Message transmission over classical quantum channels with a jammer with side information: Correlation as resource, common randomness generation

Holger Boche · Minglai Cai · Ning Cai

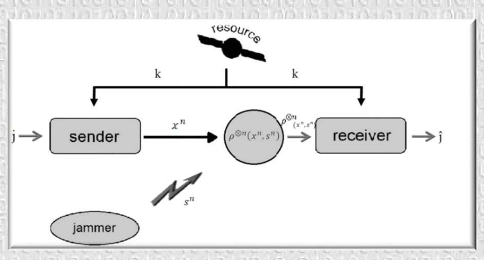
Technical University of Munich
Department of Electrical and Computer Engineering
Institute of Theoretical Information Technology

Communication Scenarios

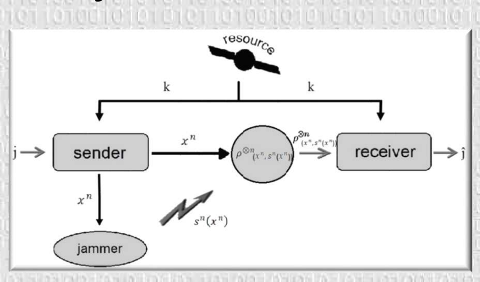
Robustness

For every $t \in \theta$ let W_t be a quantum channel A →S(H)
The set $\{W_t : t \in \theta\}$ is an **arbitrarily varying classical-quantum channel** when t varies in an arbitrary manner
⇨ We interpret it as a channel with a jammer

When the Jammer Knows Input Codeword



Conventional model: jammer does not know the channel input



In this scenario jammer knows input codeword

Previous Results

Theorem

For an AVCQC W={ρ(x,s): x∈X, s∈S} let

$$\bar{\bar{\mathcal{W}}} := \{\{\bar{\bar{\rho}}_Q(x) := \sum_s Q(s|x)\rho(x,s), x \in \mathcal{X}\} : \text{ for all } Q : \mathcal{X} \to \mathcal{S}\}$$

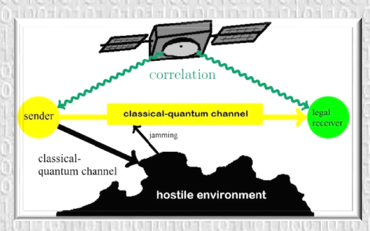
The random assisted capacity of W is

$$\max_P \min_{\bar{\bar{\rho}}(\cdot)\in\bar{\bar{\mathcal{W}}}} \chi(P, \bar{\bar{\rho}}(\cdot))$$

Outline of Proof

- If the jammer knew the random key k, The best strategy for the jammer would be to choose the most dangerous state to attack the k-th deterministic coding, which we do not want.
- To this end every used codeword must be used by "many" outcomes

Resources

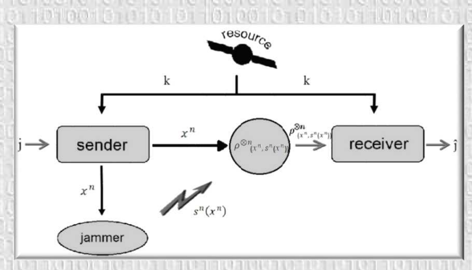


Common randomness is a helpful resource.
Problem: It is a very strong resource.

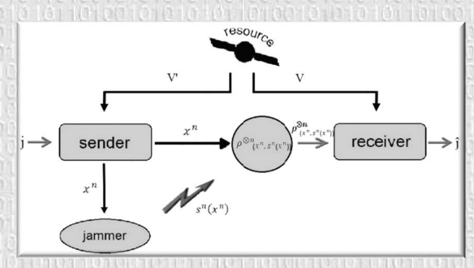
☞ Correlation is a much „cheaper" resource.

Resources

- Randomness: full coordination between Alice and Bob;
- Correlation: weakest form of coordination;



Common Randomness



Correlation

Correlation Assisted Code

Definition:

A (V', V)-correlation assisted (n, J_n) code consists of
⇨ a set of encoders $\left\{u_{v'^n} : \{1, \cdots, J_n\} \to \mathcal{X}^n : v'^n \in \mathcal{V}'^n\right\}$
⇨ a set of collections of positive-semidefinite operators $\{\{D_j^{(v^n)} : j = 1, \cdots, J_n\} : v^n \in \mathcal{V}^n\}$ on $\mathcal{H}^{\otimes n}$ which are partitions of the identity

Correlation Assisted Capacity

Definition:

A non-negative number R is an achievable (V', V)-correlation assisted rate with informed jammer for the AVCQC $\{\{\rho(x,s), x\}, s\}$ if for every $\epsilon > 0$, $\delta > 0$, and sufficiently large n there exists a (V', V)-correlation assisted (n, J_n) code $\mathcal{C}(V', V) = \{(u_{v'^n}, \{D_j^{(v^n)} : j \in \{1, \cdots, J_n\}\}) : v'^n, v^n\}$ such that $\frac{\log J_n}{n} > R - \delta$, and

$$\max_{s^n(\cdot)} \sum_{v'^n} \sum_{v^n} p(v'^n, v^n) P_e(\mathcal{C}(v'^n, v^n), s^n(\cdot)) < \epsilon$$

Where $P_e\big(C(v'^n, v^n), s^n(.)\big) = E\, tr(\rho^{\otimes n}(u_{v'^n}(J), s(u_{v'^n}(J)))(I_H - D_J^{(v^n)}))$

Main Results

Main Result

Theorem

Let (V', V) with alphabets $(\mathcal{V}', \mathcal{V})$, be an arbitrarily correlated source and $\mathcal{W} = \{\rho(x,s) : x \in \mathcal{X}, s \in \mathcal{S}\}$ be an AVCQC. When $I(V', V) > 0$ holds, then

$$C(\mathcal{W}; corr(V', V)) = \max_P \min_{\bar{\bar{\rho}}(\cdot)\in\bar{\bar{\mathcal{W}}}} \chi(P, \bar{\bar{\rho}}(\cdot)).$$

Proof Concepts

For classical arbitrarily varying channels when the jammer has no side information:

⇨ Showing Csiszar Narayan positivity condition (Ahlswede Dichotomy) is fulfilled
⇨ Creating common randomness with a pre-code
BUT! When the jammer has side information ⇨ no Ahlswede Dichotomy ⇨ Csiszar Narayan positivity condition does **not** work

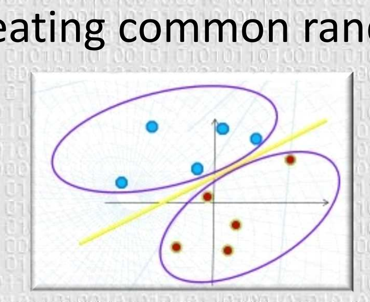
For classical arbitrarily varying channels when the jammer has side information:

⇨ Showing Kiefer Wolfowitz positivity condition (hyperplane separating the classical channel outputs into two parts in their real vector space) is fulfilled
⇨ Creating common randomness with pre-code
BUT! On the set of quantum states since they do not form a real vector space ⇨ Kiefer Wolfowitz positivity condition does **not** work

Proof of Main Result

For classical quantum arbitrarily varying channels when the jammer has side information:

⇨ At first, showing that there exists a hyperplane separating the quantum outputs into two parts
⇨ When this condition is satisfied, constructing a classical binary point to point channel with positive capacity (quantum version of the Kiefer Wolfowitz positivity condition)
⇨ Creating common randomness with a pre-code



[01100…|11010011000010110011 1……]

correlated code
random code

Applications

- Common randomness generating using correlation as resource
- Turing computability

Munich Conference on Quantum Science and Technology 2020