A direct product theorem for quantum communication with applications to device-independent QKD

Rahul Jain (CQT, NUS)
Srijita Kundu (IQC, Waterloo)

FOCS 2021 ; QIP 2022 ; ArXiv: 2106.04299

Direct product

Direct product

How much harder is doing n independent instances of a task than doing one instance?

Direct product

How much harder is doing n independent instances of a task than doing one instance?

- Algorithm $\mathcal{A}$ for doing one instance of task

Direct product

How much harder is doing *n* independent instances of a task than doing one instance?

- Algorithm $\mathcal{A}$ for doing one instance of task
- Run $\mathcal{A}$ independently on each instance

Direct product

How much harder is doing n independent instances of a task than doing one instance?

- Algorithm $\mathcal{A}$ for doing one instance of task
- Run $\mathcal{A}$ independently on each instance
- Is this the best we can do?

Direct product

How much harder is doing *n* independent instances of a task than doing one instance?

- Algorithm $\mathcal{A}$ for doing one instance of task
- Run $\mathcal{A}$ independently on each instance
- Is this the best we can do?

Direct product theorem: Yes.

Direct product

How much harder is doing n independent instances of a task than doing one instance?

- Algorithm $\mathcal{A}$ for doing one instance of task
- Run $\mathcal{A}$ independently on each instance
- Is this the best we can do?

Direct product theorem: Yes.

If c resource required for one instance (with success probability p) and if $o(cn)$ resrouce provided for n independent instances

Direct product

How much harder is doing n independent instances of a task than doing one instance?

- Algorithm $\mathcal{A}$ for doing one instance of task
- Run $\mathcal{A}$ independently on each instance
- Is this the best we can do?

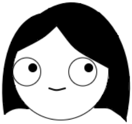
Direct product theorem: Yes.

If c resource required for one instance (with success probability p) and if $o(cn)$ resrouce provided for n independent instances

$\Rightarrow$ success probability $p^{\Omega(n)}$ for n instances

Non-local games

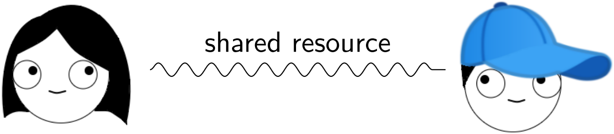
Known predicate V : $\mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B} \rightarrow \{0,1\}$
Known distribution μ on $\mathcal{X} \times \mathcal{Y}$



Non-local games

Known predicate V : $\mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B} \to \{0,1\}$

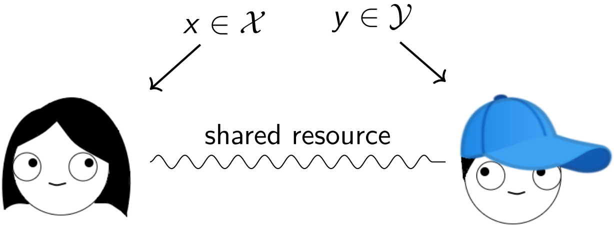
Known distribution μ on $\mathcal{X} \times \mathcal{Y}$



Non-local games

Known predicate V : $\mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B} \rightarrow \{0, 1\}$

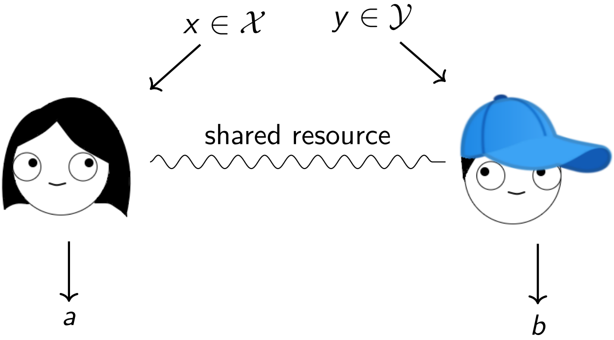
Known distribution μ on $\mathcal{X} \times \mathcal{Y}$



Non-local games

Known predicate V : $\mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B} \to \{0, 1\}$

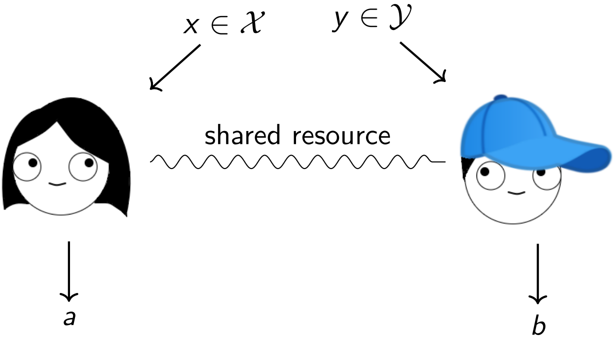
Known distribution μ on $\mathcal{X} \times \mathcal{Y}$



Non-local games

Known predicate $\mathsf{V} : \mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B} \to \{0,1\}$

Known distribution μ on $\mathcal{X} \times \mathcal{Y}$



$$\Pr[\text{Success}] = \Pr_{\mu} \Pr_{\mathcal{S}}[\mathsf{V}(x, y, a, b) = 1]$$

$$\omega^*(G) = \sup_{\mathcal{S}} \Pr[\text{Success on } \mathcal{S}] \qquad (\text{resp. } \omega(G))$$

Parallel repetition of games

Parallel repetition of games

- Parallel repetition question: If $\omega^*(G) = p$, is $\omega^*(G^n) = p^{\Omega(n)}$?
- Applications: hardness of approximation, MIP*=RE, parallel DIQKD ...

Parallel repetition of games

- Parallel repetition question: If $\omega^*(G) = p$, is $\omega^*(G^n) = p^{\Omega(n)}$?
- Applications: hardness of approximation, MIP*=RE, parallel DIQKD ...

Known results:

1. [Raz 95]; [Holenstein 07]: For 2-player G, if $\omega(G) = 1 - \varepsilon$, then

$$\omega(G^n) = (1 - \varepsilon^3)^{n/\log(|\mathcal{A}|\cdot|\mathcal{B}|)}$$

Parallel repetition of games

- Parallel repetition question: If $\omega^*(G) = p$, is $\omega^*(G^n) = p^{\Omega(n)}$?
- Applications: hardness of approximation, MIP*=RE, parallel DIQKD ...

Known results:

1. [Raz 95]; [Holenstein 07]: For 2-player G, if $\omega(G) = 1 - \varepsilon$, then

$$\omega(G^n) = (1 - \varepsilon^3)^{n/\log(|\mathcal{A}|\cdot|\mathcal{B}|)}$$

2. For $\omega^*(G)$ special cases:
   - [J., Pereszlényi, Yao 14]: Free games

Parallel repetition of games

- Parallel repetition question: If $\omega^*(G) = p$, is $\omega^*(G^n) = p^{\Omega(n)}$?
- Applications: hardness of approximation, MIP*=RE, parallel DIQKD ...

Known results:

1. [Raz 95]; [Holenstein 07]: For 2-player G, if $\omega(G) = 1 - \varepsilon$, then

$$\omega(G^n) = (1 - \varepsilon^3)^{n/\log(|\mathcal{A}|\cdot|\mathcal{B}|)}$$

2. For $\omega^*(G)$ special cases:
   - [J., Pereszlényi, Yao 14]: Free games
   - [Bavarian, Vidick, Yuen 17]: Anchored games

Parallel repetition of games

- Parallel repetition question: If $\omega^*(G) = p$, is $\omega^*(G^n) = p^{\Omega(n)}$?
- Applications: hardness of approximation, MIP*=RE, parallel DIQKD ...

Known results:

1. [Raz 95]; [Holenstein 07]: For 2-player G, if $\omega(G) = 1 - \varepsilon$, then

$$\omega(G^n) = (1 - \varepsilon^3)^{n/\log(|\mathcal{A}|\cdot|\mathcal{B}|)}$$

2. For $\omega^*(G)$ special cases:
   - [J., Pereszlényi, Yao 14]: Free games
   - [Bavarian, Vidick, Yuen 17]: Anchored games
   - XOR games [CSUU08], unique games [KRT10], projection games [DSV15]

Parallel repetition of games

- Parallel repetition question: If $\omega^*(G) = p$, is $\omega^*(G^n) = p^{\Omega(n)}$?
- Applications: hardness of approximation, MIP*=RE, parallel DIQKD ...

Known results:

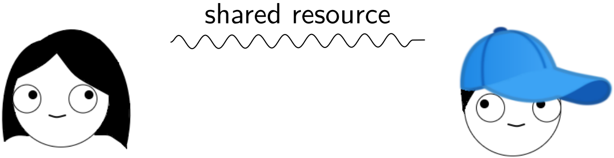
1. [Raz 95]; [Holenstein 07]: For 2-player G, if $\omega(G) = 1 - \varepsilon$, then

$$\omega(G^n) = (1 - \varepsilon^3)^{n/\log(|\mathcal{A}|\cdot|\mathcal{B}|)}$$

2. For $\omega^*(G)$ special cases:
   - [J., Pereszlényi, Yao 14]: Free games
   - [Bavarian, Vidick, Yuen 17]: Anchored games
   - XOR games [CSUU08], unique games [KRT10], projection games [DSV15]

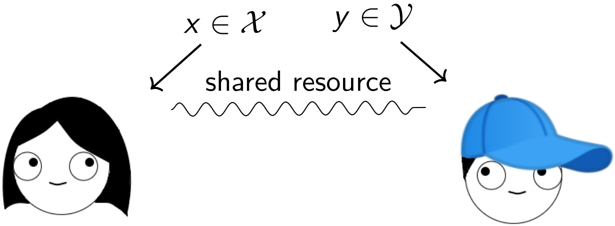
Communication complexity

Known predicate V : $\mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B} \rightarrow \{0, 1\}$



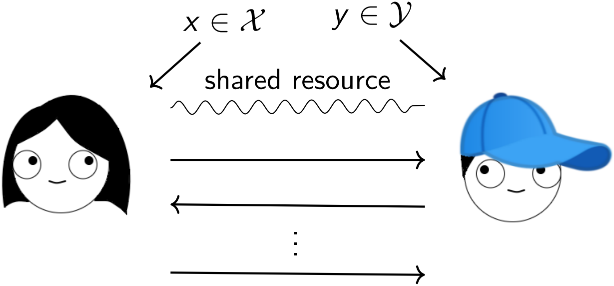
Communication complexity

Known predicate V : $\mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B} \to \{0,1\}$



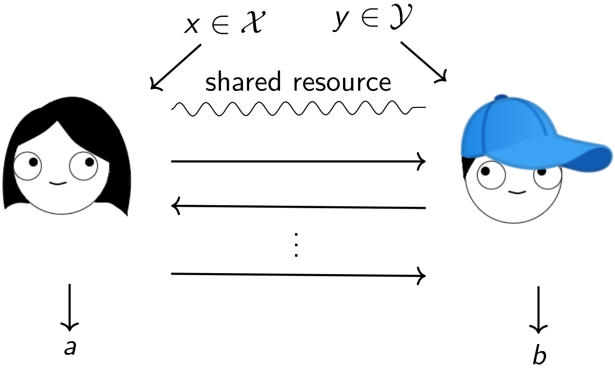
Communication complexity

Known predicate V : $\mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B} \to \{0, 1\}$



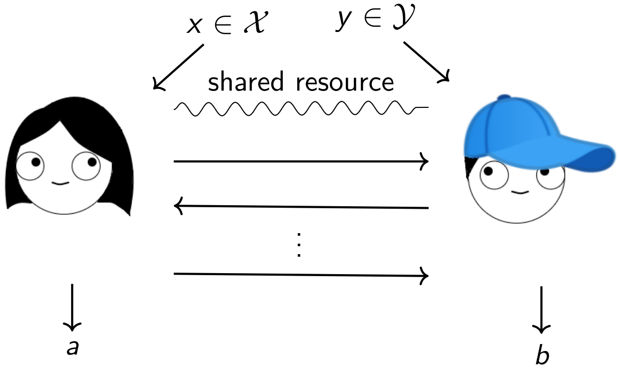
Communication complexity

Known predicate $\mathrm{V} : \mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B} \rightarrow \{0, 1\}$



Communication complexity

Known predicate $\mathrm{V} : \mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B} \to \{0, 1\}$



$\mathrm{QCC}(\mathcal{P}) =$ number of qubits communicated (resp. $\mathrm{CC}(\mathcal{P})$)

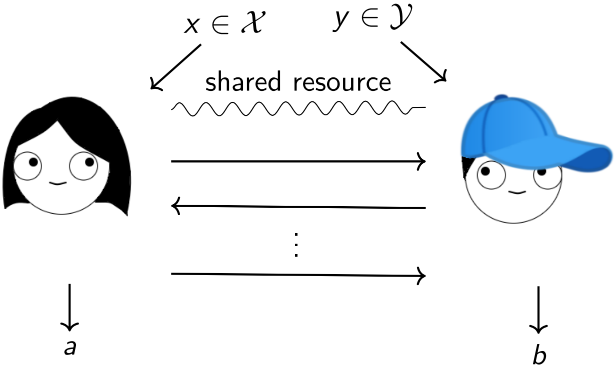
$$\Pr[\text{Success on } \mathcal{P}] = \min_{x,y} \Pr_{\mathcal{P}}[\mathrm{V}(x, y, a, b) = 1]$$

$$\mathrm{Q}^{\mathrm{cc}}_{\varepsilon}(\mathrm{V}) = \min_{\mathcal{P}:\Pr[\text{Success on } \mathcal{P}] \geq 1-\varepsilon} \mathrm{QCC}(\mathcal{P}) \quad (\text{resp. } \mathrm{R}_{\varepsilon}(\mathrm{V}))$$

Communication complexity

Known predicate $\mathsf{V} : \mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B} \rightarrow \{0, 1\}$

Known distribution μ on $\mathcal{X} \times \mathcal{Y}$



$$\Pr_\mu[\text{Success}] = \Pr_\mu \Pr_{\mathcal{S}}[\mathsf{V}(x, y, a, b) = 1]$$

$$\mathsf{Q}^{\mathsf{cc}}_\varepsilon(\mathsf{V}, \mu) = \min_{\mathcal{P}:\Pr[\text{Success on } \mathcal{P}] \geq 1-\varepsilon} \mathsf{QCC}(\mathcal{P}) \quad (\text{resp. } \mathsf{R}^{\mathsf{cc}}_\varepsilon(\mathsf{V}, \mu))$$

Yao's Lemma: $\mathsf{C}^{\mathsf{pub}}_\varepsilon(\mathsf{V}) = \max_\mu \mathsf{C}^{\mathsf{pub}}_\varepsilon(\mathsf{V}, \mu)$

Direct product for communication

- Direct product question: If c communication has success probability p on V, does $o(cn)$ communication have success probability $p^{\Omega(n)}$ on V^n?
- Applications: Lower bounds for specific functions, time-space tradeoffs, separating NC_1 and NC_2, ...

Direct product for communication

- Direct product question: If c communication has success probability p on V, does $o(cn)$ communication have success probability $p^{\Omega(n)}$ on V^n?
- Applications: Lower bounds for specific functions, time-space tradeoffs, separating NC_1 and NC_2, ...

Known results:

1. [J., Pereszlényi, Yao 12]; [Braverman, Rao, Weinstein, Yehuyadoff 13]: Direct product for bounded-round classical communication

Direct product for communication

- Direct product question: If c communication has success probability p on V, does $o(cn)$ communication have success probability $p^{\Omega(n)}$ on V^n?
- Applications: Lower bounds for specific functions, time-space tradeoffs, separating NC_1 and NC_2, ...

Known results:

1. [J., Pereszlényi, Yao 12]; [Braverman, Rao, Weinstein, Yehuyadoff 13]: Direct product for bounded-round classical communication
2. [Braverman, Rao, Weinstein, Yehuyadoff 14]: Direct product in terms of information complexity

Direct product for communication

- Direct product question: If c communication has success probability p on V, does $o(cn)$ communication have success probability $p^{\Omega(n)}$ on V^n?
- Applications: Lower bounds for specific functions, time-space tradeoffs, separating NC_1 and NC_2, ...

Known results:

1. [J., Pereszlényi, Yao 12]; [Braverman, Rao, Weinstein, Yehuyadoff 13]: Direct product for bounded-round classical communication
2. [Braverman, Rao, Weinstein, Yehuyadoff 14]: Direct product in terms of information complexity
3. [J., Kundu 20]: Direct product for 1-way quantum communication

Direct product for communication

- Direct product question: If c communication has success probability p on V, does $o(cn)$ communication have success probability $p^{\Omega(n)}$ on V^n?
- Applications: Lower bounds for specific functions, time-space tradeoffs, separating NC_1 and NC_2, ...

Known results:

1. [J., Pereszlényi, Yao 12]; [Braverman, Rao, Weinstein, Yehuyadoff 13]: Direct product for bounded-round classical communication
2. [Braverman, Rao, Weinstein, Yehuyadoff 14]: Direct product in terms of information complexity
3. [J., Kundu 20]: Direct product for 1-way quantum communication
4. [Sherstov 12]: Direct product for generalized discrepancy

Direct product for communication

- Direct product question: If c communication has success probability p on V, does $o(cn)$ communication have success probability $p^{\Omega(n)}$ on V^n?
- Applications: Lower bounds for specific functions, time-space tradeoffs, separating NC_1 and NC_2, . . .

Known results:

1. [J., Pereszlényi, Yao 12]; [Braverman, Rao, Weinstein, Yehuyadoff 13]: Direct product for bounded-round classical communication
2. [Braverman, Rao, Weinstein, Yehuyadoff 14]: Direct product in terms of information complexity
3. [J., Kundu 20]: Direct product for 1-way quantum communication
4. [Sherstov 12]: Direct product for generalized discrepancy
    - Lower bound for 2-party communication complexity of boolean functions

Our results

Our results

Main theorem: Distributional direct product theorem quantum communication complexity of any ℓ-party predicate V

Our results

Main theorem: Distributional direct product theorem quantum communication complexity of any ℓ-party predicate V

Let μ be a product distribution on inputs and $\mathcal{P}$ be a protocol for V^n with communication cn.

Our results

Main theorem: Distributional direct product theorem quantum communication complexity of any ℓ-party predicate V

Let μ be a product distribution on inputs and $\mathcal{P}$ be a protocol for V^n with communication cn.

1. If $c < 1$, then
$$\mathrm{suc}(\mathsf{V}^n, \mu^n, \mathcal{P}) \leq \left(1 - \frac{\nu}{2} + \sqrt{2\ell c}\right)^{\Omega(\nu^2 n/\ell^2)}$$
where $\nu = 1 - \omega^*(G(\mathsf{V}, \mu))$.

Our results

Main theorem: Distributional direct product theorem quantum communication complexity of any ℓ-party predicate V

Let μ be a product distribution on inputs and $\mathcal{P}$ be a protocol for V^n with communication cn.

1. If $c < 1$, then

$$\mathsf{suc}(\mathsf{V}^n, \mu^n, \mathcal{P}) \leq \left(1 - \frac{\nu}{2} + \sqrt{2\ell c}\right)^{\Omega(\nu^2 n/\ell^2)}$$

where $\nu = 1 - \omega^*(G(\mathsf{V}, \mu))$.

$\Rightarrow$ Parallel repetition for games, under product distribution, holds even with a small amount of communication

Our results

Main theorem: Distributional direct product theorem quantum communication complexity of any ℓ-party predicate V

Let μ be a product distribution on inputs and $\mathcal{P}$ be a protocol for V^n with communication cn.

1. If $c < 1$, then
$$\mathsf{suc}(\mathsf{V}^n, \mu^n, \mathcal{P}) \leq \left(1 - \frac{\nu}{2} + \sqrt{2\ell c}\right)^{\Omega(\nu^2 n/\ell^2)}$$
where $\nu = 1 - \omega^*(G(\mathsf{V}, \mu))$.

   $\Rightarrow$ Parallel repetition for games, under product distribution, holds even with a small amount of communication

2. If $1 \leq c = O(\varepsilon^2 \cdot \log \mathsf{eff}^*_{2\varepsilon}(\mathsf{V}, \mu)/\ell^3)$, then
$$\mathsf{suc}(\mathsf{V}^n, \mu^n, \mathcal{P}) \leq (1 - \varepsilon)^{\Omega(n)}$$
where $\mathsf{eff}^*(\mathsf{V}, \mu) =$ (relaxed) quantum partition bound or efficiency.

Our results

- Case 1. $\Rightarrow$ It is possible to do device-independent quantum key distribution (QKD) in the presence of leakage.

Our results

- Case 1. $\Rightarrow$ It is possible to do device-independent quantum key distribution (QKD) in the presence of leakage.
  - Protocol by [J., Miller, Shi 17] based on the Magic Square (MS) game

With devices compatible with n copies of MS, it is possible to extract $\Omega(n)$ bits of key even in the presence of cn communication.

Our results

- Case 1. $\Rightarrow$ It is possible to do device-independent quantum key distribution (QKD) in the presence of leakage.
  - Protocol by [J., Miller, Shi 17] based on the Magic Square (MS) game

With devices compatible with n copies of MS, it is possible to extract $\Omega(n)$ bits of key even in the presence of cn communication.

- Case 2. $\Rightarrow$ Direct product theorem in terms of $\max_{\text{product } \mu} \log \text{eff}^*(V, \mu)$
  - Not directly comparable to Sherstov's result for 2-party boolean functions
  - Works for more than 2 parties, non-boolean functions and predicates
  - Direct product theorem for generalized the inner-product function:

$$\mathrm{IP}_q^n = \sum_{i=1}^{n} x_i y_i \mod q.$$

Quantum partition bound

Quantum partition bound

Zero-communication protocol:

- Either party can abort or give outputs
- Conditioned on nobody aborting, outputs correct w.p. $1 - \varepsilon$
- Efficiency $=$ (probability of not aborting)$^{-1}$

Quantum partition bound

Zero-communication protocol:

- Either party can abort or give outputs
- Conditioned on nobody aborting, outputs correct w.p. $1 - \varepsilon$
- Efficiency $=$ (probability of not aborting)$^{-1}$

[Laplante, Lerays, Roland 12]: $\mathsf{eff}^*_\varepsilon(\mathsf{V}, \mu) =$ min efficiency for V w.r.t. μ

Quantum partition bound

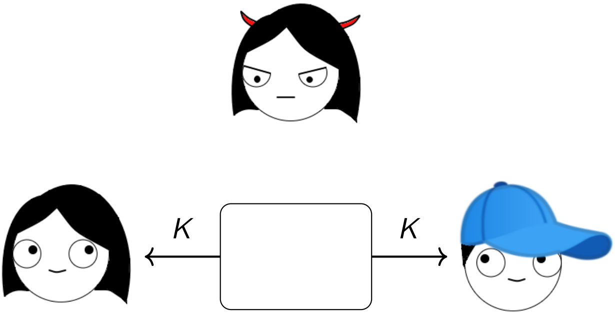
Zero-communication protocol:

- Either party can abort or give outputs
- Conditioned on nobody aborting, outputs correct w.p. $1 - \varepsilon$
- Efficiency $=$ (probability of not aborting)$^{-1}$

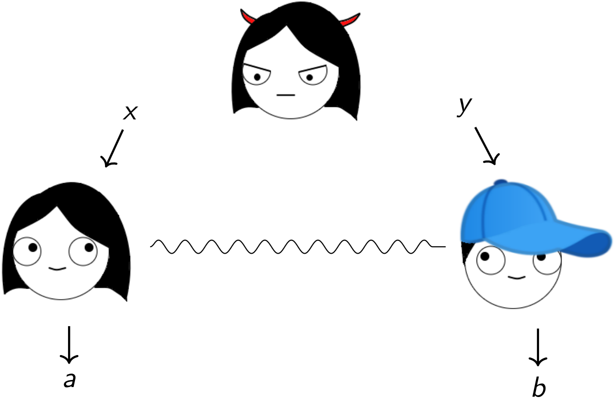
[Laplante, Lerays, Roland 12]: $\mathsf{eff}^*_\varepsilon(\mathsf{V}, \mu) =$ min efficiency for V w.r.t. μ

$$\mathsf{Q}_\varepsilon(\mathsf{V}, \mu) = \Omega(\log \mathsf{eff}^*_\varepsilon(\mathsf{V}, \mu))$$

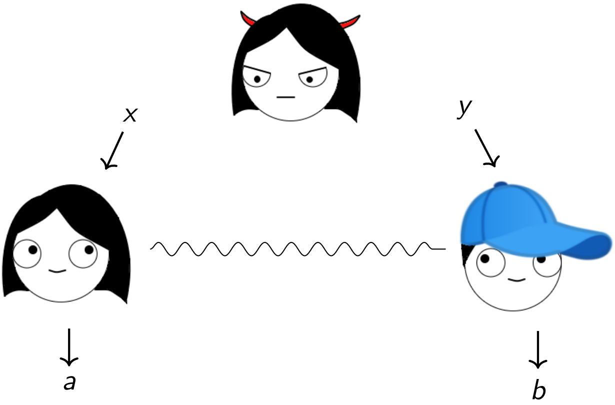
QKD application



QKD application

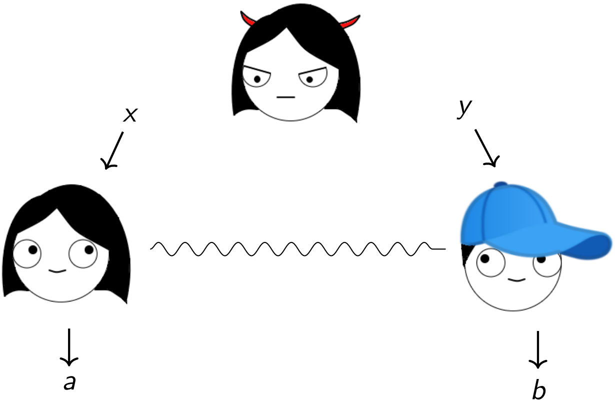


QKD application



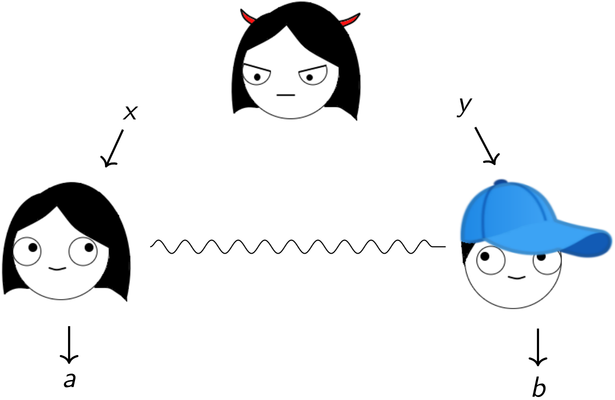
- Bell inequality violation $\Rightarrow$ shared entanglement $\Rightarrow$ secret key

QKD application



- Bell inequality violation ⇒ shared entanglement ⇒ secret key
- In device-independent framework, no need to trust shared state or measurements

QKD application



- Bell inequality violation $\Rightarrow$ shared entanglement $\Rightarrow$ secret key
- In device-independent framework, no need to trust shared state or measurements
- Using non-local games for security analysis requires no communication

DIQKD security parallel repetition/direct product

DIQKD security parallel repetition/direct product

- [J., Miller, Shi 17]; [Vidick 17]: Security proof for parallel DIQKD based on parallel repetition

DIQKD security parallel repetition/direct product

- [J., Miller, Shi 17]; [Vidick 17]: Security proof for parallel DIQKD based on parallel repetition

DIQKD security parallel repetition/direct product

- [J., Miller, Shi 17]; [Vidick 17]: Security proof for parallel DIQKD based on parallel repetition
- Fully interactive leakage of cn qubits

DIQKD security parallel repetition/direct product

- [J., Miller, Shi 17]; [Vidick 17]: Security proof for parallel DIQKD based on parallel repetition
- Fully interactive leakage of cn qubits
  - Scenario modelled by communication complexity rather than non-local game
  - Case 1. of main theorem applies
  - Key rate with leakage = key rate without leakage $-O(\sqrt{c}n)$

Proof idea: information-theoretic framework

Given protocol $\mathcal{P}$ for V^n with $\mathsf{QCC}(\mathcal{P}) = cn$, and $S \subseteq [n]$, one of these holds:

Proof idea: information-theoretic framework

Given protocol $\mathcal{P}$ for V^n with $\mathsf{QCC}(\mathcal{P}) = cn$, and $S \subseteq [n]$, one of these holds:

- $\Pr[\text{Success in } S]$ is already small

Proof idea: information-theoretic framework

Given protocol $\mathcal{P}$ for V^n with $\mathsf{QCC}(\mathcal{P}) = cn$, and $S \subseteq [n]$, one of these holds:

- $\Pr[\text{Success in } S]$ is already small
- $\exists$ "good" $i \notin S$ with $\Pr[\text{Success } i | \text{Success in } S] \leq 1 - \varepsilon$

Proof idea: information-theoretic framework

Given protocol $\mathcal{P}$ for V^n with $\mathsf{QCC}(\mathcal{P}) = cn$, and $S \subseteq [n]$, one of these holds:

- $\Pr[\text{Success in } S]$ is already small
- $\exists$ "good" $i \notin S$ with $\Pr[\text{Success } i | \text{Success in } S] \leq 1 - \varepsilon$
  1. $\Pr[\text{Success in } i | \text{Success in } S] > 1 - \varepsilon \Rightarrow$ strategy for $G(\mathsf{V}, \mu)$ with success probability $> \omega^*(G(V, \mu))$ Contradiction!

Proof idea: information-theoretic framework

Given protocol $\mathcal{P}$ for V^n with $\mathsf{QCC}(\mathcal{P}) = cn$, and $S \subseteq [n]$, one of these holds:

- Pr[Success in S] is already small
- $\exists$ "good" $i \notin S$ with Pr[Success i|Success in S] $\leq 1 - \varepsilon$
  1. Pr[Success in i|Success in S] $> 1 - \varepsilon \Rightarrow$ strategy for $G(\mathsf{V}, \mu)$ with success probability $> \omega^*(G(V, \mu))$ Contradiction!
  2. Pr[Success in i|Success in S] $> 1 - \varepsilon \Rightarrow$ zero-communication protocol for V with efficiency $< \mathrm{eff}^*_\varepsilon(\mathsf{V}, \mu)$ and error probability ε Contradiction!

Proof idea: parallel repetition for product games

Proof idea: parallel repetition for product games

Define "useful" state $|\varphi\rangle$:

- Contains registers $X_{\overline{S}} Y_{\overline{S}} A_{\overline{S}} B_{\overline{S}}$ in superposition
- $|\varphi\rangle_{x_i}, |\varphi\rangle_{y_i}, |\varphi\rangle_{x_i y_i}$: states obtained on measuring $X_i, Y_i, X_i Y_i$ registers
- Distribution $\mathrm{P}_{\hat{A}_i \hat{B}_i | X_i Y_i}$ on measuring $A_i B_i$ on $|\varphi\rangle_{x_i y_i}$:

$$\mathrm{P}_{X_i Y_i} \mathrm{P}_{\hat{A}_i \hat{B}_i | X_i Y_i} \approx \mathrm{P}_{X_i Y_i A_i B_i | \text{Success } C} \quad (\text{in } \mathcal{P})$$

Proof idea: parallel repetition for product games

Define "useful" state $|\varphi\rangle$:

- Contains registers $X_{\overline{S}} Y_{\overline{S}} A_{\overline{S}} B_{\overline{S}}$ in superposition
- $|\varphi\rangle_{x_i}, |\varphi\rangle_{y_i}, |\varphi\rangle_{x_i y_i}$: states obtained on measuring X_i, $Y_i, X_i Y_i$ registers
- Distribution $\mathrm{P}_{\hat{A}_i \hat{B}_i | X_i Y_i}$ on measuring $A_i B_i$ on $|\varphi\rangle_{x_i y_i}$:

$$\mathrm{P}_{X_i Y_i} \mathrm{P}_{\hat{A}_i \hat{B}_i | X_i Y_i} \approx \mathrm{P}_{X_i Y_i A_i B_i | \mathrm{Success}\ C} \quad (\text{in } \mathcal{P})$$

- For good $i \in \overline{S}$,

$$\varphi_{\mathrm{Bob}|x_i} \approx_\delta \varphi_{\mathrm{Bob}} \qquad \varphi_{\mathrm{Alice}|y_i} \approx_\delta \varphi_{\mathrm{Alice}}$$

Proof idea: parallel repetition for product games

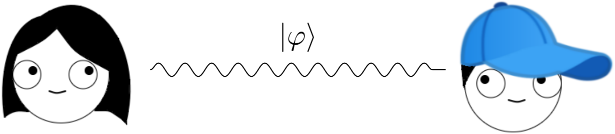
Define "useful" state $|\varphi\rangle$:

- Contains registers $X_{\overline{S}} Y_{\overline{S}} A_{\overline{S}} B_{\overline{S}}$ in superposition
- $|\varphi\rangle_{x_i}, |\varphi\rangle_{y_i}, |\varphi\rangle_{x_i y_i}$: states obtained on measuring X_i, $Y_i, X_i Y_i$ registers
- Distribution $\mathrm{P}_{\hat{A}_i \hat{B}_i | X_i Y_i}$ on measuring $A_i B_i$ on $|\varphi\rangle_{x_i y_i}$:

$$\mathrm{P}_{X_i Y_i} \mathrm{P}_{\hat{A}_i \hat{B}_i | X_i Y_i} \approx \mathrm{P}_{X_i Y_i A_i B_i | \text{Success } C} \quad (\text{in } \mathcal{P})$$

- For good $i \in \overline{S}$,

$$\varphi_{\text{Bob}|x_i} \approx_\delta \varphi_{\text{Bob}} \qquad \varphi_{\text{Alice}|y_i} \approx_\delta \varphi_{\text{Alice}}$$



Proof idea: parallel repetition for product games

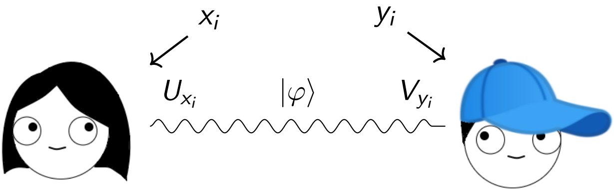
Define "useful" state $|\varphi\rangle$:

- Contains registers $X_{\overline{S}} Y_{\overline{S}} A_{\overline{S}} B_{\overline{S}}$ in superposition
- $|\varphi\rangle_{x_i}, |\varphi\rangle_{y_i}, |\varphi\rangle_{x_i y_i}$: states obtained on measuring $X_i, Y_i, X_i Y_i$ registers
- Distribution $\mathrm{P}_{\hat{A}_i \hat{B}_i | X_i Y_i}$ on measuring $A_i B_i$ on $|\varphi\rangle_{x_i y_i}$:

$$\mathrm{P}_{X_i Y_i} \mathrm{P}_{\hat{A}_i \hat{B}_i | X_i Y_i} \approx \mathrm{P}_{X_i Y_i A_i B_i | \text{Success } C} \quad (\text{in } \mathcal{P})$$

- For good $i \in \overline{S}$,

$$\varphi_{\text{Bob}|x_i} \approx_\delta \varphi_{\text{Bob}} \qquad \varphi_{\text{Alice}|y_i} \approx_\delta \varphi_{\text{Alice}}$$



Proof idea: parallel repetition for product games

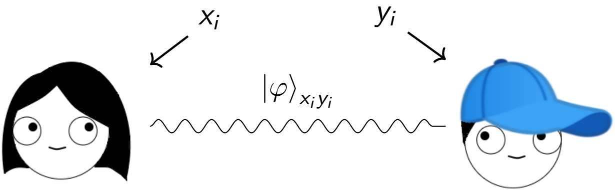
Define "useful" state $|\varphi\rangle$:

- Contains registers $X_{\overline{S}} Y_{\overline{S}} A_{\overline{S}} B_{\overline{S}}$ in superposition
- $|\varphi\rangle_{x_i}, |\varphi\rangle_{y_i}, |\varphi\rangle_{x_i y_i}$: states obtained on measuring $X_i, Y_i, X_i Y_i$ registers
- Distribution $\mathrm{P}_{\hat{A}_i \hat{B}_i | X_i Y_i}$ on measuring $A_i B_i$ on $|\varphi\rangle_{x_i y_i}$:

$$\mathrm{P}_{X_i Y_i} \mathrm{P}_{\hat{A}_i \hat{B}_i | X_i Y_i} \approx \mathrm{P}_{X_i Y_i A_i B_i | \text{Success } C} \quad (\text{in } \mathcal{P})$$

- For good $i \in \overline{S}$,

$$\varphi_{\text{Bob}|x_i} \approx_\delta \varphi_{\text{Bob}} \qquad \varphi_{\text{Alice}|y_i} \approx_\delta \varphi_{\text{Alice}}$$



Proof idea: parallel repetition for product games

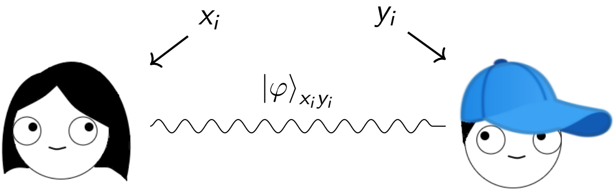
Define "useful" state $|\varphi\rangle$:

- Contains registers $X_{\overline{S}} Y_{\overline{S}} A_{\overline{S}} B_{\overline{S}}$ in superposition
- $|\varphi\rangle_{x_i}, |\varphi\rangle_{y_i}, |\varphi\rangle_{x_i y_i}$: states obtained on measuring $X_i, Y_i, X_i Y_i$ registers
- Distribution $\mathrm{P}_{\hat{A}_i \hat{B}_i | X_i Y_i}$ on measuring $A_i B_i$ on $|\varphi\rangle_{x_i y_i}$:

$$\mathrm{P}_{X_i Y_i} \mathrm{P}_{\hat{A}_i \hat{B}_i | X_i Y_i} \approx \mathrm{P}_{X_i Y_i A_i B_i | \text{Success } C} \quad (\text{in } \mathcal{P})$$

- For good $i \in \overline{S}$,

$$\varphi_{\text{Bob}|x_i} \approx_\delta \varphi_{\text{Bob}} \qquad \varphi_{\text{Alice}|y_i} \approx_\delta \varphi_{\text{Alice}}$$



Proof also works with small communication! $(c < 1)$

Proof idea: DPT in terms of efficiency

Proof idea: DPT in terms of efficiency

If $c \geq 1$,

$$\varphi_{\mathsf{Bob}|x_i} \not\approx_\delta \varphi_{\mathsf{Bob}} \qquad \varphi_{\mathsf{Alice}|y_i} \not\approx_\delta \varphi_{\mathsf{Alice}}$$

Proof idea: DPT in terms of efficiency

If $c \geq 1$,

$$\varphi_{\mathsf{Bob}|x_i} \not\approx_\delta \varphi_{\mathsf{Bob}} \qquad \varphi_{\mathsf{Alice}|y_i} \not\approx_\delta \varphi_{\mathsf{Alice}}$$

But if Alice communicates $c_1 n$ and Bob $c_2 n$,

$$\mathrm{I}(X_i : \mathsf{Bob})_\varphi \leq c_1 \qquad \mathrm{I}(Y_i : \mathsf{Alice})_\varphi \leq c_2$$

Proof idea: DPT in terms of efficiency

If $c \geq 1$,

$$\varphi_{\mathsf{Bob}|x_i} \not\approx_\delta \varphi_{\mathsf{Bob}} \qquad \varphi_{\mathsf{Alice}|y_i} \not\approx_\delta \varphi_{\mathsf{Alice}}$$

But if Alice communicates $c_1 n$ and Bob $c_2 n$,

$$\mathrm{I}(X_i : \mathsf{Bob})_\varphi \leq c_1 \qquad \mathrm{I}(Y_i : \mathsf{Alice})_\varphi \leq c_2$$

Zero-communication protocol via Quantum Substate Theorem

Proof idea: DPT in terms of efficiency

If $c \geq 1$,

$$\varphi_{\text{Bob}|x_i} \not\approx_\delta \varphi_{\text{Bob}} \qquad \varphi_{\text{Alice}|y_i} \not\approx_\delta \varphi_{\text{Alice}}$$

But if Alice communicates $c_1 n$ and Bob $c_2 n$,

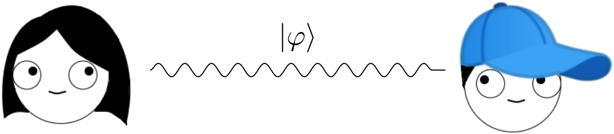
$$\mathrm{I}(X_i : \text{Bob})_\varphi \leq c_1 \qquad \mathrm{I}(Y_i : \text{Alice})_\varphi \leq c_2$$

Zero-communication protocol via Quantum Substate Theorem

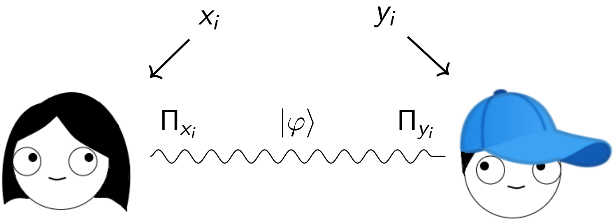
[J., Radhakrishnan, Sen 03]; [J. Nayak 12]: $\mathrm{I}(X : B)_\varphi \leq c \Rightarrow$

- $\exists \varphi'_{XB} \approx_\delta \varphi_{XB}$ s.t. $\varphi'_{XB} \leq 2^{O(c)}(\varphi_X \otimes \varphi_B)$
- $\forall X = x$, $\exists \Pi_x$ acting on A s.t. $\| \Pi_x |\varphi\rangle_{AB} \|_2^2 = 2^{-O(c)}$ and $2^{O(c)} \Pi_x |\varphi\rangle_{AB} = |\varphi'\rangle_{AB|x}$

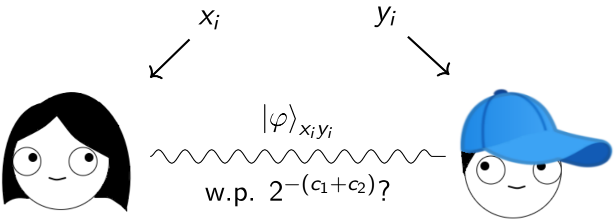
Proof idea: DPT in terms of efficiency



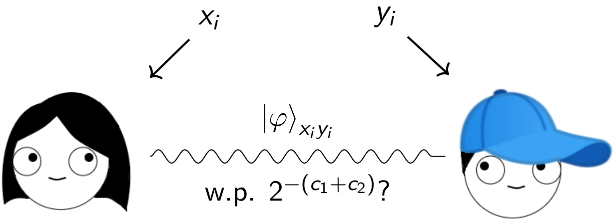
Proof idea: DPT in terms of efficiency



Proof idea: DPT in terms of efficiency

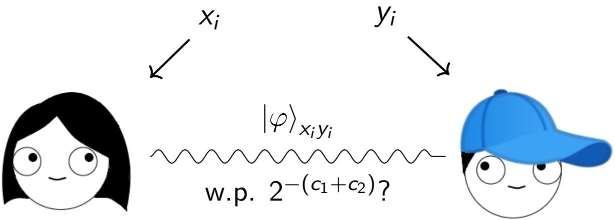


Proof idea: DPT in terms of efficiency



Π_{y_i} does not succeed on state after Π_{x_i} with probability 2^{-c_2}!

Proof idea: DPT in terms of efficiency



Π_{y_i} does not succeed on state after Π_{x_i} with probability 2^{-c_2}!

Substate Perturbation Lemma:

$$\varphi'_{YA} \leq 2^{c}(\varphi_Y \otimes \varphi_A) \text{ and } \rho_A \approx_\delta \varphi_A$$
$$\Rightarrow \exists \rho'_{YA} \approx_\delta \varphi'_{YA} \text{ s.t. } \rho'_{YA} \leq 2^{O(c)}(\varphi_Y \otimes \rho_A)$$

Conclusion and open questions

Conclusion and open questions

- Parallel repetition for games holds even with small communication

Conclusion and open questions

- Parallel repetition for games holds even with small communication
  - Device-independent QKD in the presence of leakage

Conclusion and open questions

- Parallel repetition for games holds even with small communication
  - Device-independent QKD in the presence of leakage
- Direct product theorem in terms of (relaxed) quantum partition bound under product distributions

Conclusion and open questions

- Parallel repetition for games holds even with small communication
  - Device-independent QKD in the presence of leakage
- Direct product theorem in terms of (relaxed) quantum partition bound under product distributions
  - Works for ℓ parties, general predicates
  - New technical tool: Substate Perturbation Lemma

Conclusion and open questions

- Parallel repetition for games holds even with small communication
  - Device-independent QKD in the presence of leakage
- Direct product theorem in terms of (relaxed) quantum partition bound under product distributions
  - Works for ℓ parties, general predicates
  - New technical tool: Substate Perturbation Lemma
- New applications of our results?

Conclusion and open questions

- Parallel repetition for games holds even with small communication
  - Device-independent QKD in the presence of leakage
- Direct product theorem in terms of (relaxed) quantum partition bound under product distributions
  - Works for ℓ parties, general predicates
  - New technical tool: Substate Perturbation Lemma

- New applications of our results?
- Direct product theorem:
  - in terms of (relaxed) quantum partition bound under non-product distributions?

Conclusion and open questions

- Parallel repetition for games holds even with small communication
  - Device-independent QKD in the presence of leakage
- Direct product theorem in terms of (relaxed) quantum partition bound under product distributions
  - Works for ℓ parties, general predicates
  - New technical tool: Substate Perturbation Lemma

- New applications of our results?
- Direct product theorem:
  - in terms of (relaxed) quantum partition bound under non-product distributions?
  - in terms of quantum information complexity?

Conclusion and open questions

- Parallel repetition for games holds even with small communication
  - Device-independent QKD in the presence of leakage
- Direct product theorem in terms of (relaxed) quantum partition bound under product distributions
  - Works for ℓ parties, general predicates
  - New technical tool: Substate Perturbation Lemma

- New applications of our results?
- Direct product theorem:
  - in terms of (relaxed) quantum partition bound under non-product distributions?
  - in terms of quantum information complexity?
  - for bounded round quantum protocols, 2-round protocols?

Conclusion and open questions

- Parallel repetition for games holds even with small communication
  - Device-independent QKD in the presence of leakage
- Direct product theorem in terms of (relaxed) quantum partition bound under product distributions
  - Works for ℓ parties, general predicates
  - New technical tool: Substate Perturbation Lemma

- New applications of our results?
- Direct product theorem:
  - in terms of (relaxed) quantum partition bound under non-product distributions?
  - in terms of quantum information complexity?
  - for bounded round quantum protocols, 2-round protocols?
  - in terms of partition bound for classical protocols?

Conclusion and open questions

- Parallel repetition for games holds even with small communication
  - Device-independent QKD in the presence of leakage
- Direct product theorem in terms of (relaxed) quantum partition bound under product distributions
  - Works for ℓ parties, general predicates
  - New technical tool: Substate Perturbation Lemma

- New applications of our results?
- Direct product theorem:
  - in terms of (relaxed) quantum partition bound under non-product distributions?
  - in terms of quantum information complexity?
  - for bounded round quantum protocols, 2-round protocols?
  - in terms of partition bound for classical protocols?
  - for unbounded round classical protocols (with polylog loss)?

Conclusion and open questions

- Parallel repetition for games holds even with small communication
  - Device-independent QKD in the presence of leakage
- Direct product theorem in terms of (relaxed) quantum partition bound under product distributions
  - Works for ℓ parties, general predicates
  - New technical tool: Substate Perturbation Lemma

- New applications of our results?
- Direct product theorem:
  - in terms of (relaxed) quantum partition bound under non-product distributions?
  - in terms of quantum information complexity?
  - for bounded round quantum protocols, 2-round protocols?
  - in terms of partition bound for classical protocols?
  - for unbounded round classical protocols (with polylog loss)?

Thanks for listening!