Semidefinite programming hierarchies for quantum adversaries

Mario Berta (IQIM Caltech), Omar Fawzi (ENS Lyon), Volkher Scholz (Ghent University)

(arXiv:1506.08810 - Quantum Bilinear Optimisation)

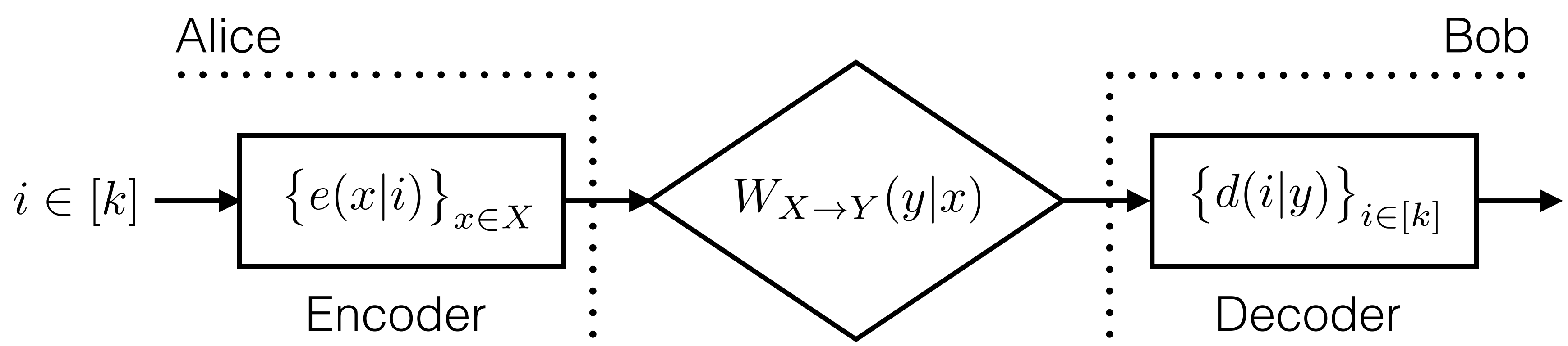
Overview

- Theoretical talk, plus start with non-cryptographic problem
- Classical noisy channel coding versus entanglement-assisted *channel coding* (**quantum assistance**)
- Semidefinite programming (sdp) hierarchies for understanding (bounding) the difference
- Cryptography: randomness extractors versus *quantum-proof randomness extractors* (**quantum adversary**)
- Conclusion / Outlook

Overview

- Theoretical talk, plus start with non-cryptographic problem
- Classical noisy channel coding versus entanglement-assisted *channel coding* (**quantum assistance**)
- Semidefinite programming (sdp) hierarchies for understanding (bounding) the difference
- Cryptography: randomness extractors versus *quantum-proof randomness extractors* (**quantum adversary**)
- Conclusion / Outlook

Classical noisy channel coding (I)



- Given noisy channel $W_{X\to Y}$ mapping X to Y with transition probability:

$$W_{X\to Y}(y|x)\ \forall (x,y) \in X \times Y$$

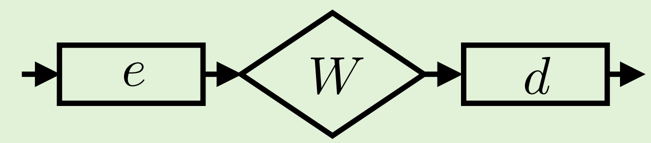
- The goal is to send k different messages using W while minimising the error probability for decoding:

"bilinear optimisation"

$$\begin{aligned} p_{\text{succ}}(W,k) := \underset{(e,d)}{\text{maximize}} \quad & \frac{1}{k} \sum_{x,y,i} W_{X\to Y}(y|x) e(x|i) d(i|y) \\ \text{subject to} \quad & \sum_x e(x|i) = 1 \quad \forall i \in [k]\,, \quad \sum_i d(i|y) = 1 \quad \forall y \in Y \\ & 0 \le e(x|i) \le 1 \quad \forall (x,i) \in X \times [k]\,, \quad 0 \le d(i|y) \le 1 \quad \forall (i,y) \in [k] \times Y\,. \end{aligned}$$

Classical noisy channel coding (II)

$$p_{\text{succ}}(W,k) := \underset{(e,d)}{\text{maximize}} \quad \frac{1}{k}\sum_{x,y,i} W_{X\to Y}(y|x)e(x|i)d(i|y)$$



$$\text{subject to} \quad \sum_x e(x|i) = 1 \quad \forall i \in [k]\,, \quad \sum_i d(i|y) = 1 \quad \forall y \in Y$$

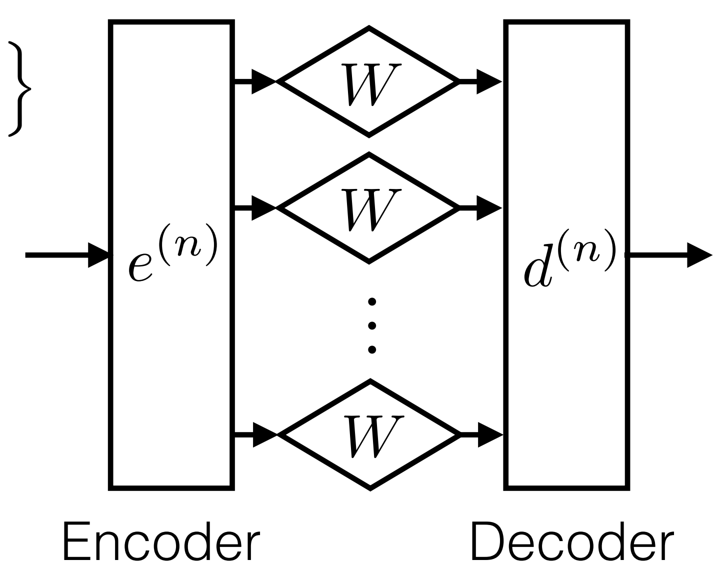
$$0 \le e(x|i) \le 1 \quad \forall (x,i) \in X \times [k]\,, \quad 0 \le d(i|y) \le 1 \quad \forall (i,y) \in [k] \times Y\,.$$

compared to

- Shannon’s asymptotic independent and identical distributed (iid) channel capacity:

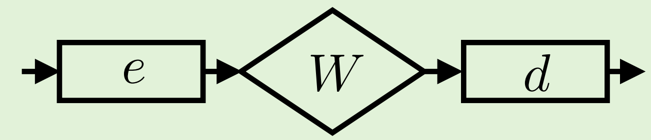
Definition: $C(W) := \sup\left\{R \,\middle|\, \forall\delta > 0 : \lim_{n\to\infty} p_{\text{succ}}\left(W^{\times n}, [R(1-\delta)]^n\right) = 1\right\}$

Answer: $C(W) = \max_{P_X} I(X:Y)$ mutual information



Classical noisy channel coding (II)

$$p_{\mathrm{succ}}(W,k) := \underset{(e,d)}{\text{maximize}} \quad \frac{1}{k}\sum_{x,y,i} W_{X\to Y}(y|x)e(x|i)d(i|y)$$



$$\text{subject to} \quad \sum_x e(x|i) = 1 \quad \forall i \in [k]\,, \quad \sum_i d(i|y) = 1 \quad \forall y \in Y$$

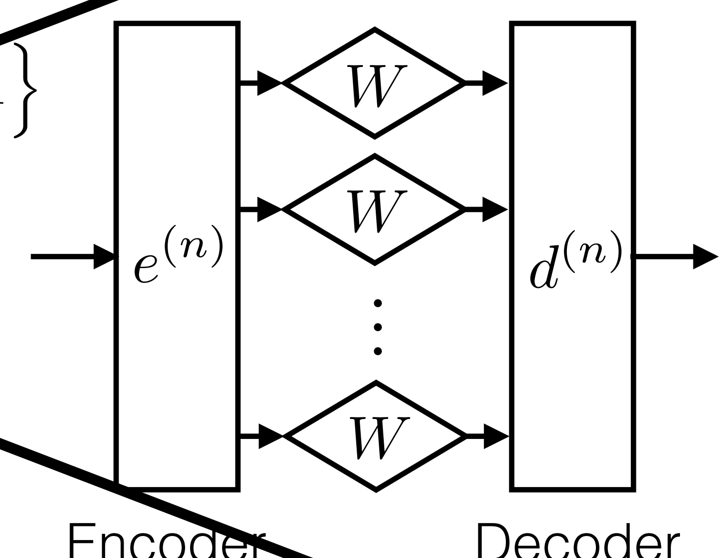
$$0 \le e(x|i) \le 1 \quad \forall (x,i) \in X \times [k]\,, \quad 0 \le d(i|y) \le 1 \quad \forall (i,y) \in [k] \times Y\,.$$

compared to

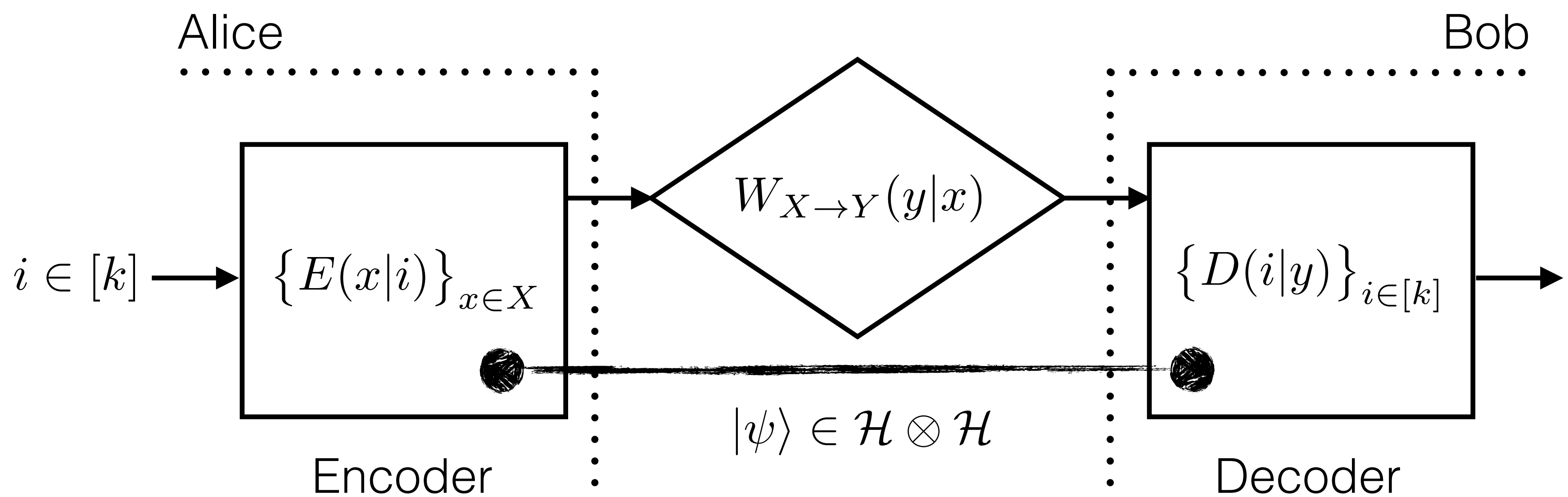
- Shannon's asymptotic independent and identical distributed (iid) channel capacity:

Definition: $C(W) := \sup\left\{R \,\middle|\, \forall \delta > 0 : \lim_{n\to\infty} p_{\mathrm{succ}}\left(W^{\times n}, [R(1-\delta)]^n\right) = 1\right\}$

Answer: $C(W) = \max_{P_X} I(X:Y)$ mutual information



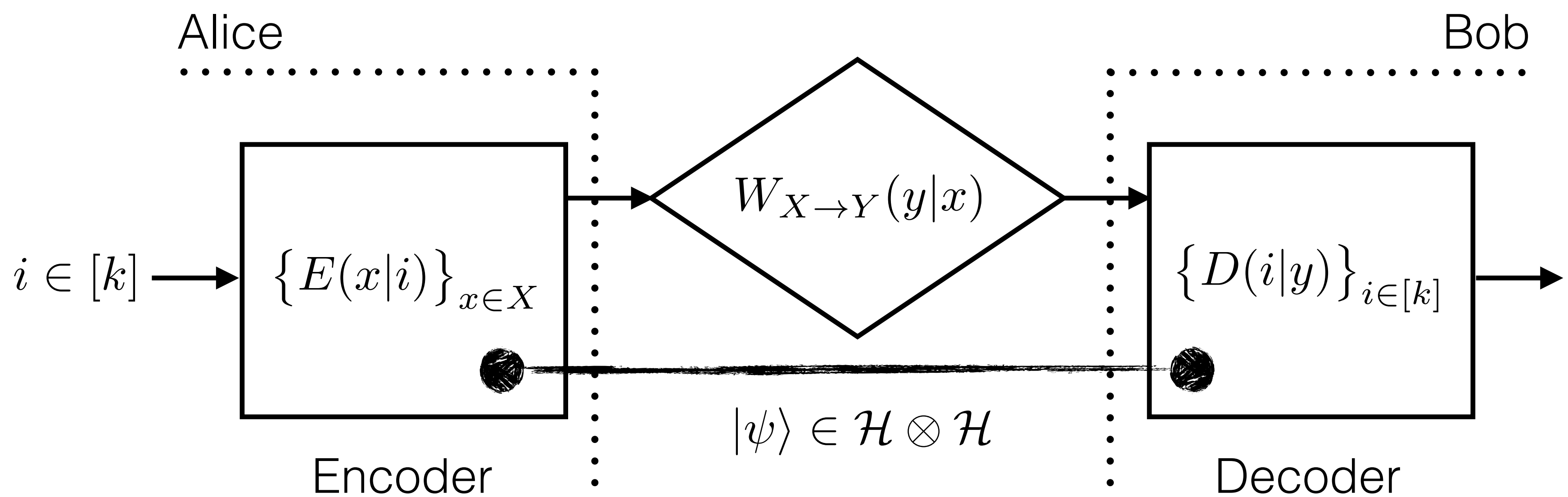
Entanglement-assisted channel coding (I)



"quantum bilinear optimisation"

$$
\begin{aligned}
p^*_{\mathrm{succ}}(W,k) := \underset{(\mathcal{H},\psi,E,D)}{\text{maximize}} \quad & \frac{1}{k}\sum_{x,y,i} W_{X\to Y}(y|x)\langle\psi|E(x|i)\otimes D(i|y)|\psi\rangle \\
\text{subject to} \quad & \sum_x E(x|i) = 1_{\mathcal{H}} \quad \forall i\in[k]\,, \quad \sum_i D(i|y) = 1_{\mathcal{H}} \quad \forall y\in Y \\
& 0 \le E(x|i) \le 1_{\mathcal{H}}\ \forall (x,i)\in X\times[k]\,, \quad 0\le D(i|y)\le 1_{\mathcal{H}}\ \forall (i,y)\in[k]\times Y\,.
\end{aligned}
$$

Entanglement-assisted channel coding (I)



"quantum bilinear optimisation"

$$p^*_{\mathrm{succ}}(W,k) := \underset{(\mathcal{H},\psi,E,D)}{\mathrm{maximize}} \ \frac{1}{k}\sum_{x,y,i} W_{X\to Y}(y|x)\langle\psi|E(x|i)\otimes D(i|y)|\psi\rangle$$

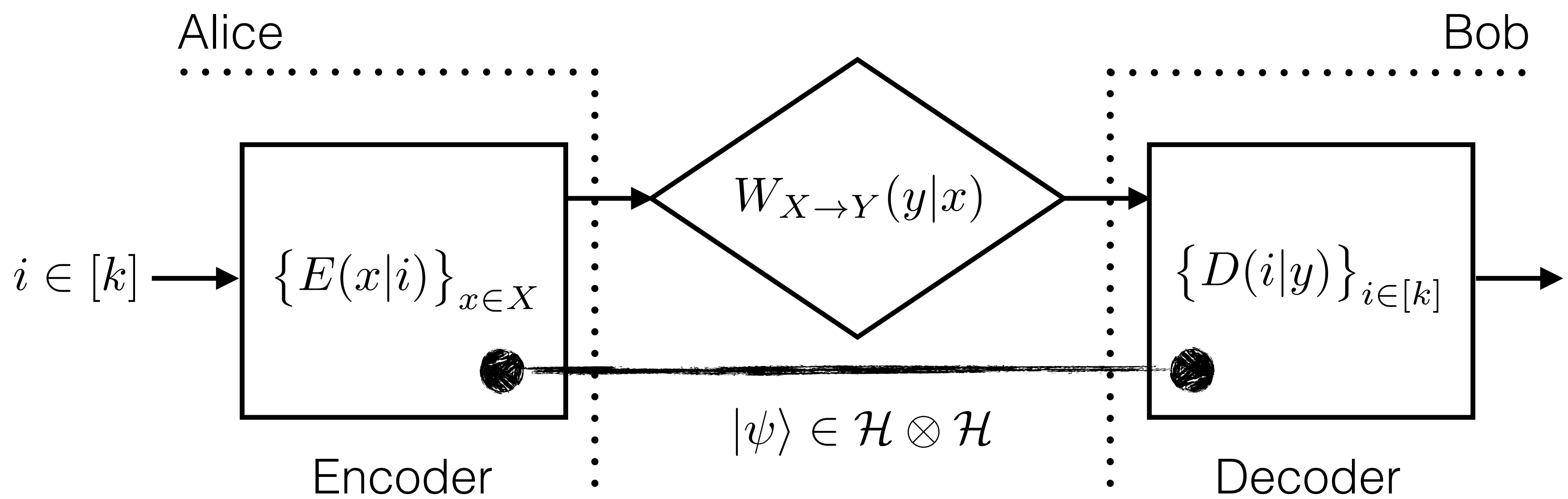
$$\text{subject to} \ \sum_x E(x|i) = 1_{\mathcal{H}} \quad \forall i \in [k]\,, \quad \sum_i D(i|y) = 1_{\mathcal{H}} \quad \forall y \in Y$$

$$0 \le E(x|i) \le 1_{\mathcal{H}} \ \forall (x,i) \in X \times [k]\,, \quad 0 \le D(i|y) \le 1_{\mathcal{H}} \ \forall (i,y) \in [k]\times Y\,.$$

- **Scalar** (commutative) versus **matrix** (non-commutative) variables:

$$p_{\mathrm{succ}}(W,k) := \underset{(e,d)}{\mathrm{maximize}} \ \frac{1}{k}\sum_{x,y,i} W_{X\to Y}(y|x)\, e(x|i)d(i|y)$$

Entanglement-assisted channel coding (I)



"quantum bilinear optimisation"

$$p^*_{\mathrm{succ}}(W,k) := \underset{(\mathcal{H},\psi,E,D)}{\mathrm{maximize}} \ \frac{1}{k}\sum_{x,y,i} W_{X\to Y}(y|x)\langle\psi|E(x|i)\otimes D(i|y)|\psi\rangle$$

$$\text{subject to} \ \sum_x E(x|i) = 1_{\mathcal{H}} \quad \forall i \in [k]\,, \quad \sum_i D(i|y) = 1_{\mathcal{H}} \quad \forall y \in Y$$

$$0 \leq E(x|i) \leq 1_{\mathcal{H}} \ \forall (x,i) \in X\times[k]\,, \quad 0 \leq D(i|y) \leq 1_{\mathcal{H}} \ \forall (i,y) \in [k]\times Y\,.$$

- **Scalar** (commutative) versus **matrix** (non-commutative) variables:

$$p_{\mathrm{succ}}(W,k) := \underset{(e,d)}{\mathrm{maximize}} \ \frac{1}{k}\sum_{x,y,i} W_{X\to Y}(y|x)\, e(x|i)d(i|y)$$

- Unknown if $p^*_{\mathrm{succ}}(W,k)$ is computable!

Entanglement-assisted channel coding (II)

- Understand the possible separation: $p_{\mathrm{succ}}(W,k) \quad \text{versus} \quad p^*_{\mathrm{succ}}(W,k)$

Entanglement-assisted channel coding (II)

- Understand the possible separation: $p_{\mathrm{succ}}(W,k) \quad \mathrm{versus} \quad p^*_{\mathrm{succ}}(W,k)$

- For the asymptotic iid capacity entanglement (quantum) assistance does not help:
  $C(W) = C^*(W)$ [Bennett et al., PRL (1999)]

Entanglement-assisted channel coding (II)

- Understand the possible separation: $p_{\mathrm{succ}}(W,k) \quad \text{versus} \quad p^*_{\mathrm{succ}}(W,k)$

- ~~For the asymptotic iid capacity entanglement (quantum) assistance does not help:~~

  ~~$C(W) = C^*(W)$ [Bennett et al., PRL (1999)]~~

Entanglement-assisted channel coding (II)

- Understand the possible separation: $p_{\mathrm{succ}}(W,k) \quad \text{versus} \quad p^*_{\mathrm{succ}}(W,k)$

- ~~For the asymptotic iid capacity entanglement (quantum) assistance does not help:~~
  ~~$C(W) = C^*(W)$ [Bennett et al., PRL (1999)]~~

- In general, there is a **separation**:

$$Z = \begin{pmatrix} 1/3 & 1/3 & 0 & 0 \\ 0 & 0 & 1/3 & 1/3 \\ 1/3 & 0 & 1/3 & 0 \\ 0 & 1/3 & 0 & 1/3 \\ 1/3 & 0 & 0 & 1/3 \\ 0 & 1/3 & 1/3 & 0 \end{pmatrix}$$

$$p_{\mathrm{succ}}(Z,2) = \frac{5}{6} \approx 0.833 \quad \text{vs.} \quad p^*_{\mathrm{succ}}(Z,2) \geq \frac{2+2^{-1/2}}{3} \approx 0.902$$

[Prevedel et al., PRL (2011)]

Entanglement-assisted channel coding (II)

- Understand the possible separation: $p_{\mathrm{succ}}(W,k) \quad \text{versus} \quad p^*_{\mathrm{succ}}(W,k)$

- ~~For the asymptotic iid capacity entanglement (quantum) assistance does not help:~~
  ~~$C(W) = C^*(W)$ [Bennett et al., PRL (1999)]~~

- In general, there is a **separation**:

$$Z = \begin{pmatrix} 1/3 & 1/3 & 0 & 0 \\ 0 & 0 & 1/3 & 1/3 \\ 1/3 & 0 & 1/3 & 0 \\ 0 & 1/3 & 0 & 1/3 \\ 1/3 & 0 & 0 & 1/3 \\ 0 & 1/3 & 1/3 & 0 \end{pmatrix}$$

$$p_{\mathrm{succ}}(Z,2) = \frac{5}{6} \approx 0.833 \quad \text{vs.} \quad p^*_{\mathrm{succ}}(Z,2) \geq \frac{2+2^{-1/2}}{3} \approx 0.902$$

[Prevedel et al., PRL (2011)]

—> this is also optimal with two-dimensional assistance

[Hemenway et al., PRA (2013)]
[Williams and Bourdon, arXiv:1109.1029]

Entanglement-assisted channel coding (II)

- Understand the possible separation: $p_{\text{succ}}(W,k) \quad \text{versus} \quad p^*_{\text{succ}}(W,k)$

- ~~For the asymptotic iid capacity entanglement (quantum) assistance does not help:~~
  ~~$C(W) = C^*(W)$ [Bennett et al., PRL (1999)]~~

- In general, there is a **separation**:

$$Z = \begin{pmatrix} 1/3 & 1/3 & 0 & 0 \\ 0 & 0 & 1/3 & 1/3 \\ 1/3 & 0 & 1/3 & 0 \\ 0 & 1/3 & 0 & 1/3 \\ 1/3 & 0 & 0 & 1/3 \\ 0 & 1/3 & 1/3 & 0 \end{pmatrix}$$

$$p_{\text{succ}}(Z,2) = \frac{5}{6} \approx 0.833 \quad \text{vs.} \quad p^*_{\text{succ}}(Z,2) \geq \frac{2+2^{-1/2}}{3} \approx 0.902$$

[Prevedel et al., PRL (2011)]

—> this is also optimal with two-dimensional assistance

[Hemenway et al., PRA (2013)]
[Williams and Bourdon, arXiv:1109.1029]

- However: $[0.902, 1] \ni p^*_{\text{succ}}(Z,2) = ?$

Entanglement-assisted channel coding (II)

- Understand the possible separation: $p_{\text{succ}}(W,k) \quad \text{versus} \quad p^*_{\text{succ}}(W,k)$

- ~~For the asymptotic iid capacity entanglement (quantum) assistance does not help:~~
  ~~$C(W) = C^*(W)$ [Bennett et al., PRL (1999)]~~

- In general, there is a **separation**:

$$Z = \begin{pmatrix} 1/3 & 1/3 & 0 & 0 \\ 0 & 0 & 1/3 & 1/3 \\ 1/3 & 0 & 1/3 & 0 \\ 0 & 1/3 & 0 & 1/3 \\ 1/3 & 0 & 0 & 1/3 \\ 0 & 1/3 & 1/3 & 0 \end{pmatrix}$$

$$p_{\text{succ}}(Z,2) = \frac{5}{6} \approx 0.833 \quad \text{vs.} \quad p^*_{\text{succ}}(Z,2) \geq \frac{2+2^{-1/2}}{3} \approx 0.902$$

[Prevedel et al., PRL (2011)]

—> this is also optimal with two-dimensional assistance

[Hemenway et al., PRA (2013)]
[Williams and Bourdon, arXiv:1109.1029]

- However: $[0.902, 1] \ni p^*_{\text{succ}}(Z,2) = ?$

"linear optimisation with semidefinite constraints"

- We give a **converging hierarchy of semidefinite programming (sdp) relaxations**:

$$p_{\text{succ}}(W,k) \leq p^*_{\text{succ}}(W,k) = \text{sdp}_\infty(W,k) \leq \ldots \leq \text{sdp}_1(W,k)$$ <— *efficiently computable!*

Overview

- Theoretical talk, plus start with non-cryptographic problem
- Classical noisy channel coding versus entanglement-assisted *channel coding* (**quantum assistance**)
- Semidefinite programming (sdp) hierarchies for understanding (bounding) the difference
- Cryptography: randomness extractors versus *quantum-proof randomness extractors* (**quantum adversary**)
- Conclusion / Outlook

First level semidefinite programming relaxation (I)

- Quantum bilinear program:

$$
\begin{aligned}
p^*_{\text{succ}}(W,k) := \underset{(\mathcal{H},\psi,E,D)}{\text{maximize}} \quad & \frac{1}{k}\sum_{x,y,i} W_{X\to Y}(y|x)\langle\psi|E(x|i)\otimes D(i|y)|\psi\rangle \\
\text{subject to} \quad & \sum_x E(x|i) = 1_{\mathcal{H}} \quad \forall i \in [k]\,, \quad \sum_i D(i|y) = 1_{\mathcal{H}} \quad \forall y \in Y \\
& 0 \le E(x|i) \le 1_{\mathcal{H}}\ \forall (x,i) \in X \times [k]\,, \quad 0 \le D(i|y) \le 1_{\mathcal{H}}\ \forall (i,y) \in [k] \times Y\,.
\end{aligned}
$$

First level semidefinite programming relaxation (I)

- Quantum bilinear program:

$$p^*_{\text{succ}}(W,k) := \underset{(\mathcal{H},\psi,E,D)}{\text{maximize}} \quad \frac{1}{k}\sum_{x,y,i} W_{X\to Y}(y|x)\langle\psi|E(x|i)\otimes D(i|y)|\psi\rangle \leq \langle\psi|E(x|i)\cdot D(y|j)|\psi\rangle$$

$$\text{with}\big[E(x,i),D(y,j)\big] = 0$$

$$\text{subject to} \quad \sum_x E(x|i) = 1_{\mathcal{H}} \quad \forall i\in[k]\,, \quad \sum_i D(i|y) = 1_{\mathcal{H}} \quad \forall y\in Y$$

$$0\leq E(x|i)\leq 1_{\mathcal{H}}\ \forall(x,i)\in X\times[k]\,, \quad 0\leq D(i|y)\leq 1_{\mathcal{H}}\ \forall(i,y)\in[k]\times Y\,.$$

First level semidefinite programming relaxation (I)

- Quantum bilinear program:

idea: relaxation of this bilinear form

$$p^*_{\mathrm{succ}}(W,k) := \underset{(\mathcal{H},\psi,E,D)}{\text{maximize}} \quad \frac{1}{k}\sum_{x,y,i} W_{X\to Y}(y|x)\langle\psi|E(x|i)\otimes D(i|y)|\psi\rangle \leq \langle\psi|E(x|i)\cdot D(y|j)|\psi\rangle$$

$$\text{with}\left[E(x,i),D(y,j)\right] = 0$$

$$\text{subject to} \quad \sum_x E(x|i) = 1_{\mathcal{H}} \quad \forall i\in[k]\,, \quad \sum_i D(i|y) = 1_{\mathcal{H}} \quad \forall y \in Y$$

$$0 \leq E(x|i) \leq 1_{\mathcal{H}}\ \forall (x,i)\in X\times[k]\,, \quad 0\leq D(i|y)\leq 1_{\mathcal{H}}\ \forall (i,y)\in[k]\times Y\,.$$

*motivated by: "**NPA hierarchy**" (Bell inequalities)*

[Lasserre, SIAM (2001)], [Parrilo, Math. Program. (2003)], [Navascues et al., PRL (2007)], [Doherty et al., IEEE CCC (2008)], [Navascues et al., NJP (2008)], [Pironio et al., SIAM (2010)]

First level semidefinite programming relaxation (I)

- Quantum bilinear program:

idea: relaxation of this bilinear form

$$p^*_{\text{succ}}(W,k) := \underset{(\mathcal{H},\psi,E,D)}{\text{maximize}} \quad \frac{1}{k}\sum_{x,y,i} W_{X\to Y}(y|x)\langle\psi|E(x|i)\otimes D(i|y)|\psi\rangle \leq \langle\psi|E(x|i)\cdot D(y|j)|\psi\rangle$$

with $[E(x,i),D(y,j)] = 0$

$$\text{subject to} \quad \sum_x E(x|i) = 1_{\mathcal{H}} \quad \forall i\in[k]\,, \quad \sum_i D(i|y) = 1_{\mathcal{H}} \quad \forall y \in Y$$

$$0 \leq E(x|i) \leq 1_{\mathcal{H}}\ \forall (x,i)\in X\times[k]\,, \quad 0\leq D(i|y)\leq 1_{\mathcal{H}}\ \forall (i,y)\in[k]\times Y\,.$$

- First step: see as the part of the upper-right block of the Gram matrix

$$\Omega = \sum_{u,v}\langle\psi|X_u X_v|\psi\rangle|u\rangle\langle v| \quad \text{with} \quad X_u = \begin{cases} E(x|i) & u=(i,x) \\ D(j|y) & u=(j,y)\end{cases}$$

for i=j

$$\Omega = \left(\begin{array}{c:c} \langle\psi|E(x|i)\cdot E(x'|i')|\psi\rangle & \langle\psi|E(x|i)\cdot D(y|j)|\psi\rangle \\ \hdashline \langle\psi|E(x'|i')\cdot D(y'|j')|\psi\rangle & \langle\psi|D(y|j)\cdot D(y'|j')]|\psi\rangle \end{array}\right)$$

---

*motivated by: “**NPA hierarchy**” (Bell inequalities)*

[Lasserre, SIAM (2001)], [Parrilo, Math. Program. (2003)], [Navascues et al., PRL (2007)], [Doherty et al., IEEE CCC (2008)], [Navascues et al., NJP (2008)], [Pironio et al., SIAM (2010)]

First level semidefinite programming relaxation (I)

- Quantum bilinear program:

idea: relaxation of this bilinear form

$$p^*_{\mathrm{succ}}(W,k) := \underset{(\mathcal{H},\psi,E,D)}{\text{maximize}} \quad \frac{1}{k}\sum_{x,y,i} W_{X\to Y}(y|x)\langle\psi|E(x|i)\otimes D(i|y)|\psi\rangle \leq \langle\psi|E(x|i)\cdot D(y|j)|\psi\rangle$$

$$\text{with } \big[E(x,i), D(y,j)\big] = 0$$

$$\text{subject to} \quad \sum_x E(x|i) = 1_{\mathcal{H}} \quad \forall i\in[k], \quad \sum_i D(i|y) = 1_{\mathcal{H}} \quad \forall y \in Y$$

$$0 \leq E(x|i) \leq 1_{\mathcal{H}}\ \forall (x,i) \in X\times[k], \quad 0\leq D(i|y) \leq 1_{\mathcal{H}}\ \forall (i,y)\in[k]\times Y\,.$$

- First step: see as the part of the upper-right block of the Gram matrix

$$\Omega = \sum_{u,v}\langle\psi|X_uX_v|\psi\rangle|u\rangle\langle v| \quad \text{with} \quad X_u = \begin{cases} E(x|i) & u=(i,x)\\ D(j|y) & u=(j,y)\end{cases}$$

for i=j

$$\Omega = \left(\begin{array}{c:c} \langle\psi|E(x|i)\cdot E(x'|i')|\psi\rangle & \langle\psi|E(x|i)\cdot D(y|j)|\psi\rangle \\ \hdashline \langle\psi|E(x'|i')\cdot D(y'|j')|\psi\rangle & \langle\psi|D(y|j)\cdot D(y'|j')]|\psi\rangle \end{array}\right)$$

- Original constraints can be formulated as positivity conditions on $\Omega:\ \mathrm{sdp}_1(W,k)$

*motivated by: "**NPA hierarchy**" (Bell inequalities)*

[Lasserre, SIAM (2001)], [Parrilo, Math. Program. (2003)], [Navascues et al., PRL (2007)], [Doherty et al., IEEE CCC (2008)], [Navascues et al., NJP (2008)], [Pironio et al., SIAM (2010)]

First level semidefinite programming relaxation (II)

- First level relaxation: $p_{\mathrm{succ}}(W,k) \leq p^*_{\mathrm{succ}}(W,k) \leq \mathrm{sdp}_1(W,k)$

$$
\begin{aligned}
\mathrm{sdp}_1(W,k) = \underset{\Omega}{\mathrm{maximize}} \quad & \frac{1}{k}\sum_{x,y,i} W_{X\to Y}(y|x)\Omega_{(i,x),(i,y)} \\
\text{subject to} \quad & \Omega \in \mathrm{Pos}(1+k|X|+k|Y|)\,, \quad \Omega_{\emptyset,\emptyset} = 1 \quad \text{with } \emptyset \text{ the empty symbol} \\
& \Omega_{u,v} \geq 0 \quad \forall u,v \in X\times[k]\cup Y\times[k]\cup\{\emptyset\} \\
& \sum_x \Omega_{w,(i,x)} = \Omega_{w,\emptyset} \quad \forall i\in[k]\,, w\in X\times[k]\cup Y\times[k]\cup\{\emptyset\} \\
& \sum_i \Omega_{w,(i,y)} = \Omega_{w,\emptyset} \quad \forall y\in Y, w\in X\times[k]\cup Y\times[k]\cup\{\emptyset\}\,.
\end{aligned}
$$

First level semidefinite programming relaxation (II)

- First level relaxation: $p_{\mathrm{succ}}(W,k) \leq p^*_{\mathrm{succ}}(W,k) \leq \mathrm{sdp}_1(W,k)$

$$
\begin{aligned}
\mathrm{sdp}_1(W,k) = \underset{\Omega}{\mathrm{maximize}} \quad & \frac{1}{k}\sum_{x,y,i} W_{X\to Y}(y|x)\Omega_{(i,x),(i,y)} \\
\text{subject to} \quad & \Omega \in \mathrm{Pos}(1+k|X|+k|Y|)\,, \quad \Omega_{\emptyset,\emptyset} = 1 \quad \text{with } \emptyset \text{ the empty symbol} \\
& \Omega_{u,v} \geq 0 \quad \forall u,v \in X\times[k]\cup Y\times[k]\cup\{\emptyset\} \\
& \sum_x \Omega_{w,(i,x)} = \Omega_{w,\emptyset} \quad \forall i \in [k]\,, w \in X\times[k]\cup Y\times[k]\cup\{\emptyset\} \\
& \sum_i \Omega_{w,(i,y)} = \Omega_{w,\emptyset} \quad \forall y \in Y, w \in X\times[k]\cup Y\times[k]\cup\{\emptyset\}\,.
\end{aligned}
$$

First level semidefinite programming relaxation (II)

- First level relaxation: $p_{\rm succ}(W,k) \leq p^*_{\rm succ}(W,k) \leq {\rm sdp}_1(W,k)$

$$
\begin{aligned}
{\rm sdp}_1(W,k) = \underset{\Omega}{\text{maximize}} \quad & \frac{1}{k}\sum_{x,y,i} W_{X\to Y}(y|x)\Omega_{(i,x),(i,y)} \\
\text{subject to} \quad & \Omega \in {\rm Pos}(1+k|X|+k|Y|)\,, \quad \Omega_{\emptyset,\emptyset} = 1 \quad \text{with } \emptyset \text{ the empty symbol} \\
& \Omega_{u,v} \geq 0 \quad \forall u,v \in X\times[k]\cup Y\times[k]\cup\{\emptyset\} \\
& \sum_x \Omega_{w,(i,x)} = \Omega_{w,\emptyset} \quad \forall i\in[k]\,, w\in X\times[k]\cup Y\times[k]\cup\{\emptyset\} \\
& \sum_i \Omega_{w,(i,y)} = \Omega_{w,\emptyset} \quad \forall y\in Y, w\in X\times[k]\cup Y\times[k]\cup\{\emptyset\}\,.
\end{aligned}
$$

- Going back to our example:

$$p_{\rm succ}(Z,2) = \frac{5}{6} \approx 0.833$$

(known before, with two-dimensional assistance)

$$p^*_{\rm succ}(Z,2) \geq \frac{2+2^{-1/2}}{3} \approx 0.902$$

$$
Z = \begin{pmatrix}
1/3 & 1/3 & 0 & 0 \\
0 & 0 & 1/3 & 1/3 \\
1/3 & 0 & 1/3 & 0 \\
0 & 1/3 & 0 & 1/3 \\
1/3 & 0 & 0 & 1/3 \\
0 & 1/3 & 1/3 & 0
\end{pmatrix}
$$

First level semidefinite programming relaxation (II)

- First level relaxation: $p_{\text{succ}}(W,k) \leq p^*_{\text{succ}}(W,k) \leq \text{sdp}_1(W,k)$

$$\begin{aligned} \text{sdp}_1(W,k) = \underset{\Omega}{\text{maximize}} \quad & \frac{1}{k}\sum_{x,y,i} W_{X\to Y}(y|x)\Omega_{(i,x),(i,y)} \\ \text{subject to} \quad & \Omega \in \text{Pos}(1+k|X|+k|Y|)\,, \quad \Omega_{\emptyset,\emptyset}=1 \quad \text{with } \emptyset \text{ the empty symbol} \\ & \Omega_{u,v} \geq 0 \quad \forall u,v \in X\times[k]\cup Y\times[k]\cup\{\emptyset\} \\ & \sum_x \Omega_{w,(i,x)} = \Omega_{w,\emptyset} \quad \forall i\in[k]\,, w\in X\times[k]\cup Y\times[k]\cup\{\emptyset\} \\ & \sum_i \Omega_{w,(i,y)} = \Omega_{w,\emptyset} \quad \forall y\in Y, w\in X\times[k]\cup Y\times[k]\cup\{\emptyset\}\,. \end{aligned}$$

- Going back to our example:

$$p_{\text{succ}}(Z,2) = \frac{5}{6} \approx 0.833$$

$$p^*_{\text{succ}}(Z,2) \geq \frac{2+2^{-1/2}}{3} \approx 0.902$$

(known before, with two-dimensional assistance)

$$Z = \begin{pmatrix} 1/3 & 1/3 & 0 & 0 \\ 0 & 0 & 1/3 & 1/3 \\ 1/3 & 0 & 1/3 & 0 \\ 0 & 1/3 & 0 & 1/3 \\ 1/3 & 0 & 0 & 1/3 \\ 0 & 1/3 & 1/3 & 0 \end{pmatrix}$$

- Relaxation: $p^*_{\text{succ}}(Z,2) \leq \text{sdp}_1(Z,2) \approx 0.908 = \frac{1}{2} + \frac{1}{\sqrt{6}}$
- Four-dimensional assistance: $p^*_{\text{succ}}(Z,2) \geq \frac{1}{2} + \frac{1}{\sqrt{6}}$

First level semidefinite programming relaxation (II)

- First level relaxation: $p_{\mathrm{succ}}(W,k) \leq p^*_{\mathrm{succ}}(W,k) \leq \mathrm{sdp}_1(W,k)$

$$\mathrm{sdp}_1(W,k) = \underset{\Omega}{\text{maximize}} \quad \frac{1}{k}\sum_{x,y,i} W_{X\to Y}(y|x)\Omega_{(i,x),(i,y)}$$

$$\text{subject to} \quad \Omega \in \mathrm{Pos}(1+k|X|+k|Y|)\,, \quad \Omega_{\emptyset,\emptyset}=1 \quad \text{with } \emptyset \text{ the empty symbol}$$

new condition —> $\Omega_{u,v} \geq 0 \quad \forall u,v \in X\times[k]\cup Y\times[k]\cup\{\emptyset\}$

$$\sum_x \Omega_{w,(i,x)} = \Omega_{w,\emptyset} \quad \forall i\in[k]\,, w\in X\times[k]\cup Y\times[k]\cup\{\emptyset\}$$

$$\sum_i \Omega_{w,(i,y)} = \Omega_{w,\emptyset} \quad \forall y\in Y, w\in X\times[k]\cup Y\times[k]\cup\{\emptyset\}\,.$$

- Going back to our example:

$$p_{\mathrm{succ}}(Z,2) = \frac{5}{6} \approx 0.833$$

$$p^*_{\mathrm{succ}}(Z,2) \geq \frac{2+2^{-1/2}}{3} \approx 0.902$$

(known before, with two-dimensional assistance)

$$Z = \begin{pmatrix} 1/3 & 1/3 & 0 & 0 \\ 0 & 0 & 1/3 & 1/3 \\ 1/3 & 0 & 1/3 & 0 \\ 0 & 1/3 & 0 & 1/3 \\ 1/3 & 0 & 0 & 1/3 \\ 0 & 1/3 & 1/3 & 0 \end{pmatrix}$$

(NPA hierarchy and non-signalling bounds are one)

- Relaxation: $p^*_{\mathrm{succ}}(Z,2) \leq \mathrm{sdp}_1(Z,2) \approx 0.908 = \frac{1}{2}+\frac{1}{\sqrt{6}}$
- Four-dimensional assistance: $p^*_{\mathrm{succ}}(Z,2) \geq \frac{1}{2}+\frac{1}{\sqrt{6}}$

First level semidefinite programming relaxation (II)

- First level relaxation: $p_{\mathrm{succ}}(W,k) \leq p^*_{\mathrm{succ}}(W,k) \leq \mathrm{sdp}_1(W,k)$

$$\mathrm{sdp}_1(W,k) = \underset{\Omega}{\mathrm{maximize}} \quad \frac{1}{k}\sum_{x,y,i} W_{X\to Y}(y|x)\Omega_{(i,x),(i,y)}$$

$$\text{subject to} \quad \Omega \in \mathrm{Pos}(1+k|X|+k|Y|)\,, \quad \Omega_{\emptyset,\emptyset} = 1 \quad \text{with } \emptyset \text{ the empty symbol}$$

new condition —> $\Omega_{u,v} \geq 0 \quad \forall u,v \in X\times[k]\cup Y\times[k]\cup\{\emptyset\}$

$$\sum_x \Omega_{w,(i,x)} = \Omega_{w,\emptyset} \quad \forall i\in[k]\,, w\in X\times[k]\cup Y\times[k]\cup\{\emptyset\}$$

$$\sum_i \Omega_{w,(i,y)} = \Omega_{w,\emptyset} \quad \forall y\in Y, w\in X\times[k]\cup Y\times[k]\cup\{\emptyset\}\,.$$

- Going back to our example:

$$p_{\mathrm{succ}}(Z,2) = \frac{5}{6} \approx 0.833$$

(known before, with two-dimensional assistance)

$$p^*_{\mathrm{succ}}(Z,2) \geq \frac{2+2^{-1/2}}{3} \approx 0.902$$

$$Z = \begin{pmatrix} 1/3 & 1/3 & 0 & 0 \\ 0 & 0 & 1/3 & 1/3 \\ 1/3 & 0 & 1/3 & 0 \\ 0 & 1/3 & 0 & 1/3 \\ 1/3 & 0 & 0 & 1/3 \\ 0 & 1/3 & 1/3 & 0 \end{pmatrix}$$

(NPA hierarchy and non-signalling bounds are one)

- Relaxation: $p^*_{\mathrm{succ}}(Z,2) \leq \mathrm{sdp}_1(Z,2) \approx 0.908 = \frac{1}{2}+\frac{1}{\sqrt{6}}$
- Four-dimensional assistance: $p^*_{\mathrm{succ}}(Z,2) \geq \frac{1}{2}+\frac{1}{\sqrt{6}}$

—> further work [Barman and Fawzi., arXiv:1508.04095]

Overview

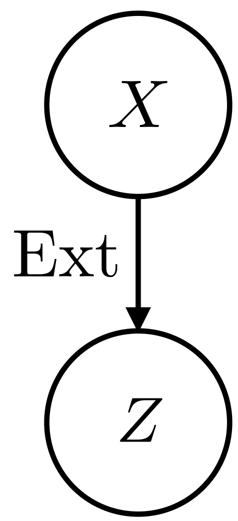
- Theoretical talk, plus start with non-cryptographic problem
- Classical noisy channel coding versus entanglement-assisted *channel coding* (**quantum assistance**)
- Semidefinite programming (sdp) hierarchies for understanding (bounding) the difference
- Cryptography: randomness extractors versus *quantum-proof randomness extractors* (**quantum adversary**)
- Conclusion / Outlook

Quantum Cryptography (I)

- Privacy amplification:

weak source of randomness $X \in \{0,1\}^n$

(with min-entropy k)



uniform random bits $Z \in \{0,1\}^m$

(up to $\epsilon \geq 0$)

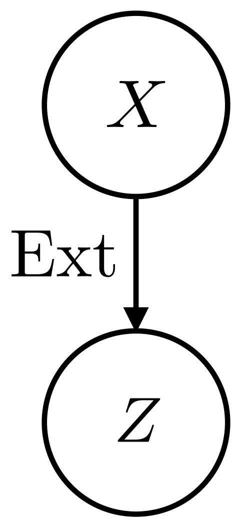
- Example: two-universal hashing

Quantum Cryptography (I)

- Privacy amplification:

weak source of randomness $X \in \{0,1\}^n$

(with min-entropy k)



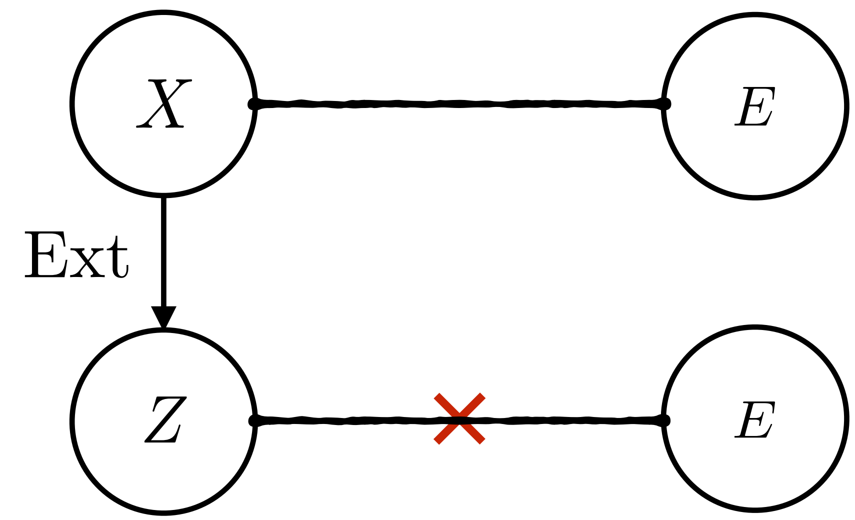
uniform random bits $Z \in \{0,1\}^m$

(up to $\epsilon \geq 0$)

- Example: two-universal hashing

- What happens for quantum adversaries?

weak source of randomness relative to E



uniform random bits relative to E

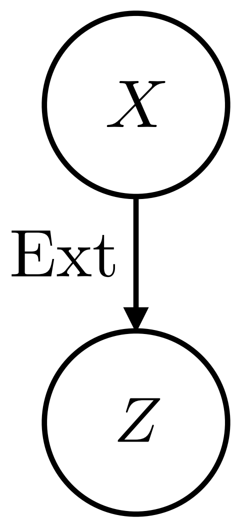
(up to $\epsilon \geq 0$)

Quantum Cryptography (I)

- Privacy amplification:

weak source of randomness $X \in \{0,1\}^n$

(with min-entropy k)



"randomness extractor"

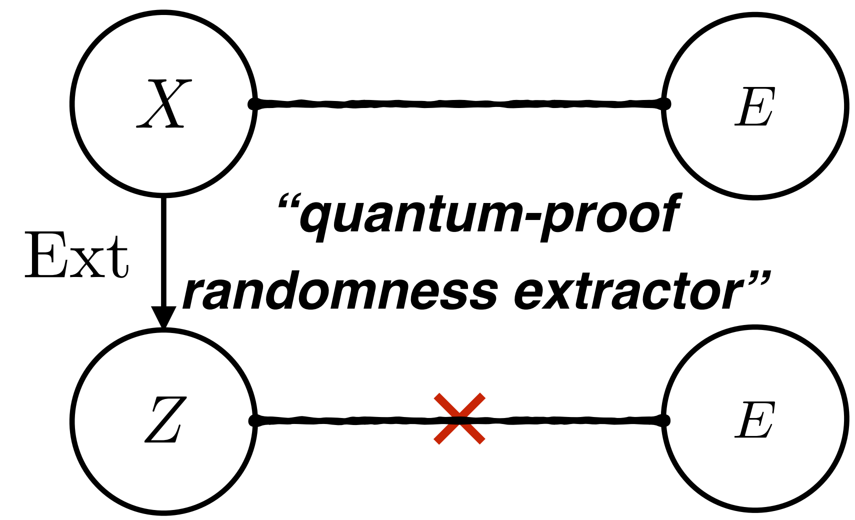
uniform random bits $Z \in \{0,1\}^m$

(up to $\epsilon \geq 0$)

- Example: two-universal hashing

- What happens for quantum adversaries?

weak source of randomness relative to E



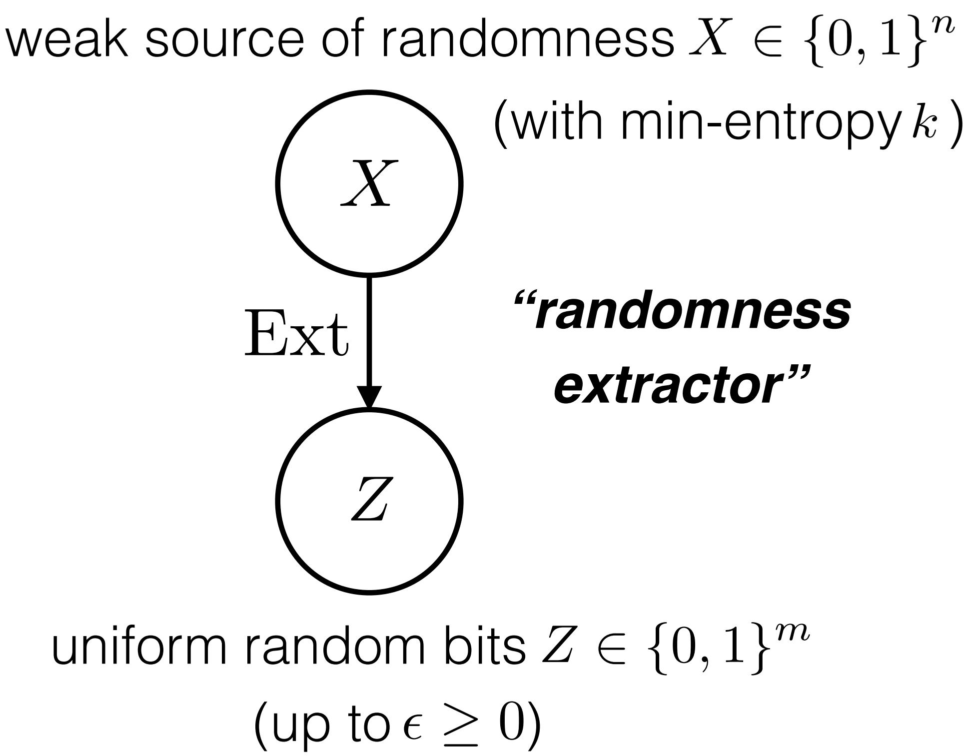
"quantum-proof randomness extractor"

uniform random bits relative to E

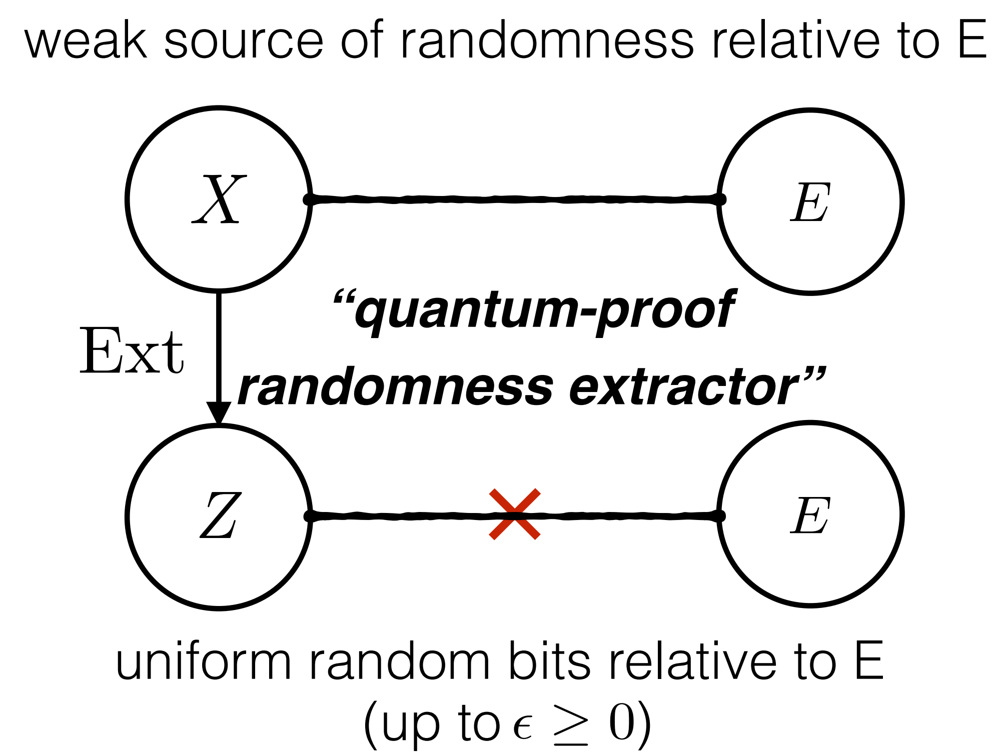
(up to $\epsilon \geq 0$)

Quantum Cryptography (I)

- Privacy amplification:



- What happens for quantum adversaries?



- Example: two-universal hashing

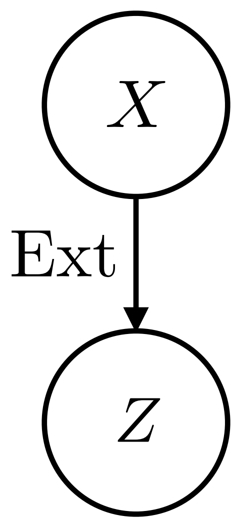
- Motivation: quantum key distribution, two-party cryptography, “quantum-safe / quantum-proof / post-quantum”

Quantum Cryptography (I)

- Privacy amplification:

weak source of randomness $X \in \{0,1\}^n$

(with min-entropy k)



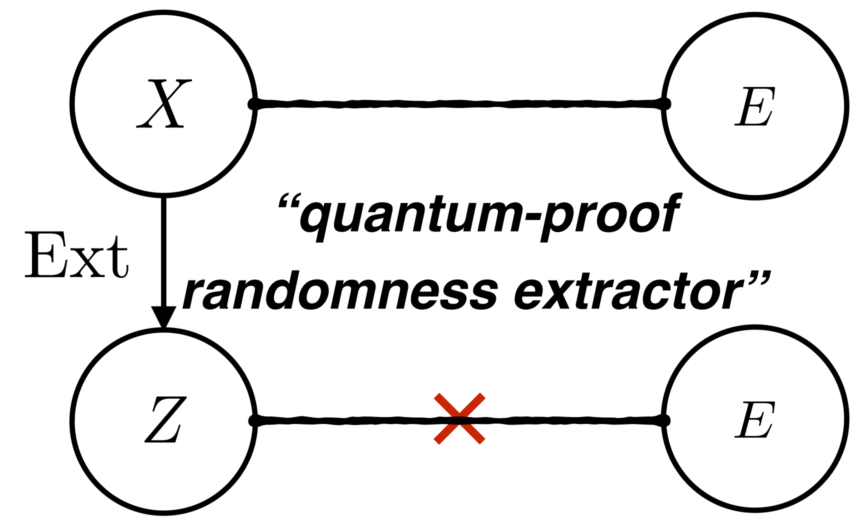
"randomness extractor"

uniform random bits $Z \in \{0,1\}^m$

(up to $\epsilon \geq 0$)

- What happens for quantum adversaries?

weak source of randomness relative to E



"quantum-proof randomness extractor"

uniform random bits relative to E

(up to $\epsilon \geq 0$)

- Example: two-universal hashing
- Motivation: quantum key distribution, two-party cryptography, "quantum-safe / quantum-proof / post-quantum"
- Classical versus quantum error (the ϵ): $C(\mathrm{Ext}, k) \quad \text{versus} \quad Q(\mathrm{Ext}, k)$ *computable?*

Quantum Cryptography (II)

- For randomness extractors: classical versus **quantum adversaries**

$C(\mathrm{Ext}, k)$ versus $Q(\mathrm{Ext}, k)$ *computable?*

classical bilinear optimisation	versus	quantum bilinear optimisation
scalar variables	versus	matrix variables

Quantum Cryptography (II)

- For randomness extractors: classical versus **quantum adversaries**

$C(\mathrm{Ext}, k)$ versus $Q(\mathrm{Ext}, k)$ *computable?*

classical bilinear optimisation versus quantum bilinear optimisation

scalar variables versus matrix variables

- Converging **hierarchy of semidefinite programming** relaxations:

$C(\mathrm{Ext}, k) \leq Q(\mathrm{Ext}, k) = \mathrm{sdp}_\infty(\mathrm{Ext}, k) \leq \ldots \leq \mathrm{sdp}_1(\mathrm{Ext}, k)$ *<— efficiently computable!*

—> upper bounding the power of quantum adversaries

Quantum Cryptography (II)

- For randomness extractors: classical versus **quantum adversaries**

$C(\mathrm{Ext}, k)$ versus $Q(\mathrm{Ext}, k)$ *computable?*

classical bilinear optimisation versus quantum bilinear optimisation

scalar variables versus matrix variables

- Converging **hierarchy of semidefinite programming** relaxations:

$C(\mathrm{Ext}, k) \leq Q(\mathrm{Ext}, k) = \mathrm{sdp}_\infty(\mathrm{Ext}, k) \leq \ldots \leq \mathrm{sdp}_1(\mathrm{Ext}, k)$ <— *efficiently computable!*

—> upper bounding the power of quantum adversaries

- See our paper for results: arXiv:1506.08810 - Quantum Bilinear Optimisation

Overview

- Theoretical talk, plus start with non-cryptographic problem
- Classical noisy channel coding versus entanglement-assisted *channel coding* (**quantum assistance**)
- Semidefinite programming (sdp) hierarchies for understanding (bounding) the difference
- Cryptography: randomness extractors versus *quantum-proof randomness extractors* (**quantum adversary**)
- Conclusion / Outlook

Conclusion / Outlook

- Understand **quantum assistance** (noisy channel coding) and **quantum adversaries** (randomness extractors) using optimisation methods

- Converging **hierarchy of semidefinite programming** relaxations:

$$C \leq Q = \mathrm{sdp}_\infty \leq \ldots \leq \mathrm{sdp}_1$$

- Apply proof method more generically, to whole cryptographic protocols?

Conclusion / Outlook

- Understand **quantum assistance** (noisy channel coding) and **quantum adversaries** (randomness extractors) using optimisation methods

- Converging **hierarchy of semidefinite programming** relaxations:

$$C \leq Q = \mathrm{sdp}_\infty \leq \ldots \leq \mathrm{sdp}_1$$

- Apply proof method more generically, to whole cryptographic protocols?

- Two-prover games (**Bell inequalities**): we get tighter hierarchy (than previous work)

  —> first level also in independent work [Sikora and Varvitsiotis, arXiv:1506.07297]

- Optimisations over the **completely positive semidefinite cone**: we get the first hierarchy (quantum graph parameters)

  [Laurent and Piovesan, arXiv:1312.6643]

Thanks!