2019.11.09. SCRATCH.

Q Protocol Zoo.

- What's new?

Science
1) Some more code with Gödzle.
2) New Protocols with certification library.
3) Planning to move some subroutines to specific pages

Pres.
4) Submission 2-step process.
5) Knowledge graph + decomposition given by Natansh now automated.
6) Planning a better home page

- A grand scale experiment:
  - Photo of Hackathon.
- What did we learn?
  - It is useful: 6 locations did use the Zoo to find and code their challenges
  - It needs to be expanded:
    - More protocols
    - More consistency
    - further doc: have links to security proofs
    - Summary of the security obtained.
    -

2019.11.09 - SCRATCH - B

What else can we plan for the protocol too?

- [redacted]
- [redacted] helping experimentalists to approach protocols

↳ what quality should I achieve for my [redacted] devices?

↳ asking this is [redacted] about composition

↳ we should provide the right decomposition

(It's also the case for the full network layer model:

- we ask for a given service, [redacted].
- is the service composable?) → picture of network layer. (quantum - classical).

⇒ We want to promote a top-down approach:

[redacted]

[redacted] + you ask a service to the layer for a purpose: [redacted]

+ you cannot build a bottom-up stack and hoping that the application layer will get the proper service

[redacted]

+ you decompose your application into freq. used elementary functions

+ show that doing so gives the proper application.

⇒ Apply the [redacted] spirit of the Foo to AC and give a value to what the quality of devices ~~will~~ shall be.

2019.11.09. SCRATCH. C

- Lets do it:
  - most used functionnality in q. protocols: send qubit from A to B.
  - why is it important? : ~~[illegible]~~ well experimentalists tell us they plan to teleport... but can I do this without endangering security?

- Constructing direct quantum channel with teleportation.
  - Direct Q. Channel. : no security.
  - Teleportation : perfect source but ~~[illegible]~~ is in control of E.

- Correctness.
  - Direct Q Channel.
  - Teleport.

- Security
  - Direct Q. Channel
  - Teleportation

...

2019.11.09 - D. SCRATCH

- We have a first decomposition but not very interesting.

  - Lets go one step further and decompose the EPR source.

- Construction.

  - Perfect EPR.
  - "Distillation."

    ↳ 1) Twirl + Symmetrization + Partial Trace. $\mathcal{E}_1$ acting on $\mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n} \longrightarrow \mathcal{H}_A^{\otimes n-m} \otimes \mathcal{H}_B^{\otimes n-m}$

    2) Fidelity verification. $\mathcal{E}_2$ acting on $\mathcal{H}_A^{\otimes n-m} \otimes \mathcal{H}_B^{\otimes n-m} \longrightarrow \mathcal{H}_A^{\otimes n-m-\ell} \otimes \mathcal{H}_B^{\otimes n-m-\ell} \otimes \mathcal{H}_2^{\otimes}$ pair

    3) Distillation. $\mathcal{E}_3$ acting on.

    $$\mathcal{H}_A^{\otimes n-m-\ell} \otimes \mathcal{H}_B^{\otimes n-m-\ell} \longrightarrow \mathcal{H}_A^{\otimes n-m-\ell-k} \otimes \mathcal{H}_B^{\otimes n-m-\ell-k} \otimes \mathcal{H}_2^{\otimes 2}$$

    4) Labelling.

Show Pictures.

- Correctness.

  * if I have a given source for which I have a working distill. protocol, I will almost always perfectly distill the expected # of pairs

2019.11.03 - E SCRATCH

Security

Setting - Perfect EPR. + Simul.

- Distill.

$\Rightarrow \rho_{ABE} \longrightarrow \mathcal{E}_4(\mathcal{E}_3(\mathcal{E}_2(\mathcal{E}_1(\rho_{ABE}))))$: distill. proto.

$= \rho^{(3)}_{ABE} \cdot (1-p_\perp) + p_\perp |\perp\rangle\langle\perp|$

$\mathcal{F}(\mathcal{E}_3(\mathcal{E}_2(\mathcal{E}_1(\rho_{ABE}))))$:

$= EPR \cdot (1-p_\perp) + p_\perp |\perp\rangle\langle\perp|$.

$\mathcal{F}$ is measuring the # of almost perfect EPR pairs produced by $\mathcal{E}_3 \circ \mathcal{E}_2 \circ \mathcal{E}_1$ and emitting that # of Perfect EPR's

$$\Rightarrow \| \mathcal{E}_4[\mathcal{E}_3 \circ \mathcal{E}_2 \circ \mathcal{E}_1(\rho_{ABE})] - \mathcal{F}[\mathcal{E}_3 \circ \mathcal{E}_2 \circ \mathcal{E}_1(\rho_{ABE})] \|$$

$$\| \mathcal{E}_4[\rho^3_{ABE}] - \mathcal{F}[\rho^3_{ABE}] \|$$

$$= \| \underbrace{\mathcal{E}_4[\rho^3_{ABE}] - \mathcal{E}_4[EPR]} + \mathcal{E}_4[EPR] - \mathcal{F}[\rho^3_{ABE}] + \mathcal{F}[EPR] - \mathcal{F}[EPR] \|$$

$$\leq \| \mathcal{E}_4(\rho^3_{ABE}) - \mathcal{E}_4(EPR) \| + \underbrace{\| \mathcal{F}(\rho^3_{ABE}) - \mathcal{F}(EPR) \|}_{=0}$$

$$\| \rho^3_{ABE} - EPR \| + \underbrace{\| \mathcal{E}_4(EPR) - \mathcal{F}(EPR) \|}_{=0}$$

$$\leq \| \rho^3_{ABE} - EPR \|$$

$$\| \mathcal{E}^3(\rho^{(2)}_{ABE}) - EPR^{\otimes n-m-l-k} \|.$$

given by $\mathcal{E}$. fixed param. of the protocol

given. that I have the correct input.

$$\| \underbrace{\mathcal{E}^3(\rho^{(2)}_{ABE}) - \mathcal{E}^3(\rho^{perfect}_{AB})}_{\rho_{AB}^{\otimes n-m-l}} + \underbrace{\mathcal{E}^3(\rho^{perf}_{AB}) - EPR}_{} \|.$$

$$\leq \| \underbrace{\quad}_{} \| + \| \underbrace{\quad}_{\varepsilon.} \|.$$

$$\| \rho^{2}_{ABE} - \rho^{perf}_{AB} \|.$$

2019.11.09. SCRATCH E

Security:

- Show setting.

- $\rho_{ABE} \xrightarrow{\mathcal{E}_{\phi}^{(1)}} \rho_{ABE}^{(1)} \xrightarrow{\mathcal{E}_{L}^{(2)}} \rho_{ABE}^{(2)} \cdot (1-p_\perp^{(1)}) + p_\perp^{(1)} |\perp\rangle\langle\perp|$

$\xrightarrow{\mathcal{E}^{(3)}}$ if pass. $\rho_{ABE}^{(3)} (1-p_\perp^{(2)})\cdot(1-p_\perp^{(3)}) + (1-p_\perp^{(2)})\cdot p_\perp^{(3)} |\perp\rangle\langle\perp|$

$+ p_\perp^{(2)} |\perp\rangle\langle\perp|$

$\xrightarrow{\mathcal{E}^{4}}$ if pass. $\rho_{ABE}^{(3)} (1-p_\perp^{(3)})\cdot(1-p_\perp^{(2)}) + |\perp\rangle\langle\perp| \cdot \left((1-p_\perp^{2})\cdot p_\perp^{3} + p_\perp^{2}\right)$

$(\mathcal{E}^{3}\circ\mathcal{E}^{2}\circ\mathcal{E}^{1})$

- $\rho_{ABE} \longrightarrow \rho_{ABE}^{(3)} (1-p_\perp^{(2)})\cdot(1-p_\perp^{(3)}) + |\perp\rangle\langle\perp| \cdots$

$\xrightarrow{\mathcal{F}}$ $|\phi^+\rangle\langle\phi^+|^{\otimes n-m-l-k} \cdot (1-p_\perp^{2})(1-p_\perp^{(3)})$

$+ \left((1-p_\perp^{2})(p_\perp^{3}) - p_\perp^{2}\right)\cdot |\perp\rangle\langle\perp|$.

difference is bounded by:

$\| \rho_{ABE}^{3} - |\phi^+\rangle\langle\phi^+|^{\otimes n-m-l-k} \|$.

- do all the analysis without $\mathcal{E}$.
- put $\mathcal{E}$ back.

$\| \underbrace{\mathcal{E}^{(3)}(\rho_{ABE}^{(2)}) - \mathcal{E}^{(3)}(\rho_{AB}^{\otimes n-m-k})} + \mathcal{E}^{(3)}(\rho_{AB}^{\otimes n-m-l}) - |\phi^+\rangle\langle\phi^+|^{\otimes \cdots} \|$

$\leq \| \rho_{ABE}^{(2)} - \rho_{AB}^{\otimes n-m-l} \|$

$+ \varepsilon_d$.

$\leq \| \underbrace{\mathcal{E}^{(2)}(\rho_{AB}^{(1)}) - \mathcal{E}^{2}(\rho_{AB}^{\otimes n-m})} + \mathcal{E}^{(2)}(\rho^{\otimes n-m}) - \rho_{AB}^{\otimes m-m-l} \|$

$+ \varepsilon_m$ $+ \varepsilon$.

$\leq \| \underbrace{\mathcal{E}^{(2)}(\rho_{AB}^{(1)}) - \mathcal{E}^{2}(\rho_{AB}^{\otimes n-m})} \| + \varepsilon_d + \varepsilon_F$

$$\leq \varepsilon_d + \varepsilon_F + \underbrace{\| \rho_{AB}^{(1)} - \rho_{AB}^{\otimes n-m} \|}_{64 \frac{n-m}{n}}.$$

- So we have a bound.
- But we cannot say anything on $\| (\rho_{AB\varepsilon}) - (\Phi^+ \times \Phi^+)^{n-m-l-k} \otimes \rho_E \|$.
- ... gentle measurement theorem

$\Rightarrow \delta \sqrt{\ldots}$

then we have the proof