channel, i.e., the channel input when Alice does not use the channel. We also assume that Alice and Bob have access to a noiseless public channel of unlimited capacity over which they can exchange messages.

We consider commitment protocols that operate in two phases as illustrated in Fig. 1.

1) In the *commit phase*, Alice chooses a message $a \in [\![1; M]\!]$. Then, she forms from a and some local randomness, denoted by S, a sequence X^n that is transmitted over the DMC. Bob observes the corresponding channel outputs Y^n with distribution P_{Y^n}. Alice's encoding function is known to all parties.
2) In the *reveal phase*, Alice announces over the public noiseless channel (a', S'). Bob runs a statistical test $\beta(a', S', Y^n)$ that returns 0 or 1 if Bob rejects or accepts Alice's revealed commitment, respectively.

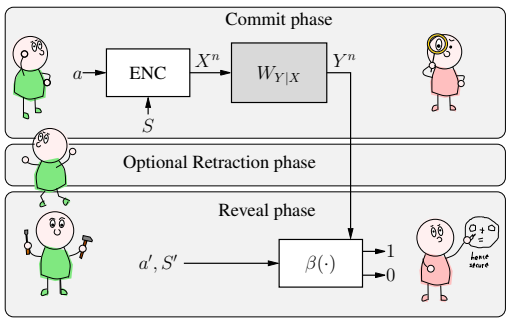

Fig. 1. Retractable commitment protocol

A commitment protocol is ϵ-concealing if for any distinct messages a and a' inducing distributions $P^a_{Y^n}$ and $P^{a'}_{Y^n}$, respectively, on $\mathcal{Y}^n$,

$$\left\| P^a_{Y^n} - P^{a'}_{Y^n} \right\|_1 \leqslant \epsilon. \tag{2}$$

A commitment protocol is δ-binding if for any $a, a' \in [\![1; M]\!]$ such that $a \neq a'$, and for any S',

$$\mathbb{P}[\beta(a, S, Y^n) = 1 = \beta(a', S', Y^n)] \leqslant \delta. \tag{3}$$

A commitment protocol is δ-sound if

$$\mathbb{P}[\beta(a, S, Y^n) = 1] \geqslant 1 - \delta. \tag{4}$$

Finally, a commitment protocol is μ-retractable if, at the end of the commit phase, we have

$$\mathbb{D}\big(P_{Y^n} \,\big\|\, Q_0^{\otimes n}\big) \leqslant \mu. \tag{5}$$

The concealing, binding, and soundness properties are identical to those of standard commitment protocols [6]. The retractability property mandates that the distribution P_{Y^n} observed by Bob be nearly indistinguishable from the independent and identically distributed (i.i.d.) distribution $Q_0^{\otimes n}$ expected if Alice were to not commit a message. It is well-known that controlling the relative entropy between the distributions P_{Y^n} and $Q_0^{\otimes n}$ amounts to controlling Bob's ability to detect the presence of a commitment, regardless of its statistical test, see, e.g., [20], [21], [22].

As we shall see that $\log M$ scales sub-linearly with n, we must identify an algebraic or transcendental function $f(n)$, increasing with n, independent of channels statistics and protocol parameters, that captures the optimal scaling of $\log M$ with n. We call $\frac{\log M}{f(n)}$ the throughput of the protocol. A throughput R is achievable if there exist commitment protocols for every n with throughput converging to R, which are ϵ–concealing, δ–binding, and μ-retractable with $\epsilon, \delta \to 0$ as $n \to \infty$. The retractable commitment capacity C_{retract} is the supremum of all achievable throughputs. If $f(n)$ were overestimated, $\frac{\log M}{f(n)}$ would converge to zero regardless of the channel; similarly, if $f(n)$ were underestimated, $\frac{\log M}{f(n)}$ would diverge.

Remark III.1. *Commitment protocols can be either interactive or non-interactive in the commit phase. Interactive protocols have been particularly useful to study the commitment capacity with adversarial control of the channel [17], [18]. In the context of retractable commitment, however, interactive protocols are incompatible with the problem setting as interactive communication with Bob during the commit phase would indicate that Alice is participating in the commit phase without the possibility for her to deny it.*

Remark III.2. *Our notion of retractability explicitly requires Alice to be undetectable with respect to (w.r.t.) a reference distribution Q_0, corresponding to a deterministic channel input x_0. One could also use a distribution induced by a channel input distribution P_X, in which case the scaling $f(n)$ would be n. This distinction is similar to that between covertness [19] and stealth [23].*

IV. Retractable Commitment Capacity

Theorem IV.1. *Consider a non-redundant DMC $(\mathcal{X}, W_{Y|X}, \mathcal{Y})$ with $\mathcal{X} \triangleq \{x_0, x_1\}$ and x_0 the innocent input symbol. Let $\mu > 0$ be retractablity parameter. The retractable*

commitment capacity is obtained for $f(n) = \sqrt{n}\log n$. *Further,*

$$C_{\text{retract}} = \sqrt{\frac{\mu}{2\chi_2\left(Q_1 \| Q_0\right)}}.$$

Theorem IV.1 is proved in Section V but we provide here a brief intuitive description of the proof. The crux of the approach is to use the insights developed in [6], by which a wiretap code with a controlled minimum distance is used to commit messages. Specifically, during the commit phase, Alice commits to a message a by encoding it along with a local secret S using the wiretap code and transmitting the resulting codeword X^n over the DMC. The semantic secrecy [24] provided by the wiretap code against the DMC $(\mathcal{X}, W_{Y|X}, \mathcal{Y})$ ensures that the protocol is concealing. During the reveal phase, Alice discloses a' and s'. The minimum distance of the wiretap code ensures that the protocol is binding because Alice cannot reveal a codeword other than X^n without the cheating being detected. We modify the wiretap code construction of [6] to operate in a covert regime, in which the fraction of symbols x_1 in the codewords is on the order of $\frac{1}{\sqrt{n}}$. Intuitively, the scaling $\sqrt{n}\log n$ in Theorem IV.1 follows because the entropy rate of the input in the covert regime scales as $\frac{\log n}{\sqrt{n}}$. In addition, the leakage to the eavesdropper scales as $\frac{1}{\sqrt{n}}$, so that the concealing property of the protocol comes almost "for free." Note that the retractable commitment capacity depends on μ, which is consistent with the absence of a strong converse in covert communication [20], [21].

Corollary IV.2. *Consider a Binary Symmetric Channel (BSC) with cross over probability* p *in which* 0 *is the innocent input. Then,*

$$C_{\text{retract}} = \sqrt{\frac{\mu p(1-p)}{2(1-2p^2)}}.$$

V. Proof of Theorem IV.1

A. Achievability proof

Our construction of a retractable commitment protocol follows the non-interactive protocol construction of [6], with the necessary modifications to operate in the regime where retractability is possible. We first establish the existence of a wiretap code with specific secrecy, minimum distance, and weight guarantees.

Proposition V.1. *Let* $\alpha, \nu \in (0;1)$, $\sigma \in (0; \frac{\alpha}{2}(1-\nu))$, *and* $\sigma_1 \in (0;\alpha)$. *Consider a distribution* P_X *on* $\mathcal{X}$ *defined as*

$$P_X(x_0) \triangleq 1 - \frac{\alpha}{\sqrt{n}} \qquad P_X(x_1) \triangleq \frac{\alpha}{\sqrt{n}}.$$

Let $Q_\alpha \triangleq P_X \circ W_{Y|X}$ *denote the corresponding channel output distribution. For all* $n \in \mathbb{N}$ *large enough, there exists integers* M, K, *and a wiretap code* $\mathcal{C} \triangleq \{\mathbf{x}(a,s) \in \mathcal{X}^n : a \in [\![1;M]\!], s \in [\![1;K]\!]\}$ *such that*

1) $\exists \gamma_0 > 0$ *such that* $\forall a$, *with* $Q_a^n(\mathbf{y}) \triangleq \frac{1}{K}\sum_{s=1}^K W_{Y|X}^{\otimes n}(\mathbf{y}|\mathbf{x}(a,s))$,
$$\left\|Q_a^n - Q_\alpha^{\otimes n}\right\|_1 \leqslant e^{-\gamma_0\sqrt{n}};$$
2) $\forall (a,s)\ (\alpha-\sigma_1)\sqrt{n} \leqslant wt(\mathbf{x}(a,s)) \leqslant (\alpha+\sigma_1)\sqrt{n}$;
3) $\forall (a',s') \neq (a,s)\ d_H(\mathbf{x}(a',s'),\mathbf{x}(a,s)) \geqslant 2\sigma\sqrt{n}$;
4) *the code size satistifes*
$$\log M \geqslant \left(\frac{\alpha}{2}(1-\nu) - \sigma\right)\sqrt{n}\log n$$
$$\log K \leqslant (1+\nu)\alpha\mathbb{D}(Q_1 \,\|\, Q_0)\sqrt{n}.$$

Proof. Let $\widetilde{M}$ and $\widetilde{K}$ be integers. Generate $\widetilde{M}\widetilde{K}$ codewords $\mathbf{x}(a,s)$, with $a \in [\![1;\widetilde{M}]\!]$ and $s \in [\![1;\widetilde{K}]\!]$, independently according to the distribution $P_X^{\otimes n}$. For $\tau > 0$, define the sets

$$\mathcal{A} \triangleq \left\{(\mathbf{x},\mathbf{y}) : \log\frac{W_{Y|X}^{\otimes n}(\mathbf{y}|\mathbf{x})}{Q^{\otimes}(\mathbf{y})} < \tau\right\},$$

and $\mathcal{A}(\mathbf{x}) \triangleq \{\mathbf{y} : (\mathbf{x},\mathbf{y}) \in \mathcal{A}\}$. For any $\theta > 0$, set

$$\tau \triangleq (1+\theta)\mathbb{I}\big(P_X; W_{Y|X}\big)n. \tag{6}$$

Lemma V.2 (adapted from [21])**.**

$$\begin{aligned}\mathbb{I}\big(P_X; W_{Y|X}\big)n &= \sqrt{n}\alpha\mathbb{D}(Q_1 \,\|\, Q_0) + o(\sqrt{n})\\ nH(P_X) &= \frac{\alpha}{2}\sqrt{n}\log n + o(\sqrt{n}\log n)\\ \mathbb{D}(Q_\alpha \,\|\, Q_0) &= \frac{\alpha^2}{2n}\chi_2\left(Q_1\|Q_0\right) + o\left(\frac{1}{n}\right).\end{aligned}$$

We shall use several tail concentration bounds to obtain Property 1 following ideas from [6], [25]. Let $\widetilde{Q}_a^n(\mathbf{y}) \triangleq \frac{1}{\widetilde{K}}\sum_{s=1}^{\widetilde{K}} W_{Y|X}^{\otimes n}(\mathbf{y}|\mathbf{x}(a,s))$. Note that

$$\begin{aligned}&\left\|\widetilde{Q}_a^n - Q_\alpha^{\otimes n}\right\|_1\\ &= \sum_{\mathbf{y}}\left|\frac{1}{\widetilde{K}}\sum_{s=1}^K W_{Y|X}^{\otimes n}(\mathbf{y}|\mathbf{x}(a,s))\mathbf{1}\{(\mathbf{x}(a,s),\mathbf{y}) \in \mathcal{A}_\tau\}\right.\\ &\left.+\frac{1}{\widetilde{K}}\sum_{s=1}^K W_{Y|X}^{\otimes n}(\mathbf{y}|\mathbf{x}(a,s))\mathbf{1}\{(\mathbf{x}(a,s),\mathbf{y}) \notin \mathcal{A}_\tau\} - Q_\alpha^{\otimes n}(\mathbf{y})\right|\\ &\leqslant \sum_{\mathbf{y}} Q_\alpha^{\otimes n}(\mathbf{y})\\ &\quad\times\left|\frac{1}{\widetilde{K}}\sum_{s=1}^K \frac{W_{Y|X}^{\otimes n}(\mathbf{y}|\mathbf{x}(a,s))}{Q_\alpha^{\otimes n}(\mathbf{y})}\mathbf{1}\{(\mathbf{x}(a,s),\mathbf{y}) \in \mathcal{A}_\tau\} - 1\right|\\ &\qquad+\frac{1}{\widetilde{K}}\sum_{s=1}^K \mathbb{P}_{W_{Y|X=\mathbf{x}(a,s)}^{\otimes n}}\left(\mathbf{Y} \notin \mathcal{A}(\mathbf{x}(a,s))\right)\end{aligned} \tag{7}$$

We first analyze the second term on the right-hand side of (7). Note that the following holds because of Bernstein's inequality (the proof is omitted due to space constraints).

Lemma V.3. *There exists* $\gamma_1 > 0$ *such that for any* $\gamma \in (0;\gamma_1]$

$$\mathbb{E}\left[\mathbb{P}_{W_{Y|X=\mathbf{x}(a,s)}^{\otimes n}}\left(\mathbf{Y} \notin \mathcal{A}(\mathbf{x}(a,s))\right)\right] \leqslant e^{-\gamma\sqrt{n}}.$$

Then, invoking a Chernoff bound, we have for any $\beta > 0$

$$\mathbb{P}\left(\forall a \in [\![1;\widetilde{M}]\!]\ \frac{1}{\widetilde{K}}\sum_{s=1}^{K}\mathbb{P}_{W_{Y|X=\mathbf{x}(a,s)}^{\otimes n}}\left(\mathbf{Y}\notin\mathcal{A}(\mathbf{x}(a,s))\right) > (1+\beta)e^{-\gamma\sqrt{n}}\right) \leqslant \widetilde{M}\exp\left(-\frac{K}{3}\beta^2 e^{-\gamma\sqrt{n}}\right). \tag{8}$$

We now focus on the first term on the right-hand side of (7). For any $a \in [\![1;\widetilde{M}]\!]$ and $\mathbf{y} \in \mathcal{Y}^n$, denote

$$Y_s \triangleq \frac{W_{Y|X}^{\otimes n}(\mathbf{y}|\mathbf{x}(a,s))}{Q^{\otimes n}(\mathbf{y})}\mathbf{1}\{(\mathbf{x}(a,s),\mathbf{y})\in\mathcal{A}_\tau\}.$$

Since $0 \leqslant Y_s \leqslant e^{\tau}$ and $\mathbb{E}[Y_s] \leqslant 1$ for all $s \in [\![1;L]\!]$, invoking again a Chernoff bound we obtain

$$\begin{aligned}
&\mathbb{P}\left(\forall a\in[\![1;\widetilde{M}]\!]\forall\mathbf{y}\in\mathcal{Y}^n\ \frac{1}{\widetilde{K}}\sum_{s=1}^{K}\frac{W_{Y|X}^{\otimes n}(\mathbf{y}|\mathbf{x}(a,s))}{Q_\alpha^{\otimes n}(\mathbf{y})}\right.\\
&\quad\left.\times\mathbf{1}\{(\mathbf{x}(a,s),\mathbf{y})\in\mathcal{A}_\tau\}\notin\left[1\pm e^{-n\theta\mathbb{I}(P_X;W_{Z|X})n}\right]\right)\\
&\leqslant \widetilde{M}|\mathcal{Y}^n|\mathbb{P}\left(\frac{1}{\widetilde{K}}\sum_{s=1}^{K}Y_s\notin\left[1\pm e^{-n\theta\mathbb{I}(P_X;W_{Z|X})n}\right]\right)\\
&\leqslant 2\widetilde{M}|\mathcal{Y}^n|\exp\left(-\frac{K}{3\cdot e^{\tau}}e^{-2\theta\mathbb{I}(P_X;W_{Z|X})n}\right).
\end{aligned}\tag{9}$$

To ensure that the exponent in the right-hand-side of (9) is positive in light of the value of τ in (6), we set

$$\log\widetilde{K} \triangleq (1+4\theta)\mathbb{I}(P_X;W_{Z|X})n. \tag{10}$$

Consequently, combining (8), (9) with (7), we obtain

$$\begin{aligned}
&\mathbb{P}\left(\forall a\in[\![1;\widetilde{M}]\!],\left\|Q_a^n-Q_\alpha^{\otimes n}\right\|_1\right.\\
&\qquad\left.>(1+\beta)e^{-\gamma\sqrt{n}}+e^{-\theta\mathbb{I}(P_X;W_{Z|X})n}\right)\\
&\leqslant\widetilde{M}\exp\left(-\frac{\beta^2}{3}e^{(1+4\theta)\mathbb{I}(P_X;W_{Z|X})n-\gamma\sqrt{n}}\right)\\
&\quad+2\widetilde{M}|\mathcal{Y}^n|\exp\left(-\frac{1}{3}e^{\theta\mathbb{I}(P_X;W_{Z|X})n}\right).
\end{aligned}$$

Since we can always choose $0<\gamma<(1+4\theta)\mathbb{I}(P_X;W_{Z|X})n$ by Lemma V.2 and Lemma V.3, for n large enough we have with probability at least $\frac{2}{3}$ that $\forall a\in[\![1;\widetilde{M}]\!]\ \|Q_a^n-Q_\alpha^{\otimes n}\|_1 \leqslant (1+\beta)e^{-\gamma\sqrt{n}}+e^{-\theta\mathbb{I}(P_X;W_{Z|X})n}\leqslant e^{-\gamma_2\sqrt{n}}$ for some $\gamma_2>0$.

We shall now prove Property 2. By a Chernoff bound,

$$\mathbb{P}\left(\mathrm{wt}(\mathbf{x}(a,s))\notin[(\alpha-\sigma_1)\sqrt{n};(\alpha+\sigma_1)\sqrt{n}]\right)\leqslant 2e^{-\frac{1}{3}\sigma_1^2\alpha\sqrt{n}}.$$

By Markov's inequality, with probability at least $\frac{2}{3}$ the fraction of codewords with weight not in $[(\alpha-\sigma_1)\sqrt{n};(\alpha+\sigma_1)\sqrt{n}]$ is at most $6e^{-\frac{1}{3}\sigma_1^2\alpha\sqrt{n}}$.

We shall now prove Property 3 using the ideas of [6] and the following lemma, whose proof is omitted due to space constraints.

Lemma V.4. *There exists $\xi_0>0$ such that for any set $\mathcal{S}\subseteq\mathcal{X}^n$ with $\mathbb{P}_{P_X^{\otimes n}}(\mathcal{S})\geqslant e^{-\xi_0\sqrt{n}}$ we have for any $\rho\in(0;1)$*

$$|\mathcal{S}|\geqslant e^{\frac{\alpha}{2}(1-\rho)\sqrt{n}\log n}.$$

for n large enough.

Let $\mathcal{B}(\mathbf{x},r)\subseteq\mathcal{X}^n$ denote the Hamming ball of radius $r>0$ centered around $\mathbf{x}\in\mathcal{X}^n$. For any $a\in[\![1;\widetilde{M}]\!]$ and $s\in[\![1;\widetilde{L}]\!]$, adapting [6]

$$\begin{aligned}
&\mathbb{P}\left(\mathbf{x}(a,s)\in\bigcup_{(a',s')\neq(a,s)}\mathcal{B}(\mathbf{x}(a',s'),2\sigma\sqrt{n})\right)\\
&\leqslant\max\left\{\mathbb{P}(\mathcal{A}):|\mathcal{A}|\leqslant\widetilde{M}\widetilde{L}\frac{1-2\sigma}{1-4\sigma}\binom{n}{2\sqrt{n}\sigma}|\mathcal{X}|^{2\sqrt{n}\sigma}\right\}.
\end{aligned}\tag{11}$$

We set

$$\log\widetilde{M}\triangleq\left(\frac{\alpha}{2}(1-2\rho)-\sigma\right)\sqrt{n}\log n \tag{12}$$

so that the right-hand side of (11) is bounded by $e^{-\xi_0\sqrt{n}}$ for n large enough. By Markov's inequality, with probability at least $\frac{2}{3}$ the fraction of codewords within distance $2\sigma\sqrt{n}$ of another in the code is at most $3e^{-\xi_0\sqrt{n}}$.

Hence, there exists a codebook with the parameters $\widetilde{K}$ in (10) and $\widetilde{M}$ in (12) such that

1) $\forall a\in[\![1;\widetilde{M}]\!]\ \|Q_a^n-Q^{\otimes n}\|_1\leqslant e^{-\gamma_2\sqrt{n}}$;
2) the fraction of codewords with weight not in $[(\alpha-\sigma_1)\sqrt{n};(\alpha+\sigma_1)\sqrt{n}]$ is at most $6e^{-\frac{1}{3}\sigma_1^2\alpha\sqrt{n}}$.
3) the fraction of codewords within distance $2\sigma\sqrt{n}$ of another in the code is at most $3e^{-\xi_0\sqrt{n}}$.

By the pigeonhole principle, there exist $M\triangleq\widetilde{M}/2$ indices a for which there are at most $(6e^{-\xi_0\sqrt{n}}+12e^{-\frac{1}{3}\sigma_1^2\alpha\sqrt{n}})\widetilde{K}$ indices s corresponding to codewords $\mathbf{x}(a,s)$ within distance $2\sigma\sqrt{n}$ of others in the code. We construct a new code $\mathcal{C}$ keeping only those indices a and the $K\triangleq(1-6e^{-\xi_0\sqrt{n}}-12e^{-\frac{1}{3}\sigma_1^2\alpha\sqrt{n}})\widetilde{K}$ indices s for which codewords all have distance $2\sigma\sqrt{n}$ to others. Without loss of generality, we assume that we keep the indices $a\in[\![1;M]\!]$ and $s\in[\![1;K]\!]$. Note that the code $\mathcal{C}$ then satisfies Property 2 and Property 3 in Proposition V.1. It remains to check that Property 1 remains true. With $Q_a^n(\mathbf{y})\triangleq\frac{1}{K}\sum_{s=1}^{K}W_{Y|X}^{\otimes n}(\mathbf{y}|\mathbf{x}(a,s))$, we have

$$\begin{aligned}
&\left\|Q_a^n-Q^{\otimes n}\right\|_1\\
&\leqslant\left\|Q_a^n-\widetilde{Q}_a^n\right\|_1+\left\|\widetilde{Q}_a^n-Q^{\otimes n}\right\|_1\\
&\leqslant 12e^{-\xi_0\sqrt{n}}+24e^{-\frac{1}{3}\sigma_1^2\alpha\sqrt{n}}+\left\|\widetilde{Q}_a^n-Q^{\otimes n}\right\|_1\leqslant e^{-\gamma_0\sqrt{n}},
\end{aligned}$$

for some $\gamma_0>0$. The result then follows by defining an appropriate constant $\nu>0$ and noticing that ν can be made arbitrarily small. □

Remark V.5. *The scaling of $\log M$ and $\log K$ is different because of our choice of a biased distribution P_X in the random codebook generation. This is consistent with the approach of [6], because $\log M$ is again scaling with $H(P_X)$*

and $\log K$ *is scaling with* $I(P_X; W_{Y|X})$ *(see (12) and (10)) but their behavior is now dictated by Lemma V.2.*

We construct a commitment protocol from the wiretap code of Proposition V.1 as follows.

1) *Commit phase:* Alice commits a message a by choosing S uniformly at random in $[\![1; K]\!]$ and transmitting $\mathbf{x}(a, S)$ over the channel, resulting in an observation Y^n for Bob;
2) *Reveal phase:* Alice publicly reveals a' and S' to Bob. Let $\mathcal{S} \triangleq \{i \in [\![1; n]\!] : x_i(a', s') = x_1\}$ and $\mathcal{Y}_0 \triangleq \{y \in \mathcal{Y} : Q_0(y) \neq Q_1(y)\}$. Bob runs the test

$$\beta(a', S', Y^n) = \begin{cases} 1 \text{ if } \forall y \in \mathcal{Y}_0 \ \left|\frac{1}{|\mathcal{S}|} N(y; Y^n_{\mathcal{S}}) - Q_1(y)\right| \leqslant \varepsilon Q_1(y) \\ 0 \text{ else} \end{cases}$$

where $\varepsilon > 0$ will be determined a bit later.

Lemma V.6. *The commitment protocol is* ϵ*-concealing with* $\epsilon = 2e^{-\gamma_0\sqrt{n}}$.

Proof.

$$\begin{aligned} \|Q^n_a - Q^n_{a'}\|_1 &\leqslant \left\|Q^n_a - Q^{\otimes n}\right\|_1 + \left\|Q_{a'} - Q^{\otimes n}\right\|_1 \\ &\leqslant 2e^{-\gamma_0\sqrt{n}}. \end{aligned}$$

□

Lemma V.7. *The commitment protocol is* μ*-retractable if* $\alpha < \sqrt{\frac{2\mu}{\chi_2(Q_1\|Q_0)}}$ *and* n *is large enough.*

Proof. let $\zeta \triangleq \min_y Q_0(y)$. The scheme is also retractable because,

$$\begin{aligned} &\mathbb{D}\left(P_{Y^n} \,\middle\|\, Q_0^{\otimes n}\right) \\ &= \mathbb{D}\left(P_{Y^n} \,\middle\|\, Q_\alpha^{\otimes n}\right) + n\mathbb{D}(Q_\alpha \,\|\, Q_0) \\ &\quad + \sum_{\mathbf{y}} \left(P_{Y^n}(\mathbf{y}) - Q_\alpha^{\otimes n}(\mathbf{y})\right) \log \frac{Q_\alpha^{\otimes n}(\mathbf{y})}{Q_0^{\otimes n}(\mathbf{y})} \\ &\leqslant 2\log\left(\frac{1}{\zeta}\right) e^{-\gamma\sqrt{n}} + \frac{\alpha^2}{2}\chi_2\left(Q_1\|Q_0\right) \\ &\quad + e^{-\gamma\sqrt{n}}|\log\zeta| + o(1), \end{aligned}$$

where we have used the reverse Pinsker inequality [26, Eq. (323)] and the convexity of $\|\cdot\|_1$ to bound the first term and Lemma V.2 to bound the second term. Note that the constraint $\mathbb{D}\left(P_{Y^n} \,\middle\|\, Q_0^{\otimes n}\right) \leqslant \mu$ can be achieved upon choosing any

$$\alpha < \sqrt{\frac{2\mu}{\chi_2\left(Q_1\|Q_0\right)}},$$

and taking n large enough. □

Lemma V.8. *The commitment protocol is* δ*-binding and* δ*-sound.*

Proof. Let $\mathbf{x} \triangleq \mathbf{x}(a, s)$ denote the sequence committed to and let $\mathbf{x}' \triangleq \mathbf{x}(a,' s')$ denote the sequence revealed. If $\mathbf{x} = \mathbf{x}'$, then

$$\mathbb{E}\left[\frac{1}{|\mathcal{S}|} N(y; Y^n_{\mathcal{S}})\right] = Q_1(y)$$

and a Chernoff bound ensures that

$$\begin{aligned} &\mathbb{P}\left(\exists y \in \mathcal{Y}_0 : \left|\frac{1}{|\mathcal{S}|} N(y; Y^n_{\mathcal{S}}) - Q_1(y)\right| > \varepsilon Q_1(y)\right) \\ &\leqslant |\mathcal{Y}_0| e^{-\frac{|\mathcal{S}| \min_y Q_1(y)\epsilon^2}{3}} \\ &\leqslant e^{-\varepsilon_1\sqrt{n}} \end{aligned}$$

for some $\varepsilon_1 > 0$, so that the protocol is sound.

Assume now that Alice cheats and reveals another codeword such that $d_H(\mathbf{x}, \mathbf{x}') \geqslant 2\sigma\sqrt{n}$. Assume that $d_H(\mathbf{x}_{\mathcal{S}}, \mathbf{x}'_{\mathcal{S}}) < (\sigma - \sigma_1)\sqrt{n}$, that is, the sequences differ on $\mathcal{S}$ on strictly less than $(\sigma - \sigma_1)\sqrt{n}$ positions. Then,

$$\begin{aligned} d_H(\mathbf{x}, \mathbf{x}') &= d_H(\mathbf{x}_{\mathcal{S}}, \mathbf{x}'_{\mathcal{S}}) + d_H(\mathbf{x}_{\mathcal{S}^c}, \mathbf{x}'_{\mathcal{S}^c}) \\ &< (\sigma - \sigma_1)\sqrt{n} + \mathrm{wt}(\mathbf{x}_{\mathcal{S}^c}) \\ &= (\sigma - \sigma_1)\sqrt{n} + \mathrm{wt}(\mathbf{x}) - \mathrm{wt}(\mathbf{x}_{\mathcal{S}}) \\ &\leqslant (\sigma - \sigma_1)\sqrt{n} + \mathrm{wt}(\mathbf{x}) - (\mathrm{wt}(\mathbf{x}') - (\sigma - \sigma_1)\sqrt{n}) \\ &\leqslant 2\sigma\sqrt{n}. \end{aligned}$$

Hence, the sequences $\mathbf{x}$ and $\mathbf{x}'$ differ on $\mathcal{S}$ in at least $(\sigma - \sigma_1)\sqrt{n}$ positions denoted by $\mathcal{D}$. Then, for any $y \in \mathcal{Y}_0$,

$$\begin{aligned} &\left|\mathbb{E}\left[\frac{1}{|\mathcal{S}|} N(y; Y^n_{\mathcal{S}})\right] - Q_1(y)\right| = \frac{|\mathcal{D}|}{|\mathcal{S}|}|Q_0(y) - Q_1(y)| \\ &\geqslant \frac{\sigma - \sigma_1}{\alpha + \sigma_1} \min_{y \in \mathcal{Y}_0} |Q_0(y) - Q_1(y)| > 0. \end{aligned} \tag{13}$$

Consequently, choosing ε sufficiently small in light of (13), another Chernoff bound ensures that

$$\begin{aligned} &\mathbb{P}\left(\forall y \in \mathcal{Y}_0 : \left|\frac{1}{|\mathcal{S}|} N(y; Y^n_{\mathcal{S}}) - Q_1(y)\right| \leqslant \varepsilon Q_1(y)\right) \\ &\leqslant e^{-\varepsilon_2\sqrt{n}} \end{aligned}$$

for some $\varepsilon_2 > 0$. □

Since $\sigma > 0$ can be chosen arbitrarily, (12) ensures

$$\sup \lim_{n\to\infty} \frac{\log M}{\sqrt{n}\log n} \geqslant \sup_{\{p_x\}_{x\neq x_0} : \sum_{x\neq x_0} p_x = 1} \sqrt{\frac{\mu}{2\chi_2\left(Q_1\|Q_0\right)}}.$$

B. Converse proof

We only sketch the converse due to space constraints. The crux of the proof is to use the retractability constraint to identify the optimal scaling of $\log M$ with n, together with the standard proof for the converse of commitment capacity in [6, Proposition 9]. A bit more specifically, upon setting $\beta_n \triangleq \sqrt{\frac{2\mu}{n\chi_2(Q_1\|Q_0)}}$, one can show that

$$\frac{\log M}{\sqrt{n}\log n} \leqslant \frac{nH_b(\beta_n)}{(1-\epsilon_n)\sqrt{n}\log(n)} + O\left(\frac{1}{\sqrt{n}\log(n)}\right) \tag{14}$$

and

$$H_b(\beta_n) \leqslant \frac{1}{2}\sqrt{\frac{2\mu}{n\chi_2(Q_1\|Q_0)(1-\sqrt{\alpha_n})}}\log(n) + o\left(\frac{\log(n)}{\sqrt{n}}\right). \tag{15}$$

from which the upper bound follows.

REFERENCES

[1] A. Juels and M. Szydlo, "A two-server, sealed-bid auction protocol," in *International conference on financial cryptography*. Springer, 2002, pp. 72–86.

[2] G. Brassard, D. Chaum, and C. Crépeau, "Minimum disclosure proofs of knowledge," *Journal of computer and system sciences*, vol. 37, no. 2, pp. 156–189, 1988.

[3] Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai, "Zero-knowledge from secure multiparty computation," in *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, 2007, pp. 21–30.

[4] C. Crépeau, J. v. d. Graaf, and A. Tapp, "Committed oblivious transfer and private multi-party computation," in *Annual International Cryptology Conference*. Springer, 1995, pp. 110–123.

[5] C. Crépeau, "Efficient cryptographic protocols based on noisy channels," in *Proc. of EUROCRYPT 1997*, Springer, Ed., 1997, pp. 306–317.

[6] A. Winter, A. C. A. Nascimento, and H. Imai, "Commitment capacity of discrete memoryless channels," in *Proc. of 9th IMA international conference*, Cirencester, UK, 2003, pp. 33–51.

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

[8] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1367, October 1975.

[9] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, July 1993.

[10] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[11] M. Hayashi and N. A. Warsi, "Commitment capacity of classical-quantum channels," in *Proc. of IEEE International Symposium on Information Theory*, Jun. 2022.

[12] 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, 2008.

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

[14] A. K. Yadav, M. Mamindlapally, A. J. Budkuley, and M. Mishra, "Commitment over compound binary symmetric channels," in *2021 National Conference on Communications (NCC)*, jul 2021.

[15] A. J. Budkuley, P. Joshi, M. Mamindlapally, and A. K. Yadav, "Commitment over unreliable noisy channels: When awareness meets control," in *Proc. of IEEE Information Theory Workshop*, 2022.

[16] A. K. Yadav, M. Mamindlapally, P. Joshi, and A. J. Budkuley, "On commitment over general compound channels," in *2022 14th International Conference on Communication Systems & Networks*, jan 2022.

[17] 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*, vol. 40, no. 3, pp. 862–870, mar 2022.

[18] C. Crepeau, 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, jun 2020.

[19] B. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1921–1930, September 2013.

[20] L. Wang, G. W. Wornell, and L. Zheng, "Fundamental limits of communication with low probability of detection," *IEEE Transactions on Information Theory*, vol. 62, no. 6, pp. 3493–3503, Jun. 2016.

[21] M. R. Bloch, "Covert communication over noisy channels: A resolvability perspective," *IEEE Transactions on Information Theory*, vol. 62, no. 5, pp. 2334–2354, May 2016.

[22] M. Tahmasbi and M. R. Bloch, "First and second order asymptotics in covert communication," *IEEE Transactions on Information Theory*, vol. 65, no. 4, pp. 2190 –2212, Apr. 2019.

[23] J. Hou and G. Kramer, "Effective secrecy: Reliability, confusion and stealth," in *Proc. of IEEE International Symposium on Information Theory*, Honolulu, HI, July 2014, pp. 601–605.

[24] M. Bellare, S. Tessaro, and A. Vardy, "Semantic security for the wiretap channel," in *Advances in Cryptology & CRYPTO 2012*, ser. Lecture Notes in Computer Science, R. Safavi-Naini and R. Canetti, Eds., vol. 7417. Springer Berlin Heidelberg, 2012, pp. 294–311, hard-copy.

[25] P. Cuff, "Soft covering with high probability," in *Proc. of IEEE International Symposium on Information Theory*, Barcelona, Spain, Jul. 2016, pp. 2963–2967.

[26] I. Sason and S. Verdú, "f -divergence inequalities," *IEEE Transactions on Information Theory*, vol. 62, no. 11, pp. 5973–6006, Nov. 2016.