Commitment over Unreliable Channels

Pranav Joshi*, Manideep Mamindlapally*, Anuj Kumar Yadav†,
Manoj Mishra‡, Amitalok J. Budkuley*
*IIT Kharagpur, †IIT Patna, ‡NISER, Bhubaneshwar, HBNI

I. Abstract

In a successful sealed-bid auction, it is imperative that two mutually distrustful parties, say Alice (bidder) and Bob (auctioneer), realize a protocol with following guarantees: firstly, Alice can *commit* to sharing a string with Bob, with the guarantee that this string remains hidden until she chooses to reveal it to him. Secondly, when revealed, Bob is able to detect precisely whether Alice cheats on her string choice. In essence, the parties seek to realize a two-phase *commitment* protocol, comprising *commit* followed by *reveal* phases. Apart from sealed-bid auctions, commitment appears as a crucial cryptographic primitive in several practical applications like coin flipping, zero knowledge proofs, contract signing and secure multiparty computation.

It is well known that *information-theoretically secure* commitment is impossible if parties communicate only noiselessly; however, as widely demonstrated, communication using a noisy channel can be a resource to realize commitment. In fact, optimum commitment throughput, i.e., *commitment capacity* has been characterized for general discrete memoryless channels (DMCs); in a recent work accepted at ISIT'21, we extend this characterization for DMCs under non-trivial costs.

Although a noisy channel offers the possibility of commitment, the two parties may often be hamstrung under incomplete knowledge of the channel's behaviour. For instance, practical communication systems employ a channel estimation protocol before actual communication commences; oftentimes, such a procedure ends up with an unreliable *compound channel* characterization where one can only localize the actual channel to a set with potentially many candidate channels. We ask the question: how to *robustify* existing commitment schemes for such unreliable channels?

In a recent unpublished result, we answer this question affirmatively. We formally study commitment capacity over a compound binary symmetric channel (compound-BSC), where parties (whether honest or dishonest) know the class of potential channels but are oblivious to the instantiated one; we determine its commitment capacity.

Historically, commitment over unreliable channels has been studied via models like the unfair noisy channels (UNCs), the elastic/reverse elastic channels (ECs/RECs). Through our work, we show that compound-BSCs offer a qualitatively different perspective of the underlying channel uncertainly (as unlike UNCs, compound-BSCs always offer non-zero commitment throughput). The capacities of the UNC and the EC were recently characterized; a conjecture, however, was presented for the REC. Utilizing the insight offered by compound-BSCs, we prove that the above conjecture is correct and settle the REC capacity. Overall, we believe our results for the compound-BSCs and RECs, coupled with the known results for UNCs and ECs, helps shed more light on commitment over general unreliable channels.

The first three authors are student authors and have contributed equally to this work.