Continuous Time Quantum Cryptography & Communication Complexity

FRIA | research project proposal

Atul Singh Arora

October 28, 2016

Promoter:
Prof Jérémie Roland
Centre for Quantum Information & Communication
Université libre de Bruxelles

Overview

Quantum Information

Quantum Information

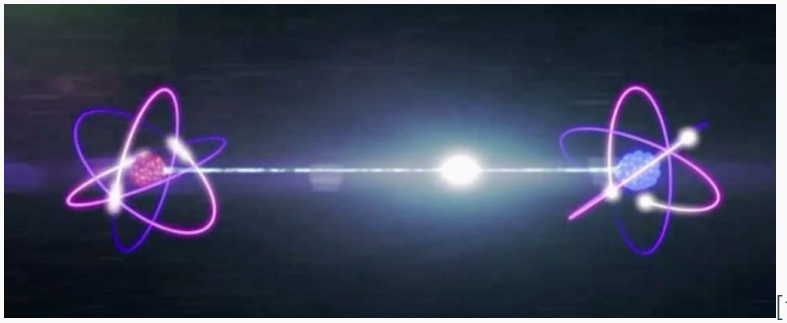
[7]

Bits, 0 and 1.

Quantum Information

[7]

Bits, 0 and 1.

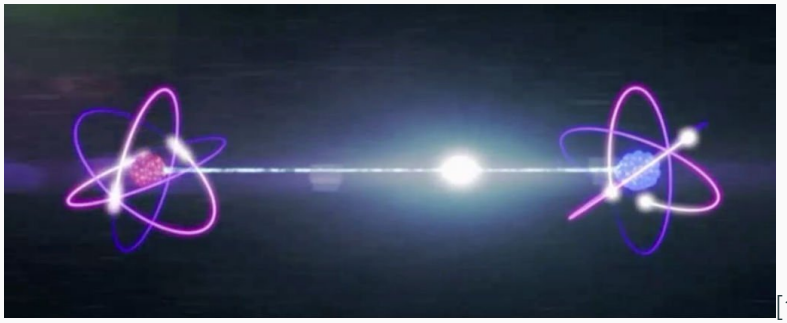

[11]

Qubits, $|0\rangle$ and $|1\rangle$

Quantum Information

[7]

Bits, 0 and 1.


[11]

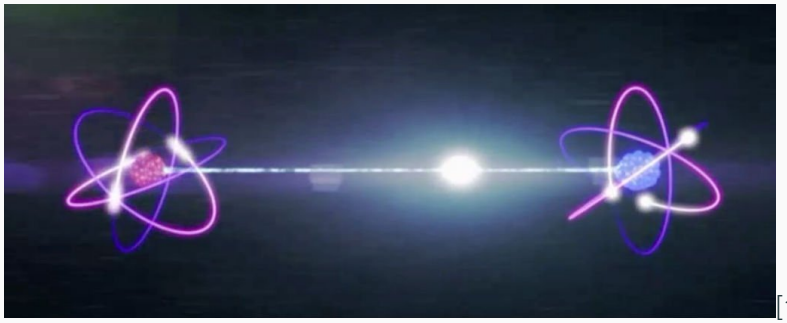
Qubits, $|0\rangle$ and $|1\rangle$

Classical	Quantum
0	
1	
‘Forbidden’	

Quantum Information

[7]

Bits, 0 and 1.


[11]

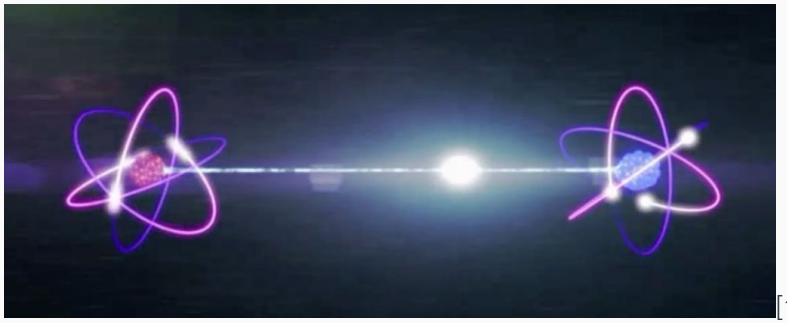
Qubits, $|0\rangle$ and $|1\rangle$

Classical		Quantum	
0	$\rightarrow$	$\|0\rangle$	$\doteq \begin{bmatrix} 1 \\ 0 \end{bmatrix}$
1			
‘Forbidden’			

Quantum Information


[7]

Bits, 0 and 1.


[11]

Qubits, $|0\rangle$ and $|1\rangle$

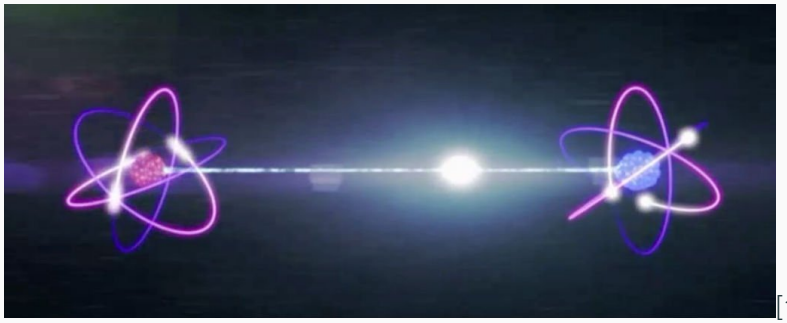
Classical		Quantum	
0	$\rightarrow$	$\|0\rangle$	$\doteq \begin{bmatrix} 1 \\ 0 \end{bmatrix}$
1	$\rightarrow$	$\|1\rangle$	$\doteq \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

'Forbidden'

Quantum Information

[7]

Bits, 0 and 1.


[11]

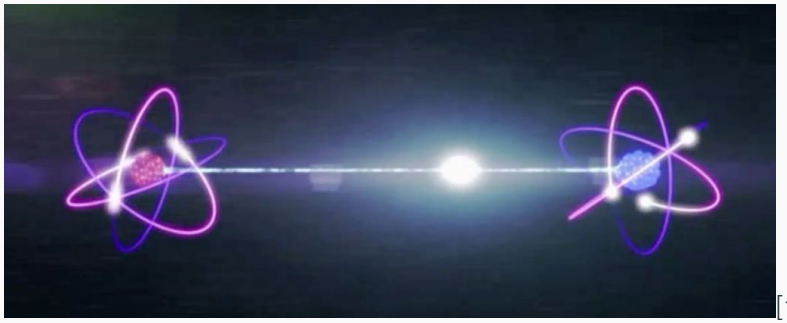
Qubits, $|0\rangle$ and $|1\rangle$

Classical		Quantum	
0	$\rightarrow$	$\|0\rangle$	$\doteq \begin{bmatrix} 1 \\ 0 \end{bmatrix}$
1	$\rightarrow$	$\|1\rangle$	$\doteq \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
'Forbidden'	$\rightarrow$	$\|\psi\rangle = \alpha \|0\rangle + \beta \|1\rangle$	$\doteq \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

Quantum Information

[7]

Bits, 0 and 1.


[11]

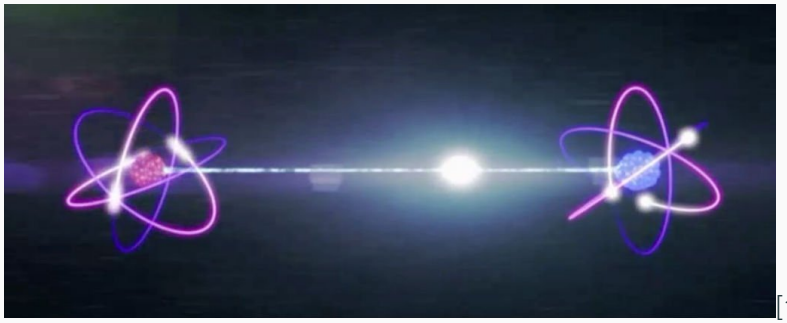
Qubits, $|0\rangle$ and $|1\rangle$

Classical		Quantum	
0	$\rightarrow$	$\|0\rangle$	$\doteq \begin{bmatrix} 1 \\ 0 \end{bmatrix}$
1	$\rightarrow$	$\|1\rangle$	$\doteq \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
'Forbidden'	$\rightarrow$	$\|\psi\rangle = \alpha \|0\rangle + \beta \|1\rangle$	$\doteq \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

Quantum Information

[7]

Bits, 0 and 1.


[11]

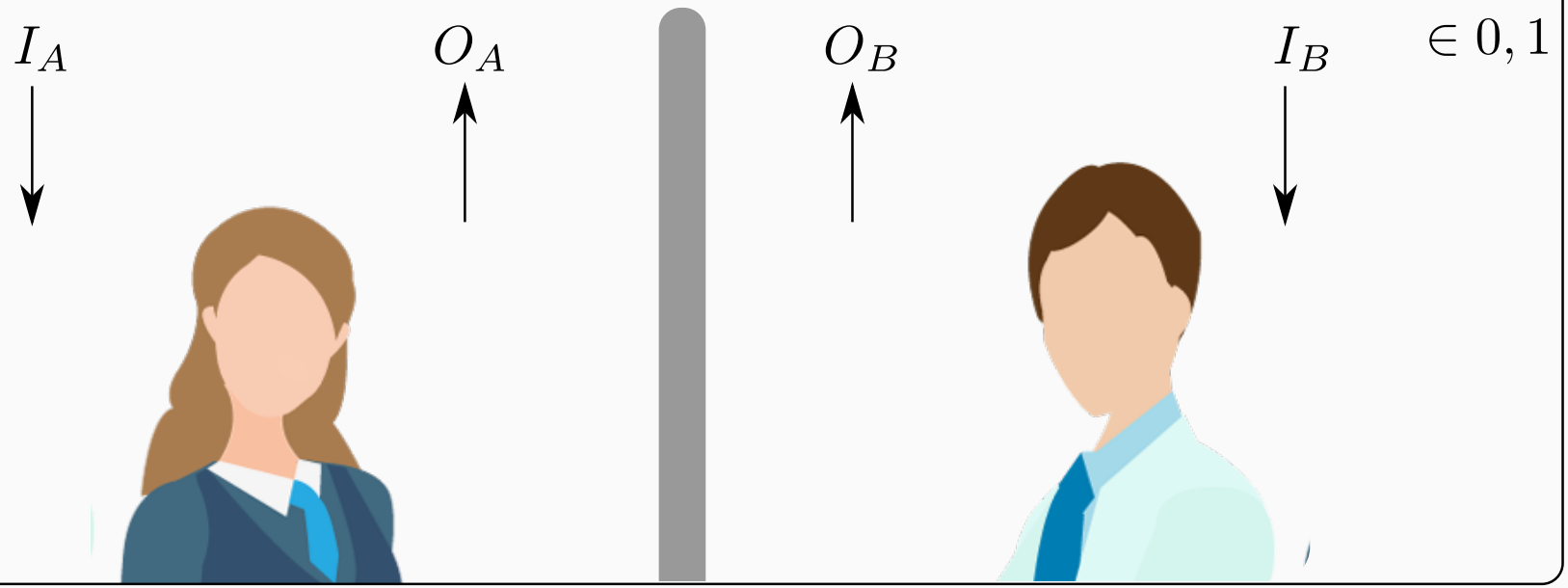
Qubits, $|0\rangle$ and $|1\rangle$

Classical $\rightarrow$ Quantum: Computational Power

e.g. Factorisation and Secure Key Distribution [20] [15]

If $f(I_A, I_B) = 1$ then anti-correlate
else correlate

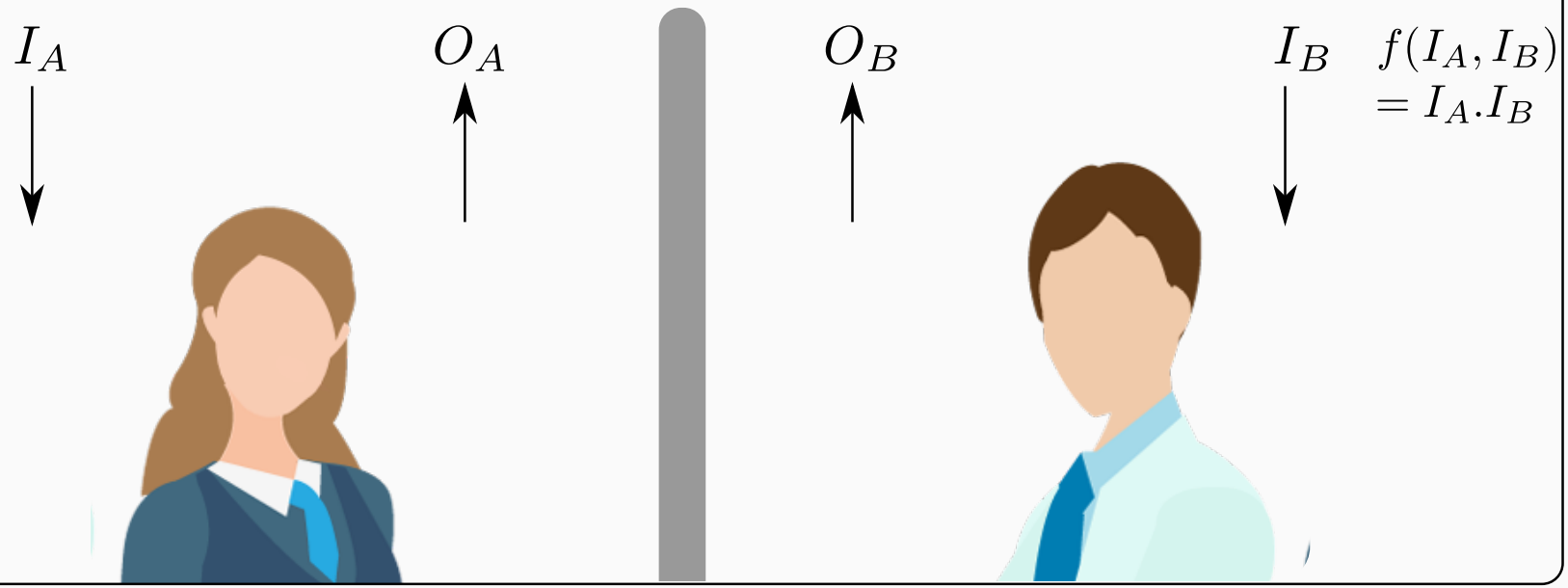
For e.g. $f(I_A, I_B) = I_A.I_B$



[1, 5, 6, 4]

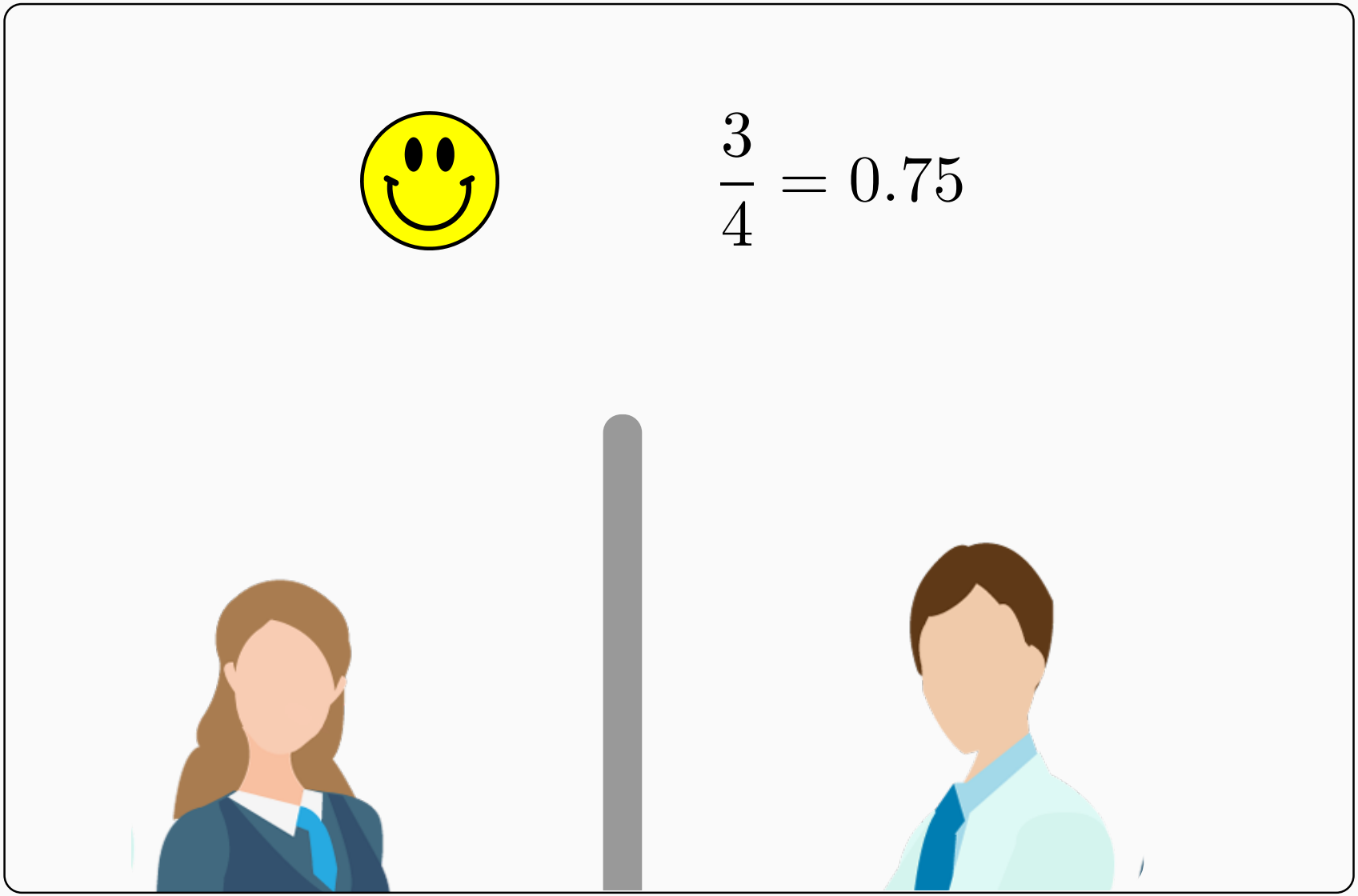
Characterising Quantum

1	1,0	anti-correlated	0,1	1	1
0	1,0	correlated	1,0	1	0
1	1,0	correlated	1,0	0	0
0	1,0	correlated	1,0	0	0



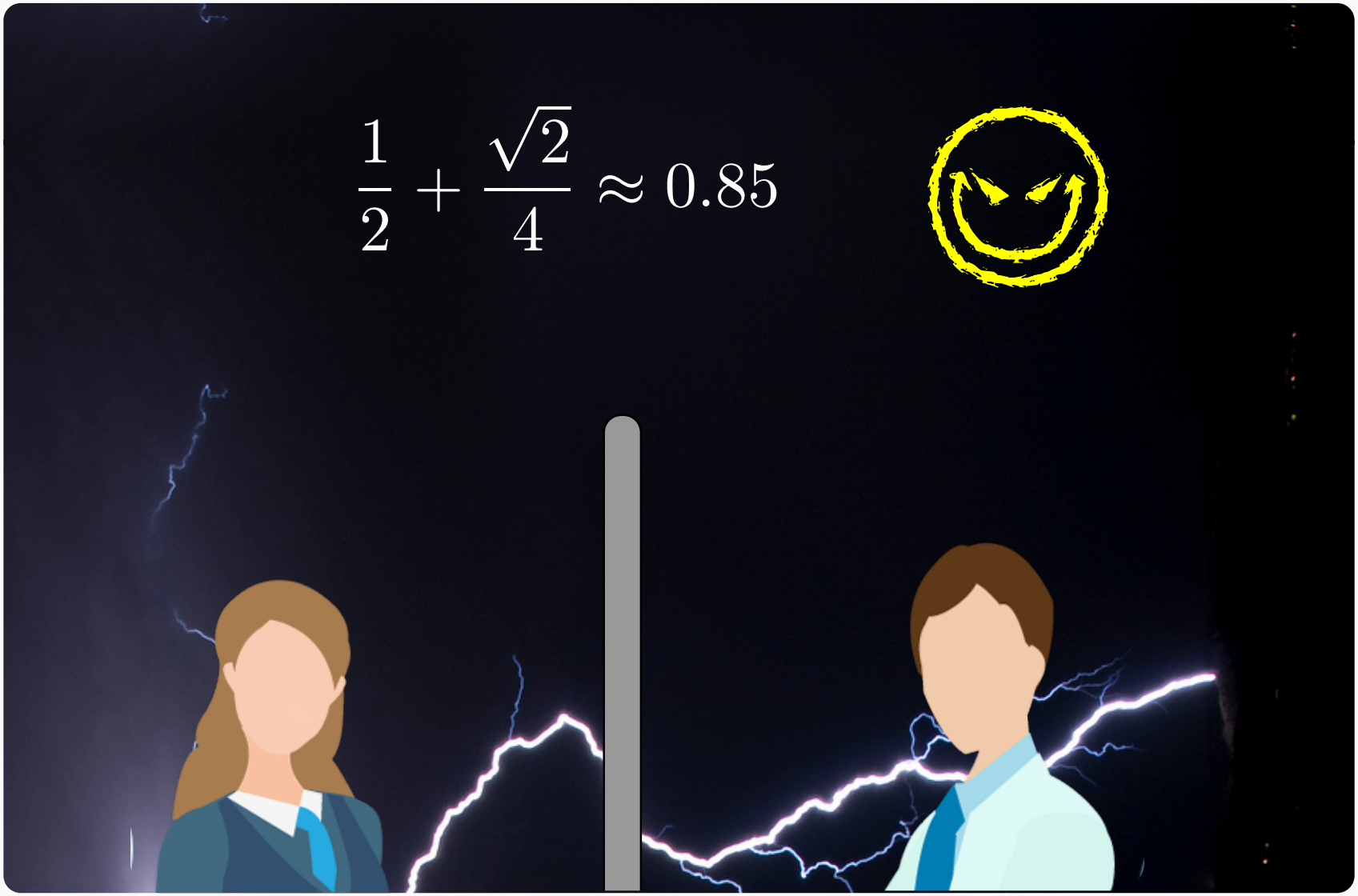
[1, 5, 6, 4]

Characterising Quantum

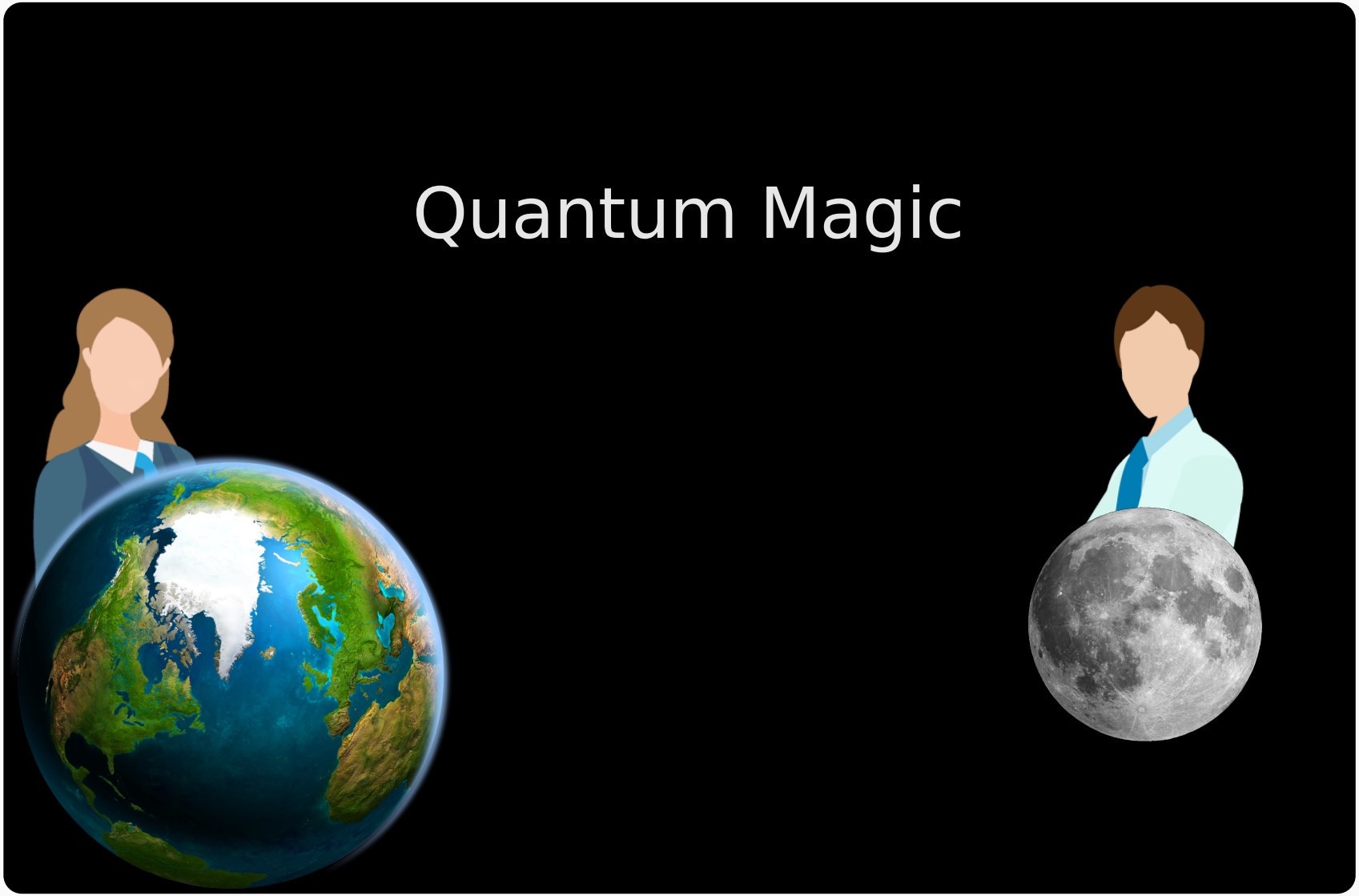


[1, 5, 6, 4]

Characterising Quantum



[1, 5, 6, 4]



[1, 5, 6, 4]

Characterising Quantum

- Non-locality: Bell Inequality

Characterising Quantum

- Non-locality: Bell Inequality
- Summer Internship: Continuous variable Bell test

- Non-locality: Bell Inequality

- Atul Singh Arora, Ali Asadian.
  Proposal for a macroscopic test of local realism with phase-space measurements,
  Physical Review A, 2015, **92**, 062107.

Characterising Quantum

- Non-locality: Bell Inequality

- Atul Singh Arora, Ali Asadian.
  Proposal for a macroscopic test of local realism with phase-space measurements,
  Physical Review A, 2015, **92**, 062107.

- Contextuality; non-locality is a special case!

Characterising Quantum

- Non-locality: Bell Inequality
- Atul Singh Arora, Ali Asadian.
  Proposal for a macroscopic test of local realism with phase-space measurements,
  Physical Review A, 2015, **92**, 062107.
- Contextuality; non-locality is a special case!
- MS Thesis: Alternative to Contextuality

Characterising Quantum

- Non-locality: Bell Inequality

- Atul Singh Arora, Ali Asadian.
  Proposal for a macroscopic test of local realism with phase-space measurements,
  Physical Review A, 2015, **92**, 062107.

- Contextuality; non-locality is a special case!

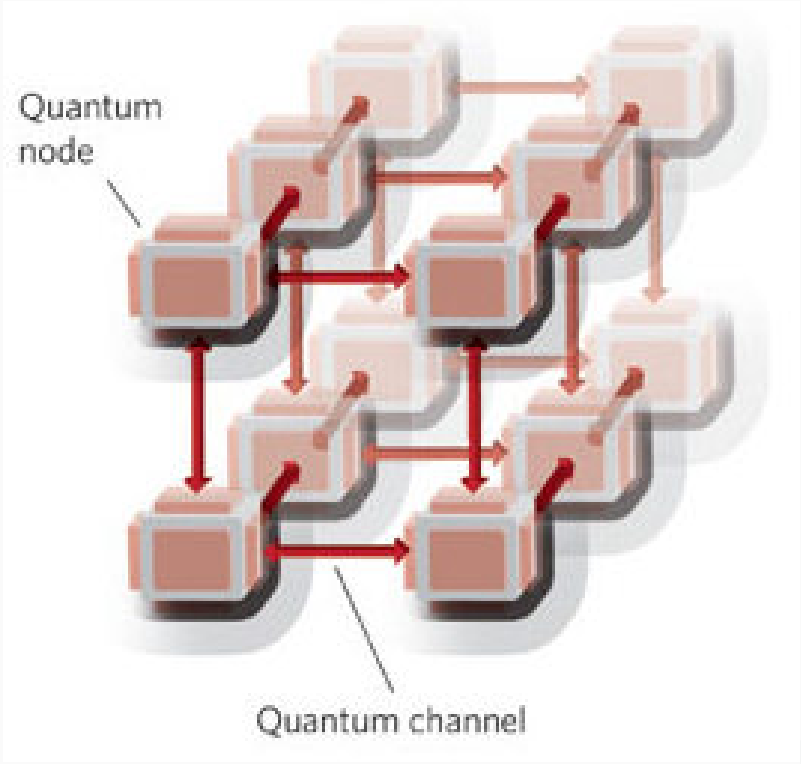
- Atul Singh Arora, Arvind.
  A non-contextual hidden variable model for quantum mechanics
  arXiv:1607.03498, submitted to *Physical Review Letters*.

Quantum Networks

Objective: Harness full capacity of a quantum computer network

Quantum Networks

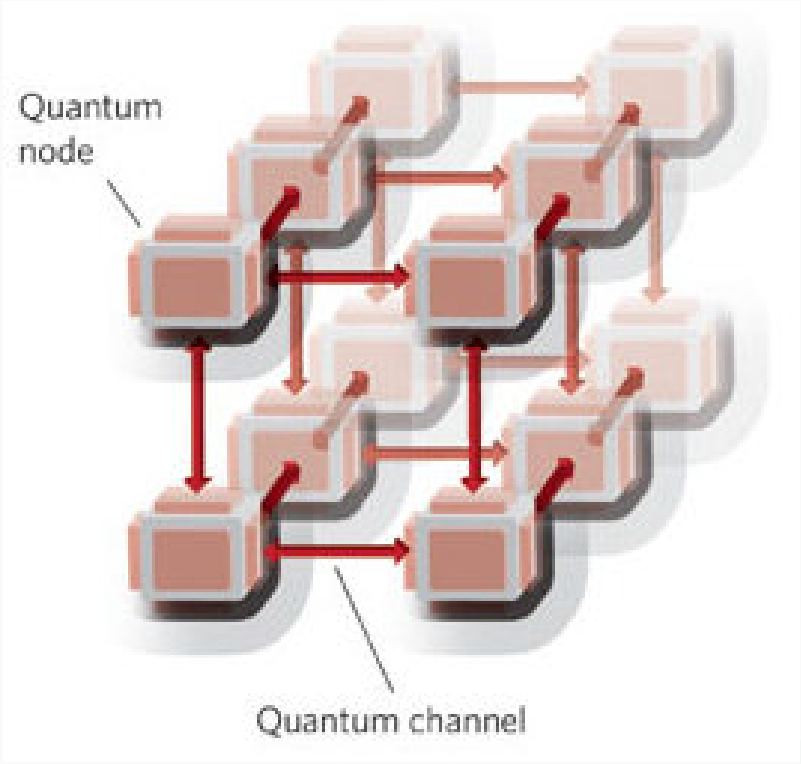
Objective: Harness full capacity of a quantum computer network



[12]

Quantum Networks

Objective: Harness full capacity of a quantum computer network



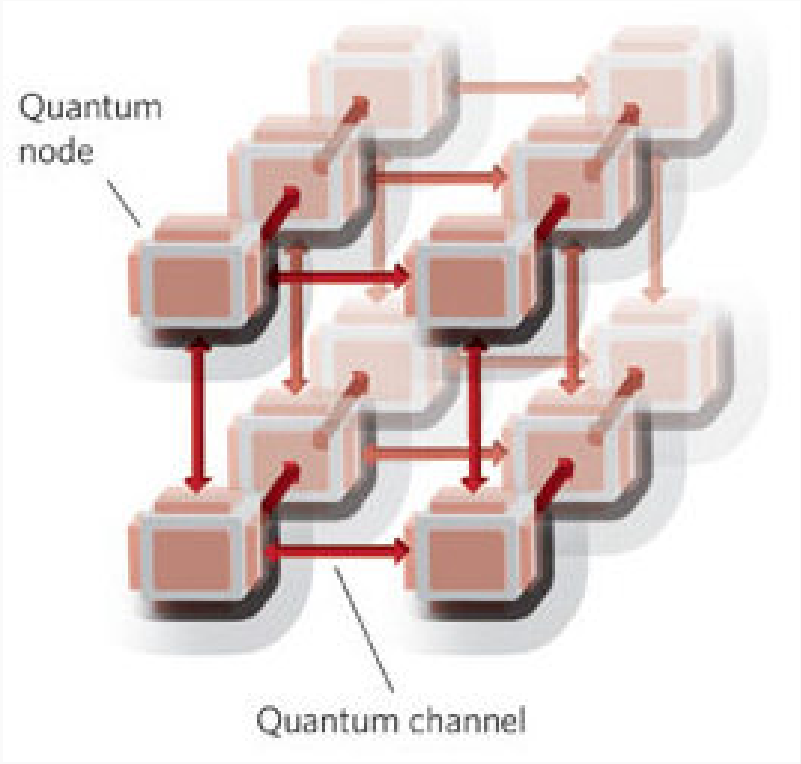
[12]

Cryptographic Primitives Building blocks of cryptographic algorithms

Communication Complexity Least bits of communication to compute a function f(x,y)

Quantum Networks

Objective: Harness full capacity of a quantum computer network



[12]

Cryptographic Primitives Building blocks of cryptographic algorithms

Communication Complexity Least bits of communication to compute a function f(x,y)

Make Quantum: More secure, more efficient.

State of the Art

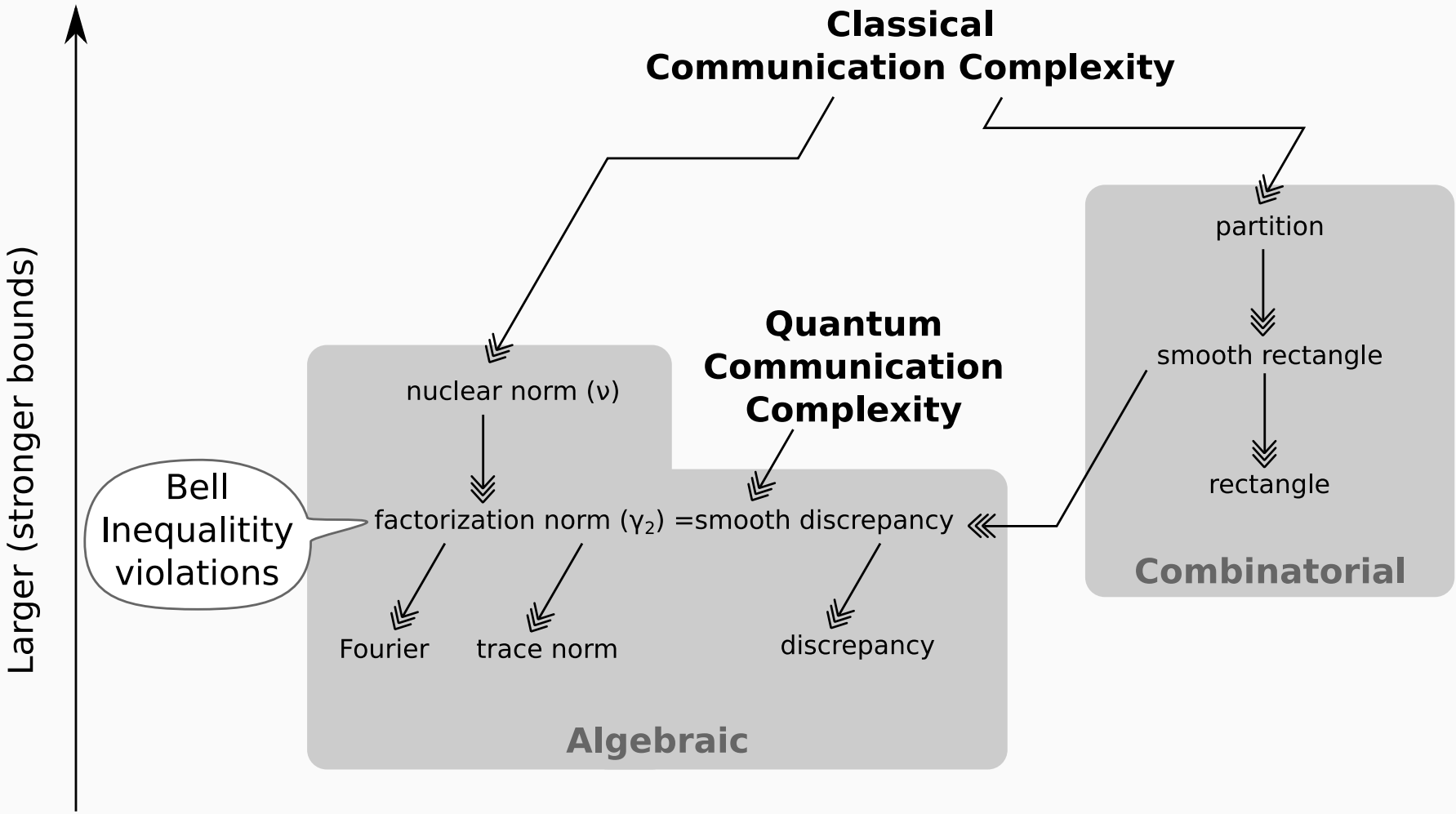
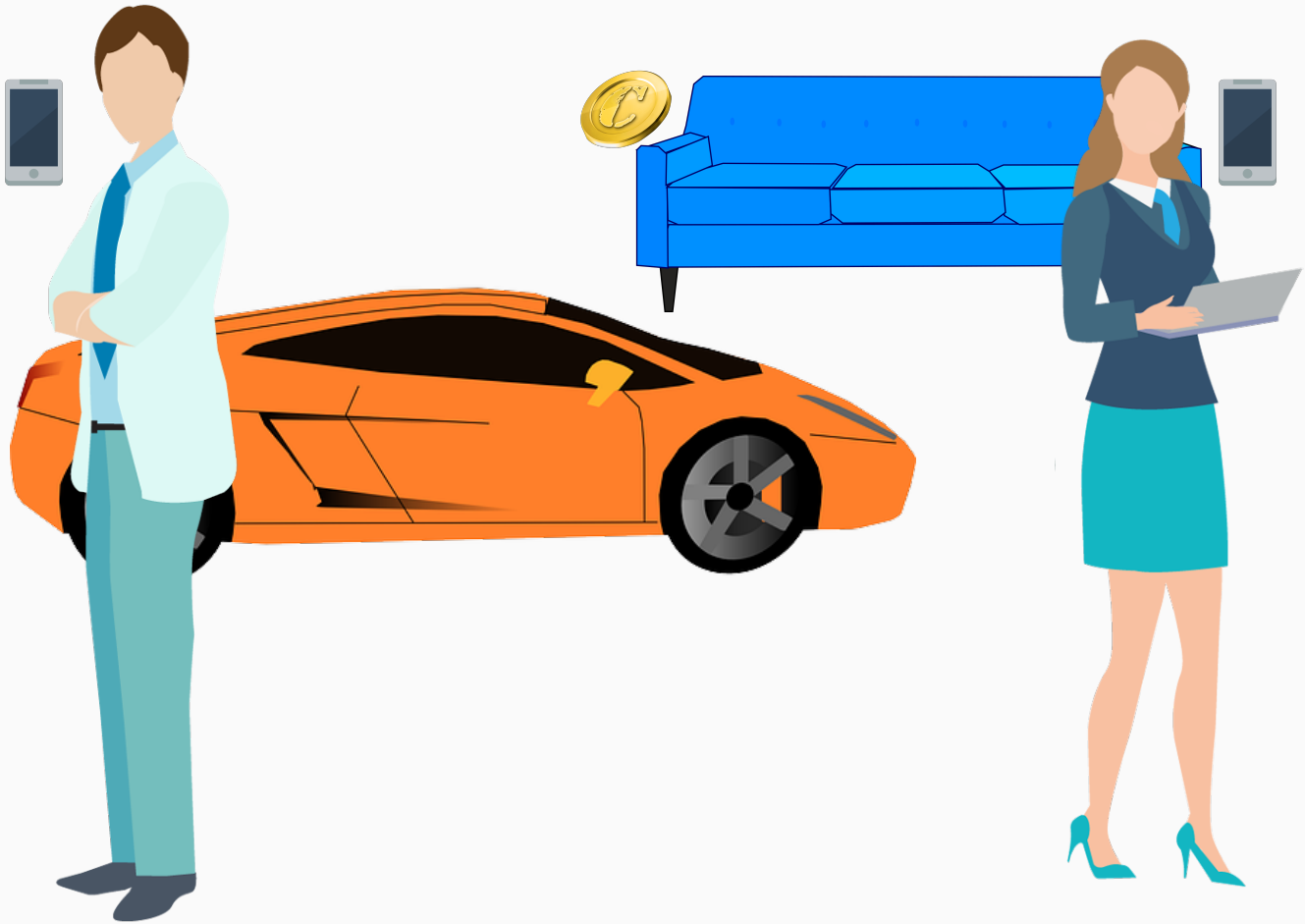


Figure 1: Schematic: Quantum Information Complexity

Cryptographic Primitives

[2]

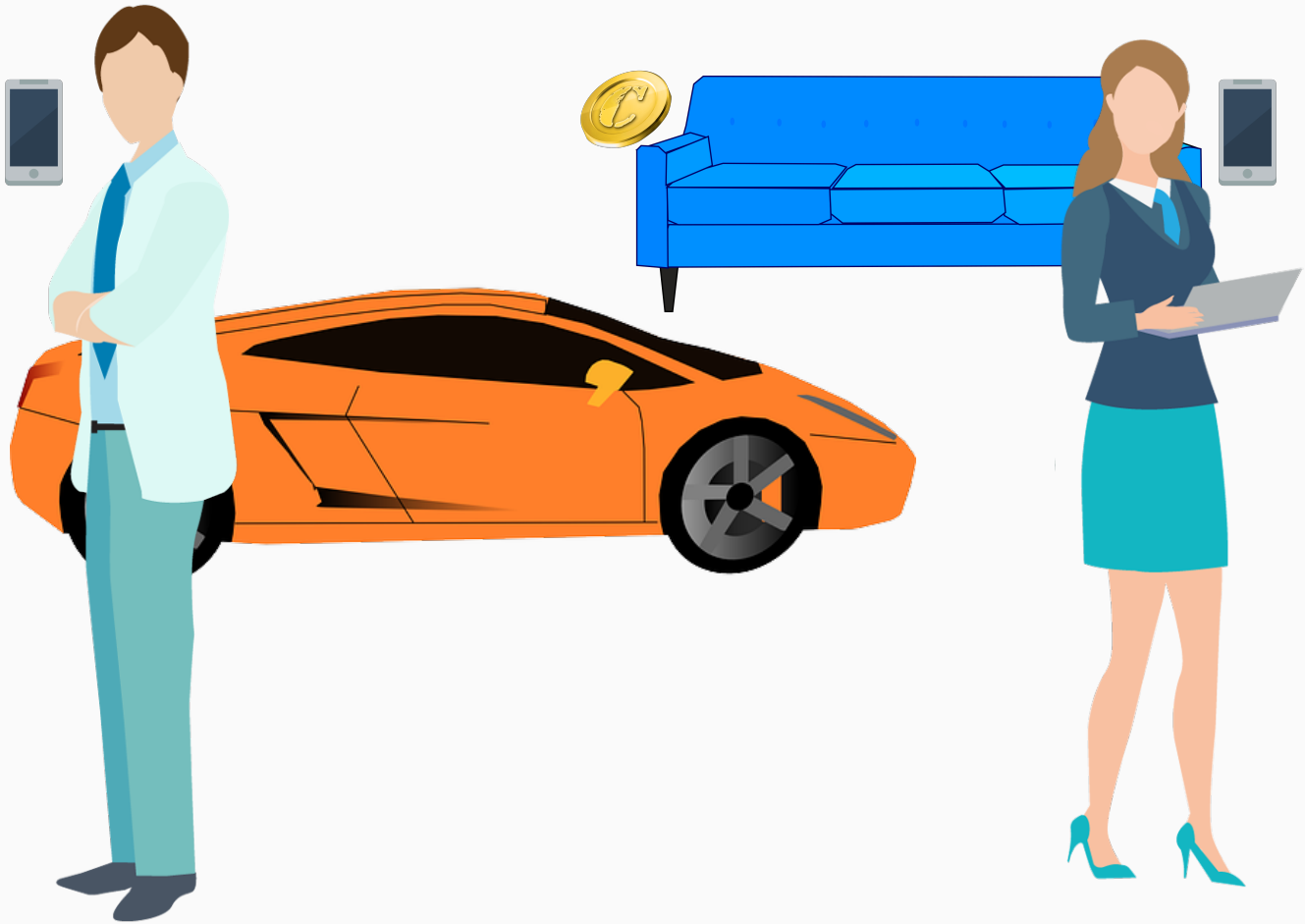
Coin flipping distrustful shared random bit.



[1, 3, 13, 10]

Coin flipping distrustful shared random bit.

Weak coin flipping preference

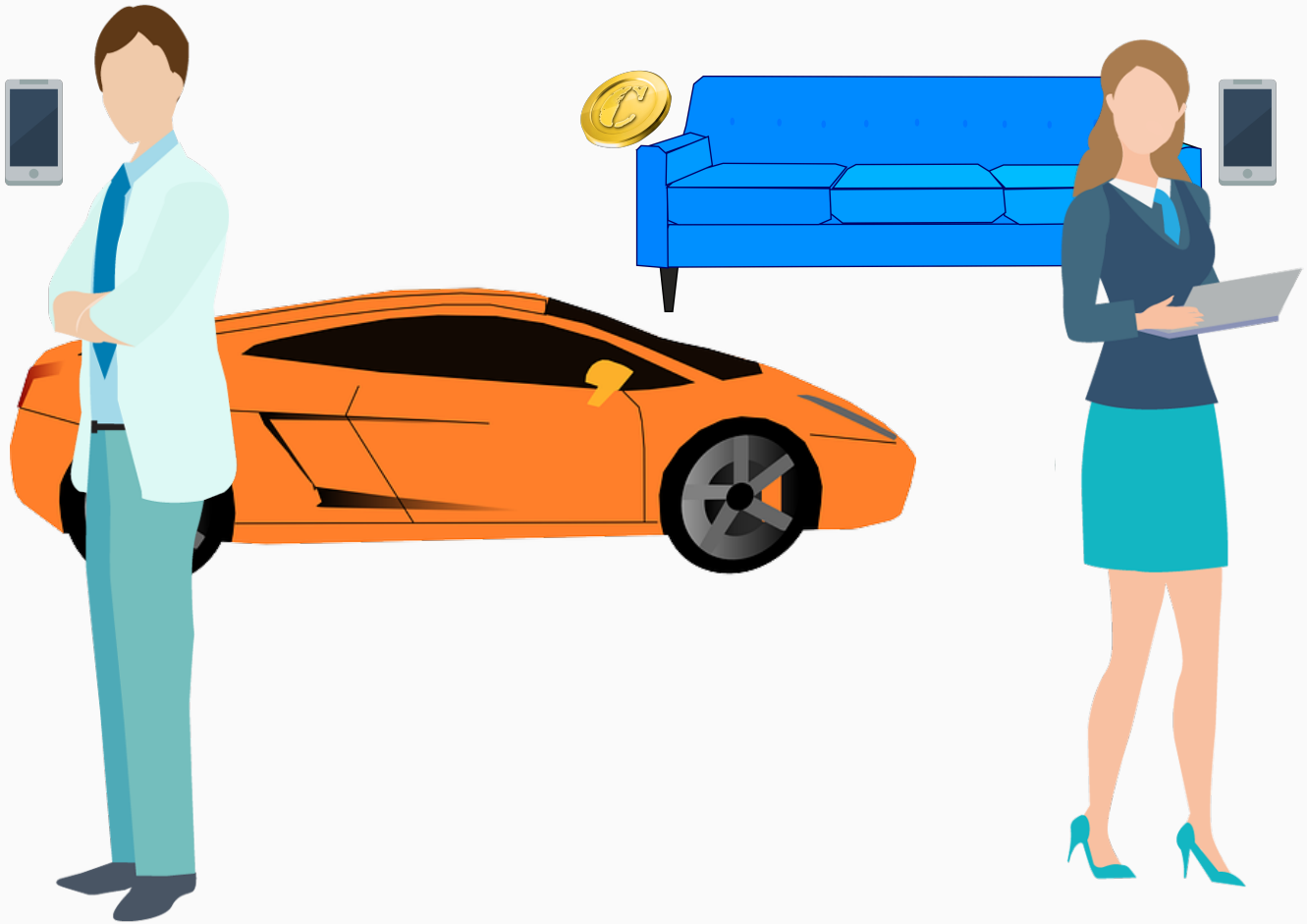


[1, 3, 13, 10]

Coin flipping distrustful shared random bit.

Weak coin flipping preference

Strong coin flipping no preference



[1, 3, 13, 10]

Cryptographic Primitives

Coin flipping distrustful shared random bit.

Weak coin flipping preference

Strong coin flipping no preference

Bias, ϵ Pr(Alice forces outcome) $< \epsilon + \frac{1}{2}$

Coin flipping distrustful shared random bit.

Weak coin flipping preference

Strong coin flipping no preference

Bias, ϵ Pr(Alice forces outcome) $< \epsilon + \frac{1}{2}$

- Classically, coin flipping is not possible.

Coin flipping distrustful shared random bit.

Weak coin flipping preference

Strong coin flipping no preference

Bias, ϵ Pr(Alice forces outcome) $< \epsilon + \frac{1}{2}$

- Classically, coin flipping is not possible.
- 'Quantumly', for strong coin flipping $\epsilon > \frac{1}{\sqrt{2}} - \frac{1}{2} \approx 0.207$. [17]

Coin flipping distrustful shared random bit.

Weak coin flipping preference

Strong coin flipping no preference

Bias, ϵ Pr(Alice forces outcome) $< \epsilon + \frac{1}{2}$

- Classically, coin flipping is not possible.
- 'Quantumly', for strong coin flipping $\epsilon > \frac{1}{\sqrt{2}} - \frac{1}{2} \approx 0.207$. [17]
- 'Quantumly', for weak coin flipping $\epsilon \to 0$; [19, 14]
  best explicit protocol has $\epsilon = \frac{1}{6}$. [18]

The Project

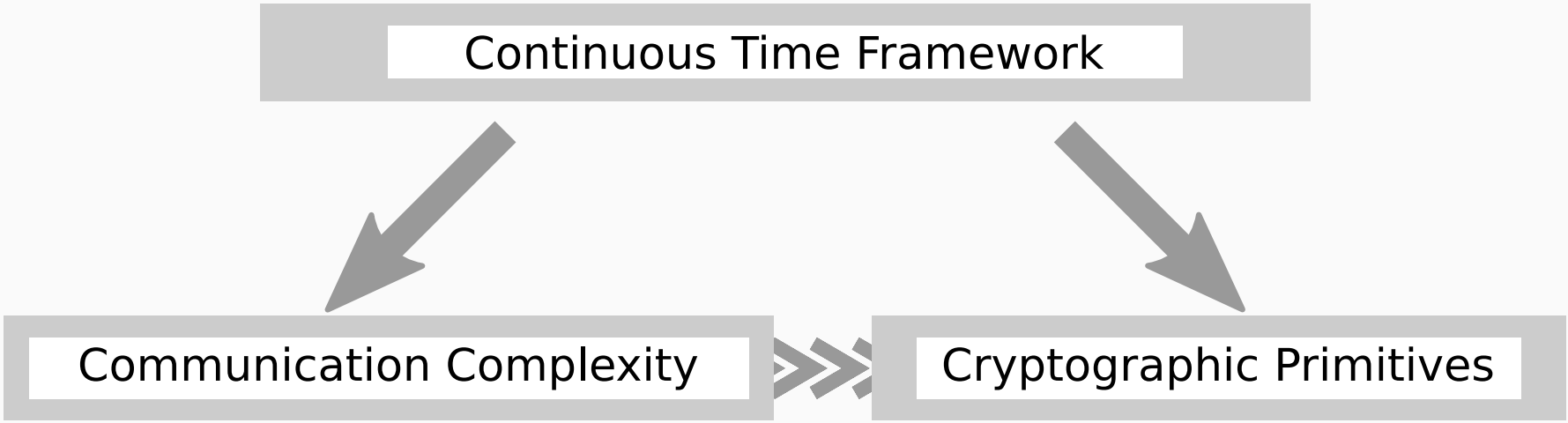


Figure 2: The approach

Discrete-Time (DT) protocols Sequential information flow

[1, 9, 8]

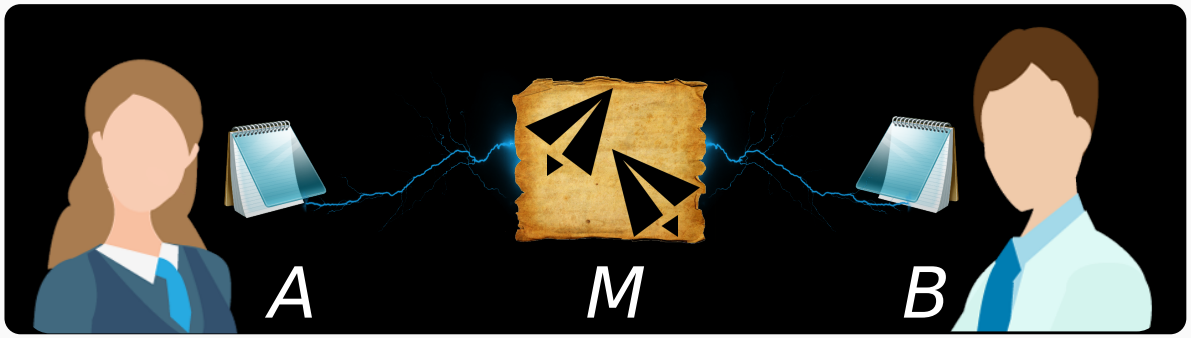
Discrete-Time (DT) protocols Sequential information flow

[1, 9, 8]

Discrete-Time (DT) protocols Sequential information flow

[1, 9, 8]

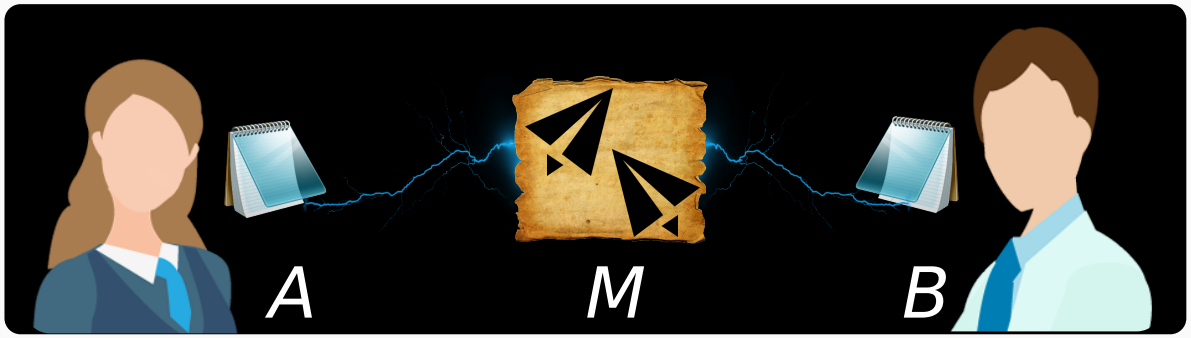
(new) Continuous-Time (CT) model Continuously coupled messaging



Discrete-Time (DT) protocols Sequential information flow

[1, 9, 8]

(new) Continuous-Time (CT) model Continuously coupled messaging

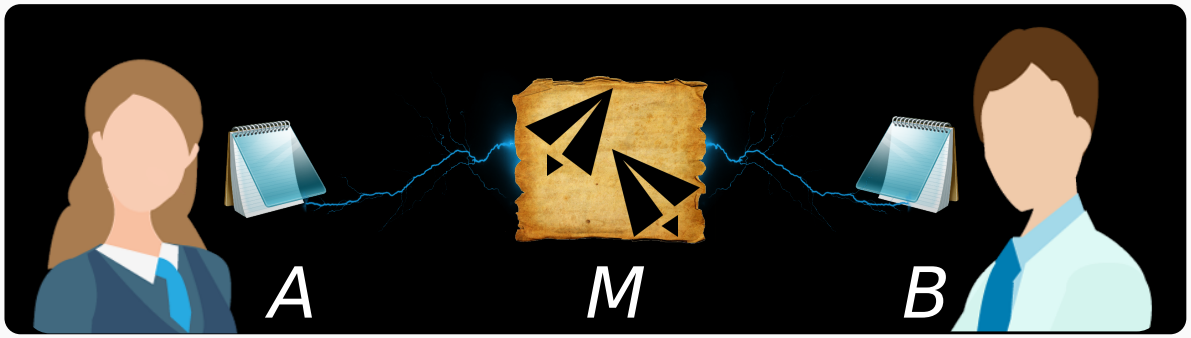


- $H = H_A \otimes I_{MB} + H_{AM} \otimes I_B + I_A \otimes H_{MB} + I_{AM} \otimes H_B$.

Discrete-Time (DT) protocols Sequential information flow

[1, 9, 8]

(new) Continuous-Time (CT) model Continuously coupled messaging



- $H = H_A \otimes I_{MB} + H_{AM} \otimes I_B + I_A \otimes H_{MB} + I_{AM} \otimes H_B$.
- CT protocol $\iff$ DT protocol (H_{AM} or H_{BM} zero).

CT Communication Complexity (CT-CC)

(new) Continuous Time Communication Complexity (CT-CC) The time required to evolve the system to the desired state where $|H_{AM}|, |H_{BM}| \leq 1$.

CT Communication Complexity (CT-CC)

(new) Continuous Time Communication Complexity (CT-CC) The time required to evolve the system to the desired state where $|H_{AM}|, |H_{BM}| \leq 1$.

- Advantage: Algebraic instead of combinatorial.

CT Communication Complexity (CT-CC)

(new) Continuous Time Communication Complexity (CT-CC) The time required to evolve the system to the desired state where $|H_{AM}|, |H_{BM}| \leq 1$.

- Advantage: Algebraic instead of combinatorial.
- Preliminary Results: Quantum query complexity characterised. [16]

(new) Continuous Time (CT) Cryptography Cryptographic algorithms constructed using the CT model.

(new) Continuous Time (CT) Cryptography Cryptographic algorithms constructed using the CT model.

Goal: Weak coin flipping

(new) Continuous Time (CT) Cryptography Cryptographic algorithms constructed using the CT model.

Goal: Weak coin flipping

- Advantage: Fresh approach to open problem.

(new) Continuous Time (CT) Cryptography Cryptographic algorithms constructed using the CT model.

Goal: Weak coin flipping

- Advantage: Fresh approach to open problem.
- Preliminary Result: $\epsilon = \frac{1}{6}$ obtained by discretising.

(new) Continuous Time (CT) Cryptography Cryptographic algorithms constructed using the CT model.

Goal: Weak coin flipping

- Advantage: Fresh approach to open problem.
- Preliminary Result: $\epsilon = \frac{1}{6}$ obtained by discretising.
- Insight: To break $\frac{1}{6}$ use

$$|\Psi\rangle = \int_{t=0}^{T} |\psi_t\rangle\,|t\rangle\,dt$$

Expected Research Flow

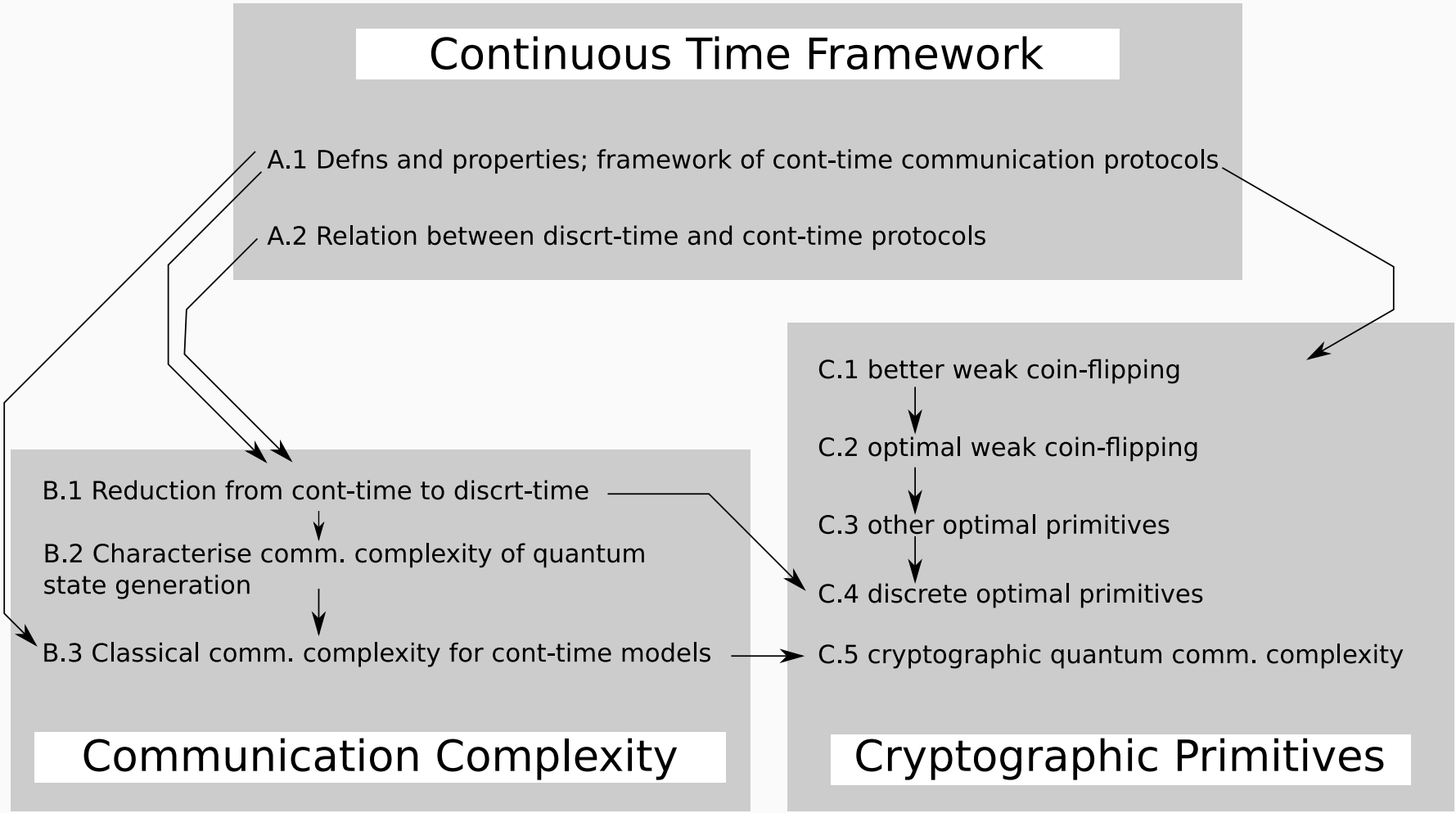


Figure 3: Schematic: Research Flow

Conclusion

Summary

- Novel and promising approach towards open and relevant problems

Summary

- Novel and promising approach towards open and relevant problems
- Promoter and his team have already produced preliminary results

Summary

- Novel and promising approach towards open and relevant problems
- Promoter and his team have already produced preliminary results
- Past work on related topic (published in two articles) namely continuous variables and non-locality.

Summary

- Novel and promising approach towards open and relevant problems
- Promoter and his team have already produced preliminary results
- Past work on related topic (published in two articles) namely continuous variables and non-locality.
- Well structured breakdown of the objective into achievable goals

Summary

- Novel and promising approach towards open and relevant problems
- Promoter and his team have already produced preliminary results
- Past work on related topic (published in two articles) namely continuous variables and non-locality.
- Well structured breakdown of the objective into achievable goals

Help make quantum computer networks a commercial reality.

Questions?

References I

[1] Alice and bob image. http://www.1designshop.com/wp-content/uploads/2016/02/1dsp-20160201-business-002.png.

[2] Alice bob happy image. http://www.1designshop.com/wp-content/uploads/2016/02/1dsp-20160201-business-008.png.

[3] Car image. http://www.pd4pic.com/images/car-cartoon-orange-transportation-sports-cars.png.

[4] Earth image. http://www.freeiconspng.com/uploads/planet-earth-png-8.png.

References II

[5] Evil smiley.
http://www.wallpapersxl.com/get/7689682.

[6] Moon image.
http://www.pngall.com/wp-content/uploads/2016/03/Moon-Transparent-PNG-180x180.png.

[7] Network image.
http://www.straighterline.com/wp/wp-content/uploads/2015/07/blog_feature_IT_Careers_072015.jpg.

[8] Notepad image.
http://www.freeiconspng.com/uploads/notepad-icon-7.png.

References III

[9] Paper image.
http://img06.deviantart.net/5b4a/i/2012/284/b/a/old_paper_texture_unsigned_by_meridiann-d5hh9a2.png.

[10] Phone image.
http://www.freeiconspng.com/uploads/device-mobile-phone-icon--small--flat-iconset--paome
png.

[11] Quantum image.
http://www.sciencealert.com/images/articles/processed/Quantum-Entanglement4_1024.jpg.

[12] Quantum internet.
http://www.nature.com/nature/journal/v453/n7198/full/nature07127.html.

[13] Sofa image.
http://www.clipartkid.com/images/29/big-image-png-QDgYpu-clipart.png.

[14] D. Aharonov, A. Chailloux, M. Ganz, I. Kerenidis, and L. Magnin.
A simpler proof of the existence of quantum weak coin flipping with arbitrarily small bias.
arXiv:1402.7166, 45(3):633–679, 2016.

[15] C. H. Bennett and G. Brassard.
Public-key distribution and coin tossing.
In *Int. Conf. on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[16] M. Brandeho and J. Roland.
A universal adiabatic quantum query algorithm.
In *10th TQC*, volume 44 of *LIPIcs*, pages 163–179, 2015.

[17] A. Kitaev.
Quantum coin flipping.
Talk at the 6th QIP, 2003.

[18] C. Mochon.
Large family of quantum weak coin-flipping protocols.
Phys. Rev. A, 72:022341, 2005.

[19] C. Mochon.
Quantum weak coin flipping with arbitrarily small bias, 2007.

[20] P. W. Shor.
Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.
SIAM J. Comput., 26(5):1484, 1997.

Tentative Timeframe

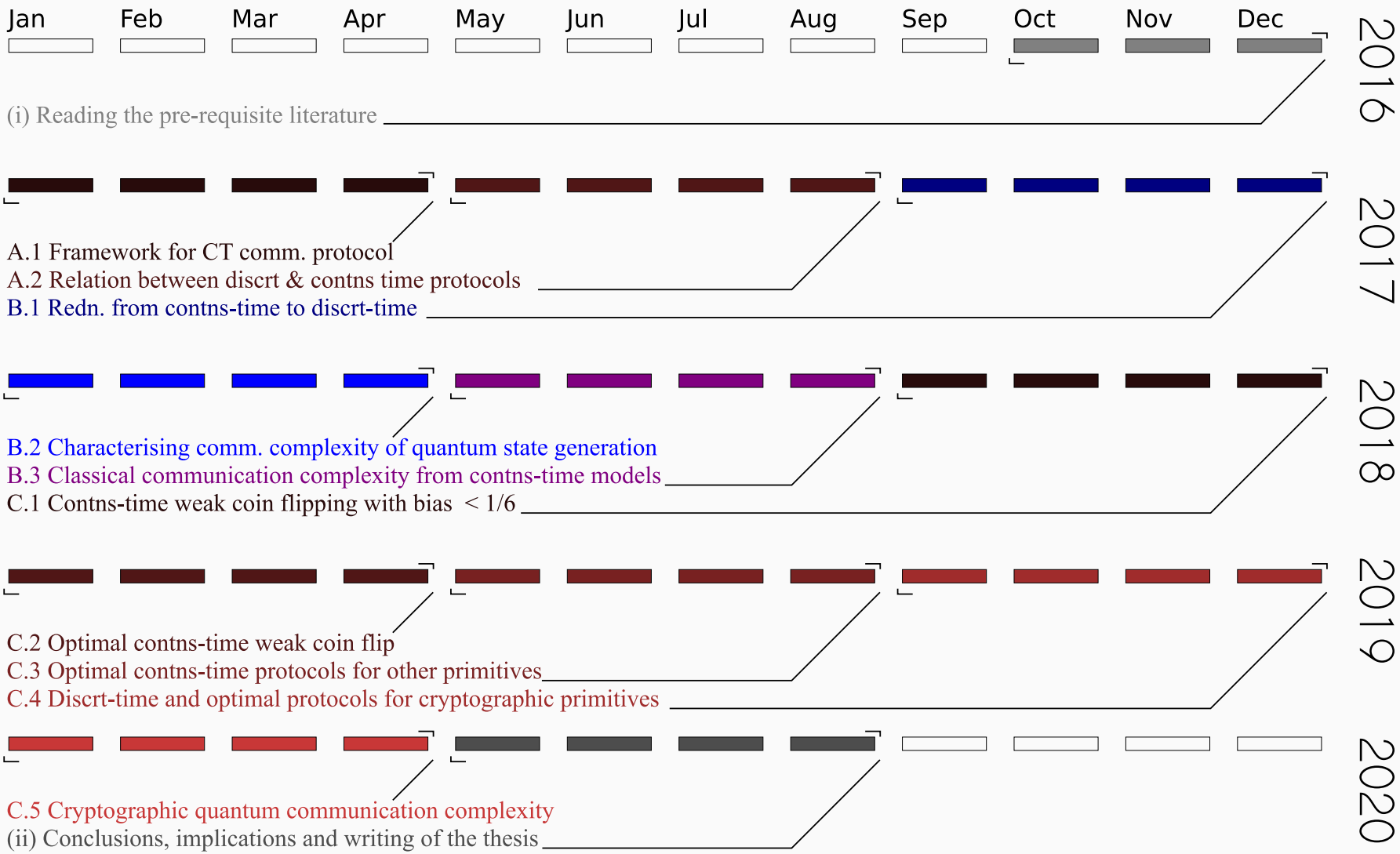


Figure 4: Schematic: Planned Schedule

MS Project

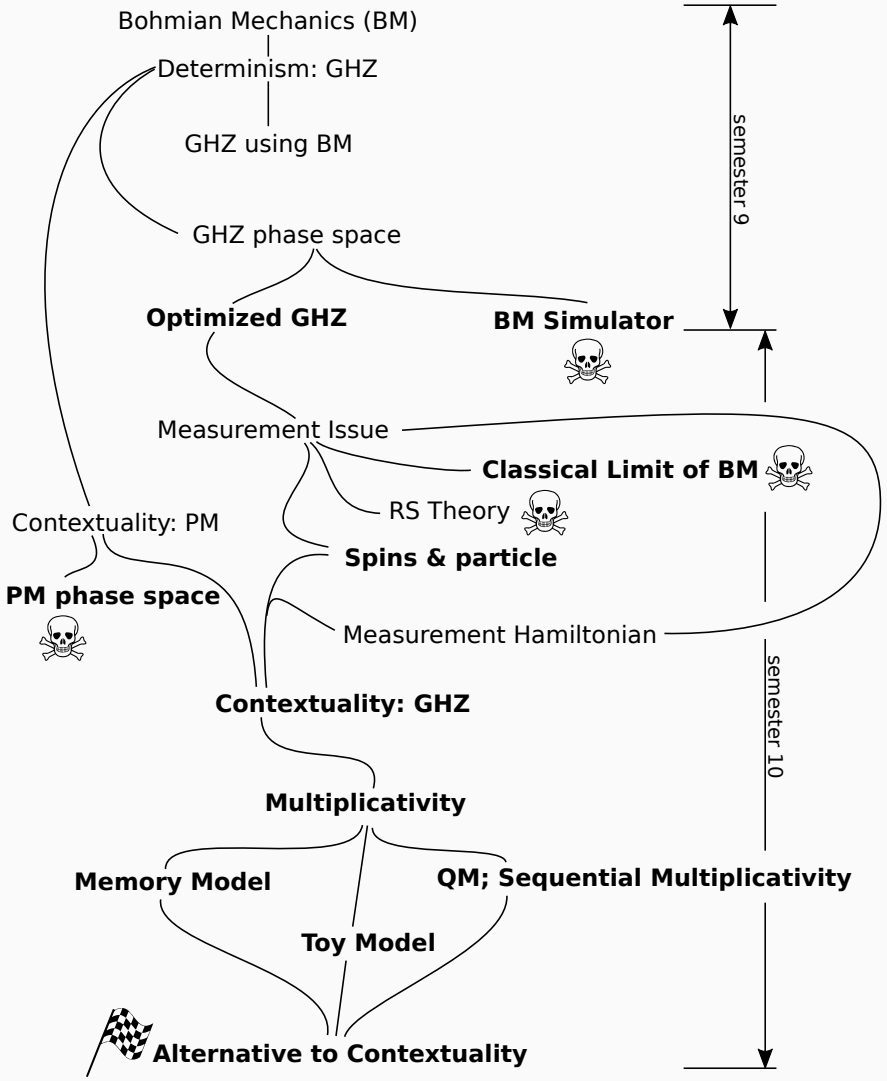


Figure 5: MS Project: Contextuality in a deterministic quantum theory.

My Publications

- A. S. A., Arvind.
  A non-contextual hidden variable model for quantum mechanics
  arXiv:1607.03498, submitted to *Physical Review Letters*.
- A. S. A., Ali Asadian.
  Proposal for a macroscopic test of local realism with phase-space measurements,
  Physical Review A, 2015, **92**, 062107.