Leveraging Spherical Codes for Commitment over Gaussian UNCs

Anuj Kumar Yadav
École Polytechnique Fédérale de Lausanne (EPFL), Switzerland

Joint work with: Manideep Mamindlapally, Amitalok J. Budkuley

Keywords: Commitment, Information-theoretic security, Gaussian Noise, Spherical codes, Unfair Noisy Channels

Abstract

We study *information-theoretically secure* commitment over a class of unreliable noisy channels i.e., a Gaussian Unfair Noisy Channel (UNC). We provide an impossibility result for the positive rate commitment under the unconstrained input power i.e., $P \to \infty$. In addition, we provide a commitment scheme based on a spherical error correcting code, hash function and randomness extractor, that achieves a positive (finite) rate for any finite power constraint $P > 0$. Moreover, together with an information-theoretic converse, we completely characterize the commitment capacity over Gaussian UNC when $P \to \infty$.

Introduction

Two mutually distrustful parties: the *committer* Alice and the *bidder* Bob seek to devise a two-phase protocol to achieve the following *secure lock* functionality: In the first phase, Alice *commits* to sharing a bit string, say C, with Bob, and shares its encrypted version seeking the following *concealment* guarantee: Bob cannot learn C until the time Alice chooses to *reveal* C to him. In the second phase when Alice does reveal a string to Bob, the protocol's *binding* guarantee enables Bob to successfully detect whether (or not) Alice has cheated by revealing a different string. The above functionality essentially defines a classic cryptographic primitive called *commitment* which is widely utilized as a crucial building block in several practical applications like sealed-bid auctions, coin flipping, zero knowledge proofs, secure multiparty computations, etc.

Commitment is impossible to realize through completely noiseless interactions when both Alice and Bob are computationally unbounded. To realize commitment without such computational limitations on the parties, one requires access to additional resources like correlated randomness, trusted third party resources, noisy channels, etc. Wyner's seminal work on wire-tap channels [8] first explored the potential of noisy channels for security; he showed that a noisy random channel can be a great asset to realize various *information-theoretically secure* cryptographic protocols. Wyner's results have subsequently spawned a wide area of research on information-theoretic security; his results have been extended and strengthened in a multitude of works. Crépeau and Kilian [2] first demonstrated the possibility of *information-theoretically secure* commitment over binary symmetric channels. Winter *et al.* [7] completely characterized the *commitment capacity* over any discrete memoryless channels (DMCs) (cf. [9]). Closer to this work, Nascimento *et al.* studied commitment over continuous alphabet additive white Gaussian noise (AWGN) channels [5]. They showed a very surprising result that the commitment capacity over any non-trivial AWGN channel is infinite. Subsequently, [6] showed a constructive commitment scheme (using lattice codes) over AWGN channels.

It is pertinent to note that despite a noisy channel being an excellent resource for realizing commitment, one needs to be mindful of potential *unreliability* in a channel– oftentimes due to imprecise channel characterization (passive unreliability) or due to channel tampering by malicious parties (active unreliability). Channel unreliabilites impact the commitment throughput potential of a noisy channel; in some cases, they may completely preclude commitment. Damgård *et al.* [4] first studied channel unreliability via the *unfair noisy channels* (UNC) over the binary alphabet. Their *Binary UNC* combines both forms of unreliability, *viz.,* active unreliability (when either of two parties are malicious) and passive unreliability (when both parties are honest). In a classic result, Damgård *et al.* [4] precisely characterized the threshold for positive-rate commitment over Binary UNCs; their commitment capacity was recently characterized in [3], albeit under some assumptions. In this work, we study commitment over a unreliable AWGN Channel i.e., Gaussian UNC (cf. Definition 1).

Our Contributions

- We provide an impossibility result on the zero-rate commitment over a Gaussian UNC (irrespective of the input power at the committer) (Theorem 1) (see also [1]).
- We provide a commitment scheme based on a spherical error correcting code. It achieves a positive commitment rate in the possibility regime (Theorem 2) (see also [1]).
- Together with an information-theoretic upper bound on the commitment rate, we completely characterize the (finite) commitment capacity over a Gaussian UNC when the input power is infinite. (Theorem 3 & Corollary 4).

Problem Setup

Definition 1 (Gaussian UNC)**.** *[1] A Gaussian unfair noisy channel with parameters* $0 < \gamma^2 \leq \delta^2$*, also called Gaussian-UNC*$[\gamma^2,\delta^2]$*, is an AWGN channel where (i) honest parties communicate over an AWGN channel where the noise variance can take values in the set* $\mathcal{T} = [\gamma^2, \delta^2]$ *and is unknown to them, (ii) any dishonest party can privately set the noise variance to any value in* $\mathcal{T}$*.*[1]

In our problem (ref Fig. 1), two mutually distrustful parties, *committer* Alice and *receiver* Bob employ a Gaussian-UNC$[\gamma^2,\delta^2]$ to realize commitment over a uniformly random string $C \in [2^{nR}]$ available to Alice (we specify $R > 0$ later). Alice and Bob have access to a one-way Gaussian-UNC$[\gamma^2,\delta^2]$. Separately, 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 authenticated. To commit to her random string C, Alice uses the Gaussian-UNC$[\gamma^2,\delta^2]$ channel n times and transmits over it her encrypted data $\mathbf{X} = (X_1, X_2, \cdots, X_n) \in \mathbb{R}^n$; Bob receives a noisy version $\mathbf{Y} \in \mathbb{R}^n$ of Alice's transmission $\mathbf{X}$. Alice has an input power constraint $P > 0$, i.e., Alice can only transmit vectors $\mathbf{X} \in \mathcal{S}(P)$, where $\mathcal{S}(P) := \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\|_2 \leq \sqrt{nP}\}$. We allow private randomization at both Alice and Bob via their respective keys $K_A \in \mathcal{K}_A$ and $K_B \in \mathcal{K}_B$. At any point in time, say time i, 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 (transcript) over the noiseless link. The rate (R) of the

[1] When $\gamma^2 = \delta^2$, the Gaussian-UNC$[\gamma^2, \delta^2]$ specializes to a zero-mean AWGN channel whose commitment capacity is known to be infinite [5].

commitment protocol is defined as the ratio of the length of the commit string C to the number of uses of the Gaussian UNC.

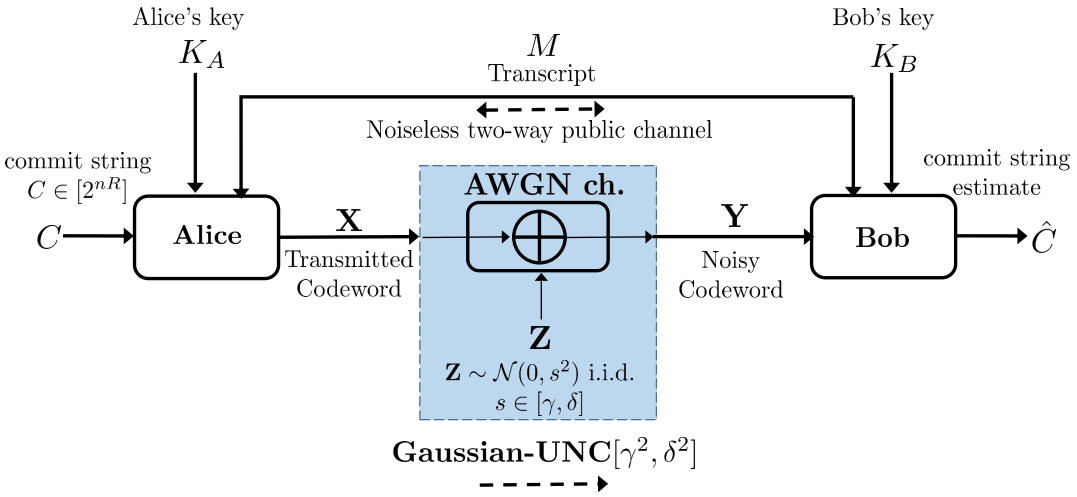

Figure 1: The problem setup: commitment over a Gaussian-UNC$[\gamma^2, \delta^2]$

Definition 2 (Commitment protocol)**.** *An $(n, R)-$commitment protocol $\mathscr{P}$ is a message-exchange procedure between the two parties to realize commitment over the random bit string $C \in [2^{nR}]$. We call R the rate of such a commitment protocol $\mathscr{P}$. There are two phases to a protocol $\mathscr{P}$:*

(a) Commit phase: Given $C \in [2^{nR}]$, Alice transmits $\mathbf{X} \in \mathcal{S}(P)$ using the Gaussian-UNC$[\gamma^2,\delta^2]$channel n times. Bob receives $\mathbf{Y}$. The two parties also exchange messages over the noiseless link. Let M denote this transcript of protocol $\mathscr{P}$. Let V_A and V_B denote Alice's view *and* Bob's view *respectively; these 'views' comprise all the random variables/vectors known to the two parties at the end of the commit phase.*

(b) Reveal phase: In this phase, Alice and Bob only communicate over the noiseless public link and do not use the Gaussian-UNC$[\gamma^2,\delta^2]$ Alice announces the commit string $\tilde{c} \in [2^{nR}]$ and $\tilde{\mathbf{X}} \in \mathbb{R}^n$. 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 $T = 0$).

The following parameters are of key interest:

Definition 3 (ϵ-sound)**.** *A protocol $\mathscr{P}$ is $\epsilon-$sound if, for honest Alice and honest Bob, we have $\mathbb{P}(T(C, \mathbf{X}, V_B) \neq 1) \leq \epsilon$.*

Definition 4 (ϵ-concealing)**.** *A protocol $\mathscr{P}$ is $\epsilon-$concealing if, for honest Alice and under any strategy of Bob, $I(C; V_B) \leq \epsilon$.*

Definition 5 (ϵ-binding)**.** *A protocol $\mathscr{P}$ is $\epsilon-$binding if, for honest Bob and under any strategy of 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 $(\bar{c},\bar{\mathbf{x}})$, $(\hat{c},\hat{\mathbf{x}})$, $\bar{c}\neq\hat{c}$, and $\bar{\mathbf{x}},\hat{\mathbf{x}}\in\mathcal{S}(P)$.

A rate R is said to be *achievable* if for every $\epsilon>0$ there exists for every $n\in\mathbb{N}$ sufficiently large, a protocol $\mathscr{P}$ such that $\mathscr{P}$ is $\epsilon-$sound, $\epsilon-$concealing and $\epsilon-$binding. The supremum of all achievable rates is called the commitment capacity $\mathbb{C}$ of the Gaussian-UNC[γ^2,δ^2].

Our Results

Theorem 1. *For a Gaussian-UNC[γ^2,δ^2] with unconstrained input ($P\to\infty$), the commitment is possible iff $\delta^2<2\gamma^2$.*

Theorem 2. *For a Gaussian-UNC[γ^2,δ^2] with $P>0$, positive-rate commitment is possible if the following holds:*

$$\delta^2 < \left(1+\frac{P}{P+\gamma^2}\right)\gamma^2. \tag{0.1}$$

The commitment capacity satisfies $\mathbb{C}\geq\mathbb{C}_L$, where

$$\mathbb{C}_L := \frac{1}{2}\log_2\left(\frac{P}{\delta^2-\gamma^2}\right)-\frac{1}{2}\log_2\left(1+\frac{P}{\gamma^2}\right) \tag{0.2}$$

The proof follows from the construction of a commitment scheme which achieves the rate $\mathbb{C}_L$. It involves the use of a spherical code where to commit to a bit string C, the committer Alice picks a codeword from an Error-Correcting Code (ECC). Our ECC is a spherical code comprising of equi-normed codewords on the surface of a n-dimensional euclidean ball. The minimum distance of the ECC is proportional to the input power P. The scheme also involves two rounds of hash challenge from Bob to Alice to bind Alice to her choice of the commit string. Additionally, a randomness extractor is used which allows Alice to extract a secret key from the transmitted codeword conditioned on the view of Bob; it is used to realize one-time pad with commit string which ensures concealment against Bob in commit phase.

Theorem 3. *For a Gaussian-UNC[γ^2,δ^2] with $P>0$, we have the following upper bound on the commitment capacity*

$$\mathbb{C}\leq\frac{1}{2}\log_2\left(1+\frac{P}{\delta^2-\gamma^2}\right)-\frac{1}{2}\log_2\left(1+\frac{P}{\gamma^2}\right) \tag{0.3}$$

As a consequence of Theorem 2 (Achievability) and Theorem 3 (Converse), we have following corollary,

Corollary 4. *For a Gaussian-UNC[γ^2,δ^2] with unconstrained input ($P \to \infty$), if $\delta^2 < 2\gamma^2$, the commitment capacity*

$$\mathbb{C} = \frac{1}{2}\log_2\left(\frac{\gamma^2}{\delta^2 - \gamma^2}\right) \tag{0.4}$$

Bibliography

[1] Amitalok Budkuley, Pranav Joshi, Manideep Mamindlapally, and Anuj Kumar Yadav. On the (im)possibility of commitment over gaussian unfair noisy channels. In *2023 IEEE International Symposium on Information Theory (ISIT)*, pages 483–488, 2023.

[2] C. Crepeau and J. Kilian. Achieving oblivious transfer using weakened security assumptions. In *[Proceedings 1988] 29th Annual Symposium on Foundations of Computer Science*, pages 42–52, October 1988.

[3] Claude Crépeau, Rafael Dowsley, and A. C. A. Nascimento. On the commitment capacity of unfair noisy channels. *IEEE Transactions on Information Theory*, 66(6):3745–3752, 2020.

[4] Ivan Damgård, Joe Kilian, and Louis 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*, pages 56–73. Springer, 1999.

[5] 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*, 54(6):2785–2789, June 2008.

[6] Frédérique Oggier and Kirill Morozov. A practical scheme for string commitment based on the gaussian channel. In *2008 IEEE Information Theory Workshop*, pages 328–332. IEEE, 2008.

[7] Andreas Winter, A. C. A. Nascimento, and Hideki Imai. Commitment capacity of discrete memoryless channels. In *IMA International Conference on Cryptography and Coding*, pages 35–51. Springer, 2003.

[8] Aaron D Wyner. The wire-tap channel. *Bell system technical journal*, 54(8):1355–1387, 1975.

[9] Anuj Kumar Yadav, Manideep Mamindlapally, and Amitalok Budkuley. Wiretapped commitment over binary channels. In *2024 IEEE International Symposium on Information Theory (ISIT)*, pages 3528–3533, 2024.