Entanglement and secret-key-agreement capacities of bipartite quantum interactions and read-only memory devices

Siddhartha Das [1*] Stefan Bäuml [2] Mark M. Wilde [1]

[1]Louisiana State University, USA

[2]Delft University of Technology, Netherlands & NTT Japan

*sdas21@lsu.edu

arXiv:1712.00827

8th International Conference on Quantum Cryptography, Shanghai, China

Bipartite quantum interactions

Bipartite unitary interactions are the most elementary many-body interactions. Due to unavoidable interaction with environment, study of bipartite noisy interactions is pertinent.

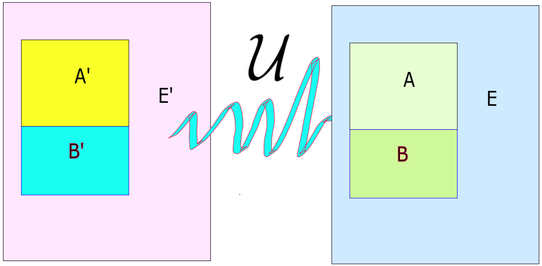


Figure: Systems of interest A' and B' interacting in presence of the bath E'.

- $\mathcal{U}$ is unitary transformation corresponding to underlying *interaction Hamiltonian* $\hat{H}$ among A', B', E'.
- Before action of interaction Hamiltonian $\hat{H}$: $\omega_{A'B'} \otimes \tau_{E'}$, where bath E' is in some fixed state and uncorrelated to $A'B'$.
- After action of $\hat{H}$:

$$\rho_{ABE} := \mathcal{U}_{A'B'E' \to ABE}(\omega_{A'B'} \otimes \tau_{E'}).$$

Bipartite quantum interactions

Bipartite unitary interactions are the most elementary many-body interactions. Due to unavoidable interaction with environment, study of bipartite noisy interactions is pertinent.

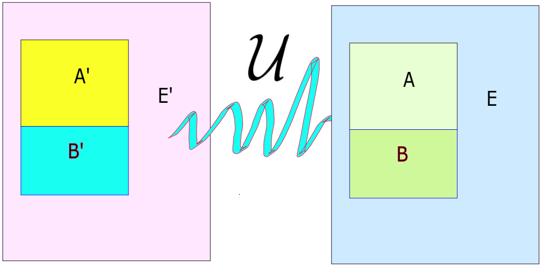


Figure: Systems of interest A' and B' interacting in presence of the bath E'.

- $\mathcal{U}$ is unitary transformation corresponding to underlying *interaction Hamiltonian* $\hat{H}$ among A', B', E'.
- Before action of interaction Hamiltonian $\hat{H}$: $\omega_{A'B'} \otimes \tau_{E'}$, where bath E' is in some fixed state and uncorrelated to $A'B'$.
- After action of $\hat{H}$:

$$\rho_{ABE} := \mathcal{U}_{A'B'E' \to ABE}(\omega_{A'B'} \otimes \tau_{E'}).$$

Bipartite quantum interactions

Bipartite unitary interactions are the most elementary many-body interactions. Due to unavoidable interaction with environment, study of bipartite noisy interactions is pertinent.

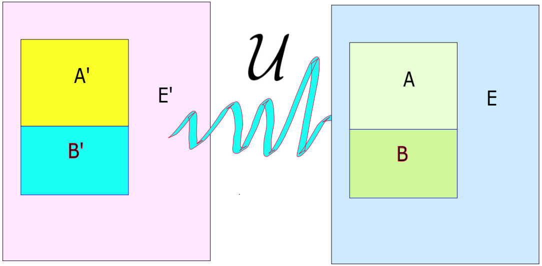


Figure: Systems of interest A' and B' interacting in presence of the bath E'.

- $\mathcal{U}$ is unitary transformation corresponding to underlying *interaction Hamiltonian* $\hat{H}$ among A', B', E'.
- Before action of interaction Hamiltonian $\hat{H}$: $\omega_{A'B'} \otimes \tau_{E'}$, where bath E' is in some fixed state and uncorrelated to $A'B'$.
- After action of $\hat{H}$:

$$\rho_{ABE} := \mathcal{U}_{A'B'E' \to ABE}(\omega_{A'B'} \otimes \tau_{E'}).$$

Bipartite quantum interactions

Bipartite unitary interactions are the most elementary many-body interactions. Due to unavoidable interaction with environment, study of bipartite noisy interactions is pertinent.

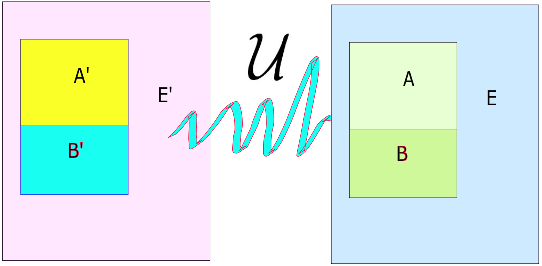


Figure: Systems of interest A' and B' interacting in presence of the bath E'.

- $\mathcal{U}$ is unitary transformation corresponding to underlying *interaction Hamiltonian* $\hat{H}$ among A', B', E'.
- Before action of interaction Hamiltonian $\hat{H}$: $\omega_{A'B'} \otimes \tau_{E'}$, where bath E' is in some fixed state and uncorrelated to $A'B'$.
- After action of $\hat{H}$:

$$\rho_{ABE} := \mathcal{U}_{A'B'E' \to ABE}(\omega_{A'B'} \otimes \tau_{E'}).$$

Bidirectional quantum channel

A bipartite quantum channel $\mathcal{N}_{A'B'\to AB}$ is a completely positive, trace-preserving map that transforms composite system $A'B'$ to AB.

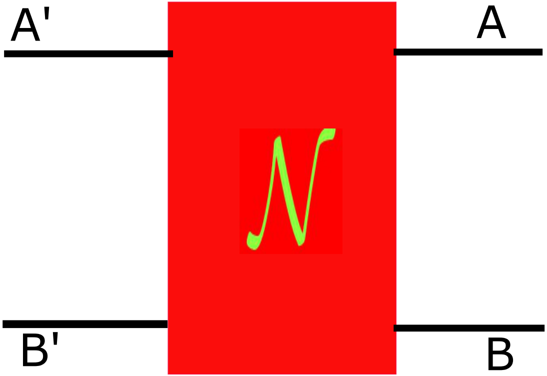


Figure: Two parties of interest: Alice holds A', A and Bob holds B', B.

- When A', A are held by Alice and B', B are held by Bob, bipartite channel $\mathcal{N}$ is called bidirectional channel.
- It corresponds to noisy bipartite interaction, when bath is inaccessible.
- For all input state $\omega_{A'B'}$:

$$\mathcal{N}(\omega_{A'B'}) = \rho_{AB}, \text{ where}$$

$$\rho_{AB} := \mathrm{Tr}_E\{\mathcal{U}_{A'B'E'\to ABE}(\omega_{A'B'} \otimes \tau_{E'})\},$$

when initial state $\tau_{E'}$ of bath is fixed.

Bidirectional quantum channel

A bipartite quantum channel $\mathcal{N}_{A'B' \to AB}$ is a completely positive, trace-preserving map that transforms composite system $A'B'$ to AB.

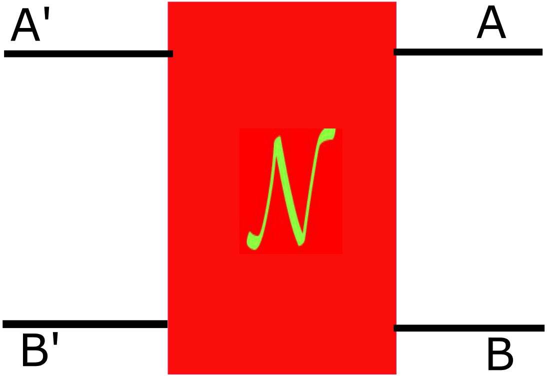


Figure: Two parties of interest: Alice holds A', A and Bob holds B', B.

- When A', A are held by Alice and B', B are held by Bob, bipartite channel $\mathcal{N}$ is called bidirectional channel.
- It corresponds to noisy bipartite interaction, when bath is inaccessible.
- For all input state $\omega_{A'B'}$:

$$\mathcal{N}(\omega_{A'B'}) = \rho_{AB}, \text{ where}$$

$$\rho_{AB} := \mathrm{Tr}_E\{\mathcal{U}_{A'B'E' \to ABE}(\omega_{A'B'} \otimes \tau_{E'})\},$$

when initial state $\tau_{E'}$ of bath is fixed.

Bidirectional quantum channel

A bipartite quantum channel $\mathcal{N}_{A'B'\to AB}$ is a completely positive, trace-preserving map that transforms composite system $A'B'$ to AB.

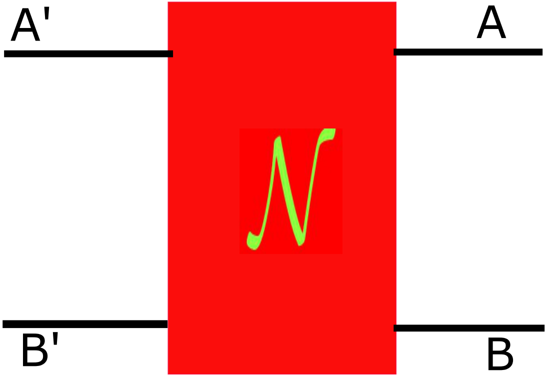


Figure: Two parties of interest: Alice holds A', A and Bob holds B', B.

- When A', A are held by Alice and B', B are held by Bob, bipartite channel $\mathcal{N}$ is called bidirectional channel.
- It corresponds to noisy bipartite interaction, when bath is inaccessible.
- For all input state $\omega_{A'B'}$:

$$\mathcal{N}(\omega_{A'B'}) = \rho_{AB}, \text{ where}$$
$$\rho_{AB} := \mathrm{Tr}_E\{\mathcal{U}_{A'B'E'\to ABE}(\omega_{A'B'} \otimes \tau_{E'})\},$$

when initial state $\tau_{E'}$ of bath is fixed.

Motivation

Bidirectional channels:

- Simple model of quantum network with 2 clients, Alice and Bob.
- Model for quantum gates – CNOT, SWAP, etc.– in noisy intermediate-scale quantum (NISQ) computers.

Entanglement may increase, decrease or not change due to bipartite quantum interactions.

Entanglement distillation: Maximally entangled states are useful resource for several information processing tasks: quantum key distribution, quantum teleportation, etc.

Secret key distillation: Need for secure communication protocols between two parties over network – private reading.

Motivation

Bidirectional channels:

- Simple model of quantum network with 2 clients, Alice and Bob.
- Model for quantum gates – CNOT, SWAP, etc.– in noisy intermediate-scale quantum (NISQ) computers.

Entanglement may increase, decrease or not change due to bipartite quantum interactions.

Entanglement distillation: Maximally entangled states are useful resource for several information processing tasks: quantum key distribution, quantum teleportation, etc.

Secret key distillation: Need for secure communication protocols between two parties over network – private reading.

Motivation

Bidirectional channels:

- Simple model of quantum network with 2 clients, Alice and Bob.
- Model for quantum gates – CNOT, SWAP, etc.– in noisy intermediate-scale quantum (NISQ) computers.

Entanglement may increase, decrease or not change due to bipartite quantum interactions.

Entanglement distillation: Maximally entangled states are useful resource for several information processing tasks: quantum key distribution, quantum teleportation, etc.

Secret key distillation: Need for secure communication protocols between two parties over network – private reading.

Motivation

Bidirectional channels:

- Simple model of quantum network with 2 clients, Alice and Bob.
- Model for quantum gates – CNOT, SWAP, etc.– in noisy intermediate-scale quantum (NISQ) computers.

Entanglement may increase, decrease or not change due to bipartite quantum interactions.

Entanglement distillation: Maximally entangled states are useful resource for several information processing tasks: quantum key distribution, quantum teleportation, etc.

Secret key distillation: Need for secure communication protocols between two parties over network – private reading.

Motivation

Bidirectional channels:

- Simple model of quantum network with 2 clients, Alice and Bob.
- Model for quantum gates – CNOT, SWAP, etc.– in noisy intermediate-scale quantum (NISQ) computers.

Entanglement may increase, decrease or not change due to bipartite quantum interactions.

Entanglement distillation: Maximally entangled states are useful resource for several information processing tasks: quantum key distribution, quantum teleportation, etc.

Secret key distillation: Need for secure communication protocols between two parties over network – private reading.

Goal

- Two different information-processing tasks relevant for bipartite quantum interactions:
    1. Entanglement distillation: generation of singlet state from two separated systems.
    2. Secret key agreement: generation of maximal classical correlation between two separated systems, such that there's no correlation with the bath.
- New secure communication protocol between two parties, called private reading.

Non-asymptotic capacity of a channel $\mathcal{N}$ for a task: Maximum rate at which a given task can be accomplished by allowing the use of $\mathcal{N}$ a finite number of times.

Goal

- Two different information-processing tasks relevant for bipartite quantum interactions:
  1. Entanglement distillation: generation of singlet state from two separated systems.
  2. Secret key agreement: generation of maximal classical correlation between two separated systems, such that there's no correlation with the bath.
- New secure communication protocol between two parties, called private reading.

Non-asymptotic capacity of a channel $\mathcal{N}$ for a task: Maximum rate at which a given task can be accomplished by allowing the use of $\mathcal{N}$ a finite number of times.

Goal

- Two different information-processing tasks relevant for bipartite quantum interactions:
  1. Entanglement distillation: generation of singlet state from two separated systems.
  2. Secret key agreement: generation of maximal classical correlation between two separated systems, such that there's no correlation with the bath.

- New secure communication protocol between two parties, called private reading.

Non-asymptotic capacity of a channel $\mathcal{N}$ for a task: Maximum rate at which a given task can be accomplished by allowing the use of $\mathcal{N}$ a finite number of times.

Goal

- Two different information-processing tasks relevant for bipartite quantum interactions:
  1. Entanglement distillation: generation of singlet state from two separated systems.
  2. Secret key agreement: generation of maximal classical correlation between two separated systems, such that there's no correlation with the bath.
- New secure communication protocol between two parties, called private reading.

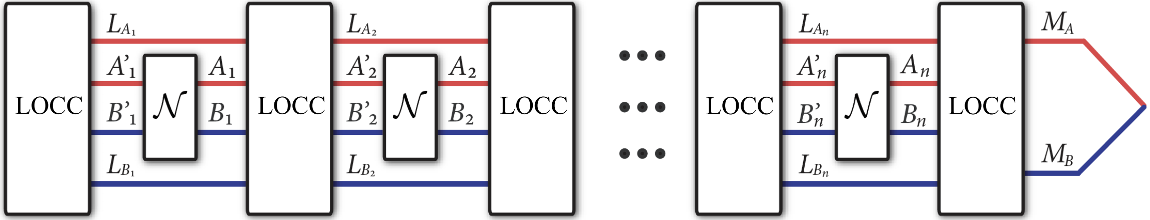
Non-asymptotic capacity of a channel $\mathcal{N}$ for a task: Maximum rate at which a given task can be accomplished by allowing the use of $\mathcal{N}$ a finite number of times.

Goal

- Two different information-processing tasks relevant for bipartite quantum interactions:
  1. Entanglement distillation: generation of singlet state from two separated systems.
  2. Secret key agreement: generation of maximal classical correlation between two separated systems, such that there's no correlation with the bath.
- New secure communication protocol between two parties, called private reading.

Non-asymptotic capacity of a channel $\mathcal{N}$ for a task: Maximum rate at which a given task can be accomplished by allowing the use of $\mathcal{N}$ a finite number of times.

Secret key generation over bidirectional channel

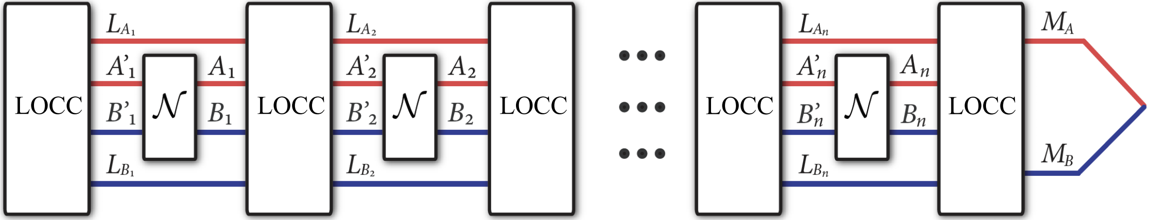


- LOCC-assisted bidirectional secret-key-agreement capacity $[\mathcal{P}^{2\to 2}_{LOCC}(\mathcal{N}_{A'B'\to AB}).]$
- Bidirectional max-relative entropy of entanglement:

$$E^{2\to 2}_{\max}(\mathcal{N}_{A'B'\to AB}) = \sup_{\psi_{S_AA'}\otimes\varphi_{B'S_B}} E_{\max}(S_AA;BS_B)_{\mathcal{N}(\psi\otimes\varphi)},$$

where $\psi_{S_AA'}, \varphi_{B'S_B}$ are pure states, $S_A \simeq A', S_B \simeq B'$,
$E_{\max}(A:B)_\rho = \min_{\sigma_{AB}\in \mathrm{SEP}} D_{\max}(\rho\|\sigma)$, such that $D_{\max}(\rho\|\sigma) = \inf\{\lambda : \rho \le 2^\lambda\sigma\}$.

Secret key generation over bidirectional channel

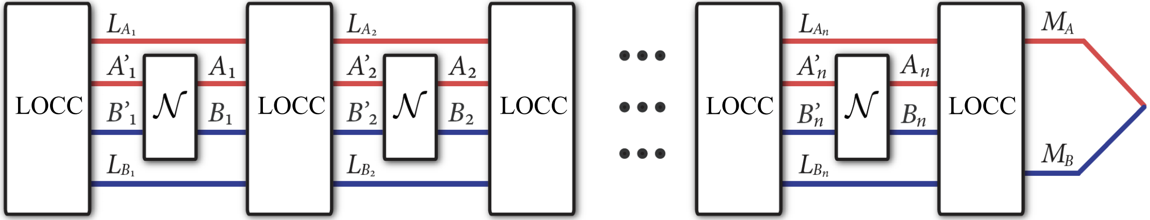


- LOCC-assisted bidirectional secret-key-agreement capacity $[\mathcal{P}^{2\to 2}_{LOCC}(\mathcal{N}_{A'B'\to AB}).]$
- Bidirectional max-relative entropy of entanglement:

$$E^{2\to 2}_{\max}(\mathcal{N}_{A'B'\to AB}) = \sup_{\psi_{S_A A'}\otimes\varphi_{B'S_B}} E_{\max}(S_A A; BS_B)_{\mathcal{N}(\psi\otimes\varphi)},$$

where $\psi_{S_A A'}, \varphi_{B'S_B}$ are pure states, $S_A \simeq A', S_B \simeq B'$,
$E_{\max}(A:B)_\rho = \min_{\sigma_{AB}\in \mathrm{SEP}} D_{\max}(\rho\|\sigma)$, such that $D_{\max}(\rho\|\sigma) = \inf\{\lambda : \rho \leq 2^\lambda \sigma\}$.

Secret key generation over bidirectional channel

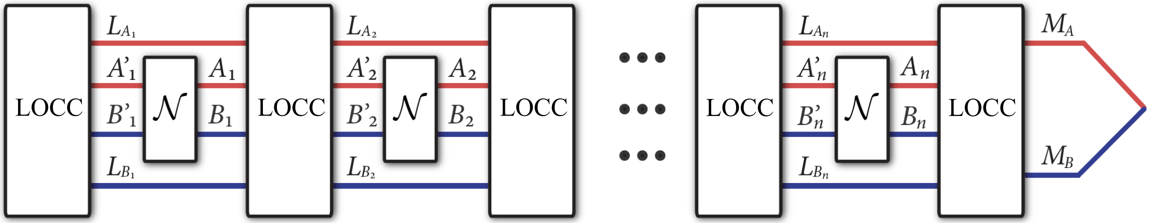


- LOCC-assisted bidirectional secret-key-agreement capacity $[\mathcal{P}^{2\to 2}_{LOCC}(\mathcal{N}_{A'B'\to AB})$.]
- Bidirectional max-relative entropy of entanglement:

$$E^{2\to 2}_{\max}(\mathcal{N}_{A'B'\to AB}) = \sup_{\psi_{S_AA'}\otimes\varphi_{B'S_B}} E_{\max}(S_AA;BS_B)_{\mathcal{N}(\psi\otimes\varphi)},$$

where $\psi_{S_AA'}, \varphi_{B'S_B}$ are pure states, $S_A \simeq A', S_B \simeq B'$,
$E_{\max}(A:B)_\rho = \min_{\sigma_{AB}\in \mathrm{SEP}} D_{\max}(\rho\|\sigma)$, such that $D_{\max}(\rho\|\sigma) = \inf\{\lambda : \rho \leq 2^\lambda \sigma\}$.

Secret key generation over bidirectional channel

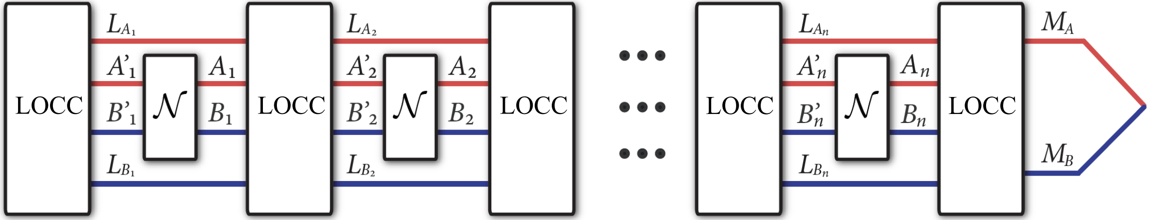


Theorem (LOCC-assisted secret key agreement)

$$\frac{1}{n}\log_2 M \leq E_{\max}^{2\to 2}(\mathcal{N}) + \frac{1}{n}\log_2\left(\frac{1}{1-\varepsilon}\right).$$

- $P_{LOCC}^{2\to 2}(\mathcal{N}_{A'B'\to AB}) \leq E_{\max}^{2\to 2}(\mathcal{N}_{A'B'\to AB})$, and this upper bound is in fact a strong converse bound.

Secret key generation over bidirectional channel

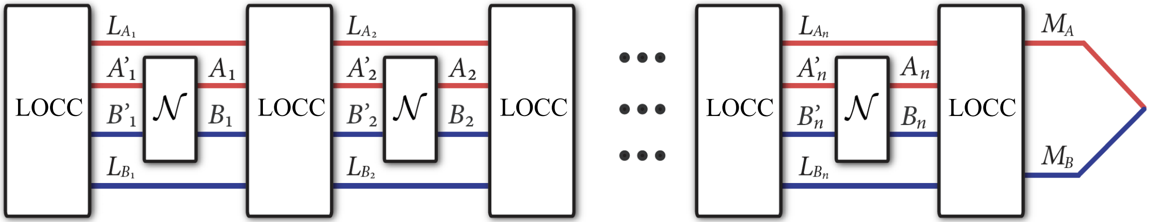


Theorem (LOCC-assisted secret key agreement)

$$\frac{1}{n}\log_2 M \leq E_{\max}^{2\to 2}(\mathcal{N}) + \frac{1}{n}\log_2\left(\frac{1}{1-\varepsilon}\right).$$

- $P_{LOCC}^{2\to 2}(\mathcal{N}_{A'B'\to AB}) \leq E_{\max}^{2\to 2}(\mathcal{N}_{A'B'\to AB})$, and this upper bound is in fact a strong converse bound.

Secret key generation over bidirectional channel

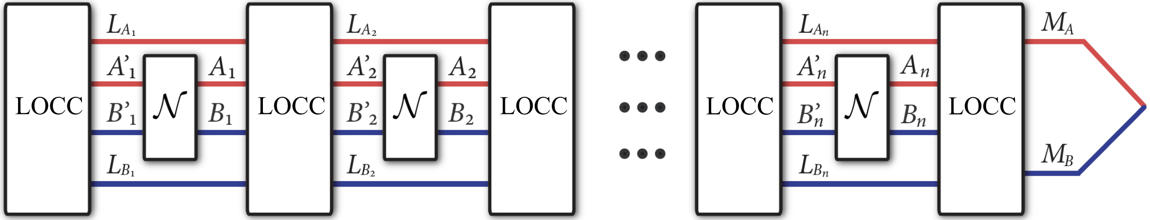


Theorem (LOCC-assisted secret key agreement)

$$\frac{1}{n}\log_2 M \leq E^{2\to 2}_{\max}(\mathcal{N}) + \frac{1}{n}\log_2\left(\frac{1}{1-\varepsilon}\right).$$

- $P^{2\to 2}_{LOCC}(\mathcal{N}_{A'B'\to AB}) \leq E^{2\to 2}_{\max}(\mathcal{N}_{A'B'\to AB})$, and this upper bound is in fact a strong converse bound.

Proof outline: Secret key generation

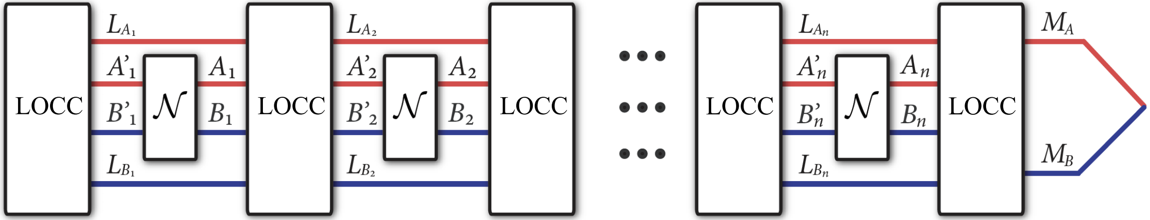


- Private states [HHHO05,HHHO09]: State $\gamma_{S_A K_A : K_B S_B}$ containing $\log_2 K$ private bits.
- Success probability in privacy test: $\text{Tr}\{\Pi^\gamma \omega\} \geq 1 - \varepsilon$. By [HHHO05,HHHO09], $\text{Tr}\{\Pi^\gamma \sigma\} \leq \frac{1}{K}$ for $\sigma \in \text{SEP}$.
- Main observation: $E_{\max}^{2\to 2}$ is not enhanced by amortization.

$$E_{\max}(S_A A; B S_B)_\sigma \leq E_{\max}(S_A A'; B' S_B)_\rho + E_{\max}^{2\to 2}(\mathcal{N}_{A'B'\to AB}),$$

where $\sigma_{S_A A B S_B} = \mathcal{N}_{A'B'\to AB}(\rho_{S_A A' B' S_B})$.

Proof outline: Secret key generation

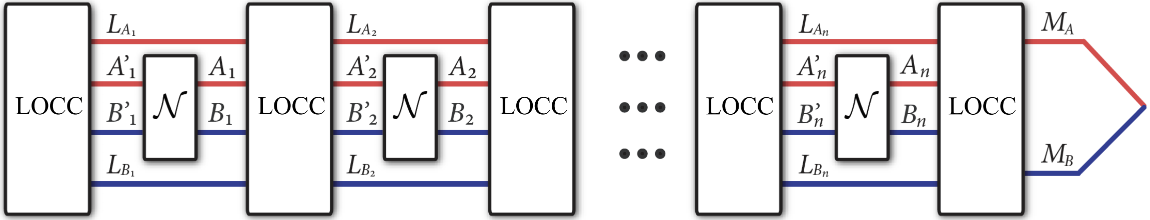


- Private states [HHHO05,HHHO09]: State $\gamma_{S_A K_A : K_B S_B}$ containing $\log_2 K$ private bits.
- Success probability in privacy test: $\text{Tr}\{\Pi^{\gamma}\omega\} \geq 1 - \varepsilon$. By [HHHO05,HHHO09], $\text{Tr}\{\Pi^{\gamma}\sigma\} \leq \frac{1}{K}$ for $\sigma \in \text{SEP}$.
- Main observation: $E_{\max}^{2\to 2}$ is not enhanced by amortization.

$$E_{\max}(S_A A; BS_B)_{\sigma} \leq E_{\max}(S_A A'; B' S_B)_{\rho} + E_{\max}^{2\to 2}(\mathcal{N}_{A'B'\to AB}),$$

where $\sigma_{S_A ABS_B} = \mathcal{N}_{A'B'\to AB}(\rho_{S_A A' B' S_B})$.

Proof outline: Secret key generation

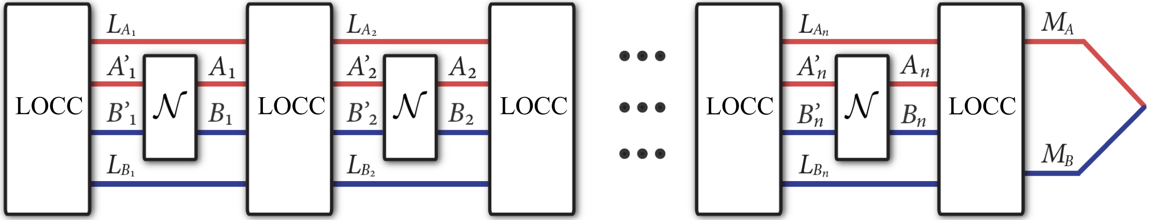


- Private states [HHHO05,HHHO09]: State $\gamma_{S_A K_A : K_B S_B}$ containing $\log_2 K$ private bits.
- Success probability in privacy test: $\operatorname{Tr}\{\Pi^{\gamma}\omega\} \geq 1 - \varepsilon$. By [HHHO05,HHHO09], $\operatorname{Tr}\{\Pi^{\gamma}\sigma\} \leq \frac{1}{K}$ for $\sigma \in \mathrm{SEP}$.
- Main observation: $E_{\max}^{2\to 2}$ is not enhanced by amortization.

$$E_{\max}(S_A A; B S_B)_{\sigma} \leq E_{\max}(S_A A'; B' S_B)_{\rho} + E_{\max}^{2\to 2}(\mathcal{N}_{A'B' \to AB}),$$

where $\sigma_{S_A A B S_B} = \mathcal{N}_{A'B' \to AB}(\rho_{S_A A' B' S_B})$.

Proof outline: Secret key generation

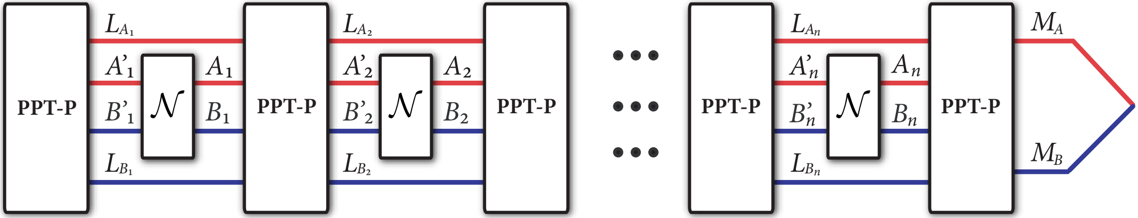


- Private states [HHHO05,HHHO09]: State $\gamma_{S_A K_A : K_B S_B}$ containing $\log_2 K$ private bits.
- Success probability in privacy test: $\text{Tr}\{\Pi^\gamma \omega\} \geq 1 - \varepsilon$. By [HHHO05,HHHO09], $\text{Tr}\{\Pi^\gamma \sigma\} \leq \frac{1}{K}$ for $\sigma \in \text{SEP}$.
- Main observation: $E^{2\to 2}_{\max}$ is not enhanced by amortization.

$$E_{\max}(S_A A; B S_B)_\sigma \leq E_{\max}(S_A A'; B' S_B)_\rho + E^{2\to 2}_{\max}(\mathcal{N}_{A'B'\to AB}),$$

where $\sigma_{S_A A B S_B} = \mathcal{N}_{A'B'\to AB}(\rho_{S_A A' B' S_B})$.

Entanglement generation over bidirectional channel

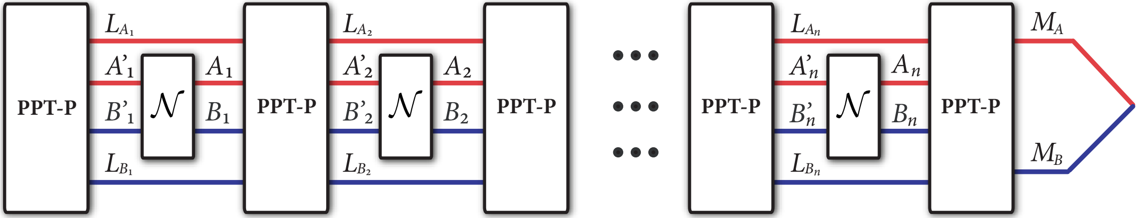


- PPT-assisted bidirectional quantum capacity $[\mathcal{Q}^{2\to 2}_{PPT}(\mathcal{N}_{A'B'\to AB}).]$
- Bidirectional max-Rains Information $[R^{2\to 2}_{\max}(\mathcal{N}_{A'B'\to AB}) = \log \Gamma^{2\to 2}(\mathcal{N}_{A'B'\to AB})]$, where

$$
\begin{aligned}
\Gamma^{2\to 2}(\mathcal{N}_{A'B'\to AB}) = \text{minimize} \quad & \|\mathrm{Tr}_{AB}\{V_{S_A ABS_B} + Y_{S_A ABS_B}\}\|_\infty \\
\text{subject to} \quad & V_{S_A ABS_B}, Y_{S_A ABS_B} \geq 0, \\
& T_{BS_B}\{V_{S_A ABS_B} - Y_{S_A ABS_B}\} \geq J^{\mathcal{N}}_{S_A ABS_B},
\end{aligned}
$$

such that $S_A \simeq A',\ S_B \simeq B'$.

Entanglement generation over bidirectional channel

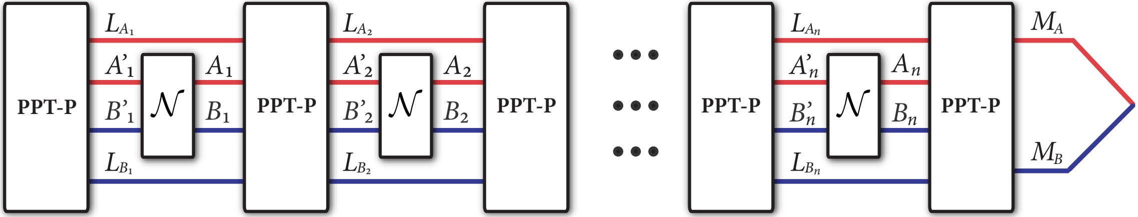


- PPT-assisted bidirectional quantum capacity $[\mathcal{Q}^{2\to 2}_{PPT}(\mathcal{N}_{A'B'\to AB}).]$
- Bidirectional max-Rains Information $[R^{2\to 2}_{\max}(\mathcal{N}_{A'B'\to AB}) = \log \Gamma^{2\to 2}(\mathcal{N}_{A'B'\to AB})]$, where

$$\begin{aligned}\Gamma^{2\to 2}(\mathcal{N}_{A'B'\to AB}) = \text{minimize} \quad & \|\mathrm{Tr}_{AB}\{V_{S_AABS_B} + Y_{S_AABS_B}\}\|_\infty \\ \text{subject to} \quad & V_{S_AABS_B}, Y_{S_AABS_B} \geq 0, \\ & T_{BS_B}\{V_{S_AABS_B} - Y_{S_AABS_B}\} \geq J^{\mathcal{N}}_{S_AABS_B},\end{aligned}$$

such that $S_A \simeq A'$, $S_B \simeq B'$.

Entanglement generation over bidirectional channel

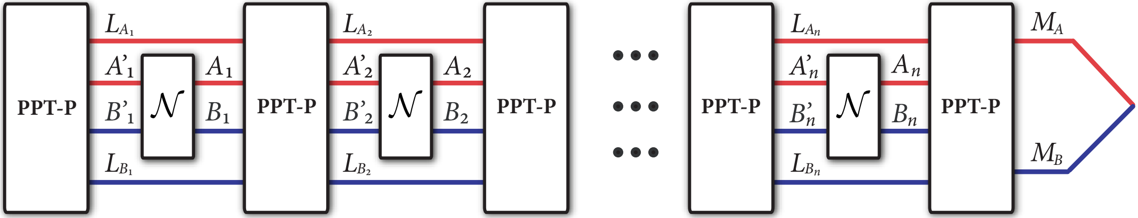


- PPT-assisted bidirectional quantum capacity $[\mathcal{Q}^{2\to 2}_{PPT}(\mathcal{N}_{A'B'\to AB}).]$
- Bidirectional max-Rains Information $[R^{2\to 2}_{\max}(\mathcal{N}_{A'B'\to AB}) = \log \Gamma^{2\to 2}(\mathcal{N}_{A'B'\to AB})]$, where

$$\begin{aligned}\Gamma^{2\to 2}(\mathcal{N}_{A'B'\to AB}) = \text{minimize} \quad & \|\mathrm{Tr}_{AB}\{V_{S_AABS_B} + Y_{S_AABS_B}\}\|_\infty \\ \text{subject to} \quad & V_{S_AABS_B}, Y_{S_AABS_B} \geq 0, \\ & T_{BS_B}\{V_{S_AABS_B} - Y_{S_AABS_B}\} \geq J^{\mathcal{N}}_{S_AABS_B},\end{aligned}$$

such that $S_A \simeq A',\ S_B \simeq B'$.

Entanglement generation over bidirectional channel

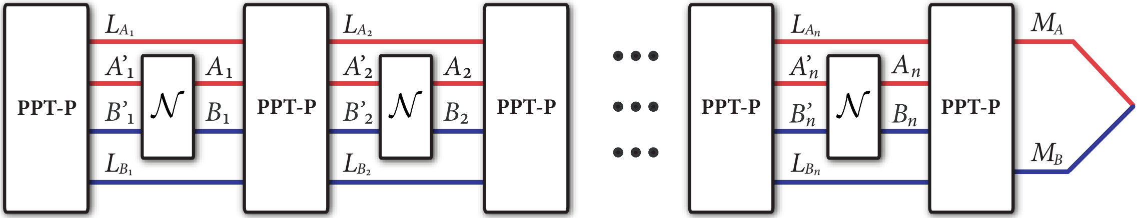


- PPT-assisted bidirectional quantum capacity $[\mathcal{Q}^{2\to 2}_{PPT}(\mathcal{N}_{A'B'\to AB}).]$
- Bidirectional max-Rains Information $[R^{2\to 2}_{\max}(\mathcal{N}_{A'B'\to AB}) = \log \Gamma^{2\to 2}(\mathcal{N}_{A'B'\to AB})]$, where

$$\begin{aligned} \Gamma^{2\to 2}(\mathcal{N}_{A'B'\to AB}) = \text{minimize} \quad & \| \operatorname{Tr}_{AB}\{V_{S_AABS_B} + Y_{S_AABS_B}\}\|_\infty \\ \text{subject to} \quad & V_{S_AABS_B}, Y_{S_AABS_B} \geq 0, \\ & T_{BS_B}\{V_{S_AABS_B} - Y_{S_AABS_B}\} \geq J^{\mathcal{N}}_{S_AABS_B}, \end{aligned}$$

such that $S_A \simeq A',\ S_B \simeq B'$.

Entanglement generation over bidirectional channel

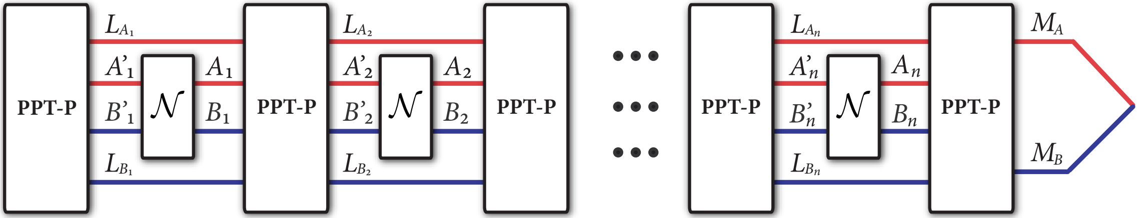


Theorem (PPT-assisted distillable entanglement generation)

$$\frac{1}{n}\log_2 M \leq R_{\max}^{2\to 2}(\mathcal{N}) + \frac{1}{n}\log_2\left(\frac{1}{1-\varepsilon}\right).$$

- $Q_{PPT}^{2\to 2}(\mathcal{N}_{A'B'\to AB}) \leq R_{\max}^{2\to 2}(\mathcal{N}_{A'B'\to AB})$, and this upper bound is in fact a strong converse bound.

Entanglement generation over bidirectional channel

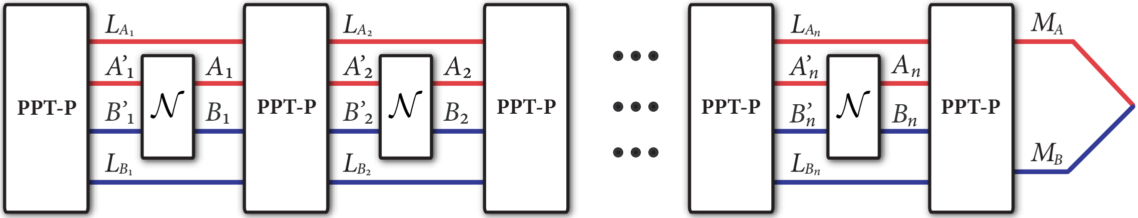


Theorem (PPT-assisted distillable entanglement generation)

$$\frac{1}{n}\log_2 M \leq R^{2\to 2}_{\max}(\mathcal{N}) + \frac{1}{n}\log_2\left(\frac{1}{1-\varepsilon}\right).$$

- $Q^{2\to 2}_{PPT}(\mathcal{N}_{A'B'\to AB}) \leq R^{2\to 2}_{\max}(\mathcal{N}_{A'B'\to AB})$, and this upper bound is in fact a strong converse bound.

Entanglement generation over bidirectional channel



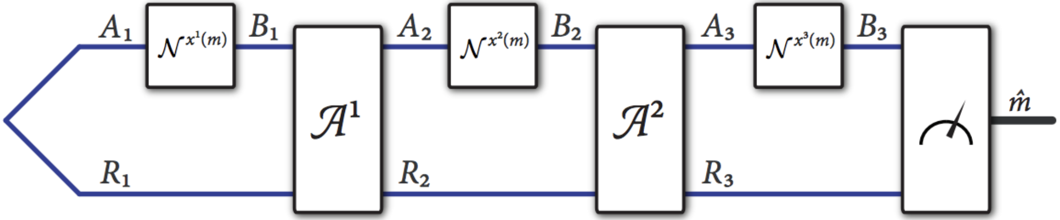
Theorem (PPT-assisted distillable entanglement generation)

$$\frac{1}{n}\log_2 M \leq R^{2\to 2}_{\max}(\mathcal{N}) + \frac{1}{n}\log_2\left(\frac{1}{1-\varepsilon}\right).$$

- $Q^{2\to 2}_{PPT}(\mathcal{N}_{A'B'\to AB}) \leq R^{2\to 2}_{\max}(\mathcal{N}_{A'B'\to AB})$, and this upper bound is in fact a strong converse bound.

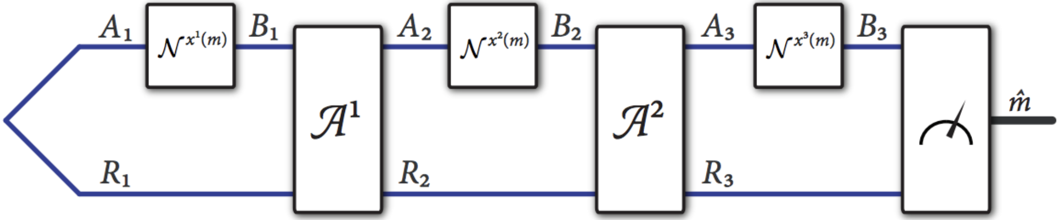
Application: Private Reading

- First recall: (Quantum) Reading [BRV00,Pir11] of memory devices.
- Memory device: message encoded into a sequence of channels from a memory cell $\mathcal{S}_{\mathcal{X}} = \{\mathcal{N}^{x}_{B'\to B}\}_{x\in\mathcal{X}}$.
- Alice encodes $m \in \mathcal{M}$ into codewords $(x_1(m), ..., x_n(m))$, and sets the device to $\left(\mathcal{N}^{x_1(m)}_{B'\to B}, ..., \mathcal{N}^{x_n(m)}_{B'\to B}\right)$.
- Bob can enter quantum states and do channel discrimination to learn m. Natural to employ adaptive strategy [DW17].



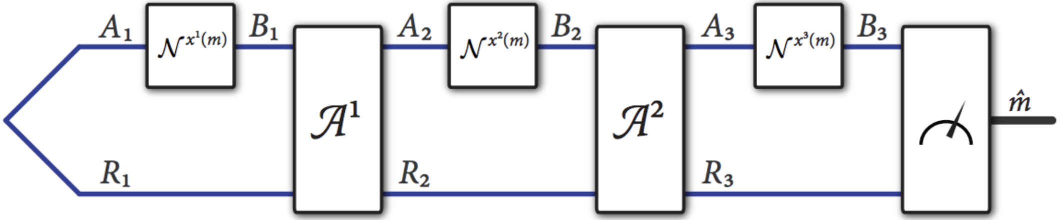
Application: Private Reading

- First recall: (Quantum) Reading [BRV00,Pir11] of memory devices.
- Memory device: message encoded into a sequence of channels from a memory cell $\mathcal{S}_{\mathcal{X}} = \{\mathcal{N}^{x}_{B'\to B}\}_{x\in\mathcal{X}}$.
- Alice encodes $m \in \mathcal{M}$ into codewords $(x_1(m), \dots, x_n(m))$, and sets the device to $\left(\mathcal{N}^{x_1(m)}_{B'\to B}, \dots, \mathcal{N}^{x_n(m)}_{B'\to B}\right)$.
- Bob can enter quantum states and do channel discrimination to learn m. Natural to employ adaptive strategy [DW17].



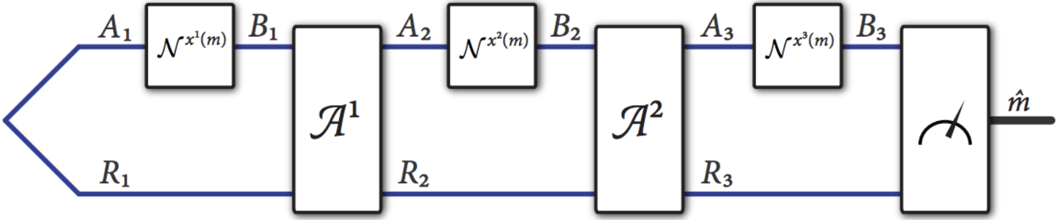
Application: Private Reading

- First recall: (Quantum) Reading [BRV00,Pir11] of memory devices.
- Memory device: message encoded into a sequence of channels from a memory cell $\mathcal{S}_{\mathcal{X}} = \{\mathcal{N}^{x}_{B'\to B}\}_{x\in\mathcal{X}}$.
- Alice encodes $m \in \mathcal{M}$ into codewords $(x_1(m), \ldots, x_n(m))$, and sets the device to $\left(\mathcal{N}^{x_1(m)}_{B'\to B}, \ldots, \mathcal{N}^{x_n(m)}_{B'\to B}\right)$.
- Bob can enter quantum states and do channel discrimination to learn m. Natural to employ adaptive strategy [DW17].

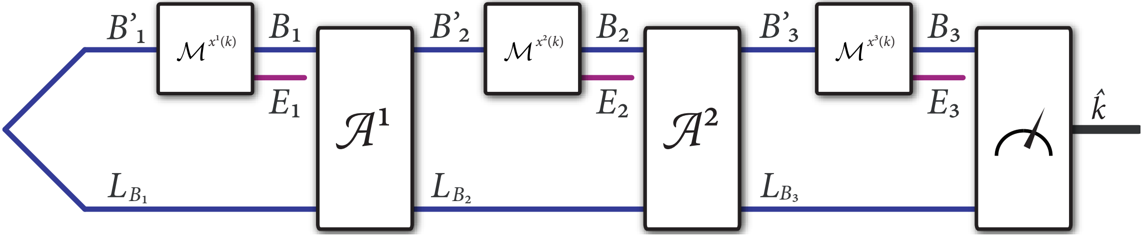


Application: Private Reading

- First recall: (Quantum) Reading [BRV00,Pir11] of memory devices.
- Memory device: message encoded into a sequence of channels from a memory cell $\mathcal{S}_{\mathcal{X}} = \{\mathcal{N}^{x}_{B'\to B}\}_{x\in\mathcal{X}}$.
- Alice encodes $m \in \mathcal{M}$ into codewords $(x_1(m), ..., x_n(m))$, and sets the device to $\left(\mathcal{N}^{x_1(m)}_{B'\to B}, ..., \mathcal{N}^{x_n(m)}_{B'\to B}\right)$.
- Bob can enter quantum states and do channel discrimination to learn m. Natural to employ adaptive strategy [DW17].



Application: Private Reading

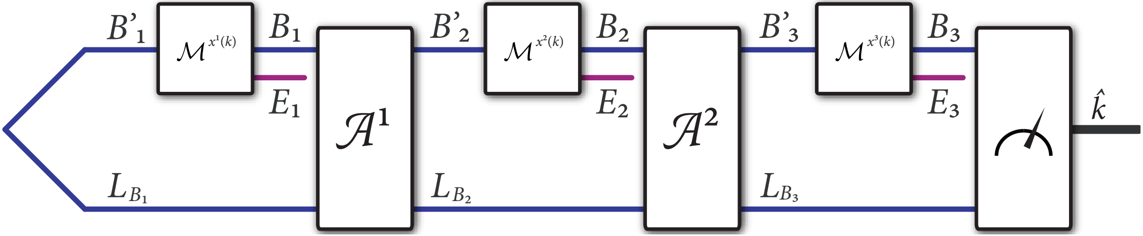


- Private reading: Eve present when Bob performs the readout: Wiretap memory cell $\bar{\mathcal{S}}_{\mathcal{X}} = \{\mathcal{M}^{x}_{B'\to BE}\}_{x\in\mathcal{X}}$. Special case: Isometric wiretap memory cell $\bar{\mathcal{S}}^{\text{iso}}_{X}$.
- The non-adaptive private reading capacity of a wiretap memory cell $\mathcal{S}_{\mathcal{X}}$ is given by

$$P^{\text{read}}_{\text{n-a}}\left(\overline{\mathcal{M}}_{\mathcal{X}}\right) = \sup_{n} \max_{p_{X^n},\sigma_{L_B B'^n}} \frac{1}{n}\left[I(X^n; L_B B^n)_\tau - I(X^n; E^n)_\tau\right],$$

where $\tau_{X^n L_B B^n E^n} := \sum_{x^n} p_{X^n}(x^n)|x^n\rangle\langle x^n|_{X^n} \otimes \mathcal{M}^{x^n}_{B'^n\to B^n E^n}(\sigma_{L_B B'^n})$.

Application: Private Reading

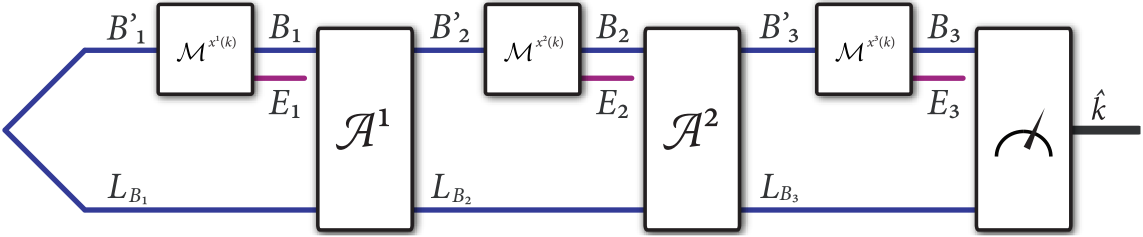


- Private reading: Eve present when Bob performs the readout: Wiretap memory cell $\bar{\mathcal{S}}_{\mathcal{X}} = \{\mathcal{M}^{x}_{B'\to BE}\}_{x\in\mathcal{X}}$. Special case: Isometric wiretap memory cell $\bar{\mathcal{S}}^{\text{iso}}_{X}$.
- The non-adaptive private reading capacity of a wiretap memory cell $\mathcal{S}_{\mathcal{X}}$ is given by

$$P^{\text{read}}_{\text{n-a}}\left(\overline{\mathcal{M}}_{\mathcal{X}}\right) = \sup_{n} \max_{p_{X^n},\sigma_{L_B B'^n}} \frac{1}{n}\left[I(X^n;L_B B^n)_\tau - I(X^n;E^n)_\tau\right],$$

where $\tau_{X^n L_B B^n E^n} := \sum_{x^n} p_{X^n}(x^n)|x^n\rangle\langle x^n|_{X^n} \otimes \mathcal{M}^{x^n}_{B'^n\to B^n E^n}(\sigma_{L_B B'^n})$.

Application: Private Reading

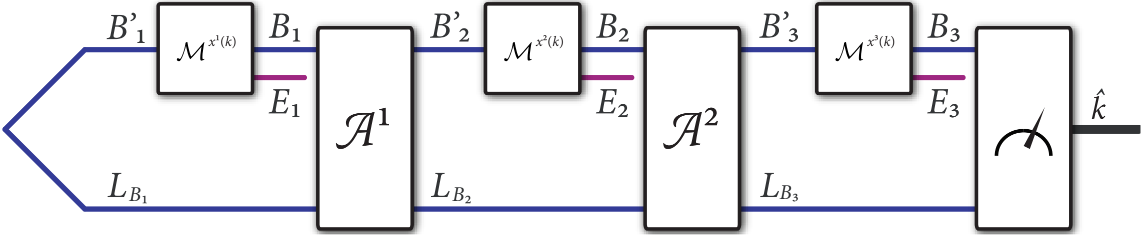


- Private reading: Eve present when Bob performs the readout: Wiretap memory cell $\bar{\mathcal{S}}_{\mathcal{X}} = \{\mathcal{M}^{x}_{B' \to BE}\}_{x \in \mathcal{X}}$. Special case: Isometric wiretap memory cell $\bar{S}^{\text{iso}}_{\mathcal{X}}$.
- The non-adaptive private reading capacity of a wiretap memory cell $\bar{\mathcal{S}}_{\mathcal{X}}$ is given by

$$P^{\text{read}}_{\text{n-a}}\left(\bar{\mathcal{S}}_{\mathcal{X}}\right) = \sup_{n} \max_{p_{X^n}, \sigma_{L_B B'^n}} \frac{1}{n} \left[I(X^n; L_B B^n)_{\tau} - I(X^n; E^n)_{\tau} \right],$$

where $\tau_{X^n L_B B^n E^n} := \sum_{x^n} p_{X^n}(x^n) |x^n\rangle\langle x^n|_{X^n} \otimes \mathcal{M}^{x^n}_{B'^n \to B^n E^n}(\sigma_{L_B B'^n})$.

Application: Private Reading

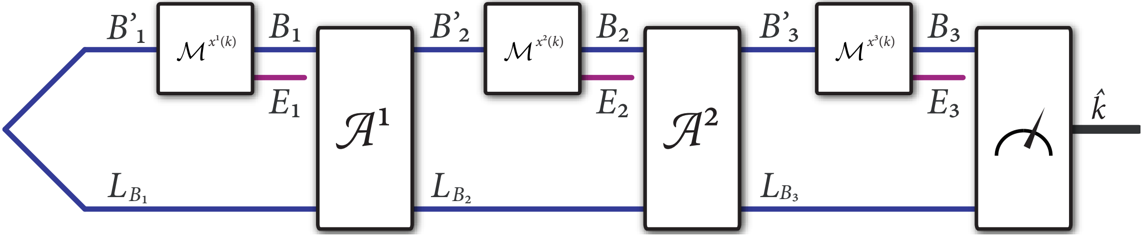


- Private reading: Eve present when Bob performs the readout: Wiretap memory cell $\bar{\mathcal{S}}_{\mathcal{X}} = \{\mathcal{M}^{x}_{B'\to BE}\}_{x\in\mathcal{X}}$. Special case: Isometric wiretap memory cell $\bar{S}^{\text{iso}}_{X}$.
- The non-adaptive private reading capacity of a wiretap memory cell $\bar{\mathcal{S}}_{\mathcal{X}}$ is given by

$$P^{\text{read}}_{\text{n-a}}\left(\bar{\mathcal{S}}_{\mathcal{X}}\right) = \sup_{n} \max_{p_{X^n},\sigma_{L_B B'^n}} \frac{1}{n}\left[I(X^n; L_B B^n)_\tau - I(X^n; E^n)_\tau\right],$$

where $\tau_{X^n L_B B^n E^n} := \sum_{x^n} p_{X^n}(x^n)|x^n\rangle\langle x^n|_{X^n} \otimes \mathcal{M}^{x^n}_{B'^n\to B^n E^n}(\sigma_{L_B B'^n})$.

Application: Private Reading

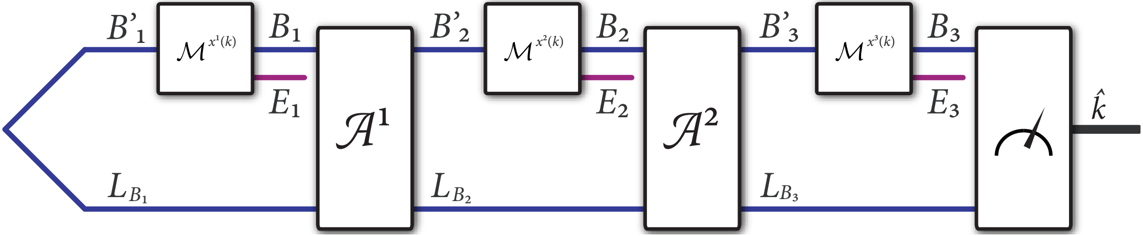


- Private reading: Eve present when Bob performs the readout: Wiretap memory cell $\bar{\mathcal{S}}_{\mathcal{X}} = \{\mathcal{M}^{x}_{B' \to BE}\}_{x\in\mathcal{X}}$. Special case: Isometric wiretap memory cell $\bar{S}^{\text{iso}}_{X}$.
- The non-adaptive private reading capacity of a wiretap memory cell $\bar{\mathcal{S}}_{\mathcal{X}}$ is given by

$$P^{\text{read}}_{\text{n-a}}\left(\bar{\mathcal{S}}_{\mathcal{X}}\right) = \sup_{n} \max_{p_{X^n}, \sigma_{L_B B'^n}} \frac{1}{n}\left[I(X^n; L_B B^n)_\tau - I(X^n; E^n)_\tau\right],$$

where $\tau_{X^n L_B B^n E^n} := \sum_{x^n} p_{X^n}(x^n)|x^n\rangle\langle x^n|_{X^n} \otimes \mathcal{M}^{x^n}_{B'^n \to B^n E^n}(\sigma_{L_B B'^n})$.

Application: Private Reading



- Private reading: Eve present when Bob performs the readout: Wiretap memory cell $\bar{\mathcal{S}}_{\mathcal{X}} = \{\mathcal{M}^{x}_{B'\to BE}\}_{x\in\mathcal{X}}$. Special case: Isometric wiretap memory cell $\bar{S}^{\text{iso}}_{X}$.
- The non-adaptive private reading capacity of a wiretap memory cell $\bar{\mathcal{S}}_{\mathcal{X}}$ is given by

$$P^{\text{read}}_{\text{n-a}}\left(\bar{\mathcal{S}}_{\mathcal{X}}\right) = \sup_{n} \max_{p_{X^n},\sigma_{L_B B'^n}} \frac{1}{n}\left[I(X^n; L_B B^n)_\tau - I(X^n; E^n)_\tau\right],$$

where $\tau_{X^n L_B B^n E^n} := \sum_{x^n} p_{X^n}(x^n)|x^n\rangle\langle x^n|_{X^n} \otimes \mathcal{M}^{x^n}_{B'^n\to B^n E^n}(\sigma_{L_B B'^n})$.

Private reading capacity

The strong converse private reading capacity $\widetilde{P}^{\text{read}}(\bar{\mathcal{S}}^{\text{iso}}_{\mathcal{X}})$ of an isometric wiretap memory cell $\bar{\mathcal{S}}^{\text{iso}}_{\mathcal{X}} = \{\mathcal{U}^{\mathcal{M}^x}_{B'\to BE}\}_{x\in\mathcal{X}}$ is bounded from above as

$$\widetilde{P}^{\text{read}}(\bar{\mathcal{S}}^{\text{iso}}_{\mathcal{X}}) \leq E^{2\to 2}_{\max}(\mathcal{N}^{\bar{\mathcal{S}}}_{XB'\to XB}),$$

where

$$\mathcal{N}^{\bar{\mathcal{S}}}_{XB'\to XB}(\cdot) := \operatorname{Tr}_E\left\{U^{\bar{\mathcal{S}}}_{XB'\to XBE}(\cdot)\left(U^{\bar{\mathcal{S}}}_{XB'\to XBE}\right)^{\dagger}\right\},$$

such that

$$U^{\bar{\mathcal{S}}}_{XB'\to XBE} := \sum_{x\in\mathcal{X}} |x\rangle\langle x|_X \otimes U^{\mathcal{M}^x}_{B'\to BE}.$$

Conclusion

- We derived upper bounds on entanglement generation and secret-key-agreement capacities over bidirectional channels. Sizes of reference systems are same as size of input systems (Open question in [BHLS03]).
- Obtain tighter upper bounds for channels obeying certain symmetries, see [DBW17].
- Introduced secure protocol for reading of memory devices under scrutiny of an eavesdropper. Both upper and lower bounds for this protocol can be found in [DBW17].

[DBW17] arXiv : 1712.00827

Conclusion

- We derived upper bounds on entanglement generation and secret-key-agreement capacities over bidirectional channels. Sizes of reference systems are same as size of input systems (Open question in [BHLS03]).
- Obtain tighter upper bounds for channels obeying certain symmetries, see [DBW17].
- Introduced secure protocol for reading of memory devices under scrutiny of an eavesdropper. Both upper and lower bounds for this protocol can be found in [DBW17].

[DBW17] arXiv : 1712.00827

Conclusion

- We derived upper bounds on entanglement generation and secret-key-agreement capacities over bidirectional channels. Sizes of reference systems are same as size of input systems (Open question in [BHLS03]).
- Obtain tighter upper bounds for channels obeying certain symmetries, see [DBW17].
- Introduced secure protocol for reading of memory devices under scrutiny of an eavesdropper. Both upper and lower bounds for this protocol can be found in [DBW17].

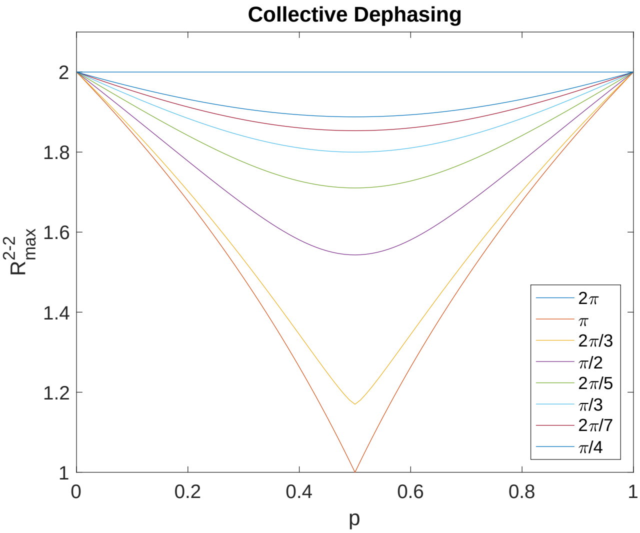
[DBW17] arXiv : 1712.00827

Conclusion

- We derived upper bounds on entanglement generation and secret-key-agreement capacities over bidirectional channels. Sizes of reference systems are same as size of input systems (Open question in [BHLS03]).
- Obtain tighter upper bounds for channels obeying certain symmetries, see [DBW17].
- Introduced secure protocol for reading of memory devices under scrutiny of an eavesdropper. Both upper and lower bounds for this protocol can be found in [DBW17].

[DBW17] arXiv : 1712.00827

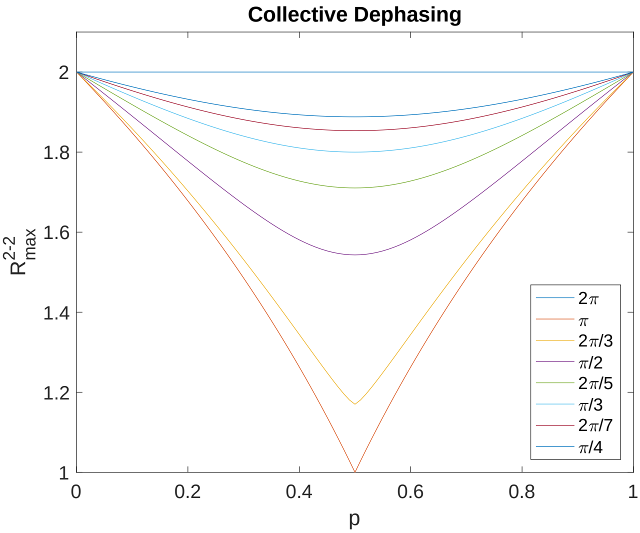
SWAP and Collective dephasing



- Collective dephasing: $|00\rangle \to |00\rangle$, $|01\rangle \to e^{i\phi}|01\rangle$, $|10\rangle \to e^{i\phi}|10\rangle$, $|11\rangle \to e^{2i\phi}|11\rangle$.
- Swap operator $S = \sum_{ij} |ij\rangle\langle ji|$ and collective dephasing:

$$\mathcal{N}_{A'B'\to AB}(\rho) = pS\rho S^\dagger + (1-p)U^\phi S\rho S^\dagger U^{\phi\dagger}$$

SWAP and Collective dephasing



- Collective dephasing: $|00\rangle \to |00\rangle$, $|01\rangle \to e^{i\phi}|01\rangle$, $|10\rangle \to e^{i\phi}|10\rangle$, $|11\rangle \to e^{2i\phi}|11\rangle$.
- Swap operator $S = \sum_{ij} |ij\rangle\langle ji|$ and collective dephasing:

$$\mathcal{N}_{A'B'\to AB}(\rho)$$
$$= pS\rho S^\dagger + (1-p)U^\phi S\rho S^\dagger U^{\phi\dagger}$$