Perfect Secrecy in the Wild

Abstract:

Alice wishes to reveal the state X to Bob, if he knows some other information Y also known to her. If Bob does not, she wishes to reveal nothing about X at all. When can Alice accomplish this? We provide a simple necessary and sufficient condition on the joint distribution of X and Y. Shannon's result on the perfect secrecy of the one-time pad follows as a special case. We further ask more broadly what information about X can be feasibly communicated and derive some properties of the Blackwell frontier. We discuss applications on data privacy, fairness and price discrimination by monopolist data providers.