

Paul Cuff
cuff@stanford.edu

Research Directions

The theory of information, as charted by Claude Shannon, has influenced many fields and introduced a new way of thinking about information. Beyond the immediate applications in digital communication and data compression, the ideas introduced by information theory have found their way into the study of biology and DNA, computation and complexity, and machine learning. Indeed, the field provides a concrete way of dealing with the otherwise nebulous substance of information. Although many of the basic questions have been answered, some by Shannon himself, many fundamental questions dealing with multiple users and sources of information have remained unanswered for decades. We are still lacking in our understanding of how to best structure and correlate codebooks for communicating in network settings. Answers to the building blocks of network information theory provide insight into how information can be reinforced in a complex setting, ultimately giving us principles for better technology and greater understanding.

My experience in the field has taught me that beyond the intriguing open problems related to communicating in networks, the field itself is open to broader interpretation. By considering new purposes for communication, besides transporting information from one location to another, we find many new problems of interest.

Communication Requirements for Coordinated Behavior and Computation:

Communication need not be about reconstructing a source of information at another location. Perhaps instead we wish to coordinate actions at different locations or perform distributed computations. Imagine cells in a body communicating in order to contract a muscle or to divide and create an organ. In the context of coordination, new source coding network settings become interesting subjects of analysis. We can ask, for example, how much communication is necessary to distribute tasks to computers in a network.

The communication burden in a network due to distributed computation is becoming a technological bottleneck. Large scale parallel computation such as the Stanford protein folding project (Folding@home) as well as service oriented internet applications run by companies like Google are faced with both the issue of moving information and coordinating computation. Consider, for example, the task Google faces for handling each search query. After the query makes its way to a data center, the search task is farmed out to a number of different servers working in cooperation. Yet, the minimum communication requirement to perform such a task is not well understood. In my recent research [1], some basic settings are addressed for distributing computation and coordination. A lot will be learned by boiling these issues down to essential and fundamental questions.

Relaxed Encryption:

In general, a random sequence of bits known at multiple locations in a network enables distributed randomized behavior. In communication settings, randomized communication protocols can be used to communicate secretly over a public channel. The common randomness becomes the

secret key for encryption. I plan to investigate some new uses of common randomness for secrecy—a relaxation of data encryption.

Channel capacity results for point-to-point memoryless channels to a large extent have materialized in working communication systems. However, encryption took a different route to practice than the one prescribed by Shannon, who's negative result requires a one-time pad of secret key as long as the data itself. Instead, the requirement of absolute secrecy was abandoned for the more approachable requirement of computational security. That is, breaking the secrecy is forbiddingly difficult for the current state of the art. Yet, recent work on information theoretic secrecy, such as using channel noise to assist in secret communication or using quantum entanglement to exchange secret keys, removes some of the barriers for absolute secrecy. In that light, a new range of questions opens up in the field of encryption.

One such question that arises is how we might naturally relax the problem of encryption to reduce the secret key requirements without compromising secrecy. For example, if we allow the intended receiver of the information to receive only something correlated with the information, how much does that relax the communication and secret key requirements? My recent work [2] on the topic sheds light on two surprising observations. First, the encryption and the lossy source coding benefit from being done in a joint fashion. Second, the required secret key length is greater than the communication requirement, even though both quantities are reduced through the relaxation of the problem. These results scratch the surface of exploring the diverse roles of absolute secrecy and how to utilize common randomness.

Coordination in Game Theory:

The fields of source coding and encryption benefit from an exploration of their motivations. We can place secrecy and encryption in a larger context by asking a simple question. Why do we need secrecy? If eavesdroppers had access to the information, might they use it against us? From this point of view, a natural counterpart to encryption is game theory, since both settings admit an adversary. When we view encrypted communication as a means of coordinating actions in a multi-player game, new questions present themselves. How should we best use a secret key and communication in order to perform well in a game? Does the problem change dramatically when the game has random state information known only to some of the parties involved?

I've identified an optimal tradeoff between the rate of secure communication and performance in a repeated multi-player game [2]. The communication is used to generate random actions that are needed to implement a correlated mixed strategy. However, game theory encounters a multitude of important scenarios, more complex than the one considered. I want to know how the communication changes when the payoffs are unequal for the cooperating participants, or when game state information is known to some of the players of the game. Perhaps this framework can be used to correctly model the incentives and requirements for encryption.

Related Work:

- [1] P. Cuff, H. Permuter, T. Cover, "Coordination Capacity," in preparation.
- [2] P. Cuff, "Communication Requirements for Generating Correlated Random Variables," *Proc. IEEE Int. Symp. Info. Theory*, Toronto, Canada, July 2008 (Best Student Paper Award).