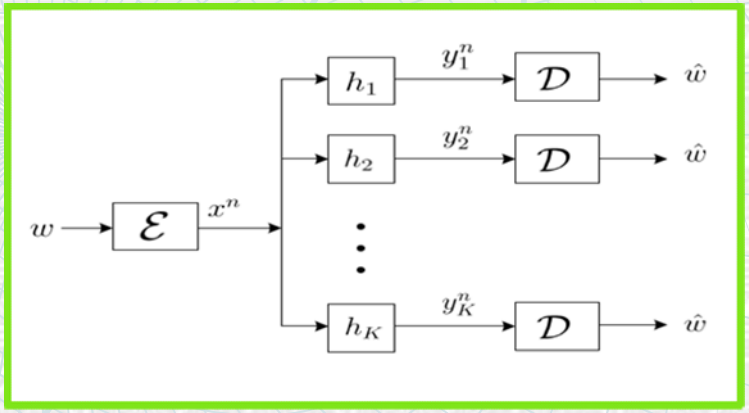
Message Transmission over Classical Quantum Channels with a Jammer with Side Information: Message Transmission Capacity and Resources

Holger Boche · Minglai Cai · Ning Cai

Quantum Arbitrarily Varying Channel When the Jammer Knows Input Codeword

Robustness

Let S := {1;…;T} be a finite set.
For every s ∈ S let $\rho(\,.\,,s)$ be a quantum channel X → S(H).
The set of $\{\rho(x,s): x \in X, s \in S\}$ is an **arbitrarily varying classical-quantum channel** (AVCQC) when s varies in an arbitrary manner.



Quantum Arbitrarily Varying Channel When the Jammer Knows Input Codeword

Robustness

The jammer may know

- coding scheme
- input codeword
- message

Jammer knows only coding scheme:

- R. Ahlswede and V. Blinovsky, 2007
- R. Ahlswede, I. Bjelaković , H. Boche, and J. Nötzel, 2013

Quantum Arbitrarily Varying Channel When the Jammer Knows Input Codeword

Communication Scenarios

Definition:

- A code $\gamma := (\mathcal{U}, \{\mathcal{D}(i), i \in \mathcal{I}\})$ of length n consists of its code book $\mathcal{U} := \{\mathbf{u}(i), i \in \mathcal{I}\} \subset \mathcal{X}^n$ and the decoding measurement $\{\mathcal{D}(i), i \in \mathcal{I}\} \subset \mathcal{S}(\mathcal{H}^{\otimes n})$: $\mathcal{D}(i) \geq 0$ for all i and $\sum_{i \in \mathcal{I}}, \mathcal{D}(i) = id.$

- A random correlated code Γ is a uniformly distributed random variable taking values in a set of codes $\{(\mathcal{U}(k), \{\mathcal{D}(j,k), j \in \mathcal{J}\}), k \in \mathcal{K}\}$ with a common message set $\mathcal{J}$, where $|\mathcal{K}|$ is called the key size.

Quantum Arbitrarily Varying Channel When the Jammer Knows Input Codeword

Random Code

Deterministic capacity:

- Jammer does not know codeword ⇨ Ahlswede dichotomy
- Jammer knows codeword ⇨ no dichotomy (example in extended version)

Deterministic code

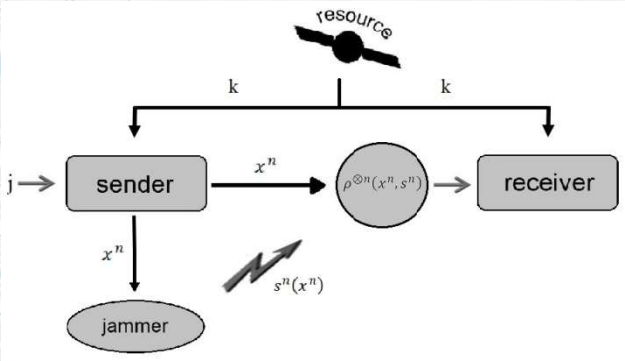
⇨ Knowing the message = knowing the input of the channel

Random code

⇨ Knowing the message ≠ knowing the input of the channel.

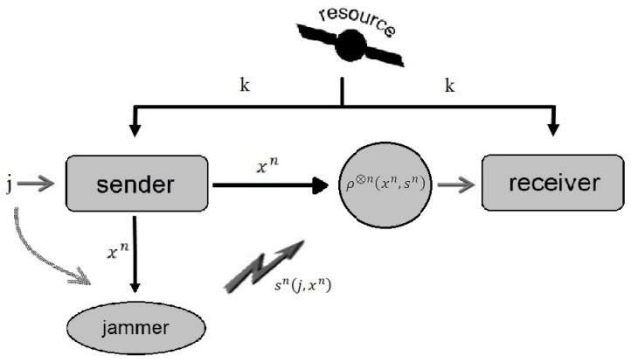
Quantum Arbitrarily Varying Channel When the Jammer Knows Input Codeword Communication Scenarios

Scenario 1:



In this scenario jammer knows input codeword

Scenario 2:



Now the jammer knows both input codeword and message

Quantum Arbitrarily Varying Channel When the Jammer Knows Input Codeword Communication Scenarios

Definition:

- We define the average probability of error in scenario 1 by

$$p_a(\Gamma) = \max_s Etr[\rho^{\otimes n}(\mathbf{u}(J,K), s(\mathbf{u}(J,K)))(I_{\mathcal{H}} - \mathcal{D}(J,K))]$$

- The maximum probability of error is defined as

$$p_m(\Gamma) = \max_{j \in \mathcal{J}} \max_s Etr[\rho^{\otimes n}(\mathbf{u}(j,K), s(\mathbf{u}(j,K)))(I_{\mathcal{H}} - \mathcal{D}(j,K))].$$

Quantum Arbitrarily Varying Channel When the Jammer Knows Input Codeword

Communication Scenarios

Definition:

We define the average probability of error in scenario 2 by

$$p_a(\Gamma) = \max_s Etr[\rho^{\otimes n}(\mathbf{u}(J,K), s(\mathbf{u}(J,K),J))(I_{\mathcal{H}} - \mathcal{D}(J,K))]$$

The maximum probability of error is defined as

$$p_m(\Gamma) = \max_{j \in \mathcal{J}} \max_s Etr[\rho^{\otimes n}(\mathbf{u}(j,K), s(\mathbf{u}(j,K),j))(I_{\mathcal{H}} - \mathcal{D}(j,K))].$$

the jammer knows not only the coding scheme but also the message

Quantum Arbitrarily Varying Channel When the Jammer Knows Input Codeword

Communication Scenarios

2 jamming scenarios + 2 error criteria

⇨ 4 combinations:

- random correlated capacity under the average error criterion in scenario 1, denoted by $C^*(W)$
- random correlated capacity under the maximal error criterion in scenario 1, denoted by $C_m^*(W)$
- random correlated capacity under the average error criterion in scenario 2, denoted by $C^{**}(W)$
- random correlated capacity under the maximal error criterion in scenario 2, denoted by $C_m^{**}(W)$

It is easy to show that $C^*(W) \geq C_m^*(W) = C^{**}(W) = C_m^{**}(W)$

Quantum Arbitrarily Varying Channel When the Jammer Knows Input Codeword

Main Results

Theorem:

For an AVCQC W={ρ(x,s): x∈X, s∈S} let

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

We have

$$C^*(\mathcal{W}) = C_m^*(\mathcal{W}) = C^{**}(\mathcal{W}) = C_m^{**}(\mathcal{W}) = \max_P \min_{\bar{\bar{\rho}}(\cdot)\in\bar{\bar{\mathcal{W}}}} \chi(P, \bar{\bar{\rho}}(\cdot))$$

Moreover all capacities can be achieved by codes with vanishing key rates.

Quantum Arbitrarily Varying Channel When the Jammer Knows Input Codeword

Previous Works

Capacity of classical arbitrarily varying channels in this scenario was first considered by Sarwate in 2008

- List decoding
- Vanishing key rate

Quantum Arbitrarily Varying Channel When the Jammer Knows Input Codeword

Previous Works

How to apply list decoding for quantum channels is still an open problem

We need a different approach

Quantum Arbitrarily Varying Channel When the Jammer Knows Input Codeword

Outline of Proof

The proof to the converse is simple.
The idea of the proof to the direct part:

- 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

Quantum Arbitrarily Varying Channel When the Jammer Knows Input Codeword

Outline of Proof

vanishing key rate

Instead of generating codebooks from the whole product set of the alphabet or the typical set

⇨ we randomly generate a ground set B with a cardinality $|I_n|$ "slightly" (polynomially) larger that our desired size of codebooks

Quantum Arbitrarily Varying Channel When the Jammer Knows Input Codeword

Outline of Proof

randomly uniformly generate $|K_n|$ codebooks
U(k) := {u(j,k), j∈ J_n, k∈ K_n} with size $|J_n|$ from this ground set

$|J_n|$ smaller than $2^{-n[\min_{\bar{\bar{\rho}}(\cdot)\in\bar{\bar{\mathcal{W}}}} \chi(P_X,\bar{\bar{\rho}}(\cdot))]}$
$|K_n|$ = Poly(n)

Quantum Arbitrarily Varying Channel When the Jammer Knows Input Codeword

Outline of Proof

We show that with a high probability
every codeword x(i) appears in “sufficiently many” codebooks
and each state sequence is “bad” only in “very few” of those codebooks.

Quantum Arbitrarily Varying Channel When the Jammer Knows Input Codeword

Outline of Proof

By some modification we can show:

$C^*(W)=C^{**}(W)$

Further knowing message to be sent, may not help a jammer to reduce the capacity.

Quantum Arbitrarily Varying Channel When the Jammer Knows Input Codeword

Further perspective

Extending the scenario that the jammer knows input codeword to:

- **AVCQC with quantum jammer**
- **correlation as resource instead of randomness**
- **secrecy capacity of an AVCQC with an eavesdropper**
- **deterministic capacity**


Thank you