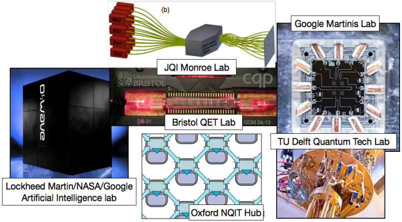
Price of Trust

Elham Kashefi
(joint work with A. Gheorghiu and P. Walden)

TQI 2016 Workshop

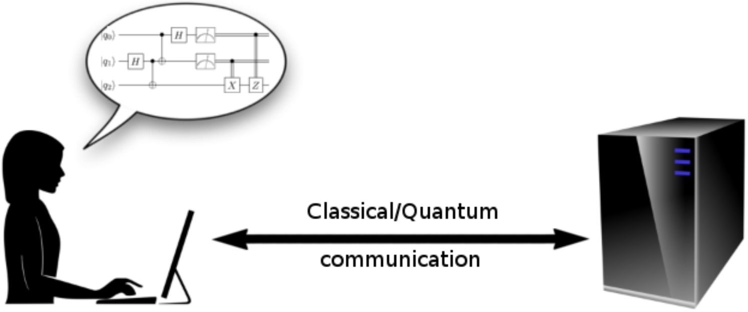
University of Edinburgh
Paris Centre for Quantum Computing
NQIT Quantum Technology Hub
Laboratoire traitement et communication de l'information

Quantum Machines



- These devices become relevant when they are no longer classically simulatable
- **Efficient** verification methods for testing quantum devices ?

Quantum Verification



- Computationally limited verifier
- Powerful quantum server(s)
- Certify the correctness of the computation

Existing approaches (with Privacy)

Single server

- Restricted quantum verifier
  [*Aharonov, Ben-Or, Eban '10*], [*Fitzsimons, Kashefi '12*]
- Measurement-only verifier
  [*Morimae '14*], [*Hayashi, Morimae '15*]
- Device-independent verifier
  [*Gheorghiu, Kashefi, Wallden '15*], [*Hajdusek, Perez-Delgado, Fitzsimons '15*]
- Classical verifier
  open problem

Existing approaches (with Privacy)

Single server

- Restricted quantum verifier
  [*Aharonov, Ben-Or, Eban '10*], [*Fitzsimons, Kashefi '12*]
- Measurement-only verifier
  [*Morimae '14*], [*Hayashi, Morimae '15*]
- Device-independent verifier
  [*Gheorghiu, Kashefi, Wallden '15*], [*Hajdusek, Perez-Delgado, Fitzsimons '15*]
- Classical verifier
  open problem

Non-communicating, entangled servers

- Classical verifier, 2 servers
  [*Reichardt, Unger, Vazirani '12*]
- Classical verifier, multiple servers
  [*McKague '13*]

Existing approaches (without Privacy)

Universal

- Post hoc verification [*Morimae, Fitzsimons '16*], [*Fitzsimons, Hajdusek '15*]
- Direct certification of quantum simulations [*Hangleiter, Kliesch, Schwarz, Eisert '16*]

Existing approaches (without Privacy)

Universal

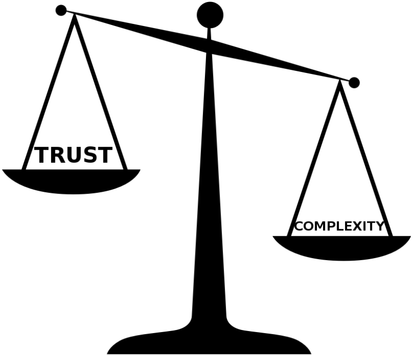
- Post hoc verification [*Morimae, Fitzsimons '16*], [*Fitzsimons, Hajdusek '15*]
- Direct certification of quantum simulations [*Hangleiter, Kliesch, Schwarz, Eisert '16*]

non-Universal

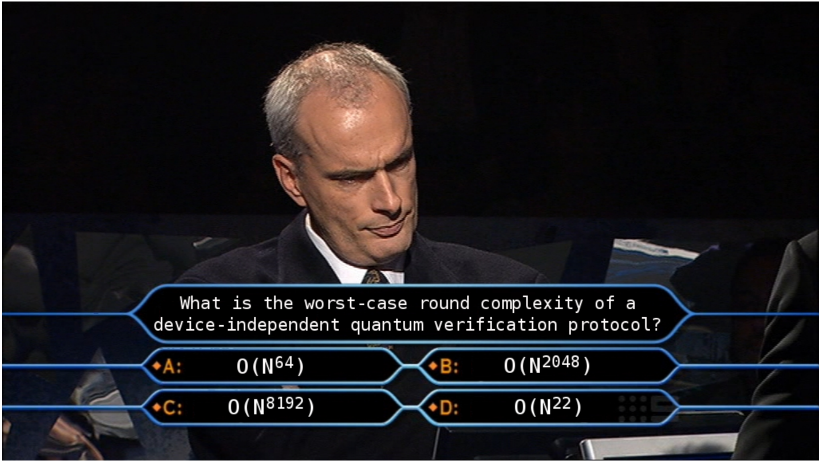
- IQP Hypothesis Testing [*Bremner, Shepherd '08*]
- Boson Sampling Hypothesis Testing [*Spagnolo et. al. '14*]
- Verification of one-clean Qubit Model [*Kapourniotis, Kashefi, Datta '14*]

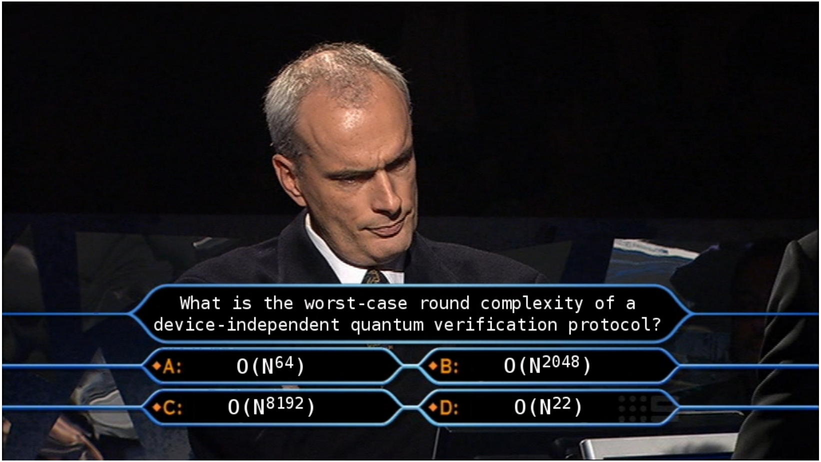
Assumptions

- Prepare and send vs. entanglement-based
- Single vs. multiple servers
- Online vs. offline
- Device-independent vs. one-sided device-independent
- I.i.d. states vs. general states
- Privacy preserving vs non-hiding
- Universal vs non-universal
- And others



The price of trust





Central question

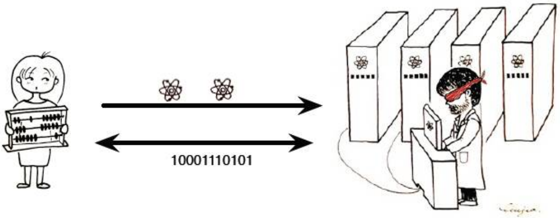
How do trust assumptions affect the complexity of the protocol?

Prepare and send - Outline

Protocols such as those of: [*Aharonov, Ben-Or, Eban '10*], [*Fitzsimons, Kashefi '12*] (FK)

Prepare and send - Outline

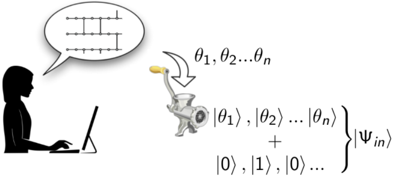
Protocols such as those of: [*Aharonov, Ben-Or, Eban '10*], [*Fitzsimons, Kashefi '12*] (FK)

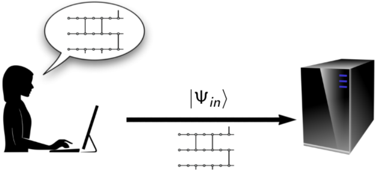


- Verifier *prepares and sends* quantum states to server
- Verifier instructs server on how to use the states for a computation
- They interact classically
- W.h.p. verifier accepts correct result or aborts

Prepare and send - Characteristics

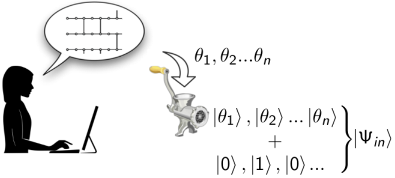
- Minimally quantum verifier (trusted preparation device)
- Prepared states are qubits or qudits (no entanglement) [*Dunjko, Kashefi '16*]
- Can achieve **linear** classical round complexity and one-shot quantum communication complexity [*Kashefi, Wallden '15*]





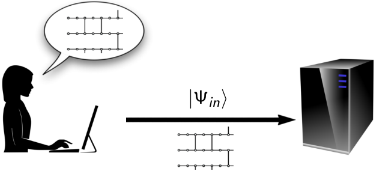
Prepare and send - Characteristics

- Minimally quantum verifier (trusted preparation device)



- Prepared states are qubits or qudits (no entanglement) [*Dunjko, Kashefi '16*]

- Can achieve **linear** classical round complexity and one-shot quantum communication complexity [*Kashefi, Wallden '15*]



Towards entanglement-based

Replace preparation device with trusted entanglement + measurement device.

Entanglement-based - Outline

Single server

- Verifier has only measurement device
- Shared entanglement between verifier and server
- Measurement + entanglement *mimic prepare and send*

Entanglement-based - Outline

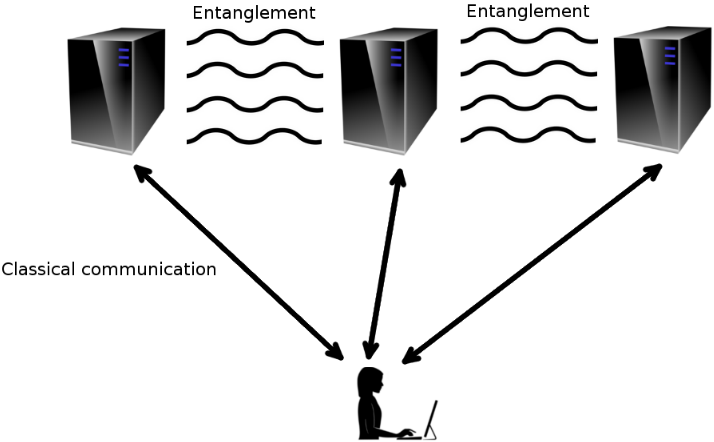
Single server

- Verifier has only measurement device
- Shared entanglement between verifier and server
- Measurement + entanglement *mimic prepare and send*

Multiple servers

- Verifier has no quantum device
- Servers share entanglement and *cannot communicate*
- Verifier interacts classically with servers

Multiple servers



Multiple servers price of trust

Constant number of servers

- Protocol: [*Reichardt, Unger, Vazirani '12*]
- Round complexity: $O(N^{8192})$
- Based on rigidity of CHSH games
- Certifying entanglement and measurements
- Huge overhead for establishing tensor product of Bell pairs

Multiple servers price of trust

Constant number of servers

- Protocol: [*Reichardt, Unger, Vazirani '12*]
- Round complexity: $O(N^{8192})$
- Based on rigidity of CHSH games
- Certifying entanglement and measurements
- Huge overhead for establishing tensor product of Bell pairs

Linear number of servers

- Protocol: [*McKague '13*]
- Round complexity: $O(N^{22})$
- Based on self-testing graph states
- Reduced overhead because of assumed tensor product structure

Multiple servers price of trust

Constant number of servers

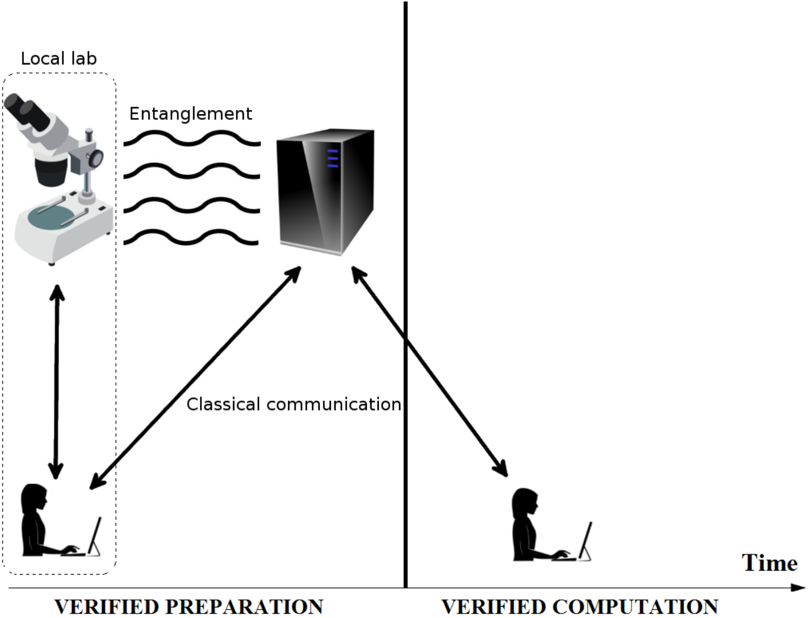
- Protocol: [*Reichardt, Unger, Vazirani '12*]
- Round complexity: $O(N^{8192})$
- Based on rigidity of CHSH games
- Certifying entanglement and measurements
- Huge overhead for establishing tensor product of Bell pairs

Linear number of servers

- Protocol: [*McKague '13*]
- Round complexity: $O(N^{22})$
- Based on self-testing graph states
- Reduced overhead because of assumed tensor product structure

Measurements are always untrusted (performed by servers)

Single server



Single server price of trust

Protocols: [*Gheorghiu, Kashefi, Wallden '15*], [*Hajdušek, Pérez-Delgado, Fitzsimons '15*], [*Gheorghiu, Wallden, Kashefi '15*]

Single server price of trust

Protocols: [*Gheorghiu, Kashefi, Wallden '15*], [*Hajdušek, Pérez-Delgado, Fitzsimons '15*], [*Gheorghiu, Wallden, Kashefi '15*]

Entanglement / Measurements	Trusted	Semi-trusted (i.i.d.)	Untrusted
Trusted	$O(N)$	$O(N^4 logN)$	$O(N^{13} log(N))$
Untrusted	$O(N^4 logN)$	$O(N^4 logN)$	$O(N^{64})$

Bounds are not tight!

Single server price of trust

Protocols: [*Gheorghiu, Kashefi, Wallden '15*], [*Hajdušek, Pérez-Delgado, Fitzsimons '15*], [*Gheorghiu, Wallden, Kashefi '15*]

Measurements \ Entanglement	Trusted	Semi-trusted (i.i.d.)	Untrusted
Trusted	$O(N)$	$O(N^4 logN)$	$O(N^{13} log(N))$
Untrusted	$O(N^4 logN)$	$O(N^4 logN)$	$O(N^{64})$

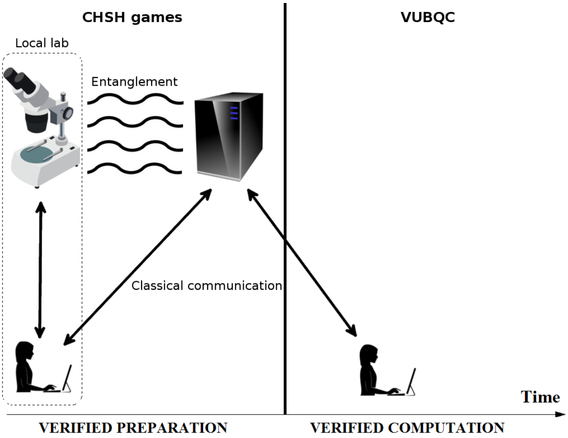
Bounds are not tight!

Assuming untrusted entanglement...

Untrusted measurements $\rightarrow$ **device independence**
Trusted measurements $\rightarrow$ **one-sided device independence**

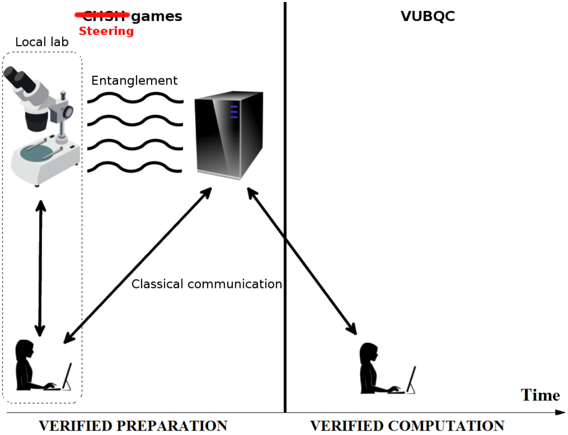
Device-independent single server verification

- Based on rigidity of CHSH games [*Reichardt, Unger, Vazirani '12*]
- Certify tensor product of Bell pairs
- Certify correct measurements
- Verified preparation = prepare input states
- Verified computation = FK protocol
- Similar in multi server setting



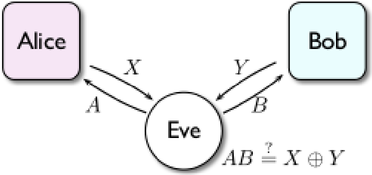
One-sided device-independent single server verification

- Based on rigidity of steering games [*Gheorghiu, Wallden, Kashefi '16*]
- Certify tensor product of Bell pairs
- Certify correct server measurements
- Analogous to DI protocols
- Reduced overhead because of added trust



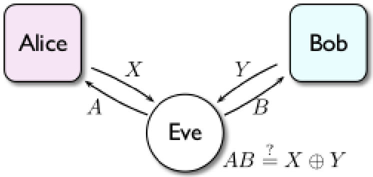
Rigidity

- Saturating correlations determines states and strategy
- Up to local isometry
- DI $\rightarrow$ non-local correlations (CHSH)
- 1sDI $\rightarrow$ steering correlations



Rigidity

- Saturating correlations determines states and strategy
- Up to local isometry
- DI $\rightarrow$ non-local correlations (CHSH)
- 1sDI $\rightarrow$ steering correlations



Proof idea:

1. Self-testing with i.i.d. states
2. Removing i.i.d. assumption (one shot rigidity)
3. Game-based induction $\rightarrow$ state and strategy determination

Self-testing i.i.d. states

Suppose Alice and Bob share many copies of a state $|\psi\rangle$

Alice measures observables A'_0, A'_1

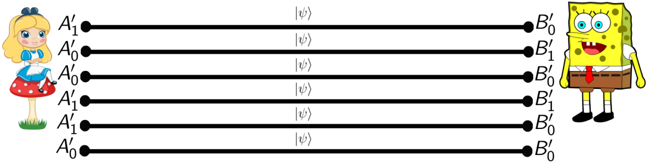
Bob measures observables B'_0, B'_1

Self-testing i.i.d. states

Suppose Alice and Bob share many copies of a state $|\psi\rangle$

Alice measures observables A'_0, A'_1

Bob measures observables B'_0, B'_1

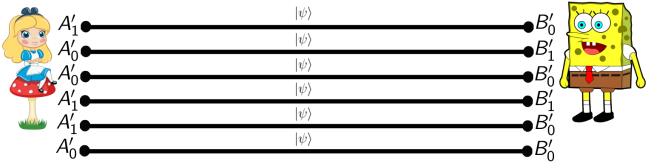


Self-testing i.i.d. states

Suppose Alice and Bob share many copies of a state $|\psi\rangle$

Alice measures observables A'_0, A'_1

Bob measures observables B'_0, B'_1

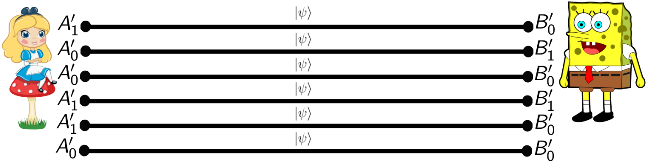


$$\langle\psi| A'_0 B'_0 + A'_0 B'_1 + A'_1 B'_0 - A'_1 B'_1 |\psi\rangle \geq 2\sqrt{2} - \epsilon \tag{1}$$

$$\langle\psi| A_0 B'_0 + A_1 B'_1 |\psi\rangle \geq 2 - \epsilon \tag{2}$$

Self-testing i.i.d. states

Suppose Alice and Bob share many copies of a state $|\psi\rangle$
Alice measures observables A'_0, A'_1
Bob measures observables B'_0, B'_1



$$\langle\psi| A'_0 B'_0 + A'_0 B'_1 + A'_1 B'_0 - A'_1 B'_1 |\psi\rangle \geq 2\sqrt{2} - \epsilon \qquad (1)$$

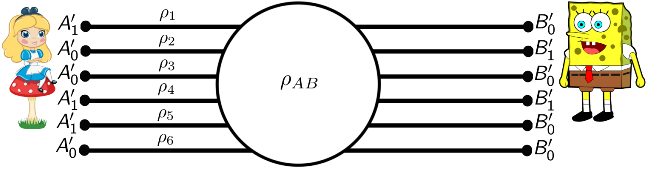
$$\langle\psi| A_0 B'_0 + A_1 B'_1 |\psi\rangle \geq 2 - \epsilon \qquad (2)$$

Self-testing theorem

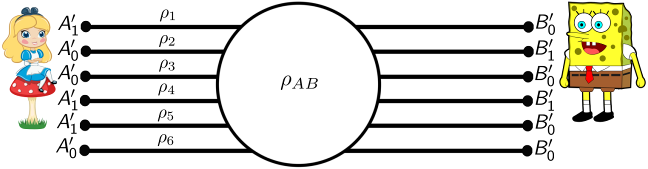
If inequality 1 is satisfied in the DI case, or inequality 2 in the 1sDI case, then there exists a local isometry $\Phi = \Phi_A \otimes \Phi_B$ such that, for all $M'_A \in \{I, A'_0, A'_1\}$, $N'_B \in \{I, B'_0, B'_1\}$:

$$||\Phi(M'_A N'_B |\psi\rangle) - |junk\rangle M_A N_B |\phi_+\rangle || \leq O(\sqrt{\epsilon})$$

Removing i.i.d.

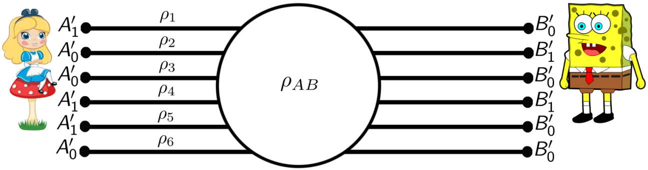


Removing i.i.d.



1. Model measurement process as a *martingale*
2. Use Azuma-Hoeffding inequality
3. Observed correlation close to true correlation for averaged state: $\rho_{avg} = \frac{1}{K}\sum_i \rho_i$
4. From self-testing ρ_{avg} is close to $|\phi_+\rangle$ (under isometry)
5. Optimization argument implies a randomly chosen ρ_i is also close to $|\phi_+\rangle$

Removing i.i.d.



1. Model measurement process as a *martingale*
2. Use Azuma-Hoeffding inequality
3. Observed correlation close to true correlation for averaged state: $\rho_{avg} = \frac{1}{K}\sum_i \rho_i$
4. From self-testing ρ_{avg} is close to $|\phi_+\rangle$ (under isometry)
5. Optimization argument implies a randomly chosen ρ_i is also close to $|\phi_+\rangle$

Non-i.i.d. self-testing theorem

If Alice and Bob's correlation saturates the CHSH/steering inequality to order ϵ then for a randomly chosen i:

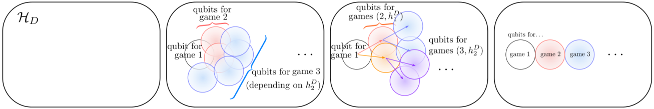
$$||\Phi(\mathcal{E}'_{AB}(\rho_i)) - \mathcal{E}_{AB}(|\phi_+\rangle\langle\phi_+|)|| \leq O(\epsilon^{1/6})$$

State and strategy determination

Suppose we play K games to certify one Bell pair.
Does playing NK games certify N pairs?

Suppose we play K games to certify one Bell pair.
Does playing NK games certify N pairs?

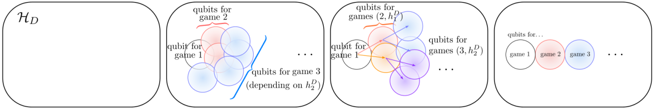
Not implicitly, because of overlap...



(a) General strategy (b) Single-qubit ideal strategy (c) Multi-qubit ideal strategy (d) Ideal strategy

Suppose we play K games to certify one Bell pair. Does playing NK games certify N pairs?

Not implicitly, because of overlap...



(a) General strategy (b) Single-qubit ideal strategy (c) Multi-qubit ideal strategy (d) Ideal strategy

- Assume the state and strategy of Alice and Bob is $\mathcal{S}_{real} = (\rho_{AB}, \mathcal{E}'_A, \mathcal{E}'_B)$
- Assume the ideal strategy is $\mathcal{S}_{id} = (\otimes |\phi_+\rangle, \mathcal{E}_A, \mathcal{E}_B)$
- Can consider intermediate strategies $\mathcal{S}$ (e.g. Alice guesses Bob's outcomes)
- Use non-i.i.d. self testing to show $\mathcal{S}_{real} \approx \mathcal{S} \approx \mathcal{S}_{id}$
- Closeness **depends on whether Alice is trusted or not**!
- DI $\rightarrow O(N^{64})$, 1sDI $\rightarrow O(N^{13} log(N))$

Necessity of Bell pairs

Assume we have an entanglement-based protocol, $\mathcal{P}$, satisfying the following:

- One-sided device-independent
- Shared entangled state consists of copies of 2-qubit state ρ_{VP}
- Blindness, $Tr_V(\rho_{VP}) = \rho_P = I/2$
- Arbitrary quantum input

Necessity of Bell pairs

Assume we have an entanglement-based protocol, $\mathcal{P}$, satisfying the following:

- One-sided device-independent
- Shared entangled state consists of copies of 2-qubit state ρ_{VP}
- Blindness, $Tr_V(\rho_{VP}) = \rho_P = I/2$
- Arbitrary quantum input

Maximal entanglement theorem

In $\mathcal{P}$, ρ_{VP} is maximally entangled.

Necessity of Bell pairs

Assume we have an entanglement-based protocol, $\mathcal{P}$, satisfying the following:

- One-sided device-independent
- Shared entangled state consists of copies of 2-qubit state ρ_{VP}
- Blindness, $Tr_V(\rho_{VP}) = \rho_P = I/2$
- Arbitrary quantum input

Maximal entanglement theorem

In $\mathcal{P}$, ρ_{VP} is maximally entangled.

Proof: From the constraints, we find that:

$$\rho_{VP} = \frac{1}{2(|f|^2+1)} \begin{pmatrix} |f|^2 & f & f & e^{i\phi_1}|f|^2 \\ f^* & 1 & e^{i\phi_2} & -f \\ f^* & e^{-i\phi_2} & 1 & -f \\ e^{-i\phi_1}|f|^2 & -f^* & -f^* & |f|^2 \end{pmatrix}$$

$Tr(\rho_{VP}^2) = 1$ and $Tr_V(\rho_{VP}) = I/2 \rightarrow \rho_{VP}$ is maximally entangled!

Conclusions

Prepare and send $\rightarrow O(N)$

Conclusions

Prepare and send $\rightarrow O(N)$

Online, measurement-only $\rightarrow O(N)$

Conclusions

Prepare and send $\rightarrow O(N)$

Online, measurement-only $\rightarrow O(N)$

Entanglement-based, single server

Measurements \ Entanglement	Trusted	Semi-trusted (i.i.d.)	Untrusted
Trusted	$O(N)$	$O(N^4 logN)$	$O(N^{13} log(N))$
Untrusted	$O(N^4 logN)$	$O(N^4 logN)$	$O(N^{64})$

Conclusions

Prepare and send $\rightarrow$ $O(N)$

Online, measurement-only $\rightarrow$ $O(N)$

Entanglement-based, single server

Measurements \ Entanglement	Trusted	Semi-trusted (i.i.d.)	Untrusted
Trusted	$O(N)$	$O(N^4 logN)$	$O(N^{13} log(N))$
Untrusted	$O(N^4 logN)$	$O(N^4 logN)$	$O(N^{64})$

Entanglement-based, multiple servers

Constant number of servers $\rightarrow$ $O(N^{8192})$
Linear number of servers $\rightarrow$ $O(N^{22})$

Open problems

- Tight bounds?
- Bounded quantum memory adversary?
- No communication vs. space-like separation
- Fault tolerance?
- Classical client single server verification?

References and further reading

Presentation based primarily on this work:
[Gheorghiu, Kashefi, Wallden, '15] - arXiv:1512.07401

Other relevant works:

[Hoban, Šupić '16] - arXiv:1601.01552
[Kashefi, Wallden '15] - arXiv:1510.07408
[Kapourniotis, Dunjko, Kashefi '15] - arxiv:1506.06943
[Gheorghiu, Kashefi, Wallden '15] - arXiv:1502.02571
[Reichardt, Unger, Vazirani '12] - arXiv:1209.0448
[Morimae '12] - arXiv:1208.1495
[McKague, Yang, Scarani '12] - arXiv:1203.2976