Quantum Protocols: Updating and Using the Zoo

Harold Ollivier

2019-11-12

Outline

Part I: Updating the zoo

Part II: Using the zoo

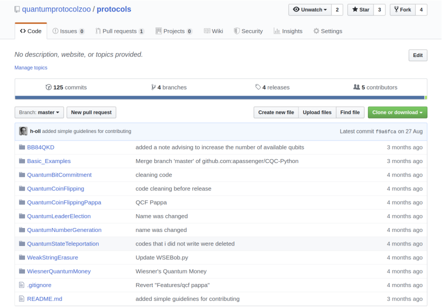
Part III: Going further

Conclusion

Part I: Updating the zoo

What's new: Code

- 9 protocols available
- 2 more under review
- more to come thanks to the hackathon
- higher-order functions



quantumprotocolzoo / **protocols**

No description, website, or topics provided.

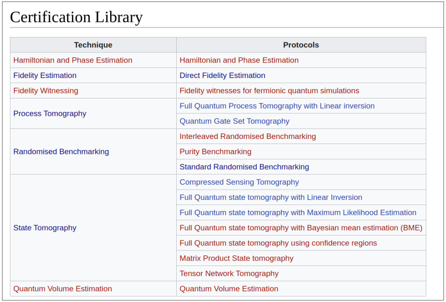
h-oll added simple guidelines for contributing — Latest commit `f9a6fca` on 27 Aug

BB84QKD	added a note advising to increase the number of available qubits	3 months ago
Basic_Examples	Merge branch 'master' of github.com:apassenger/CQC-Python	3 months ago
QuantumBitCommitment	cleaning code	4 months ago
QuantumCoinFlipping	code cleaning before release	4 months ago
QuantumCoinFlippingPappa	QCF Pappa	4 months ago
QuantumLeaderElection	Name was changed	4 months ago
QuantumNumberGeneration	name was changed	4 months ago
QuantumStateTeleportation	codes that i did not write were deleted	4 months ago
WeakStringErasure	Update WSEBob.py	4 months ago
WiesnerQuantumMoney	Wiesner's Quantum Money	4 months ago
.gitignore	Revert "Features/qcf pappa"	4 months ago
README.md	added simple guidelines for contributing	3 months ago

`https://www.github.com/quantumprotocolzoo/protocols`

What's new: Certification library

- 7 classes
- 7 protocols described
- 9 more being worked out

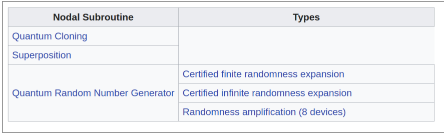


Certification Library

Technique	Protocols
Hamiltonian and Phase Estimation	Hamiltonian and Phase Estimation
Fidelity Estimation	Direct Fidelity Estimation
Fidelity Witnessing	Fidelity witnesses for fermionic quantum simulations
Process Tomography	Full Quantum Process Tomography with Linear inversion
	Quantum Gate Set Tomography
Randomised Benchmarking	Interleaved Randomised Benchmarking
	Purity Benchmarking
	Standard Randomised Benchmarking
State Tomography	Compressed Sensing Tomography
	Full Quantum state tomography with Linear Inversion
	Full Quantum state tomography with Maximum Likelihood Estimation
	Full Quantum state tomography with Bayesian mean estimation (BME)
	Full Quantum state tomography using confidence regions
	Matrix Product State tomography
	Tensor Network Tomography
Quantum Volume Estimation	Quantum Volume Estimation

What's new: Local information processing library

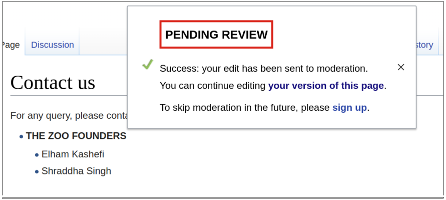
- Planning a separate "local information processing" page
- Distinguish comm. / cert. / local IP



Nodal Subroutine	Types
Quantum Cloning	
Superposition	
Quantum Random Number Generator	Certified finite randomness expansion
	Certified infinite randomness expansion
	Randomness amplification (8 devices)

What's new: 2-step submission process

- Each submission needs approval
- Pages needing approval are visible to logged in users
- Log in!



PENDING REVIEW

✓ Success: your edit has been sent to moderation. ×

You can continue editing **your version of this page**.

To skip moderation in the future, please **sign up**.

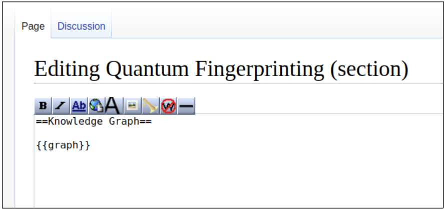
Contact us

For any query, please conta

- **THE ZOO FOUNDERS**
  - Elham Kashefi
  - Shraddha Singh

What’s new: Knowledge graph

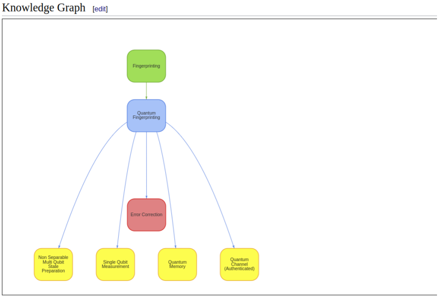
- A page for exploring the full KG
- A local KG per protocol
- Single source of truth
- Soon fixing the I-don’t-see-what-I-should-do problem



Editing Quantum Fingerprinting (section)

```
==Knowledge Graph==

{{graph}}
```



Knowledge Graph [edit]

What's new: Planning a new home page

- Short(er)
- Shows what you can find
- Visual

./draw_me_a_protocol.jpg

What's new: What should you remember?

Contribute, promote, use!

- `https://wiki.veriqloud.fr`
- `https://www.github.com/quantumprotocolzoo/protocols`

Quantum
Protocol
Zoo

Part II: Using the zoo

Using it: It works!

- 6 locations
- About 80 participants
- Impressive presentations

Using it: What did we learn?

It is useful

- Enough to find the challenges
- (Almost) enough to code

It needs expansion

- More protocols
- More code (examples + higher-order functions)
- More details (links to security proof, type of security achieved)

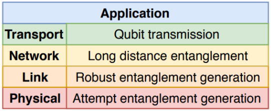
Using it: Planning the future

The "Delft" approach...

- Simulate
- Build network layers on what you can do

... raises some challenges

- Experimentalists want to know if they'll publish in Nature!
  - Simulate or not simulate?
- Reconciling the use of network model layers with security proofs
  - Calling lower-layers for services implies decomposing protocols
  - Is it legitimate ?



Application	
Transport	Qubit transmission
Network	Long distance entanglement
Link	Robust entanglement generation
Physical	Attempt entanglement generation

Using it: Planning the future

Adopt a top-down approach

- Applications is what matters
- Proper services should be provided (experimentalists will know if it's worth working on a protocol)
- Abstract crypto as much as possible (quantum networks should be secure by design)

Now better than later!

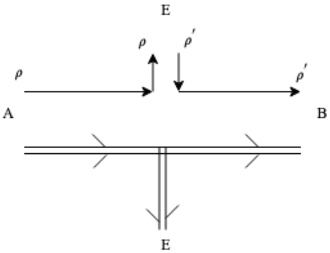
Part III: Going further

Direct link or teleportation ?

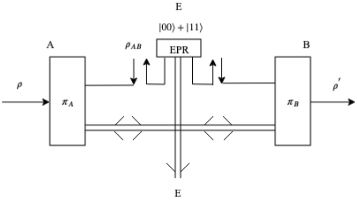
- Protocols make use of direct links between players:
    - Send qubit from A to B
- Network stack is not planning to send qubits but to teleport them
    - Is it working ?
    - Does it compose ?
- And if it's OK doesn't it use sources of EPR pairs ?
    - How do I get one ?
    - Are all implementations OK ?

Constructing a Direct Quantum Link with Teleportation

Direct Quantum Link

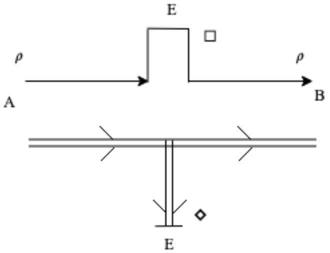


Teleportation

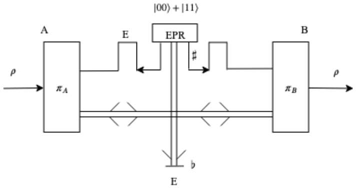


Teleportation correctly implements Direct Quantum Link

Direct Quantum Link



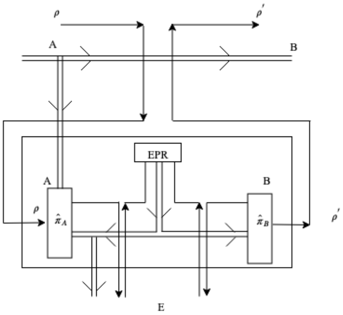
Teleportation



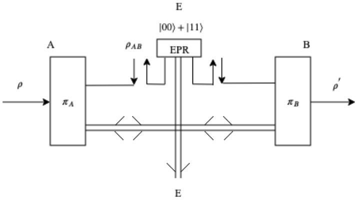
When no one is listening, teleportation works (perfectly)

Teleportation securely implements Direct Quantum Link

Direct Quantum Link + simulator



Teleportation

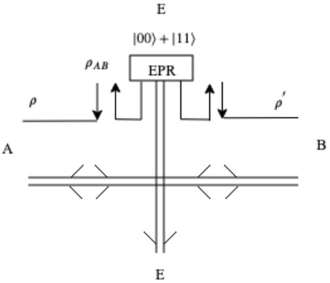


Isn't it cheating?
No! The Direct Quantum Link does not achieve any security; the simulator rightfully gets the to-be-transmitted quantum state.

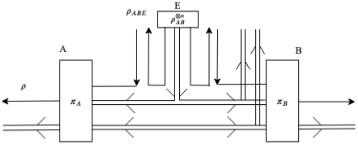
Constructing a perfect EPR-source from Distillation

Using a perfect EPR-source is no fun

Perfect EPR-source



Distillation



More on distillation (1/2)

3-step process

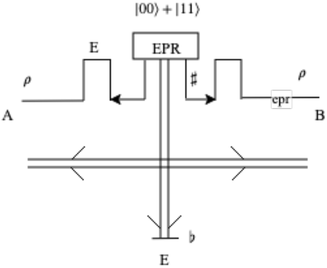
- Apply Twirl + Symmetrisation
- Verify that fidelity is what you expect or abort
- Choose and apply a suitable distillation protocol

More on distillation (2/2)

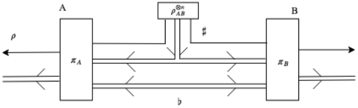
- Initial state: $\rho_{ABE} \in \mathcal{H}_2^{\otimes n} \otimes \mathcal{H}_2^{\otimes n} \otimes \mathcal{H}_E$
- Entering protocol: $\rho = \mathrm{Tr}_E(\rho_{ABE}) \in \mathcal{H}_2^{\otimes n} \otimes \mathcal{H}_2^{\otimes n}$
- Twirl + Symmetrisation: $\rho_1 = \mathcal{E}_1(\rho) \in \mathcal{H}_2^{\otimes n-m} \otimes \mathcal{H}_2^{\otimes n-m}$
- Fidelity est.: $\rho_2 = \mathcal{E}_2(\rho_1) \in \mathcal{H}_2^{\otimes n-m-l} \otimes \mathcal{H}_2^{\otimes n-m-l} \oplus \mathcal{H}_\perp$
- Distillation $\rho_3 = \mathcal{E}_3(\rho_2) \in \mathcal{H}_2^{\otimes n-m-l-k} \otimes \mathcal{H}_2^{\otimes n-m-l-k} \oplus \mathcal{H}_\perp$

Distillation correctly implements a perfect EPR-source (1/2)

Perfect EPR-source



Distillation



Distillation correctly implements a perfect EPR-source (2/2)

- Twirl + Symmetrization

$$\rho_1 = \rho_{\text{source}}^{\otimes n-m}$$

- Finite precision fidelity estimation

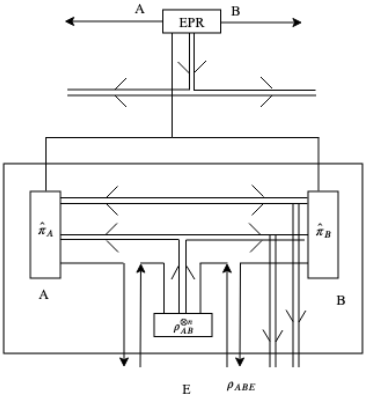
$$\rho_2 \approx (1 - p_\perp)\rho_W^{\otimes n-m-l} + p_\perp \left|\perp\right\rangle \left\langle\perp\right|$$

- Strictly positive rate distillation

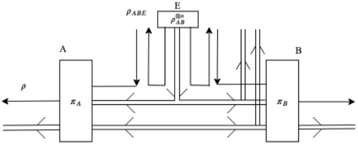
$$\rho_3 \approx (1 - p'_\perp) \left|\Phi^+\right\rangle \left\langle\Phi^+\right|^{\otimes n-m-l-k} + p'_\perp \left|\perp\right\rangle \left\langle\perp\right|$$

Distillation securely implements a perfect EPR-source (1/3)

Perfect EPR-source + simulator



Distillation



Distillation securely implements a perfect EPR-source (2/3)

We should be looking at ρ_{ABE}, but in fact we can get away by (almost only) looking at ρ_{AB}!

- Tracing out

$$\rho = \mathrm{Tr}_E(\rho_{ABE})$$

- Twirl + Symmetrization

$$\rho_1 \approx \rho_{2\times 2}^{\otimes n-m}$$

- Finite precision fidelity estimation

$$\rho_2 \approx (1-p_\perp)\rho_W^{\otimes n-m-l} + p_\perp \left|\perp\right\rangle\left\langle\perp\right|$$

- Strictly positive rate distillation

$$\rho_3 \approx (1-p'_\perp)\left|\Phi^+\right\rangle\left\langle\Phi^+\right|^{\otimes n-m-l-k} + p'_\perp \left|\perp\right\rangle\left\langle\perp\right|$$

Distillation securely implements a perfect EPR-source (3/3)

We should be looking at ρ_{ABE}, but in fact we can get away by (almost only) looking at ρ_{AB}!

- The analysis without E gives

$$(\mathcal{E}_3 \circ \mathcal{E}_2 \circ \mathcal{E}_1)\mathrm{Tr}_E \rho_{ABE} \approx (1 - p'_\perp) \left|\Phi^+\right\rangle \left\langle\Phi^+\right|^{\otimes n-m-l-k} + p'_\perp \left|\perp\right\rangle \left\langle\perp\right|$$

- Gentle measurement theorem implies (because we are next to a pure state when pairs are produced)

$$((\mathcal{E}_3 \circ \mathcal{E}_2 \circ \mathcal{E}_1) \otimes \mathrm{Id}_E)\rho_{ABE} \approx ((1 - p'_\perp) \left|\Phi^+\right\rangle \left\langle\Phi^+\right|^{\otimes n-m-l-k}$$

$$+ \mathrm{p}'_\perp \left|\perp\right\rangle \left\langle\perp\right|) \otimes \mathrm{Tr}_{AB}(\rho_{ABE})$$

Conclusion

- We have a great tool to expand at `https://wiki.veriqloud.fr`
- It's directly useful to the community and also to ourselves
- Expand this kind of analysis
  - Look at other elementary functions
  - Take noise into account