Round Complexity in the Local Transformations of Quantum and Classical States

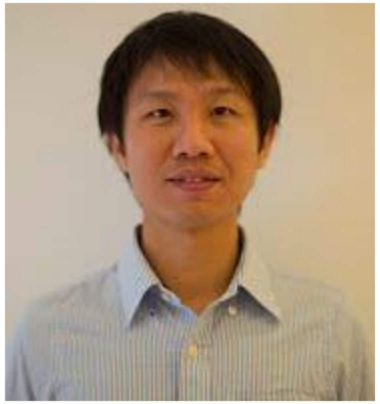
QIP 2017

January 19, 2017

Southern Illinois University Carbondale

Eric Chitambar

Min-Hsiu Hsieh



UNIVERSITY OF TECHNOLOGY SYDNEY

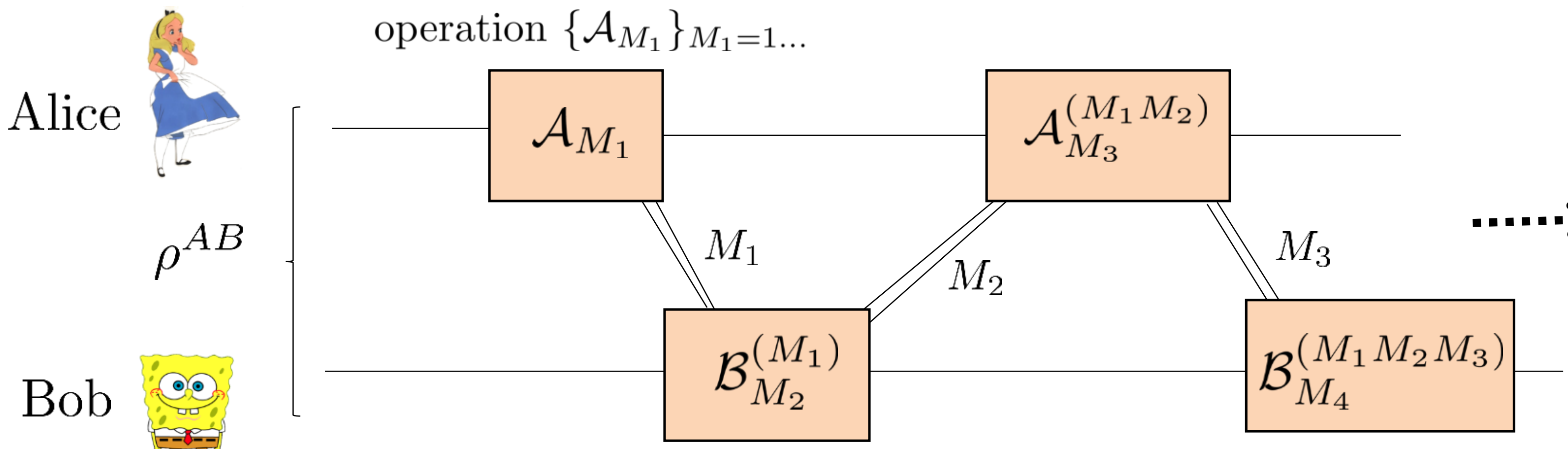
arXiv:1610.01998

Bipartite Entanglement Resource Theory

- States are bipartite density matrices ρ^{AB}
- States are manipulated using

Local Operations and Classical Communication (LOCC)

Alice performs quantum operation $\{\mathcal{A}_{M_1}\}_{M_1=1\dots}$



Bob performs conditional quantum operation $\{\mathcal{B}^{(M_1)}_{M_2}\}_{M_2=1\dots}$

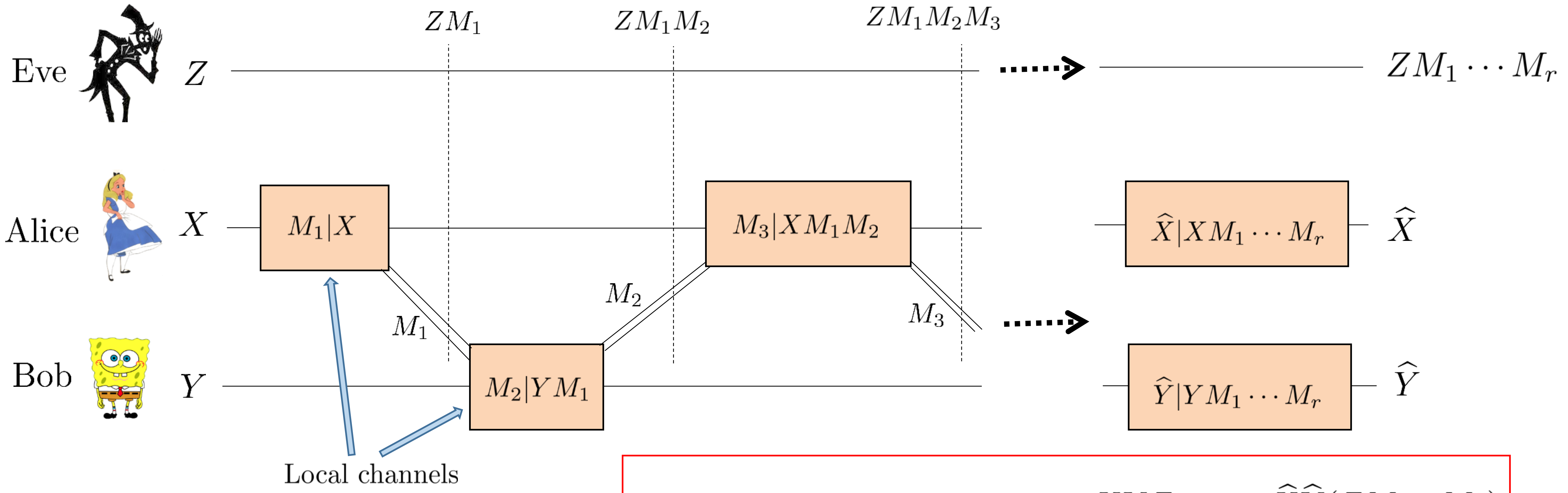
$$\sigma^{AB} = \sum_{M_1 \cdots M_r = \vec{m}} \mathcal{A}^{tot}_{\vec{m}} \otimes \mathcal{B}^{tot}_{\vec{m}}(\rho^{AB})$$

LOCC transformation: $\rho^{AB} \to \sigma^{AB}$

Bipartite Secrecy Resource Theory (Classical)

- "States" are random variables X, Y, Z held by three parties.
- States are manipulated using

Local Operations and Public Communication (LOPC)



LOPC transformation: $P^{XYZ} \to P^{\widehat{X}\widehat{Y}(ZM_1 \cdots M_r)}$

Entanglement and Secrecy: Similar Structures

	Quantum	Classical
Resource	Entanglement	Secrecy

Entanglement and Secrecy: Similar Structures

	Quantum	Classical
Resource	Entanglement	Secrecy
Free Operations	LOCC	LOPC

Entanglement and Secrecy: Similar Structures

	Quantum	Classical
Resource	Entanglement	Secrecy
Free Operations	LOCC	LOPC
Resource Unit	Entangled bit (ebit): $\vert\Phi^+\rangle = \frac{1}{\sqrt{2}}(\vert 00\rangle^{AB} + \vert 11\rangle^{AB})$	Secret bit (sbit): $\Phi^+ = \frac{1}{2}([0,0]^{XY} + [1,1]^{XY}) \otimes P^Z$

Entanglement and Secrecy: Similar Structures

	Quantum	Classical
Resource	Entanglement	Secrecy
Free Operations	LOCC	LOPC
Resource Unit	Entangled bit (ebit): $\lvert\Phi^+\rangle = \frac{1}{\sqrt{2}}(\lvert 00\rangle^{AB} + \lvert 11\rangle^{AB})$	Secret bit (sbit): $\Phi^+ = \frac{1}{2}([0,0]^{XY} + [1,1]^{XY}) \otimes P^Z$
Free Operations + Resource = Universal Operations	Teleportation	One-Time Pad

Entanglement and Secrecy: Similar Structures

	Quantum	Classical
Resource	Entanglement	Secrecy
Free Operations	LOCC	LOPC
Resource Unit	Entangled bit (ebit): $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle^{AB} + |11\rangle^{AB})$	Secret bit (sbit): $\Phi^+ = \frac{1}{2}([0,0]^{XY} + [1,1]^{XY}) \otimes P^Z$
Free Operations + Resource = Universal Operations	Teleportation	One-Time Pad
Single Copy Resource Conversion	Convertibility of Pure States Governed by Majorization	Convertibility of "Pure States" Governed by Majorization[1]

[1] Collins and Popescu – PRA 2002

Entanglement and Secrecy: Similar Structures

	Quantum	Classical
Resource	Entanglement	Secrecy
Free Operations	LOCC	LOPC
Resource Unit	Entangled bit (ebit): $\vert\Phi^+\rangle = \frac{1}{\sqrt{2}}(\vert 00\rangle^{AB} + \vert 11\rangle^{AB})$	Secret bit (sbit): $\Phi^+ = \frac{1}{2}([0,0]^{XY} + [1,1]^{XY}) \otimes P^Z$
Free Operations + Resource = Universal Operations	Teleportation	One-Time Pad
Single Copy Resource Conversion	Convertibility of Pure States Governed by Majorization	Convertibility of "Pure States" Governed by Majorization[1]
Asymptotic Resource Conversion	Entanglement Formation/ Entanglement Distillation	Secrecy Formation/ Secrecy Distillation[2]

[1] Collins and Popescu – PRA 2002

[2] Renner and Wolf – EUROCRYPT 2003

Entanglement and Secrecy: Similar Structures

	Quantum	Classical
Resource	Entanglement	Secrecy
Free Operations	LOCC	LOPC
Resource Unit	Entangled bit (ebit): $\vert\Phi^+\rangle = \frac{1}{\sqrt{2}}(\vert 00\rangle^{AB} + \vert 11\rangle^{AB})$	Secret bit (sbit): $\Phi^+ = \frac{1}{2}([0,0]^{XY} + [1,1]^{XY}) \otimes P^Z$
Free Operations + Resource = Universal Operations	Teleportation	One-Time Pad
Single Copy Resource Conversion	Convertibility of Pure States Governed by Majorization	Convertibility of "Pure States" Governed by Majorization[1]
Asymptotic Resource Conversion	Entanglement Formation/ Entanglement Distillation	Secrecy Formation/ Secrecy Distillation[2]
Bound Resource	Yes	???[3]

[1] Collins and Popescu – PRA 2002

[2] Renner and Wolf – EUROCRYPT 2003

[3] Gisin and Wolf – CRYPTO 2000

Entanglement and Secrecy: Similar Structures

	Quantum	Classical
Resource	Entanglement	Secrecy
Free Operations	LOCC	LOPC
Resource Unit	Entangled bit (ebit): $\vert\Phi^+\rangle = \frac{1}{\sqrt{2}}(\vert 00\rangle^{AB} + \vert 11\rangle^{AB})$	Secret bit (sbit): $\Phi^+ = \frac{1}{2}([0,0]^{XY} + [1,1]^{XY}) \otimes P^Z$
Free Operations + Resource = Universal Operations	Teleportation	One-Time Pad
Single Copy Resource Conversion	Convertibility of Pure States Governed by Majorization	Convertibility of "Pure States" Governed by Majorization[1]
Asymptotic Resource Conversion	Entanglement Formation/ Entanglement Distillation	Secrecy Formation/ Secrecy Distillation[2]
Bound Resource	Yes	???[3]
Asymptotic Reversible Resource	- "Flagged" Pure States - ????	- Classical "Flagged Pure States"[4] - ????

[1] Collins and Popescu – PRA 2002

[2] Renner and Wolf – EUROCRYPT 2003

[3] Gisin and Wolf – CRYPTO 2000

[4] C. and Hsieh – PRL 2016

Round Complexity in LOCC and LOPC

How does increased rounds of interactive classical/pubic communication enhance the ability to process quantum/secret information?

- Previous and related work -

Bounded-round communication complexity

- Braverman *et al.* (2015): Quantum Disjointness Problem -
  (QIP 2016)

$$QCC_r(DISJ_n, 1/3) \geq \widetilde{\Omega}(\tfrac{n}{r})$$

- Klauck *et al.* (2007): For any r, there is a problem S_r such that

$$QCC_{r-1}(S_r, \epsilon) \geq \Omega(n^{1/r})$$

$$QCC_r(S_r, \epsilon) = \Theta(\log n)$$

r-round quantum communication

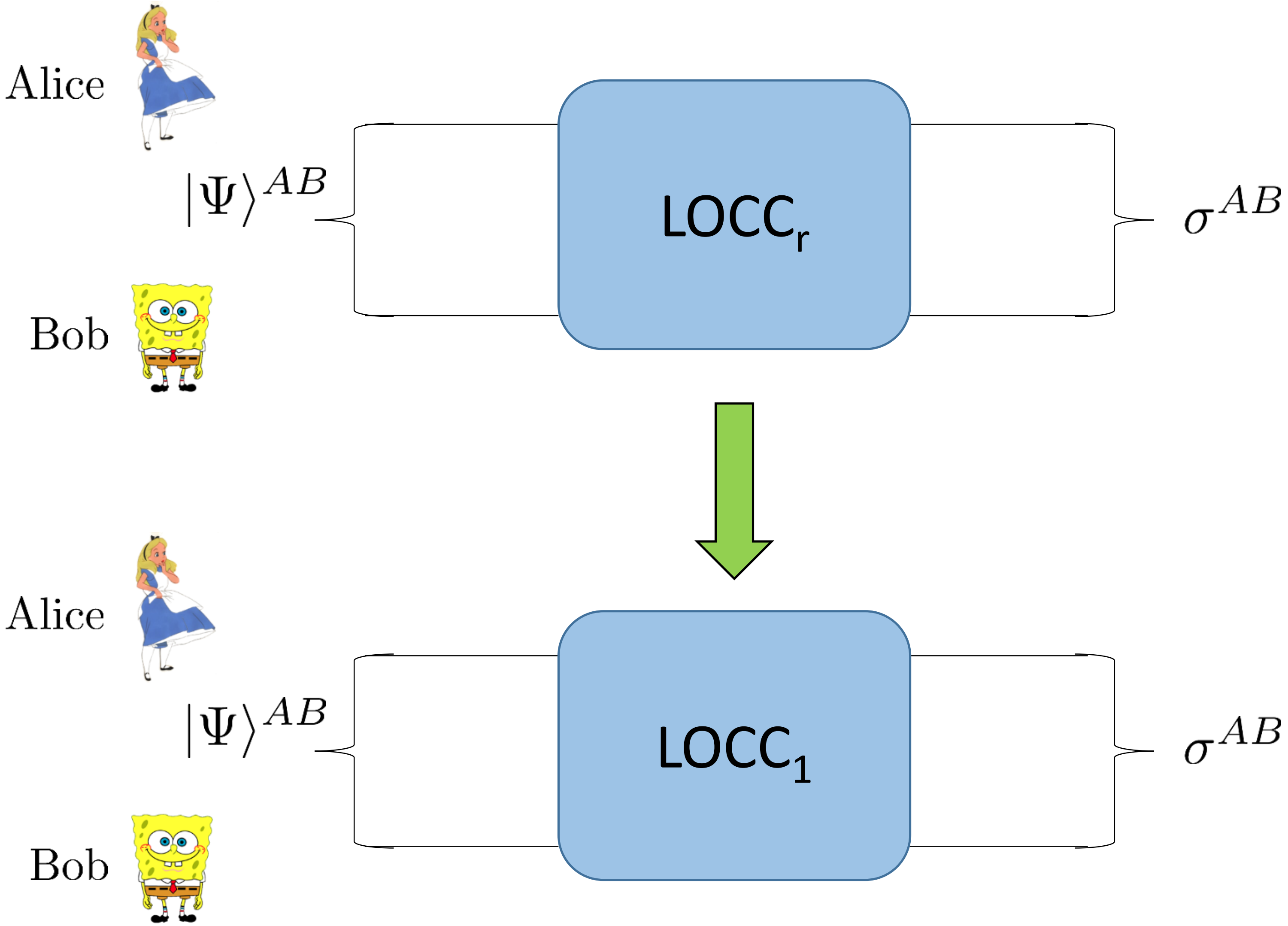
Some Previous Results in LOCC Round Separation

- Asymptotic Entanglement Distillation
  - $\text{LOCC}_2 > \text{LOCC}_1$
    - (Bennett, DiVincenzo, Smolin, Wootters - PRA 1996)
    - (Leditzky, Datta, Smith - QIP 2017)

- State Discrimination
  - $\text{LOCC}_2 > \text{LOCC}_1$
    - (Peres and Wootters - PRL 1991)
    - (Owari and Hayashi - NJP 2008)
    - (Leung and Winter - 2011)
    - (Nathanson - PRA 2013)
    - (C. and Hsieh - JMP 2014)
    - (Croke and Barnett - QIP 2017)
  - $\text{LOCC}_r > \text{LOCC}_{r-1}$ (Xin and Duan - PRA 2008)

- Multipartite LOCC State Transformation
  - $\text{LOCC}_\infty > \text{LOCC}_r$ (C. - PRL 2011)

An Example that Fails to Separate the Rounds



An Example that Fails to Separate the Rounds

Alice

If $|\psi\rangle^{AB} \to \sigma^{AB}$ in r rounds of LOCC, then the transformation can be achieved using a one-round LOCC protocol.[5]

This round compression holds for arbitrary dimensions!

[5] Lo and Popescu – PRA 2001

Bob

Round Separation in State Transformations

- $|\psi\rangle^{AB} \xrightarrow{\text{LOCC}} \sigma^{AB}$ requires only one round of LOCC.

- Does $\rho^{AB} \xrightarrow{\text{LOCC}} \sigma^{AB}$ require only one round of LOCC?

Theorem:

For every r, there exists a state transformation $\rho_r^{AB} \xrightarrow{\text{LOCC}} |\phi\rangle^{AB}$ needing r rounds of LOCC to achieve.

Construction of States

- Step 1: Define a tripartite probability distribution $\mathbf{b}^{(1)}$.

$\mathbf{b}^{(1)} =$

Y \ X (entries: Z)	0	1	2	3
0	0	·	·	1
1	·	0	1	·
2	2	3	·	·
3	·	·	3	2

Consists of
8 equiprobable events

Construction of States

- Step 1: Define a tripartite probability distribution $\mathbf{b}^{(1)}$.

$$\mathbf{b}^{(1)} = \quad Y \; \begin{array}{c|cccc} & \multicolumn{4}{c}{X} \\ & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & \cdot & \cdot & 1 \\ 1 & \cdot & 0 & 1 & \cdot \\ 2 & 2 & 3 & \cdot & \cdot \\ 3 & \cdot & \cdot & 3 & 2 \end{array} \; Z$$

Consists of
8 equiprobable events

This is the event

$X = 2$

$Y = 1$

$Z = 1$

$$\mathbf{b}^{(1)}(2, 1, 1) = 1/8$$

Construction of States

- Step 1: Define a tripartite probability distribution $\mathbf{b}^{(1)}$.

$\mathbf{b}^{(1)} =$ (rows Y, columns X, entries Z)

$Y \backslash X$	0	1	2	3
0	0	·	·	1
1	·	0	1	·
2	2	3	·	·
3	·	·	3	2

Key Property:

- Given Z, Alice and Bob have one bit of perfectly shared randomness.
- If they can determine Z using public communication (without revealing the value of X or Y), then they will have one bit of secret correlations.

Construction of States

- Step 1: Define a tripartite probability distribution $\mathbf{b}^{(1)}$.

$\mathbf{b}^{(1)} =$

Y \ X	0	1	2	3
0	0	·	·	1
1	·	0	1	·
2	2	3	·	·
3	·	·	3	2

Z

One-Way Protocol:

- Bob announces whether Y belongs to $\{0, 1\}$ or $\{2, 3\}$.
- Eve learns nothing new with this annoucement.
- Alice learns exactly the value of Y.

Construction of States

- Step 2: Embed the distribution into a tripartite quantum state and trace out E.

$\mathbf{b}^{(1)} =$ (entries: Z)

Y \ X	0	1	2	3
0	0	·	·	1
1	·	0	1	·
2	2	3	·	·
3	·	·	3	2

$$|\mathbf{b}^{(1)}\rangle^{ABE} = \sum_{xyz} \sqrt{\mathbf{b}^{(1)}(x,y,z)}|x\rangle^A|y\rangle^B|z\rangle^E$$

$$\Updownarrow$$

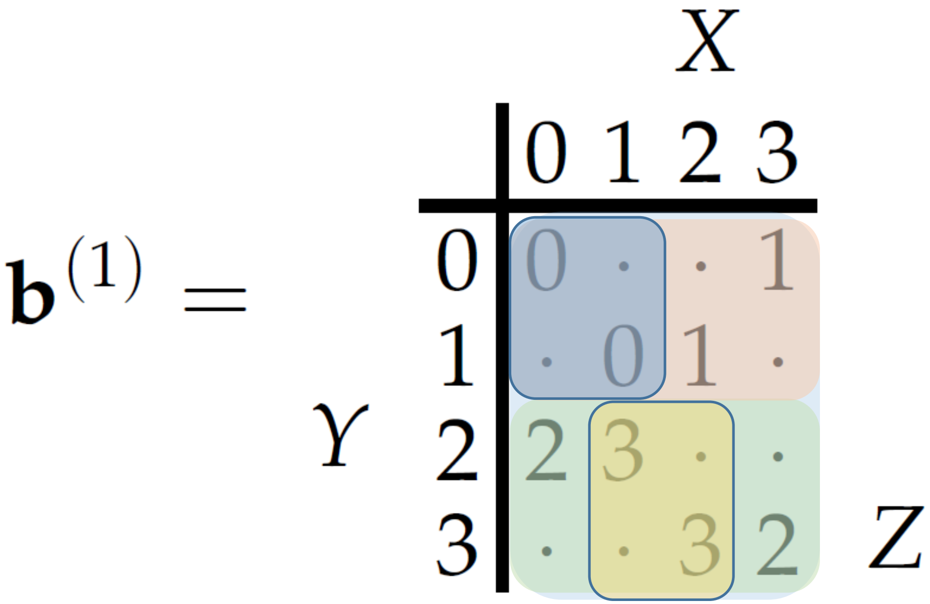
$$\rho^{AB}_{\mathbf{b}^{(1)}} = \frac{1}{\sqrt{4}} \sum_z |\psi_z\rangle\langle\psi_z|^{AB}$$

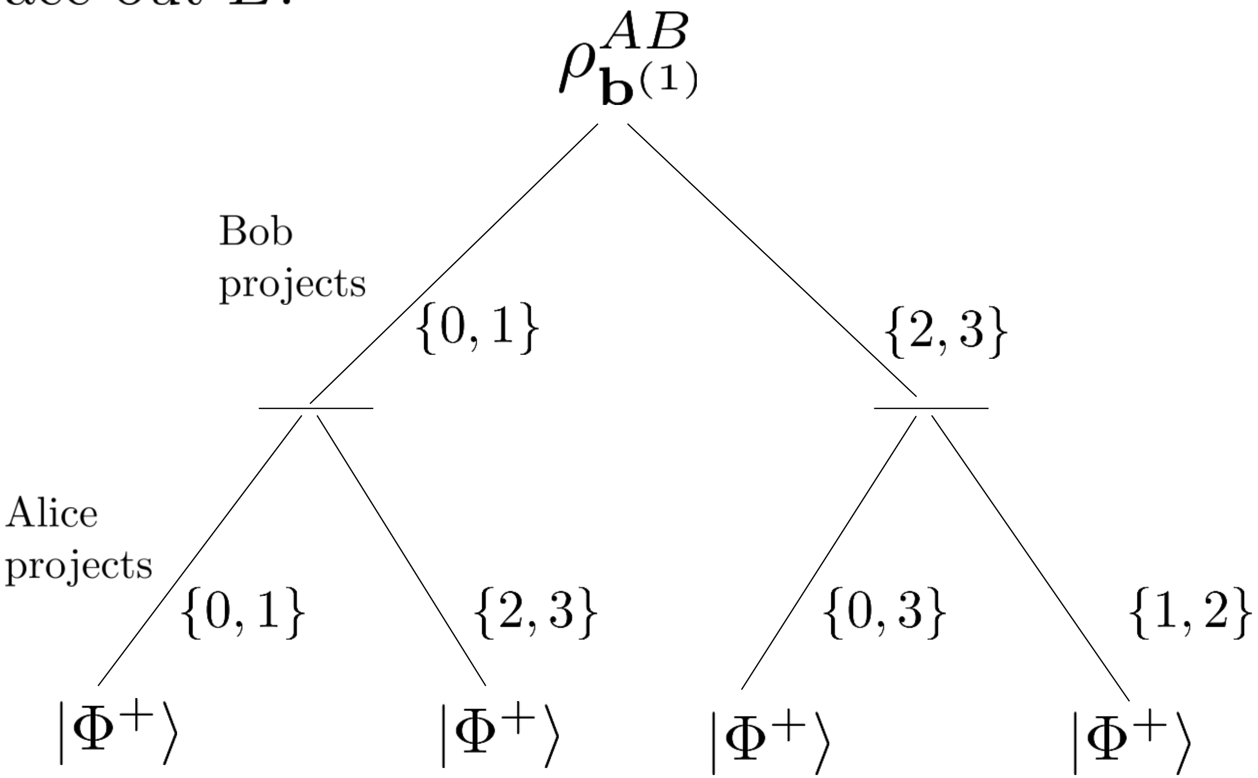
$$|\psi_z\rangle = \sum_{x,y} \sqrt{\mathbf{b}^{(1)}(x,y|z)}|x\rangle|y\rangle$$

$$\overset{\text{LU}}{\approx} |\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Construction of States

- Step 2: Embed the distribution into a tripartite quantum state and trace out E.





$$\rho^{AB}_{\mathbf{b}^{(1)}} \xrightarrow{\text{LOCC}_1} |\Phi^+\rangle$$

Construction of States

- Step 3: Permute and reiterate.

$\mathbf{b}^{(1)} =$

Y \ X	0	1	2	3
0	0	·	·	1
1	·	0	1	·
2	2	3	·	·
3	·	·	3	2

Z

$\mathbf{b}^{(2)} =$

Y \ X	0	1	2	3	4	5	6	7
0	0	·	·	1	4	·	·	5
1	·	0	1	·	·	·	7	6
2	2	3	·	·	6	7	·	·
3	·	·	3	2	·	4	5	·

Z

Columns 0–3: $\mathbf{b}^{(1)}$; columns 4–7: $\overline{\mathbf{b}^{(1)}}$

- Each level is obtained from the last by doubling Eve's alphabet and either Alice or Bob's.
- "Origami" distributions

$\mathbf{b}^{(3)} =$

Y \ X	0	1	2	3	4	5	6	7
0	0	·	·	1	4	·	·	5
1	·	0	1	·	·	·	7	6
2	2	3	·	·	6	7	·	·
3	·	·	3	2	·	4	5	·
4	8	·	·	13	12	·	·	9
5	·	·	9	14	·	8	15	·
6	10	15	·	·	14	11	·	·
7	·	12	11	·	·	·	13	10

Z

Rows 0–3: $\mathbf{b}^{(2)}$; rows 4–7: $\overline{\mathbf{b}^{(2)}}$

$\mathbf{b}^{(4)} =$

Y \ X	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	·	·	1	4	·	·	5	16	·	·	17	20	·	·	21
1	·	0	1	·	·	·	7	6	·	·	25	30	·	24	31	·
2	2	3	·	·	6	7	·	·	18	19	·	·	22	23	·	·
3	·	·	3	2	·	4	5	·	·	28	27	·	·	·	29	26
4	8	·	·	13	12	·	·	9	24	·	·	29	28	·	·	25
5	·	·	9	14	·	8	15	·	·	16	17	·	·	·	23	22
6	10	15	·	·	6	11	·	·	26	31	·	·	30	27	·	·
7	·	12	11	·	·	·	13	10	·	·	19	18	·	20	21	·

Z

Columns 0–7: $\mathbf{b}^{(3)}$; columns 8–15: $\overline{\mathbf{b}^{(3)}}$

Construction of States

- Step 3: Permute and reiterate.

$\mathbf{b}^{(1)} =$ (rows Y, columns X, entries Z)

Y \ X	0	1	2	3
0	0	·	·	1
1	·	0	1	·
2	2	3	·	·
3	·	·	3	2

$\mathbf{b}^{(2)} =$ (rows Y, columns X, entries Z; columns 0–3: $\mathbf{b}^{(1)}$, columns 4–7: $\overline{\mathbf{b}^{(1)}}$)

Y \ X	0	1	2	3	4	5	6	7
0	0	·	·	1	4	·	·	5
1	·	0	1	·	·	·	7	6
2	2	3	·	·	6	7	·	·
3	·	·	3	2	·	4	5	·

$\mathbf{b}^{(3)} =$ (rows Y, columns X, entries Z; rows 0–3: $\mathbf{b}^{(2)}$, rows 4–7: $\overline{\mathbf{b}^{(2)}}$)

Y \ X	0	1	2	3	4	5	6	7
0	0	·	·	1	4	·	·	5
1	·	0	1	·	·	·	7	6
2	2	3	·	·	6	7	·	·
3	·	·	3	2	·	4	5	·
4	8	·	·	13	12	·	·	9
5	·	·	9	14	·	8	15	·
6	10	15	·	·	14	11	·	·
7	·	12	11	·	·	·	13	10

$$\rho_{\mathbf{b}^{(r)}} = \frac{1}{\sqrt{2^{r+1}}} \sum_z |\psi_z\rangle\langle\psi_z|$$

$$|\psi_z\rangle = \sum_{x,y} \sqrt{\mathbf{b}^{(r)}(x,y|z)}|x\rangle|y\rangle$$

$$\rho_{\mathbf{b}^{(r)}} \xrightarrow{\text{LOCC}_r} |\Phi^+\rangle$$

in r rounds by different sequences of local projections

- What about fewer than r rounds?

Lower Bounding the Round Number

- Key observation:

$$\rho_{\mathbf{b}^{(r)}} = \frac{1}{\sqrt{2^{r+1}}} \sum_{z} |\psi_z\rangle\langle\psi_z| \longrightarrow |\Phi+\rangle$$

$$\text{iff} \quad |\psi_z\rangle \longrightarrow |\Phi^+\rangle \qquad \text{for all } z.$$

- Every $|\psi_z\rangle$ has Schmidt rank 2.

- Schmidt rank is an SLOCC monotone.

- Therefore in each round of measurement, $|\psi_z\rangle$ must either be eliminated or its Schmidt rank remains the same.

Lower Bounding the Round Number

- In each round of measurement, $|\psi_z\rangle$ must either be eliminated or its Schmidt rank remains the same.

Example:

$\mathbf{b}^{(3)} =$

Y \ X	0	1	2	3	4	5	6	7
0	0	·	·	1	4	·	·	5
1	·	0	1	·	·	·	7	6
2	2	3	·	·	6	7	·	·
3	·	·	3	2	·	4	5	·
4	8	·	·	13	12	·	·	9
5	·	·	9	14	·	8	15	·
6	10	15	·	·	14	11	·	·
7	·	12	11	·	·	·	13	10

Z

- This rank constraint forces Alice and Bob to perform the correct measurement sequences.
- For example, suppose that Alice wishes to eliminate $|\psi_1\rangle$.

  Then she must eliminate her local subspace spanned by $\{|2\rangle, |3\rangle\}$.

Lower Bounding the Round Number

- In each round of measurement, $|\psi_z\rangle$ must either be eliminated or its Schmidt rank remains the same.

Example:

$\mathbf{b}^{(3)} =$

Y \ X	0	1	2	3	4	5	6	7
0	0	·	·	1	4	·	·	5
1	·	0	1	·	·	·	7	6
2	2	3	·	·	6	7	·	·
3	·	·	3	2	·	4	5	·
4	8	·	·	13	12	·	·	9
5	·	·	9	14	·	8	15	·
6	10	15	·	·	14	11	·	·
7	·	12	11	·	·	·	13	10

Z

- The rank constraint forces Alice and Bob to perform the correct measurement sequences.

- For example, suppose that Alice wishes to eliminate $|\psi_1\rangle$.

  Then she must eliminate her local subspace spanned by $\{|2\rangle, |3\rangle\}$.

  This would decrase the rank of $|\psi_2\rangle$, $|\psi_3\rangle$, $|\psi_9\rangle$, $|\psi_{11}\rangle$, $|\psi_{13}\rangle$, and $|\psi_{14}\rangle$.

Lower Bounding the Round Number

- In each round of measurement, $|\psi_z\rangle$ must either be eliminated or its Schmidt rank remains the same.

Example:

$\mathbf{b}^{(3)} =$

Y \ X	0	1	2	3	4	5	6	7
0	0	·	·	1	4	·	·	5
1	·	0	1	·	·	·	7	6
2	2	3	·	·	6	7	·	·
3	·	·	3	2	·	4	5	·
4	8	·	·	13	12	·	·	9
5	·	·	9	14	·	8	15	·
6	10	15	·	·	14	11	·	·
7	·	12	11	·	·	·	13	10

Z

- The rank constraint forces Alice and Bob to perform the correct measurement sequences.

- For example, suppose that Alice wishes to eliminate $|\psi_1\rangle$.

  Then she must eliminate her local subspace spanned by $\{|2\rangle, |3\rangle\}$.

  This would decrase the rank of $|\psi_2\rangle$, $|\psi_3\rangle$, $|\psi_9\rangle$, $|\psi_{11}\rangle$, $|\psi_{13}\rangle$, and $|\psi_{14}\rangle$.

- So to prevent the decrease in ranks, she would also have to eliminate her local subspace spanned by $\{|0\rangle, |1\rangle, |4\rangle, |5\rangle, |6\rangle, |7\rangle\}$.

Impossible!!

Alice cannot eliminate any states in the mixture if she were to measure. $\Leftarrow$

Lower Bounding the Round Number

- This scenario is avoided only if Bob measures and eliminates either the $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$ subspace or the $\{|4\rangle, |5\rangle, |6\rangle, |7\rangle\}$ subspace.

$\mathbf{b}^{(3)} =$ (X columns, Y rows, Z entries)

Y \ X	0	1	2	3	4	5	6	7
0	0	·	·	1	4	·	·	5
1	·	0	1	·	·	·	7	6
2	2	3	·	·	6	7	·	·
3	·	·	3	2	·	4	5	·
4	8	·	·	13	12	·	·	9
5	·	·	9	14	·	8	15	·
6	10	15	·	·	14	11	·	·
7	·	12	11	·	·	·	13	10

or

Y \ X	0	1	2	3	4	5	6	7
0	0	·	·	1	4	·	·	5
1	·	0	1	·	·	·	7	6
2	2	3	·	·	6	7	·	·
3	·	·	3	2	·	4	5	·
4	8	·	·	13	12	·	·	9
5	·	·	9	14	·	8	15	·
6	10	15	·	·	14	11	·	·
7	·	12	11	·	·	·	13	10

- In either case, what remains is a state SLOCC equivalent to $\rho_{\mathbf{b}^{(2)}}$.

Lower Bounding the Round Number

- At the end of $r-1$ rounds:

$$\rho_{\mathbf{b}^{(r)}} \longrightarrow \overset{\text{SLOCC}}{\approx} \rho_{\mathbf{b}^{(1)}} \qquad \mathbf{b}^{(1)} =$$

Y \ X	0	1	2	3
0	0	·	·	1
1	·	0	1	·
2	2	3	·	·
3	·	·	3	2

Z

Impossible to convert to a pure entangled state without additional communication

$$\rho_{\mathbf{b}^{(1)}} \not\longrightarrow |\Phi^+\rangle$$

- Thus, $\rho_{\mathbf{b}^{(r)}} \xrightarrow{\text{LOCC}} |\Phi^+\rangle$ is possible only under r rounds of LOCC.

The Analogous Classical Problem

- In the classical resource theory of secrecy, Alice and Bob want to obtain secret key

$$\Phi^+ = \frac{1}{2}([0,0]^{XY} + [1,1]^{XY}) \otimes P^Z.$$

- How many rounds of LOPC does it take Alice and Bob to transform $\mathbf{b}^{(r)} \to \Phi^+$?

- In the entanglement case, the proof relies crucially on the Schmidt rank.

- What is the classical analog of Schmidt rank?

The Secrecy Rank

• Consider the Schmidt decomposition of a bipartite pure state $|\varphi\rangle^{AB}$:

$$|\varphi\rangle^{AB} = \sum_{w=1}^{Srk(|\varphi\rangle)} \sqrt{p_w}|\alpha_w\rangle^A|\beta_w\rangle^B.$$

$Srk(|\varphi\rangle)$ is the minimum number of product states whose span contains $|\varphi\rangle$.

• When Alice and Bob measure in their Schmidt bases, they generate a distribution:

$$P^{XY}(x,y) = \sum_{\omega} p_\omega \delta_{x\omega}\delta_{y\omega}$$

There exists an auxiliary random variable W such that X and Y are independent given W:

$$X - W - Y$$

Definition (Secrecy Rank):

For uncorrelated Eve,

$$Srk(P^{XY}) = \min_{X-W-Y} |W|$$

The range of W

The Secrecy Rank

• What about for correlated Eve?

• Recall the definition of Schmidt rank for bipartite mixed states[6]:

$$Srk[\rho^{AB}] = \min_{\substack{\{p_i, |\varphi_i\rangle\} \\ \rho^{AB} = \sum_i p_i |\varphi_i\rangle\langle\varphi_i|}} \max_{|\varphi_i\rangle} Srk(|\varphi_i\rangle)$$

• For tripartite distributions, we can think of P^{XYZ} as defining an ensemble of bipartite distributions $\{P^{XY|Z=z}, P^Z(z)\}$.

Definition (Secrecy Rank):

$$Srk(P^{XYZ}) = \max_z Srk(P^{XY|Z=z})$$

[6] Terhal and Horodecki – PRA 2000

The Secrecy Rank

- What about for correlated Eve?

- Recall the definition of Schmidt rank for bipartite mixed states[6]:

$$Srk[\rho^{AB}] = \min_{\substack{\{p_i, |\varphi_i\rangle\} \\ \rho^{AB} = \sum_i p_i |\varphi_i\rangle\langle\varphi_i|}} \max_{|\varphi_i\rangle} Srk(|\varphi_i\rangle)$$

- For tripartite distributions, we can think of P^{XYZ} as defining an ensemble of bipartite distributions $\{P^{XY|Z=z}, P^Z(z)\}$.

Definition (Secrecy Rank):

$$Srk(P^{XYZ}) = \max_z Srk(P^{XY|Z=z}) = \min_{X-WZ-Y} \max_z |W^{|Z=z}|$$

[6] Terhal and Horodecki – PRA 2000

The Secrecy Rank

<u>Quantum</u>		<u>Classical</u>
$Srk(\rho^{AB})$	$\Leftrightarrow$	$Srk(P^{XYZ})$

Theorem:

The Secrecy Rank is an SLOPC monotone.

- For any sequence of messages in an LOPC protocol, $Srk(P^{XYZ})$ is monotonically decreasing.
- The lower bound in rounds for $\rho_{\mathbf{b}^{(r)}} \xrightarrow{\text{LOCC}} |\Phi^+\rangle$ translates directly into the classical problem.

Theorem:

$$\mathbf{b}^{(r)} \xrightarrow{\text{LOPC}} \frac{1}{2}([0,0]^{XY} + [1,1]^{XY}) \otimes P^Z$$

only with r rounds of LOPC.

Conclusions/Remarks

- For every r, the state transformations

$$\rho_{\mathbf{b}^{(r)}} \xrightarrow{\text{LOCC}} |\Phi^+\rangle$$

$$\mathbf{b}^{(r)} \xrightarrow{\text{LOPC}} \Phi^+$$

need r rounds of LOCC/LOPC to achieve.

Slight Strengthening:

- For every r, there exists an $\epsilon > 0$ such that

$$\left.\begin{aligned} \rho_{\mathbf{b}^{(r)}} &\xrightarrow{\text{LOCC}} \sigma^{AB} \overset{\epsilon}{\approx} |\Phi^+\rangle \\ \mathbf{b}^{(r)} &\xrightarrow{\text{LOPC}} P^{XYZ} \overset{\epsilon}{\approx} \Phi^+ \end{aligned}\right\}$$

← Follows from compactness of finite-round LOCC/LOPC

need r rounds of LOCC/LOPC to achieve.

Conclusions/Remarks

- Since the proof is based on Schmidt/Secrecy ranks, we can generalize:

$$|\Phi_\lambda^+\rangle = \sqrt{\lambda}|00\rangle^{AB} + \sqrt{1-\lambda}|11\rangle^{AB} \qquad \Phi_\lambda^+ = (\lambda[0,0]^{XY} + (1-\lambda)[1,1]^{XY}) \otimes P^Z$$

- For every r and any $0 < \lambda \leq 1/2$, the state transformations

$$\rho_{\mathbf{b}^{(r)}} \xrightarrow{\text{LOCC}} |\Phi_\lambda^+\rangle$$

$$\mathbf{b}^{(r)} \xrightarrow{\text{LOPC}} \Phi_\lambda^+$$

need r rounds of LOCC/LOPC to achieve.

- $$\lim_{\lambda\to 0} \min\{k : \rho_{\mathbf{b}^{(r)}} \xrightarrow{\text{LOCC}_k} |\Phi_\lambda^+\rangle\} \neq \min\{k : \rho_{\mathbf{b}^{(r)}} \xrightarrow{\text{LOCC}_k} |\Phi_0^+\rangle\}$$

Open Questions/Future Work

- The dimension of states scales poorly!

$$\rho_{\mathbf{b}^{(r)}} = \frac{1}{\sqrt{2^{r+1}}} \sum_z |\psi_z\rangle\langle\psi_z|$$

Can examples be found in bipartite systems with bounded dimension?

- For every r, there exists an $\epsilon > 0$ such that

$$\rho_{\mathbf{b}^{(r)}} \xrightarrow{\text{LOCC}} \sigma^{AB} \overset{\epsilon}{\approx} |\Phi^+\rangle$$

$$\mathbf{b}^{(r)} \xrightarrow{\text{LOPC}} P^{XYZ} \overset{\epsilon}{\approx} \Phi^+$$

need r rounds of LOCC/LOPC to achieve.

Can lower bounds on ϵ be computed?

Open Questions/Future Work

- What about asymptotic transformations?

$$\rho_{\mathbf{b}^{(r)}}^{\otimes n} \xrightarrow{\text{LOCC}} \sigma \overset{\epsilon}{\approx} |\Phi^+\rangle^{\otimes m}$$

$$(\mathbf{b}^{(r)})^{\otimes n} \xrightarrow{\text{LOPC}} P^{XYZ} \overset{\epsilon}{\approx} (\Phi^+)^{\otimes m}$$

What is the r-round asymptotic distillation rate of $\rho_{\mathbf{b}^{(r)}}$ and $\mathbf{b}^{(r)}$?

Can one bit of entanglement/key be asymptotically distilled in fewer than r rounds?

- Note:

$$E_C(\rho_{\mathbf{b}^{(r)}}) = E_D(\rho_{\mathbf{b}^{(r)}})$$

Entanglement cost — Distillable entanglement

Asymptotic entanglement reversibility may require r-round protocols.

$\Rightarrow$ The states with reversible entanglement can have very complex structure.

Thank You!!