

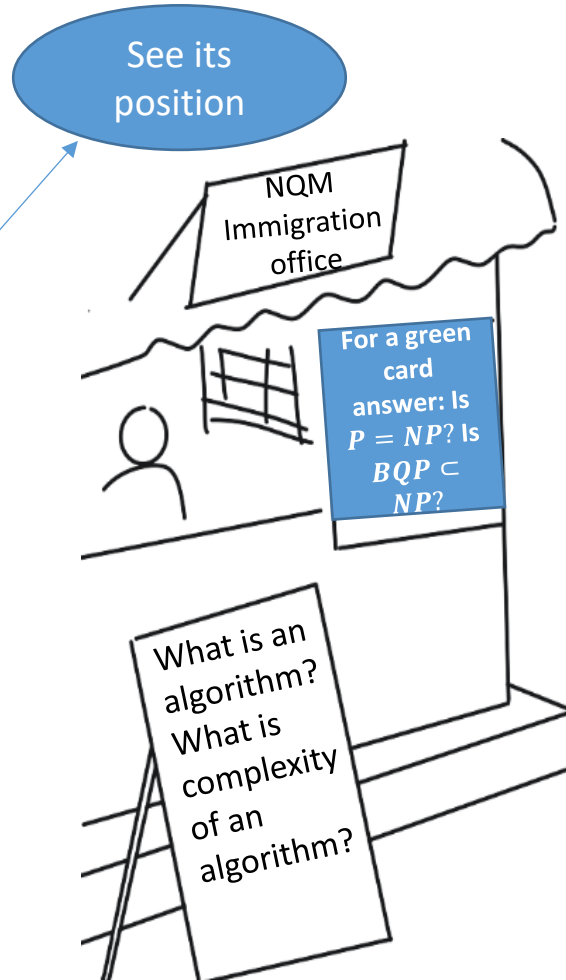
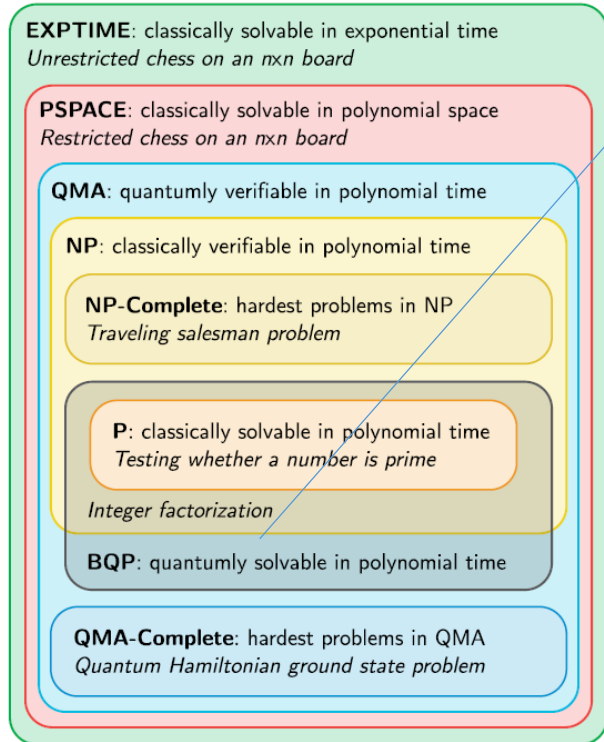
Many facets of security in the post-quantum world

Anirban Pathak
 Jaypee Institute of Information Technology, Noida
 To discuss after the lecture use
anirbanpathak@yahoo.co.in or 9717066494



International Symposium on Quantum Information and Communication (ISQIC), 2025, CQuERE, TCG CREST, Kolkata, March 31, 2025 to April 2, 2025 (talk date March 31, 2025)

What do we mean by difficulty of a computational task?



1231
2312

3543

12
X34

48
36X

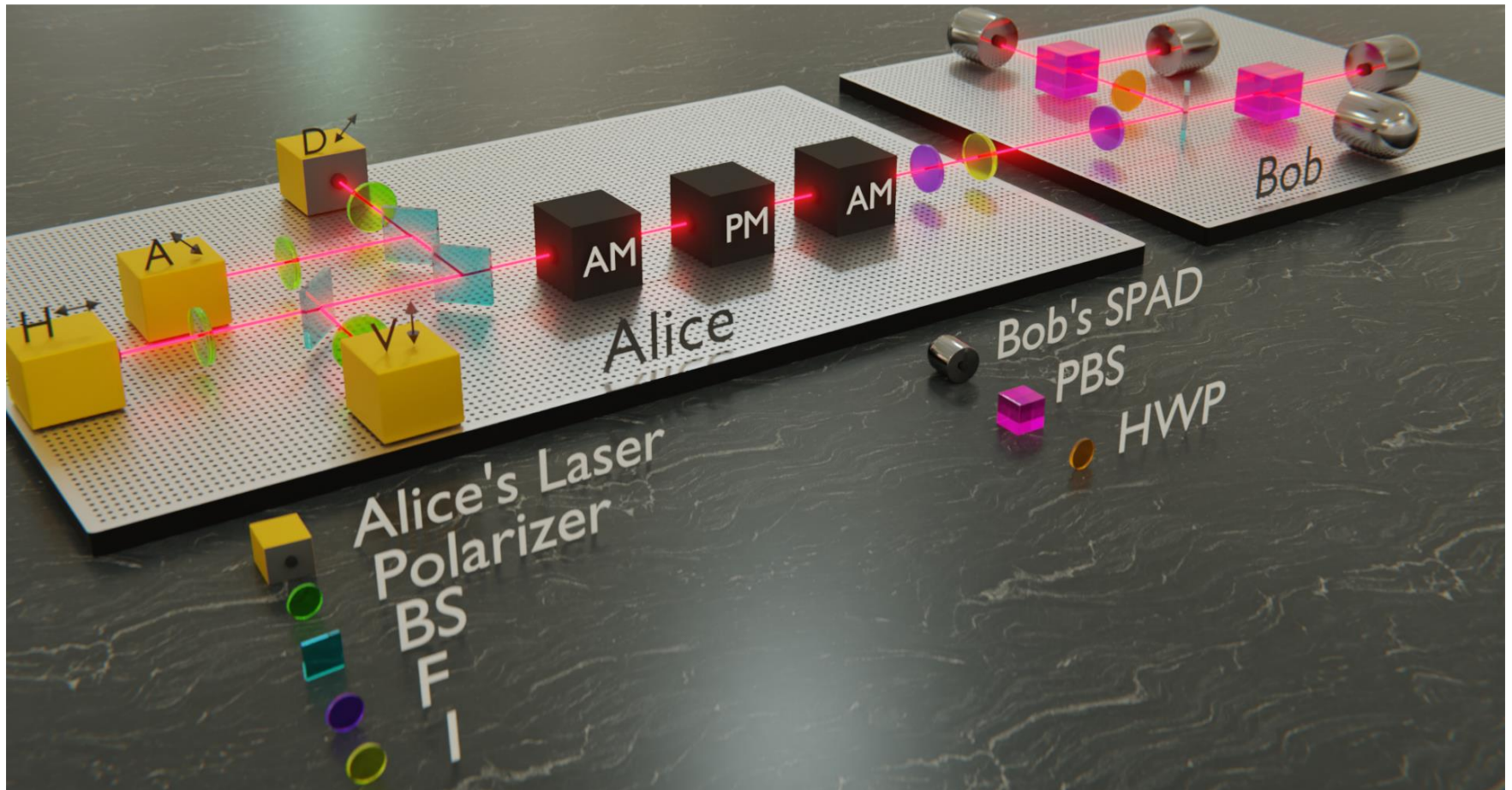
408

You are doing addition with an algorithm which takes n steps to add two n digit numbers. Multiplication is more complex, but not too complex, but factorization of product of two large primes is too complex.

Let me give you $N=pq$, where p and q are large primes, and ask you to find p and q , what will you do?

Rev. Mod. Phys. 94 (2022) 015004; **relations between classes are not proven.**
Restricted \Rightarrow polynomial upper bound on the number of moves.

Can we do cryptography without using a background computational task?



Are we using nonclassical light in this experiment? To avoid PNS attack, we need to use single photon state $|1\rangle$ which is nonclassical as its Wigner function is negative

Essence of the security in the quantum world through cartoons



Splitting of information into two or more pieces to ensure that Eve does not get access to "Special basis"

Renner's approach on Security

Protocol is ϵ_{cor} correct if for all adversarial strategies

$$\Pr[K_A \neq K_B] \leq \epsilon_{cor}$$

K_A and K_B are describing Alice's and Bob's output.

Protocol is ϵ_{sec} secret if for all adversarial strategies

$$(1 - p^\perp)D(\rho_{AE}^\top, \sigma_A \otimes \rho_E^\top) \leq \epsilon_{sec}$$

$D(.,.)$ is the trace distance and σ_A is the fixed mixed state.

$$\epsilon = \epsilon_{cor} + \epsilon_{sec}$$

Composable security: $\epsilon_1 + \epsilon_2$



p^\perp be the probability that the protocol aborts.

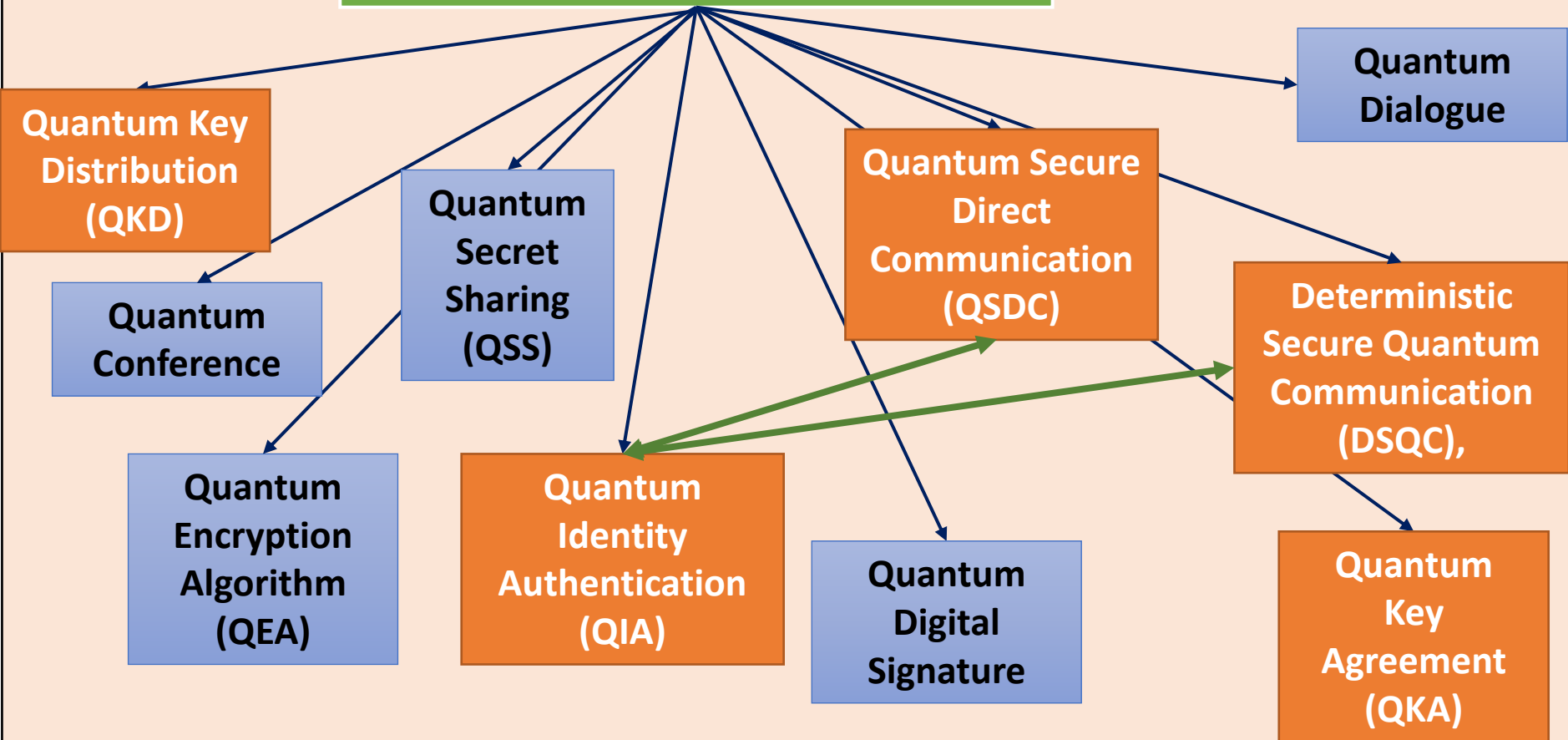
ρ_{AE}^\top be the resulting state of the AE subsystems conditioned on not aborting, and the joint state of the final key K and the quantum information gathered by an eavesdropper.

σ_A Ideal key that is perfectly uniform and independent from the adversary's information ρ_E^\top .

Portmann, C., & Renner, R. (2022). Security in quantum cryptography. *Reviews of Modern Physics*, 94(2), 025008.

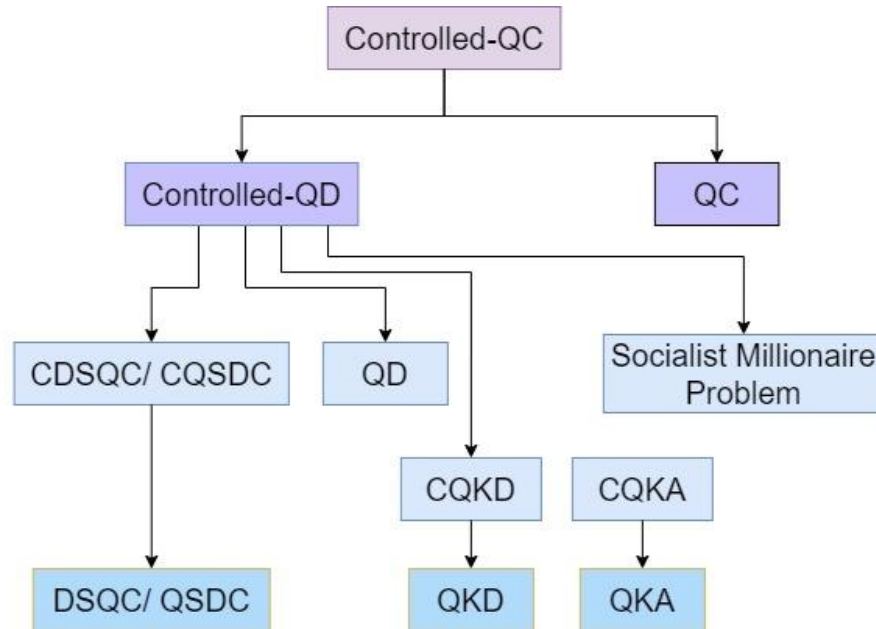
Note: In the case of DPS and COW, the unconditional security against coherent attacks is still to be proven So, a universal composable proof is not there.

Quantum cryptography and communication (security required)



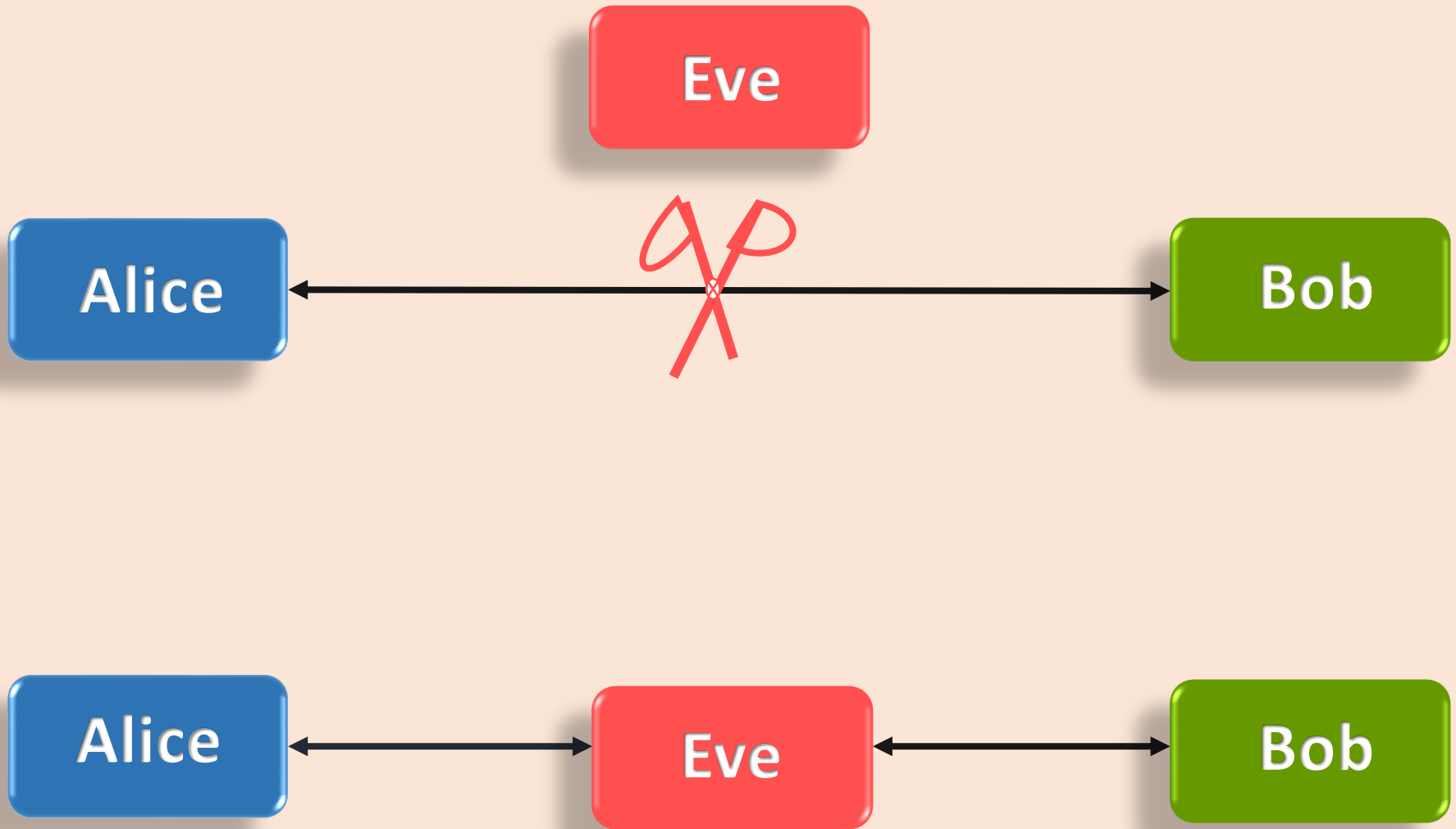
Quantum Cryptographic Schemes (with some secure multi-party computation tasks)

QC: Quantum Conference
QD: Quantum Dialogue
QSDC: Quantum Secure Direct Communication
DSQC: Direct Secure Quantum Communication
QKD: Quantum Key Distribution
QKA: Quantum Key Agreement



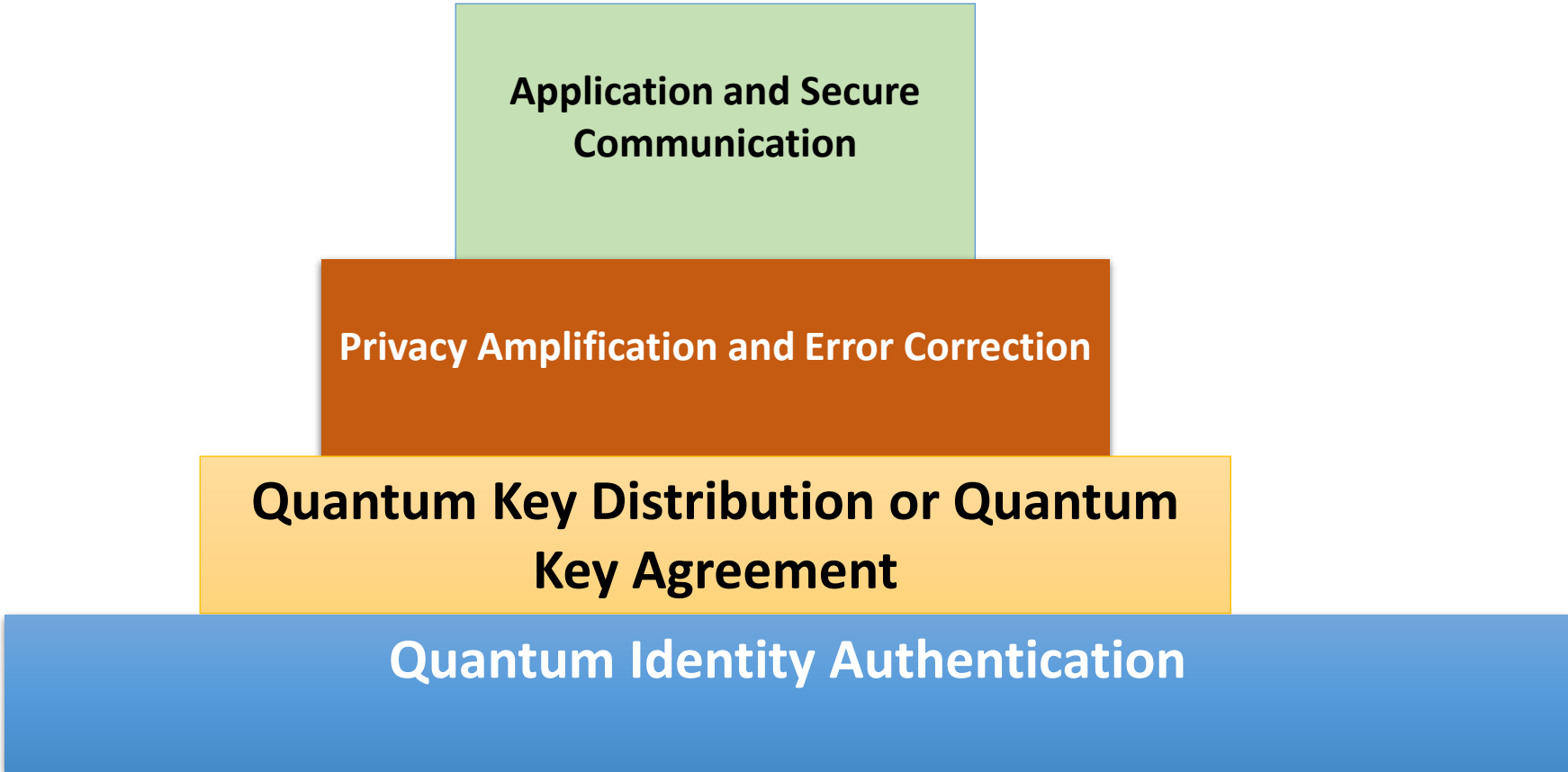
Capability of performing a task placed above in this chart implies the capability of performing a task placed at position lower it and connected by arrows. If tasks are placed in some layer and not connected by arrow, then are not reducible to each other in general.

The risk appears without Authentication



Basic Structure

BB84 paper: “The need for the public (non-quantum) channel in this scheme to be immune to active eavesdropping can be relaxed if the Alice and Bob have agreed beforehand on a small secret key, which they use to create Wegman-Carter authentication tags [*] for their messages over the public channel”.



**Application and Secure
Communication**

Privacy Amplification and Error Correction

**Quantum Key Distribution or Quantum
Key Agreement**

Quantum Identity Authentication

Quantum Identity Authentication (QIA)

Based on the quantum resources

Based on the computational or communication tasks

See A. Dutta and A. Pathak, *Quant. Infor. Proc.* 21 (2022) 369.

Use entangled state

Does not use Entangled state

Schemes of QKD

Quantum error detection code

QSDC and DSQC

Schemes of Teleportation

Quantum blind computing

Quantum secret sharing

Secure computation tasks

Quantum oblivious transfer

Quantum private comparison

Many of these schemes require quantum memory which is not available

First protocol: Claude Crépeau and Louis Salvail, "Quantum oblivious mutual identification", in *International Conference on the Theory and Applications of Cryptographic Techniques* (1995), pp. 133--146.

Previous quantum identity authentication schemes

Proposed by	Quantum Resource	Pre-Shared Key	Third Party	Channel(s) Used	Quantum Memory	Quantum Task
Dušek et al.	<i>SP</i>	<i>CS</i>	<i>N</i>	<i>C, Q</i>	<i>N</i>	QKD
Zeng et al.	<i>B, SP</i>	<i>CS</i>	<i>N</i>	<i>C, Q</i>	<i>N</i>	QSDC/DSQC
Mihara et al.	<i>B</i>	<i>B</i>	<i>T</i>	<i>C, Q</i>	<i>Y</i>	QSS
Li et al.	<i>B</i>	<i>B</i>	<i>N</i>	<i>Q</i>	<i>Y</i>	QSDC/DSQC
Zhou et al.	<i>B</i>	<i>B</i>	<i>T</i>	<i>C, Q</i>	<i>Y</i>	Teleportation
Zhang et al.	<i>B, SP</i>	<i>QKD</i>	<i>N</i>	<i>Q</i>	<i>Y</i>	QSDC/DSQC
Lee et al.	<i>GHZ</i>	<i>CS, HF</i>	<i>UT</i>	<i>C, Q</i>	<i>Y</i>	QSDC/DSQC
Yu-Guang et al.	<i>GHZ</i>	<i>CS, HF</i>	<i>T</i>	<i>C, Q</i>	<i>N</i>	QSS
Dan et al.	<i>B, SP</i>	<i>CS</i>	<i>N</i>	<i>C, Q</i>	<i>Y</i>	QSDC/DSQC
Chang et al.	<i>FC</i>	<i>CS</i>	<i>UT</i>	<i>Q</i>	<i>N</i>	QSDC/DSQC
Yuan et al.	<i>SP</i>	<i>CS</i>	<i>N</i>	<i>Q</i>	<i>N</i>	QSDC/DSQC

B Bell state, ***C*** classical, ***CS*** classical identity sequence, ***FC*** five-particle cluster state, ***HF*** single one-way hash function, ***N*** no, ***Q*** quantum, ***ST*** semi-trusted, ***SP*** single photon, ***T*** trusted, ***UT*** un-trusted, ***Y*** yes.

Previous quantum identity authentication schemes

Proposed by	Quantum Resource	Pre-Shared Key	Third Party	Channel Used	Quantum Memory	Quantum Task
Ho Hong et al.	<i>SP</i>	<i>CS</i>	<i>N</i>	<i>C, Q</i>	<i>N</i>	QKD
Kang et al.	<i>GHZ-like</i>	<i>CS</i>	<i>UT</i>	<i>C, Q</i>	<i>Y</i>	QSDC/DSQC
Liu et al.	<i>SP</i>	<i>CS</i>	<i>N</i>	<i>Q</i>	<i>N</i>	QKD
Wen et al.	<i>GHZ-like, W</i>	<i>CS, HF</i>	<i>N</i>	<i>C, Q</i>	<i>Y</i>	Teleportation
Zheng et al.	<i>FC</i>	<i>QKD</i>	<i>T</i>	<i>C, Q</i>	<i>N</i>	QSS
Zhang et al.	<i>B</i>	<i>CS</i>	<i>ST</i>	<i>C, Q</i>	<i>N</i>	QSDC/DSQC
Qu et al.	<i>GHZ-like</i>	<i>CS</i>	<i>N</i>	<i>C, Q</i>	<i>N</i>	QECC
Zhu et al.	<i>SP</i>	<i>CS</i>	<i>N</i>	<i>C, Q</i>	<i>N</i>	QSDC/DSQC

B Bell state, **C** classical, **CS** classical identity sequence, **FC** five-particle cluster state, **HF** single one-way hash function, **N** no, **Q** quantum, **ST** semi-trusted, **SP** single photon, **T** trusted, **UT** un-trusted, **Y** yes.

Old and new QKA scheme

Proposed by	NoP	QR	QC	QM	TR
Huang et al.	2	EPR pair	One-way	Y	N
Xu et al.	3	GHZ state	One-way	Y	N
Shukla et al.	2	EPR pair	Two-way	Y	N
He et al.	2	four-qubit cluster state	Two-way	Y	N
Yang et al.	2	four-qubit cluster state	One-way	Y	N
Tang et al.	2	GHZ state	Two-way	Y	Y
Our Protocol 1	2	EPR pair, single qubit	One-way	N	Y
Our Protocol 2	2	EPR pair, single qubit	One-way	N	N

Y - required, **N** - not required, **QR** - quantum resources, **QC** – quantum channel, **QM** - quantum memory, **TR** - third party, **QE** - quantum efficiency, **NoP** - number of parties.

Quantum identity authentication schemes with different quantum resources

Quantum Information Processing (2022) 21:369

<https://doi.org/10.1007/s11128-022-03717-0>



A short review on quantum identity authentication protocols: how would Bob know that he is talking with Alice?

Arindam Dutta¹ · Anirban Pathak¹

Received: 22 December 2021 / Accepted: 20 October 2022

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract

Secure communication has achieved a new dimension with the advent of the schemes of quantum key distribution (QKD) as in contrast with classical cryptography, quantum cryptography can provide unconditional security. However, a successful implementation of a scheme for QKD requires identity authentication as a prerequisite. A security loophole in the identity authentication scheme may lead to the vulnerability of the entire secure communication scheme. Consequently, identity authentication is extremely important, and in the last three decades several schemes for identity authentication using quantum resources have been proposed. The chronological development

Quantum Information Processing (2023) 22:13

<https://doi.org/10.1007/s11128-022-03767-4>



Controlled secure direct quantum communication inspired scheme for quantum identity authentication

Arindam Dutta¹ · Anirban Pathak¹

Received: 12 September 2022 / Accepted: 29 November 2022

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract

To achieve unconditional security through quantum key distribution (QKD), users involved in key distribution first need to authenticate each other. Classical identity authentication schemes were used in all the early implementations of QKD, but realizing their potential vulnerability, a few protocols for quantum identity authentication (QIA) have been proposed in the recent past. Here, we propose a new protocol for QIA which is constructed by modifying the concept of controlled secure direct quantum communication. The proposed controlled secure direct quantum communication inspired scheme for QIA allows two users Alice and Bob to mutually authenticate each other's identity with the help of a third-party Charlie using Bell states. The security of the proposed protocol is critically analyzed, and it is shown that the proposed protocol is secure against several known attacks including impersonation attack, intercept and resend attack, and impersonated fraudulent attack. Further, the relevance of the

Simultaneous quantum identity authentication scheme utilizing entanglement swapping with secret key preservation

Arindam Dutta[✉] and Anirban Pathak[✉]

*Department of Physics and Materials Science & Engineering,
Jaypee Institute of Information Technology, A 10, Sector 62, Noida, UP-201309, India*

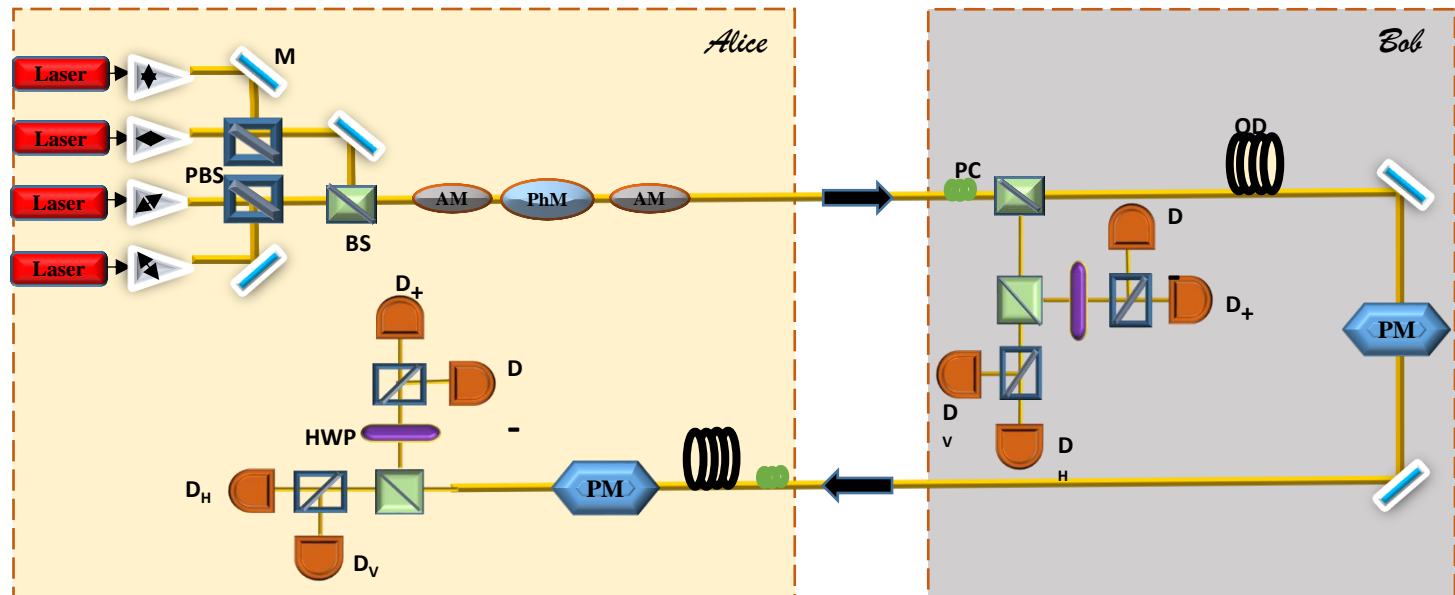
Unconditional security in quantum key distribution (QKD) relies on authenticating the identities of users involved in key distribution. While classical identity authentication schemes were initially utilized in QKD implementations, concerns regarding their vulnerability have prompted the exploration of quantum identity authentication (QIA) protocols. In this study, we introduce a new protocol for QIA, derived from the concept of controlled secure direct quantum communication. Our proposed scheme facilitates simultaneous authentication between two users, Alice and Bob, leveraging Bell states with the assistance of a third party, Charlie. Through rigorous security analysis, we demonstrate that the proposed protocol withstands various known attacks, including impersonation, intercept and resend and impersonated fraudulent attacks. Additionally, we establish the relevance of the proposed protocol by comparing it with the existing protocols of similar type.

Mod. Phys. Lett. A **40**
(2025) 2450196.

QUANTUM DIALOGUE: BA AN PROTOCOL

1. Bob prepares large number of copies of a Bell state $|\phi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$.
He keeps the first photon of each qubit with himself as home photon and encodes her secret message 00, 01, 10 and 11 by applying unitary operations U_0, U_1, U_2 and U_3 respectively on the second qubit. Without loss of generality, we may assume that $U_0 = I$, $U_1 = X$, $U_2 = iY$ and $U_3 = Z$.
2. Bob then sends the second qubit (travel qubit) to Alice and confirms that Alice has received a qubit.
3. Alice encodes her secret message by using the same set of encoding operations as was used by Bob and sends back the travel qubit to Bob. After receiving the encoded travel qubit Bob measures it in Bell Basis.
4. Bob decodes Alice's bits and announces his Bell basis measurement result. Alice uses that result to decode Bob's bits.

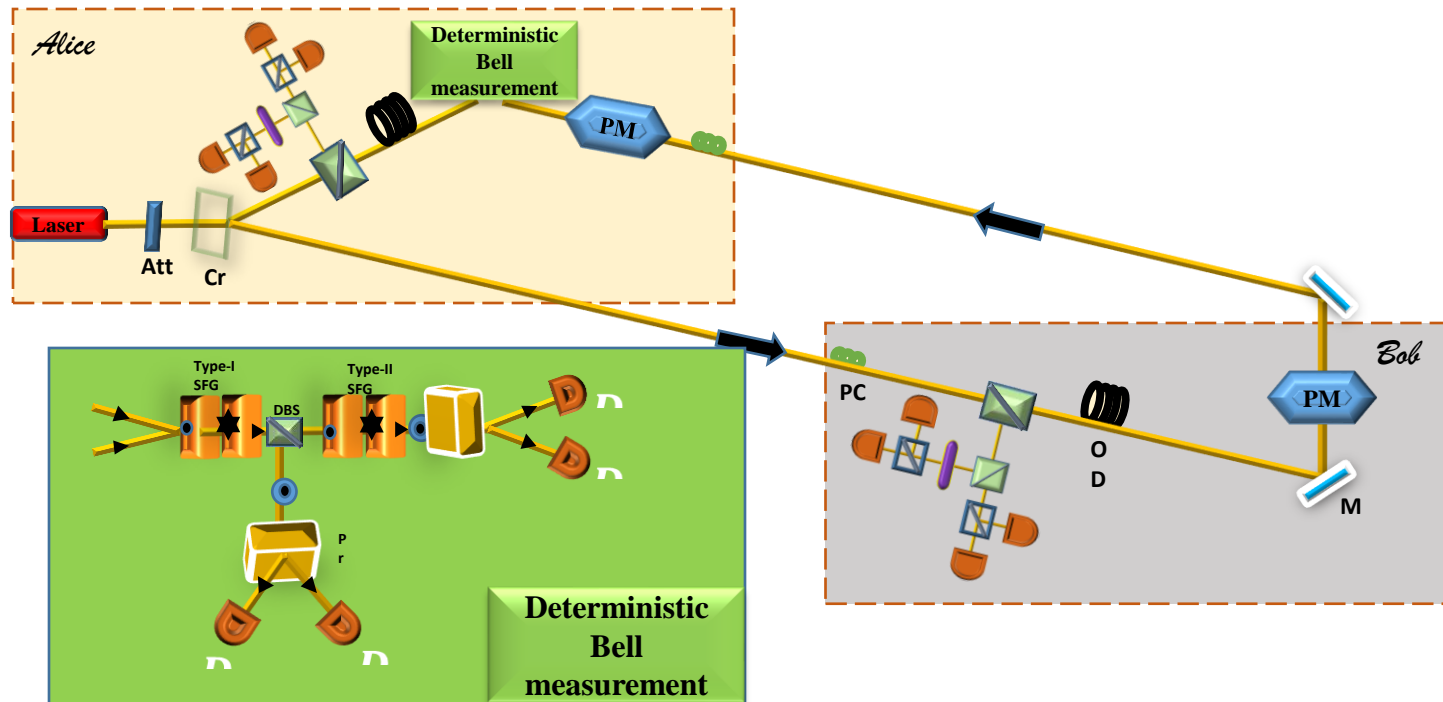
Can we do something more than state-of-art Chinese experiments on QSDC: Single photon based quantum dialogue protocol



As the quantum dialogue protocol is reducible to various other cryptographic schemes, so does the present single photon based implementation.

Optical designs for realization of a set of schemes for quantum cryptography, M. Sisodia, K. Thapliyal and **A. Pathak**, *Optical and Quantum Electronics* **53** (2021) 206.

Entangled state based quantum dialogue protocol



Optical designs for realization of a set of schemes for quantum cryptography, M. Sisodia, K. Thapliyal and **A. Pathak**, *Optical and Quantum Electronics* **53** (2021) 206.

What is one-sided two-party computation?

- Alice and Bob have secret inputs
 $i \in \{1, 2, \dots, n\}$ and $j \in \{1, 2, \dots, n\}$,
respectively.
- An *ideal* one-sided two-party secure computation: Alice helps Bob to compute a prescribed function

$$f(i, j) \in \{1, 2, \dots, p\}$$

in such a way that, at the end of the protocol, (a) Bob learns $f(i, j)$ unambiguously, (b) Alice learns nothing about j or $f(i, j)$, and (c) Bob knows nothing about i more than what logically follows from the values of j and $f(i, j)$.

We will call these conditions as condition (a), (b) and (c).

Special cases of one-sided two-party computation?

- Socialist millionaire problem:

Compute (i) $f(i,j)=1$ if $i=j$ and else $f(i,j)=0$

or, (ii) $f(i,j)=1$ if $i>j$ and else $f(i,j)=0$

or, (iii) $f(i,j)=1$ if $i>j$ and else $f(i,j)=0$

Other SMC tasks
of interest

Quantum e-
commerce,

Quantum Veto,

Quantum Voting,

Quantum Lottery,

Quantum e-

auction

- Quantum private comparison (QPC) is a special case of socialist millionaire problem

The task is to check equality of private

information: (i) $f(i,j)=1$ if $i=j$ and else $f(i,j)=0$

A more general case of two-party secure computation is SMC.

Expected properties of a voting scheme

- **Security:** (i) A user can vote only once (**non-reusability**), (ii) only legitimate users can vote (**eligibility**) and no one can learn any intermediate result (**fairness**).
- **Verifiability:** Any voter can verify the correctness of the result, however none of them will be able to prove how he or she voted. (This is the strongest version of the verifiability condition)
- **Privacy:** It ensures secrecy of the ballots, i.e., the anonymity of the voters. Ideally, no one should be able to tell how a particular voter has voted.

Quantum democracy: A democracy whose integrity is protected by quantum voting process.

First protocol of quantum voting: Hillery's protocol or HZBB06 protocol

Step 1: An honest (non-cheating) authority Charlie prepares an entangled state

$$|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle|k\rangle,$$

where N is the number of voters. Ex. for $N = 3$, $|\psi_0\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)$

Step 2: Charlie keeps one of the qubits (say the second one) and sends the first one to the first voter (say Alice₁), who registers her “no” vote by applying Identity operator (thus doing nothing) and “yes” vote by applying

$$U_{yes} : U_{yes} |k\rangle = |k + 1\rangle,$$

where $+$ denotes a modulo N addition.

Part of our
views: Protocols
for quantum
binary voting, K.
Thapliyal, R. D.
Sharma, A.
Pathak, Int. J.
Quant. Infor. 15
(2017) 1750007

Election and us: Voting, veto and our group

Open Access

EPJ Quantum Technol. (2022) 9: 14

<https://doi.org/10.1140/epjqt/s40507-022-00133-2>

Research

Quantum anonymous veto: a set of new protocols

Sandeep Mishra¹, Kishore Thapliyal², Abhishek Parakh³ and  Anirban Pathak^{1d}

Experimental realization of quantum anonymous veto protocols using IBM quantum computer

Published: 17 September 2022

Volume 21, article number 311, (2022) [Cite this article](#)

Download PDF 

Access provided by Jaypee Institute of Information Technology Noida

[Satis Kumar & Anirban Pathak](#) 

International Journal of Quantum Information | Vol. 15, No. 01, 1750007 (2017)

Protocols for quantum binary voting

Kishore Thapliyal, Rishi Dutt Sharma, and Anirban Pathak

arXiv > quant-ph > arXiv:2206.03182

Quantum Physics

[Submitted on 7 Jun 2022]


Anonymous voting scheme using quantum assisted blockchain

Sandeep Mishra, Kishore Thapliyal, S Krish Rewanth, Abhishek Parakh, Anirban Pathak

Voting forms the most important tool for arriving at a decision in any institution. The changing needs of the civilization currently demands a practical yet secure electronic voting system, but any flaw related to the applied voting technology can lead to tampering of the results with the malicious outcomes. Currently, blockchain technology due to its transparent structure forms an emerging area of investigation for the development of voting systems with a far

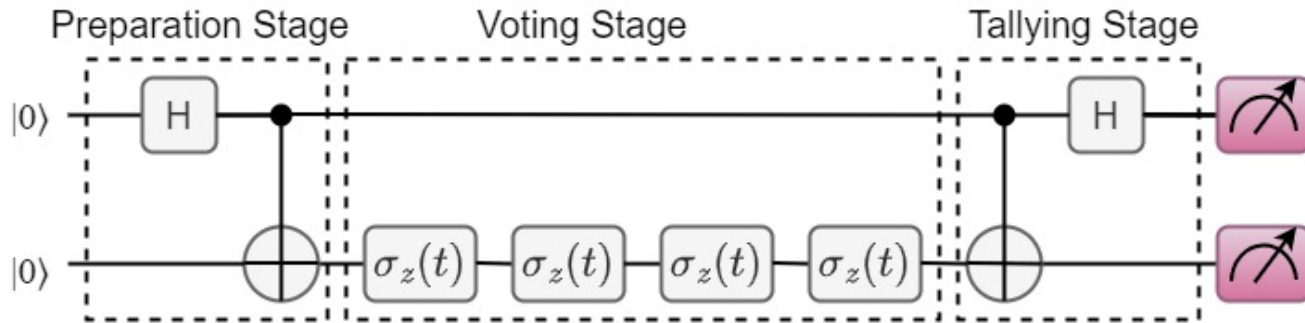


Experimental realization of quantum anonymous veto protocols using IBM quantum computer

Satish Kumar¹ · Anirban Pathak¹ 

Received: 18 November 2021 / Accepted: 3 August 2022

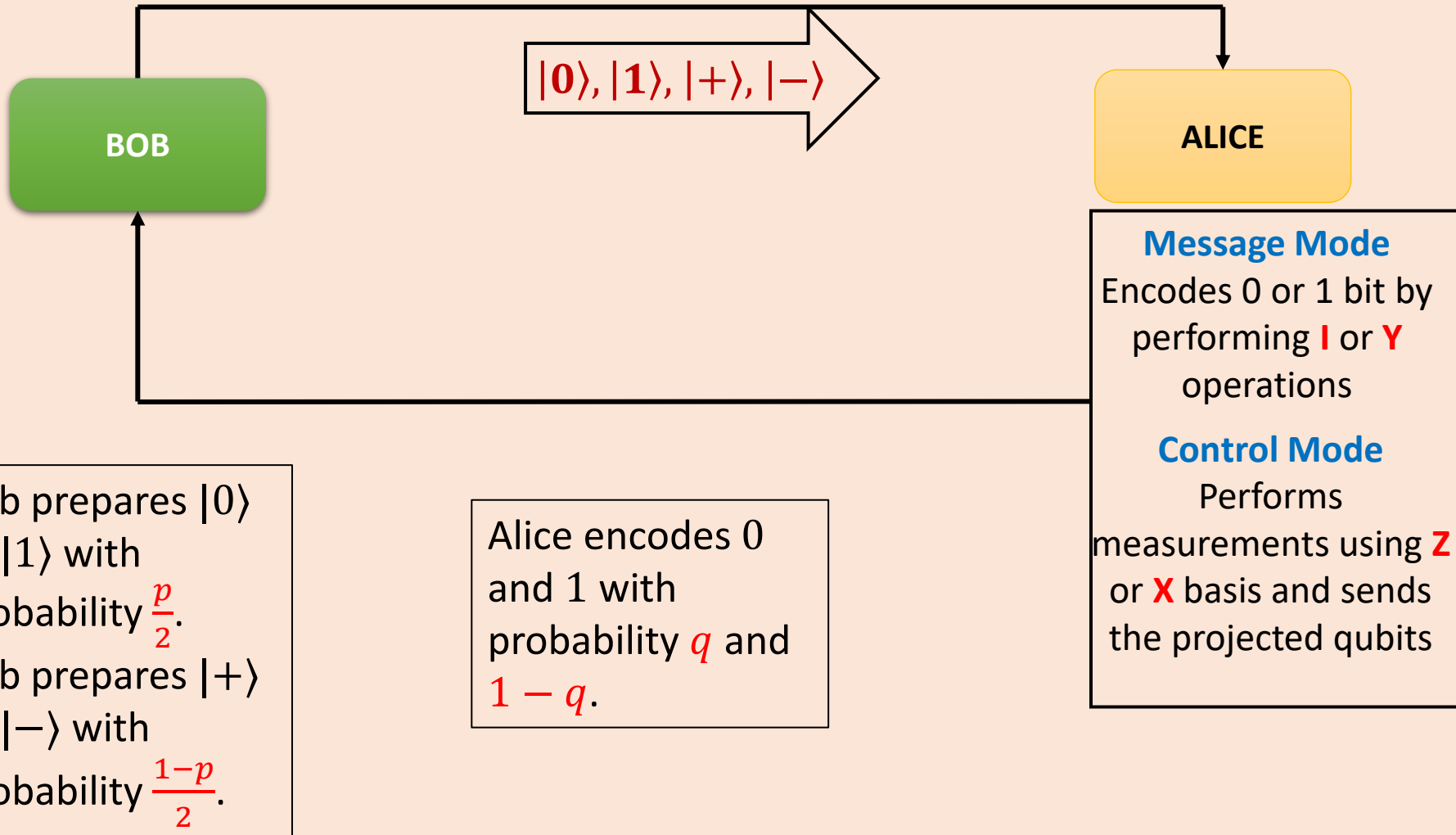
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022



A quantum circuit for experimental realization of Protocol A in case of 4 voters.

- Voter applies $\sigma_z(t) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2^t}} \end{bmatrix}$ in t^{th} iteration if he wishes to perform a veto, otherwise he applies identity operation $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

DL04 Protocol



Lucid ideas of game theory in our context

- **Nash equilibrium:** A situation where no player can gain (obtain higher payoff) by changing his/her own strategy only (i.e., by holding all other players' strategies fixed). This provides the optimal solution in a non-cooperative game.
- **Pareto optimal point:** A game's strategy set is considered Pareto efficient (or Pareto optimal) when there does not exist another strategy set that can improve the outcome for one player without negatively affecting any other player.
- **Pure and mixed strategies:** A mixed strategy exists in a strategic game, when the player does not choose one definite action, but rather, chooses according to a probability distribution. In contrast, a pure strategy involves a player choosing a single, specific action with certainty
- **Cooperative and noncooperative games:** In non-cooperative games focus on strategic behavior, where players act independently to maximize their own payoffs, whereas a non-cooperative game is a game in which there are no external rules or binding agreements that enforce the cooperation of the players.

Quantized game vs gaming the quantum

- **Quantized game:** Quantum resources are used to play a traditional game that can also be played without any quantum resources, but the use of quantum resources provide some advantages.
- **Gaming the quantum:** A quantum mechanical scenario (say, the realisation of DL04 protocol) is described using the concepts of the game theory.

What do we wish to do?

- We want to do ‘gaming the quantum’ by applying non-cooperative game theory to DL04 protocol to demonstrate how Nash equilibrium can serve as a viable solution concept, and to show that in our case, Pareto optimal Nash equilibrium point does not exist within the game scenarios considered, but mixed strategy Nash equilibrium points can be identified and employed to establish both upper and lower bounds for QBER. Further, to establish the vulnerability of the DL04 protocol to Pavičić attack in the message mode.

Matching pennies is an excellent example of zero-sum noncooperative game where no pure strategy nash equilibrium exist.

Zero-sum games: The total payoff is constant, and gains for one player result in losses for the other player(s).

Non-zero-sum games: It uses a tree-like diagram to represent sequential and simultaneous decision-making.



	Heads	Tails
Heads	+1, -1	-1, +1
Tails	-1, +1	+1, -1

Matching pennies

“Gaming the quantum” to get secure bound for quantum communication protocol

IOP Publishing

Phys. Scr. 99 (2024) 095106

<https://doi.org/10.1088/1402-4896/ad635f>

Physica Scripta



PAPER



Use of Nash equilibrium in finding game theoretic robust security bound on quantum bit error rate

RECEIVED
19 April 2024

REVISED
7 July 2024

ACCEPTED FOR PUBLICATION
15 July 2024

PUBLISHED
6 August 2024

Arindam Dutta*  and Anirban Pathak 

Department of Physics and Materials Science & Engineering, Jaypee Institute of Information Technology, A 10, Sector 62, Noida, UP-201309, India

* Author to whom any correspondence should be addressed.

E-mail: arindamsalt@gmail.com and anirban.pathak@gmail.com

Keywords: Nash equilibrium, quantum secure direct communication (QSDC), secure bound on QBER, quantum game

Abstract

Nash equilibrium is employed to find a game theoretic robust security bound on quantum bit error rate (QBER) for DL04 protocol which is a scheme for quantum secure direct communication that has been experimentally realized recently. The receiver, sender and eavesdropper (Eve) are considered to be quantum players (players having the capability to perform quantum operations). Specifically, Eve is considered to have the capability of performing quantum attacks (e.g., Wójcik’s original attack, Wójcik’s symmetrized attack and Pavičić attack) and classical intercept and resend attack. Game

Security analysis of DL04 against collective attacks

E_1 : $Q_{txy} = \text{SWAP}_{tx} \text{CPBS}_{txy} H_y$ Wójcik's original attack

E_2 : $S_{ty} = X_t Z_t \text{CNOT}_{ty} X_t$ Wójcik's symmetrized attack

E_3 : $Q_{txy} = \text{CNOT}_{ty} (\text{CNOT}_{tx} \otimes I_y) (I_t \otimes \text{PBS}_{xy})$
 $\times \text{CNOT}_{ty} (\text{CNOT}_{tx} \otimes I_y) (I_t \otimes H_x \otimes H_y)$, Pavičić attack

E_4 : Intercept and Resend.

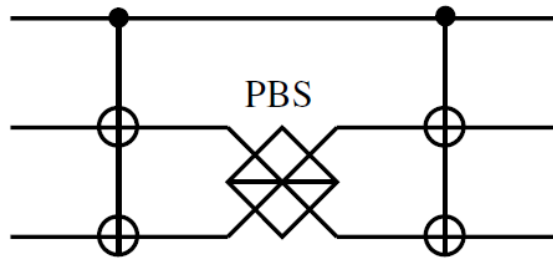
These attacks result in the state being in a higher dimensional Hilbert space with Eve's unitary operations, leading to a higher degree of randomization through quantum superposition. This affects the final joint probabilities of Alice's, Bob's and Eve's measurement outcomes.

Collective attack E_1 (Wójcik's attack)

$$Q_{txy} = \text{SWAP}_{tx} \text{CPBS}_{txy} H_y \equiv \text{SWAP}_{tx} \otimes I_y \text{CPBS}_{ixy} I_t \otimes I_x \otimes H_y \quad \text{Bob to Alice attack}$$

$$Q_{txy}^\dagger (\equiv Q_{txy}^{-1})$$

Alice to Bob attack



Controlled polarization beam splitter (CPBS). The polarization beam splitter (PBS) transmits (reflects) photons in the state $|0\rangle$ ($|1\rangle$).

Q_{txy} operates on three spatial modes t , x , and y , where t denotes the travel photon mode, two auxiliary modes x , y are Eve's ancillary state.

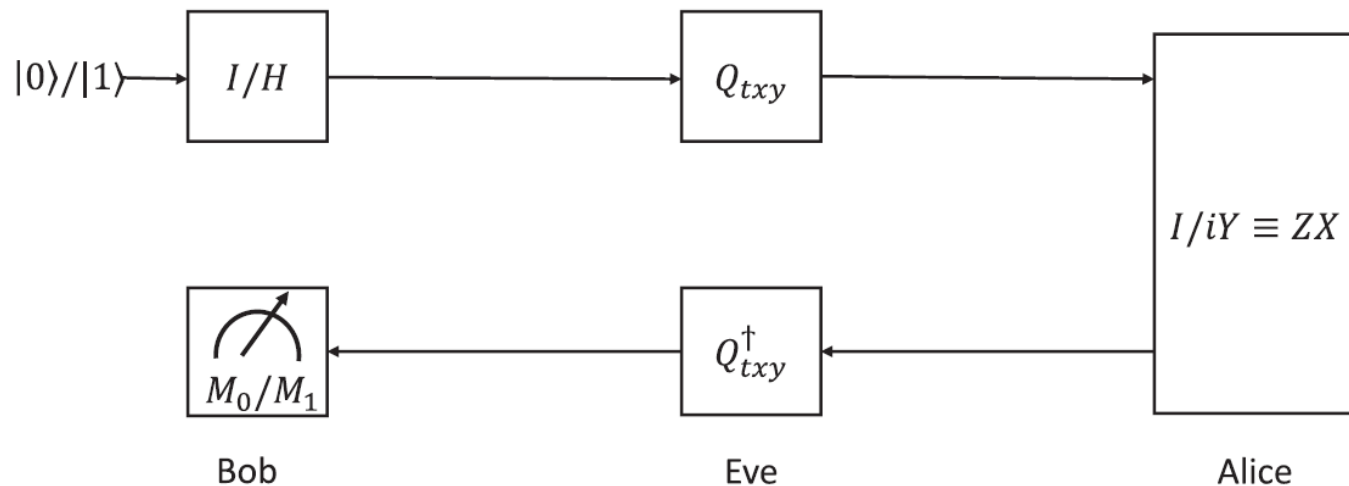
Transformation relation by Eve's operations

$$\left. \begin{array}{l} |0\rangle|\text{vac}\rangle|0\rangle \\ |0\rangle|\text{vac}\rangle|1\rangle \\ |1\rangle|\text{vac}\rangle|0\rangle \\ |1\rangle|\text{vac}\rangle|1\rangle \end{array} \right\} \xrightarrow{\text{CPBS}} \left\{ \begin{array}{l} |0\rangle|0\rangle|\text{vac}\rangle \\ |0\rangle|\text{vac}\rangle|1\rangle \\ |1\rangle|\text{vac}\rangle|0\rangle \\ |1\rangle|1\rangle|\text{vac}\rangle \end{array} \right\}$$

$$\left. \begin{array}{l} |0\rangle|\text{vac}\rangle|0\rangle \\ |0\rangle|\text{vac}\rangle|1\rangle \\ |1\rangle|\text{vac}\rangle|0\rangle \\ |1\rangle|\text{vac}\rangle|1\rangle \end{array} \right\} \xrightarrow{Q} \left\{ \begin{array}{l} |0\rangle|0\rangle|\text{vac}\rangle + |\text{vac}\rangle|0\rangle|1\rangle \\ |0\rangle|0\rangle|\text{vac}\rangle - |\text{vac}\rangle|0\rangle|1\rangle \\ |\text{vac}\rangle|1\rangle|0\rangle + |1\rangle|1\rangle|\text{vac}\rangle \\ |\text{vac}\rangle|1\rangle|0\rangle - |1\rangle|1\rangle|\text{vac}\rangle \end{array} \right\}$$

Wójcik, A. (2003). Eavesdropping on the "ping-pong" quantum communication protocol. *Physical Review Letters*, 90(15), 157901.

DL04 as a quantum game



Our approach: Evaluate mixed strategy Nash equilibrium by taking three sets of game scenarios E_1 - E_2 , E_1 - E_3 and E_2 - E_3 scenario where each player is looking to play a mixed quantum strategy that makes her opponent indifferent between her pure quantum strategies. Based on this assumption, we compare the results derived from Nash equilibrium points to obtain the secure bound of QBER

Q_{txy} operation on travel photon in Bob-Alice attack

$$\begin{aligned}
 |B - A\rangle_{|0\rangle_{E_1}} &= Q_{txy} |0\rangle_t |\text{vac}\rangle_x |0\rangle_y \\
 &= \text{SWAP}_{tx} \text{CPBS}_{txy} H_y (|0\rangle |\text{vac}\rangle |0\rangle)_{txy} \\
 &= \text{SWAP}_{tx} \text{CPBS}_{txy} \frac{1}{\sqrt{2}} (|0\rangle |\text{vac}\rangle |0\rangle + |0\rangle |\text{vac}\rangle |1\rangle)_{txy} \\
 &= \text{SWAP}_{tx} \frac{1}{\sqrt{2}} (|0\rangle |0\rangle |\text{vac}\rangle + |0\rangle |\text{vac}\rangle |1\rangle)_{txy} \\
 &= \frac{1}{\sqrt{2}} [|0\rangle |0\rangle |\text{vac}\rangle + |\text{vac}\rangle |0\rangle |1\rangle]_{txy},
 \end{aligned}$$

Q_{txy}^{-1} operation on travel photon in Alice-Bob attack after encoding 0 bit by Alice.

$$\begin{aligned}
 |A - B\rangle_{|0\rangle_{E_1}}^0 &= Q_{txy}^{-1} |B - A\rangle_{|0\rangle_{E_1}}^0 \\
 &= Q_{txy}^{-1} \frac{1}{\sqrt{2}} [|0\rangle |0\rangle |\text{vac}\rangle + |\text{vac}\rangle |0\rangle |1\rangle]_{txy} \\
 &= H_y \text{CPBS}_{txy} \text{SWAP}_{tx} \frac{1}{\sqrt{2}} [|0\rangle |0\rangle |\text{vac}\rangle + |\text{vac}\rangle |0\rangle |1\rangle]_{txy} \\
 &= H_y \text{CPBS}_{txy} \frac{1}{\sqrt{2}} [|0\rangle |0\rangle |\text{vac}\rangle + |0\rangle |\text{vac}\rangle |1\rangle]_{txy} \\
 &= H_y \frac{1}{\sqrt{2}} [|0\rangle |\text{vac}\rangle |0\rangle + |0\rangle |\text{vac}\rangle |1\rangle]_{txy} \\
 &= |0\rangle_t |\text{vac}\rangle_x |0\rangle_y.
 \end{aligned}$$

Rest cases when Alice encodes 0 bit

$$|A - B\rangle_{|1\rangle_{E_1}}^0 = |1\rangle_t |\text{vac}\rangle_x |0\rangle_y,$$

$$|A - B\rangle_{|+\rangle_{E_1}}^0 = |+\rangle_t |\text{vac}\rangle_x |0\rangle_y,$$

$$|A - B\rangle_{|-\rangle_{E_1}}^0 = |-\rangle_t |\text{vac}\rangle_x |0\rangle_y,$$

Continue...

$$|B - A\rangle_{|0\rangle} = \frac{1}{\sqrt{2}} [|0\rangle |0\rangle |\text{vac}\rangle + |\text{vac}\rangle |0\rangle |1\rangle]_{txy}$$

$$\begin{aligned} |A - B\rangle_{|0\rangle E_1} &= Q_{txy}^{-1} iY_t^1 \frac{1}{\sqrt{2}} [|0\rangle |0\rangle |\text{vac}\rangle + |\text{vac}\rangle |0\rangle |1\rangle]_{txy} \\ &= Q_{txy}^{-1} \frac{1}{\sqrt{2}} [-|1\rangle |0\rangle |\text{vac}\rangle + |\text{vac}\rangle |0\rangle |1\rangle]_{txy} \\ &= H_y \text{CPBS}_{txy} \text{SWAP}_{tx} \frac{1}{\sqrt{2}} [-|1\rangle |0\rangle |\text{vac}\rangle + |\text{vac}\rangle |0\rangle |1\rangle]_{txy} \\ &= H_y \text{CPBS}_{txy} \frac{1}{\sqrt{2}} [-|0\rangle |1\rangle |\text{vac}\rangle + |0\rangle |\text{vac}\rangle |1\rangle]_{txy} \\ &= H_y \frac{1}{\sqrt{2}} [-|0\rangle |1\rangle |\text{vac}\rangle + |0\rangle |\text{vac}\rangle |1\rangle]_{txy} \\ &= \left[-\frac{1}{\sqrt{2}} |0\rangle |1\rangle |\text{vac}\rangle + \frac{1}{2} |0\rangle |\text{vac}\rangle |0\rangle - \frac{1}{2} |0\rangle |\text{vac}\rangle |1\rangle \right]_{txy} . \end{aligned}$$

$$\begin{aligned} |B - A\rangle_{|1\rangle E_1} &= Q_{txy} |1\rangle_t |\text{vac}\rangle_x |0\rangle_y \\ &= \frac{1}{\sqrt{2}} [|\text{vac}\rangle |1\rangle |0\rangle + |1\rangle |1\rangle |\text{vac}\rangle]_{txy} . \end{aligned}$$

$$\begin{aligned} |A - B\rangle_{|1\rangle E_1} &= Q_{txy}^{-1} iY_t^1 \frac{1}{\sqrt{2}} [|\text{vac}\rangle |1\rangle |0\rangle + |1\rangle |1\rangle |\text{vac}\rangle]_{txy} \\ &= \left[\frac{1}{\sqrt{2}} |1\rangle |0\rangle |\text{vac}\rangle + \frac{1}{2} |1\rangle |\text{vac}\rangle |0\rangle + \frac{1}{2} |1\rangle |\text{vac}\rangle |1\rangle \right]_{txy} . \end{aligned}$$

$$|B - A\rangle_{|+\rangle E_1} = \frac{1}{2} [|0\rangle |0\rangle |\text{vac}\rangle + |\text{vac}\rangle |0\rangle |1\rangle + |\text{vac}\rangle |1\rangle |0\rangle + |1\rangle |1\rangle |\text{vac}\rangle]_{txy} ,$$

$$\begin{aligned} |A - B\rangle_{|+\rangle E_1} &= \left[\frac{1}{2} \{ |+\rangle |\text{vac}\rangle |0\rangle - |-\rangle |\text{vac}\rangle |1\rangle \} \right. \\ &\quad \left. + \frac{1}{2\sqrt{2}} \{ -|+\rangle |1\rangle |\text{vac}\rangle - |-\rangle |1\rangle |\text{vac}\rangle + |+\rangle |0\rangle |\text{vac}\rangle - |-\rangle |0\rangle |\text{vac}\rangle \} \right]_{txy} , \end{aligned}$$

$$|B - A\rangle_{|-\rangle E_1} = \frac{1}{2} [|0\rangle |0\rangle |\text{vac}\rangle + |\text{vac}\rangle |0\rangle |1\rangle - |\text{vac}\rangle |1\rangle |0\rangle - |1\rangle |1\rangle |\text{vac}\rangle]_{txy} ,$$

$$\begin{aligned} |A - B\rangle_{|-\rangle E_1} &= \left[\frac{1}{2} \{ |-\rangle |\text{vac}\rangle |0\rangle - |+\rangle |\text{vac}\rangle |1\rangle \} \right. \\ &\quad \left. + \frac{1}{2\sqrt{2}} \{ -|+\rangle |1\rangle |\text{vac}\rangle - |-\rangle |1\rangle |\text{vac}\rangle - |+\rangle |0\rangle |\text{vac}\rangle + |-\rangle |0\rangle |\text{vac}\rangle \} \right]_{txy} . \end{aligned}$$

Continue...

p_{jmk} where j , m and k represent Alice, Bob and Eve's encoding, decoding, and decoding information, respectively.

$k = 0$ if the auxiliary state is $|\text{vac}\rangle_x|0\rangle_y$,

$k = 1$ if the auxiliary states are $|0\rangle_x|\text{vac}\rangle_y$, $|1\rangle_x|\text{vac}\rangle_y$ and $|\text{vac}\rangle_x|1\rangle_y$.

$$|A - B\rangle_{|0\rangle_{E_1}}^0 = |0\rangle_t |\text{vac}\rangle_x |0\rangle_y.$$

$$\frac{p}{2}, q$$

$$|A - B\rangle_{|1\rangle_{E_1}}^0 = |1\rangle_t |\text{vac}\rangle_x |0\rangle_y,$$

$$\frac{p}{2}, q$$

$$|A - B\rangle_{|+\rangle_{E_1}}^0 = |+\rangle_t |\text{vac}\rangle_x |0\rangle_y,$$

$$\frac{1-p}{2}, q$$

$$|A - B\rangle_{|-\rangle_{E_1}}^0 = |-\rangle_t |\text{vac}\rangle_x |0\rangle_y,$$

$$\frac{1-p}{2}, q$$

Continue...

$$|A - B\rangle_{|0\rangle E_1}^1 = \left[-\frac{1}{\sqrt{2}}|0\rangle|1\rangle|\text{vac}\rangle + \frac{1}{2}|0\rangle|\text{vac}\rangle|0\rangle - \frac{1}{2}|0\rangle|\text{vac}\rangle|1\rangle \right]_{txy}$$

$$\frac{p}{2}, 1 - q$$

$$|A - B\rangle_{|1\rangle E_1}^1 = \left[\frac{1}{\sqrt{2}}|1\rangle|0\rangle|\text{vac}\rangle + \frac{1}{2}|1\rangle|\text{vac}\rangle|0\rangle + \frac{1}{2}|1\rangle|\text{vac}\rangle|1\rangle \right]_{txy}$$

$$\frac{p}{2}, 1 - q$$

$$|A - B\rangle_{|+\rangle E_1}^1 = \left[\frac{1}{2}\{|+\rangle|\text{vac}\rangle|0\rangle - |-\rangle|\text{vac}\rangle|1\rangle\} + \frac{1}{2\sqrt{2}}\{-|+\rangle|1\rangle|\text{vac}\rangle - |-\rangle|1\rangle|\text{vac}\rangle + |+\rangle|0\rangle|\text{vac}\rangle - |-\rangle|0\rangle|\text{vac}\rangle\} \right]_{txy}$$

$$\frac{1 - p}{2}, 1 - q$$

$$|A - B\rangle_{|-\rangle E_1}^1 = \left[\frac{1}{2}\{|-\rangle|\text{vac}\rangle|0\rangle - |+\rangle|\text{vac}\rangle|1\rangle\} + \frac{1}{2\sqrt{2}}\{-|+\rangle|1\rangle|\text{vac}\rangle - |-\rangle|1\rangle|\text{vac}\rangle - |+\rangle|0\rangle|\text{vac}\rangle + |-\rangle|0\rangle|\text{vac}\rangle\} \right]_{txy}$$

$$\frac{1 - p}{2}, 1 - q$$

Payoff Functions

Generalized Form

$$P_A^{\mathcal{E}}(p, q) = \omega_a I(A, B) - \omega_b I(A, E) - \omega_c I(B, E) + \omega_d \left(\frac{P_d + \text{QBER}}{2} \right)$$

$$P_B^{\mathcal{E}}(p, q) = \omega_a I(A, B) - \omega_c I(A, E) - \omega_b I(B, E) + \omega_d \left(\frac{P_d + \text{QBER}}{2} \right)$$

$$P_E^{\mathcal{E}}(p, q) = -\omega_e I(A, B) + \omega_f I(A, E) + \omega_g I(B, E) + \omega_h \left(1 - \frac{P_d + \text{QBER}}{2} \right) - \omega_i n_1 - \omega_j n_2 - \omega_k n_3$$

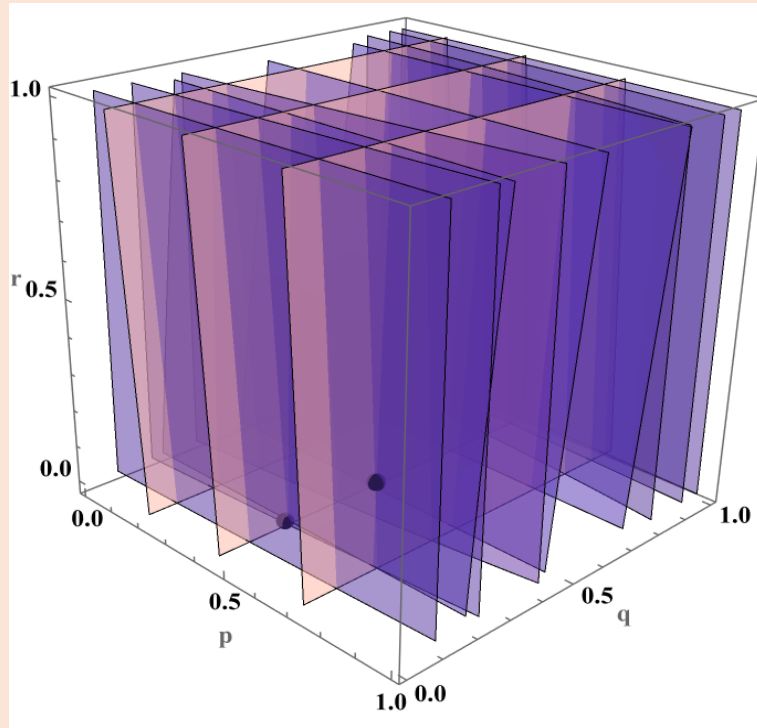
Simplified Form

$$P_A^{\mathcal{E}}(p, q) = 0.25 \times \left[I(A, B) - I(A, E) - I(B, E) + \left(\frac{P_d + \text{QBER}}{2} \right) \right]$$

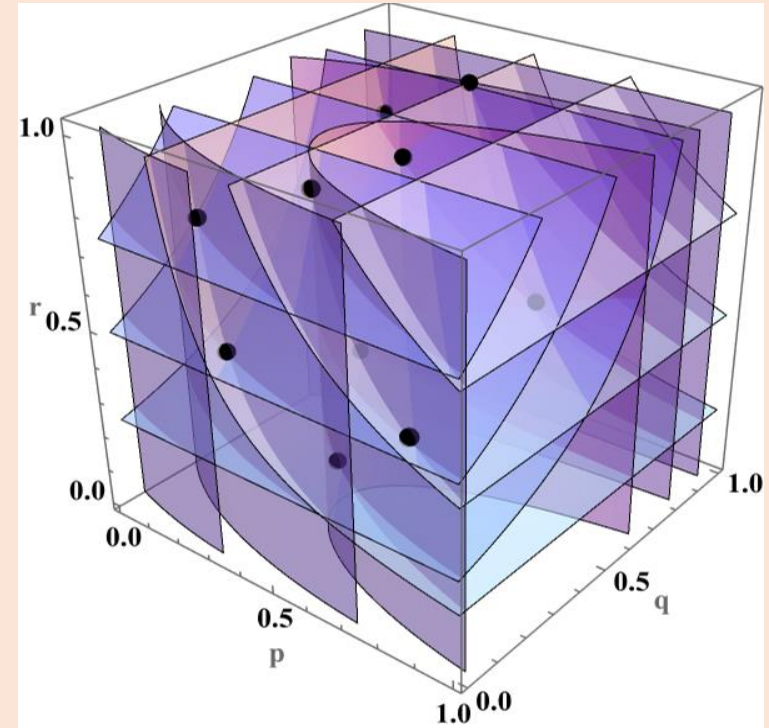
$$P_B^{\mathcal{E}}(p, q) = 0.25 \times \left[I(A, B) - I(A, E) - I(B, E) + \left(\frac{P_d + \text{QBER}}{2} \right) \right]$$

$$P_E^{\mathcal{E}}(p, q) = 0.25 \times \left[-I(A, B) + I(A, E) + I(B, E) + \left(1 - \frac{P_d + \text{QBER}}{2} \right) \right]$$

Nash Equilibrium Graph



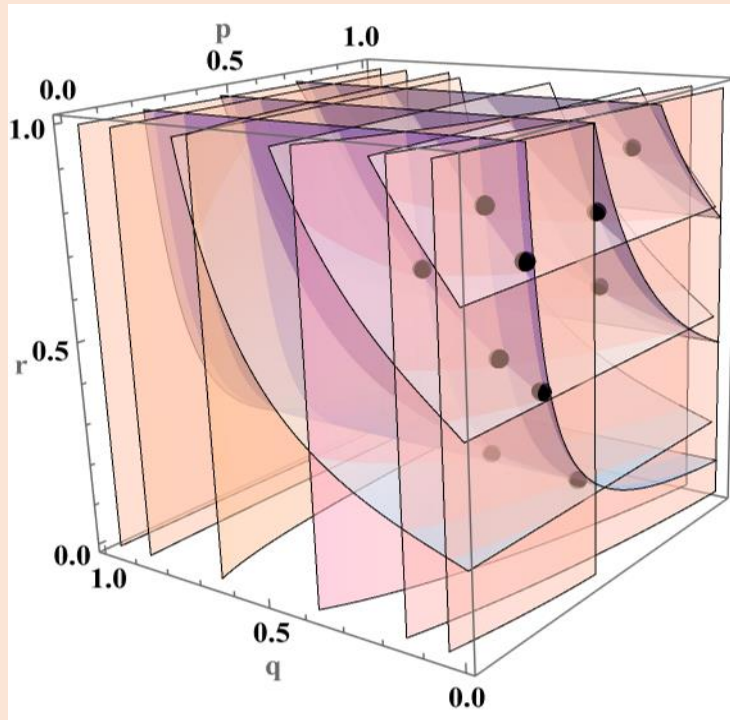
(a) $E_1 - E_2$ game



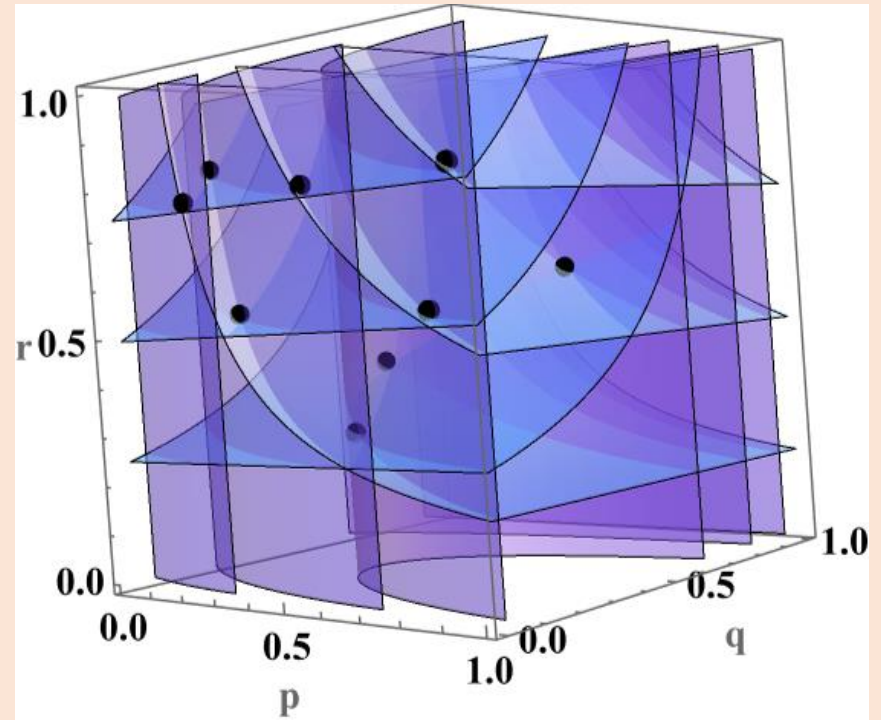
(b) $E_1 - E_3$ game

The low-density layer, medium-density layer, and high-density layer correspond to the best response functions of Alice, Bob, and Eve, respectively

Nash Equilibrium Graph



(c) $E_2 - E_3$ game



(d) $E_1 - E_4$ game

The low-density layer, medium-density layer, and high-density layer correspond to the best response functions of Alice, Bob, and Eve, respectively

Result Analysis

E_1-E_2 game scenario	Nash equilibrium point (p, q, r)	Alice's/Bob's payoff	Eve's payoff	Payoff difference	$\epsilon_{E_1-E_2}$
	(0.72, 0.208, 0.225)	0.055457	0.194543	0.13908	0.692404
	(0.45, 0.195, 0.005)	0.0446318	0.205368	0.16073	0.610303
E_1-E_3 game scenario	Nash equilibrium point (p, q, r)	Alice's/Bob's payoff	Eve's payoff	Payoff difference	$\epsilon_{E_1-E_3}$
	(0.22, 0.716, 0.88)	-0.110497	0.360497	0.47099	0.152451
	(0.442, 0.75, 0.999)	-0.0862188	0.336219	0.42243	0.18007
	(0.41, 0.39, 0.412)	-0.157149	0.407149	0.56429	0.177181
	(0.76, 0.577, 0.585)	-0.136264	0.386264	0.52252	0.21776
	(0.56, 0.14, 0.292)	-0.0796824	0.329682	0.40936	0.195874
	(0.325, 0.064, 0.532)	-0.0134987	0.263499	0.27699	0.329893
	(0.84, 0.047, 0.525)	0.0324084	0.217592	0.18518	0.460299
	(0.485, 0.465, 0.915)	-0.090828	0.340828	0.43165	0.363472
	(0.235, 0.096, 0.83)	-0.013356	0.263356	0.27671	0.463323
	(0.47, 0.195, 0.93)	-0.0182231	0.268223	0.28644	0.550258

Most potent
 attack is **E_3** and
 upper bound of
 QBER is **14.38%**

Result Analysis

E_2-E_3 game scenario	Nash equilibrium point (p, q, r)	Alice's/Bob's payoff	Eve's payoff	Payoff difference	$\epsilon_{E_2-E_3}$
	(0.385, 0.215, 0.262)	-0.111965	0.361965	0.47393	0.151087
	(0.47, 0.055, 0.205)	-0.0276507	0.277651	0.3053	0.143882
	(0.25, 0.096, 0.54)	-0.0216673	0.271667	0.29633	0.31482
	(0.24, 0.268, 0.71)	-0.0436386	0.293639	0.33727	0.35838
	(0.70, 0.138, 0.58)	-0.00442078	0.254421	0.25884	0.430969
	(0.284, 0.02, 0.472)	0.0188573	0.231143	0.21228	0.298653
	(0.235, 0.02, 0.758)	0.0320242	0.217976	0.18595	0.461603
	(0.222, 0.10, 0.865)	0.015688	0.234312	0.21862	0.492488
	(0.54, 0.048, 0.795)	0.0558727	0.194127	0.13825	0.587155
	(0.80, 0.115, 0.885)	0.0722149	0.177785	0.10557	0.709991
E_1-E_4 game scenario	Nash equilibrium point (p, q, r)	Alice's/Bob's payoff	Eve's payoff	Payoff difference	$\epsilon_{E_1-E_4}$
	(0.23, 0.095, 0.825)	-0.00433851	0.254339	0.25867	0.502924
	(0.245, 0.008, 0.76)	0.0492999	0.2007	0.1514	0.529315
	(0.572, 0.02, 0.765)	0.0750153	0.174985	0.0999	0.648014
	(0.928, 0.032, 0.774)	0.0997124	0.150288	0.0505	0.77876
	(0.324, 0.065, 0.535)	0.0114311	0.238569	0.22713	0.447399
	(0.85, 0.045, 0.522)	0.0603314	0.189669	0.12933	0.580622
	(0.405, 0.387, 0.415)	-0.124349	0.374349	0.49869	0.324962
	(0.54, 0.15, 0.295)	-0.0471361	0.297136	0.34427	0.369328
	(0.75, 0.57, 0.582)	-0.114078	0.364078	0.47815	0.323478

What else we do using nonclassical states?

Quantum Information Processing (2020) 19:132
<https://doi.org/10.1007/s11128-020-02627-3>



Continuous variable direct secure quantum communication using Gaussian states

S. Srikara¹ · Kishore Thapliyal² · Anirban Pathak³

Received: 29 September 2019 / Accepted: 27 February 2020 / Published online: 10 March 2020
© Springer Science+Business Media, LLC, part of Springer Nature 2020

Abstract

Continuous variable one-way and controlled two-way direct secure quantum communication schemes have been designed using Gaussian states. Specifically, a scheme for continuous variable quantum secure direct communication and another scheme for continuous variable controlled quantum dialogue are proposed using single-mode squeezed coherent states. The security of the proposed schemes against a set of attack

Uses single mode squeezed coherent state

Single mode squeezed coherent state is also used for experimental realisation of our scheme

IL NUOVO CIMENTO 45 C (2022) 176
DOI 10.1393/ncc/i2022-22176-6

COMMUNICATIONS: SIF Congress 2021

Implementation and security analysis of continuous variable quantum secure direct communication protocols

I. PAPARELLE⁽¹⁾, M. G. A. PARIS⁽²⁾ and A. ZAVATTA⁽³⁾

- ⁽¹⁾ *Istituto Nazionale di Ottica (CNR-INO), Sezione di Trieste - Trieste, Italy*
⁽²⁾ *Dipartimento di Fisica Aldo Pontremoli, Università degli Studi di Milano - Milano, Italy*
⁽³⁾ *Istituto Nazionale di Ottica (CNR-INO) - Firenze, Italy*

received 31 January 2022

Summary. — The development of supercomputers and quantum computers will threaten current secure communication protocols. However, quantum mechanics offers a solution guaranteeing physical layer and provable security of communications. In particular, quantum secure direct communication (QSDC) allows secret messages to be directly and securely communicated over a quantum channel. We investigate

What else we do using nonclassical states?

Foundations of Physics (2023) 53:21
<https://doi.org/10.1007/s10701-022-00661-y>



Continuous Variable Controlled Quantum Conference

Ashwin Saxena¹ · Anirban Pathak¹

Received: 10 September 2022 / Accepted: 13 December 2022 / Published online: 20 December 2022

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract

Using different quantum states (e.g., two mode squeezed-state, multipartite GHZ-like-states) as quantum resources, two protocols for "continuous variable (CV) controlled quantum conference" are proposed. These CV protocols for controlled quantum conferences (CQCs) are the first of their kind and can be reduced to CV protocols for various other cryptographic tasks. In the proposed protocols, Charlie is considered the controller, having the power to terminate the protocol at any time and to control the flow of information among the other users by using a parameterised control switch. Based on the information shared by Charlie with the participants of the conference, the control power of Charlie is evaluated and compared to the proposed protocols. The comparison of the efficiency of the proposed protocols has revealed that, under certain constraints, the 4-mode GHZ state-based protocol is more efficient than the two-mode squeezed state-based protocol. The control power

What else we do using nonclassical states?

International Journal of Quantum Information
Vol. 18, No. 4 (2020) 2050009 (17 pages)
© World Scientific Publishing Company
DOI: [10.1142/S0219749920500094](https://doi.org/10.1142/S0219749920500094)



Continuous variable controlled quantum dialogue and secure multiparty quantum computation

Two-mode
squeezed state

Ashwin Saxena^{*,‡}, Kishore Thapliyal^{*,†,§} and Anirban Pathak^{*,¶}

A continuous variable (CV) controlled quantum dialogue (QD) scheme is proposed. The scheme is further modified to obtain two other protocols of (CV) secure multiparty computation. The first one of these protocols provides a solution of two-party socialist millionaire problem, while the second protocol provides a solution for a special type of multi-party socialist millionaire problem which can be viewed as a protocol for multiparty quantum private comparison. It is shown that the proposed scheme of (CV) controlled (QD) can be performed using bipartite entanglement and can be reduced to obtain several other two- and three-party cryptographic schemes in the limiting cases. The security of the proposed scheme and its advantage over corresponding discrete variable (DV) counterpart are also discussed. Specifically, the ignorance of an eavesdropper, i.e., information encoded by Alice/Bob, in the proposed scheme is shown to be more than that in the corresponding (DV) scheme, and thus the present scheme is less prone to information leakage inherent with the (DV) (QD) based schemes. It is further established that the proposed scheme can be viewed as a

What else we do using nonclassical states?

[Home](#) > [Quantum Information Processing](#) > [Article](#)

Continuous variable B92 quantum key distribution protocol using single photon added and subtracted coherent states

Published: 06 October 2020

Volume 19, article number 371, (2020) [Cite this article](#)

Entanglement routing problem: Tools (operations) and tricks (protocols) used

- An undirected finite graph $G = (V, E)$ is defined by a set of vertices $V \subsetneq \mathbb{N}$ and a set $E \subseteq V \times V$ of edges.
- A simple graph is a graph without any loop (an edge that connects a vertex with itself) and multiple edges connecting the same pair of vertices.
- The set of all vertices having a shared edge with a given vertex a is called the neighborhood of a and is denoted by N_a .
- **(Vertex Deletion):** Deleting a vertex v results in a graph where the vertex v and all the edges connected to it are removed.

$$G - v = (V \setminus v, \{e \in E : e \cap v = \emptyset\})$$

- **(Local complementation):** A local complementation LC_v is a graph operation specified by a vertex v , taking a graph G to $LC_v(G)$ by replacing the neighborhood of v by its complement.

Local complementation acts on the neighbourhood of a vertex by removing edges if they are present and adding missing edges, if any.

- **(Vertex-minor):** A graph H is called a vertex-minor of G if a sequence of local complementations and vertex-deletions maps G to H .

Understand entanglement routing problem: Tools (operations) and tricks (protocols) used by us (continued)

The simple graph $G=(V,E)$ defined in last slide is a mathematical entity.

In the quantum world, we can associate a pure quantum state $|G\rangle$ with it, called a graph state.

A Graph state is defined on a Hilbert space $H_V = (\mathbb{C}^2)^{\otimes V}$.

Each vertex in V is assigned a qubit in the state $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$. Subsequently, a controlled-Z operation is applied to a pair of qubits sharing an edge to construct the graph state $|G\rangle$ associated with the graph G as $\prod_{(i,j) \in E} CZ_{i,j} |+\rangle^{\otimes V}$.

- **Proposition 1.** (Z-measurement)
Measurement of a qubit, corresponding to the vertex v , in the Z-basis is represented by the vertex deletion of v .

$$Z_v(G) = G - v$$

- **Proposition 2.** (Y-measurement)
Measurement of a qubit, corresponding to the vertex v , in the Y-basis is represented by,

$$Y_v(G) = Z_v LC_v(G)$$

- **Proposition 3.** (X-measurement)
Measurement of a qubit, corresponding to the vertex v , in the X-basis is represented by

$$X_v(G) = LC_w Z_v LC_v LC_w(G),$$

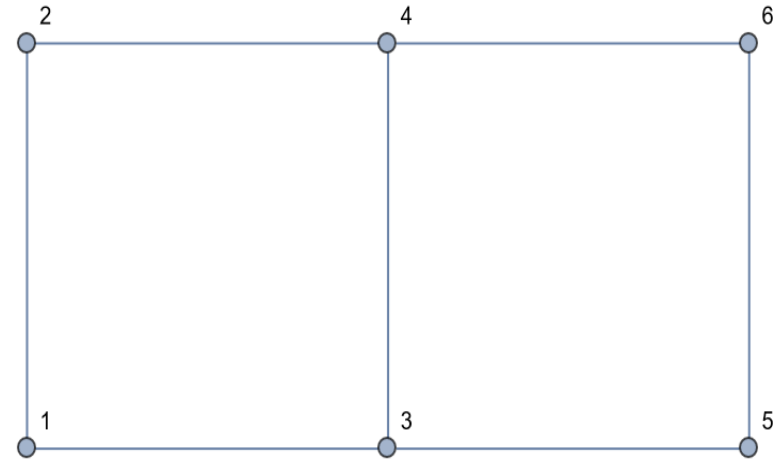
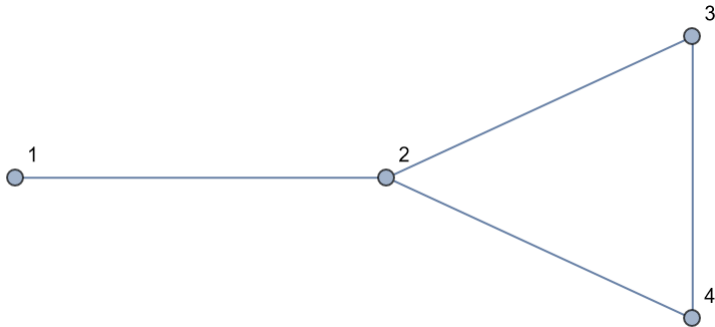
where $w \in N_v$.

Let's visualize

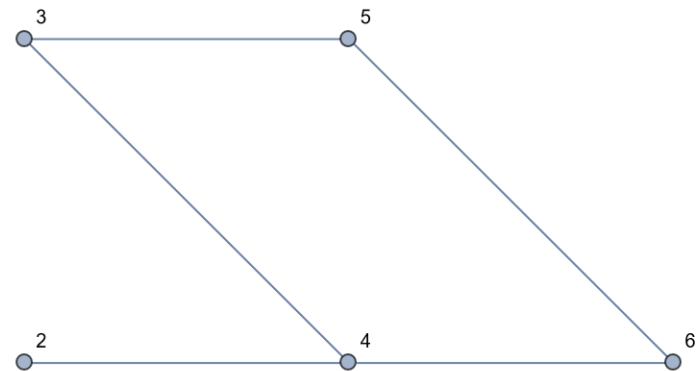
- A simple graph which is too simple



- NEIGHBOURHOOD OF 3 IS $\{2,4\}$ which are not connected so if we apply



Apply Z_1

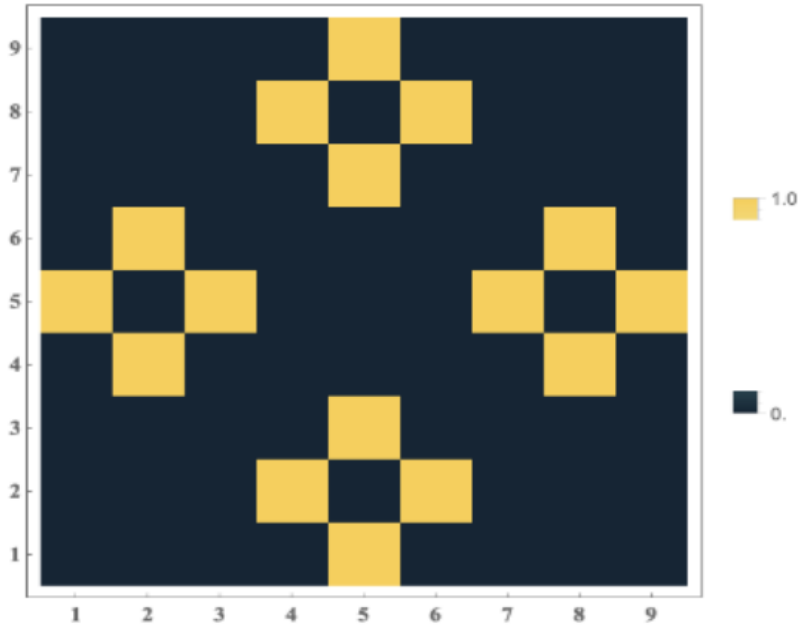


A bit of simulation on the possibility of removing bottlenecks in grid network

- How to create matrix maps of the simulation data reveal pairs of nodes in the grid networks that are more likely to run into a situation with bottlenecks while using the shortest path protocol?
- Given a graph $G(V, E)$ and two distinct vertices $a, b \in V$
- Check whether it's possible to establish a bell pair between a, b , and simultaneously with some other pair $c, d \in V$.
- Denote success, i.e., simultaneous entanglement generation, with '1' and failure with '0',
- Sum this variable over all possible c, d to yield an integer for any a, b , denoted $e_{a,b}$.
- Do this for all possible pairs of vertices a, b . This gives us a matrix M , where the matrix element $M_{i,j} = e_{i,j}$.
- M_{SP} : Matrix generated using the shortest path protocol; M_{RL} : Matrix generated using our protocol
- $M_{RL} - M_{SP}$: Quantify the advantage of our protocol.
- If $|E_{SP}|$ is length of the shortest path between two vertices, consider possible paths with edge lengths $|E_{SP}| + L$ for $0 \leq L \leq 6$. For M_{SP} , path length is $|E_{SP}|$.

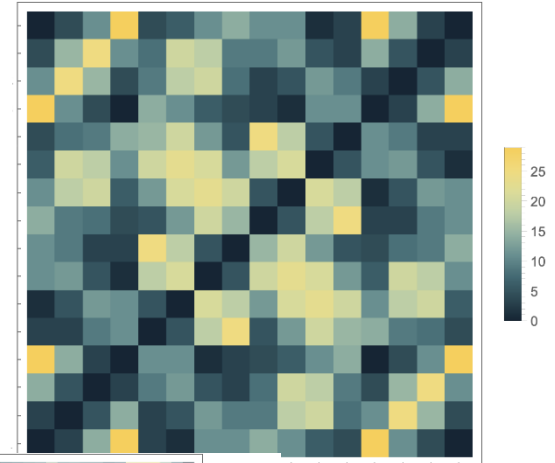
The higher is $e_{a,b}$ the lower the chances of a bottleneck issue

Simulation Results

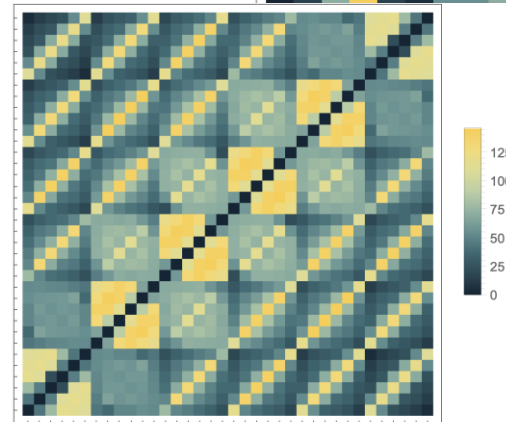


$M_{RL} - M_{SP}$ for 3X3 Grid Graph; 1 and 5.
Our protocol resolves 1 additional bottleneck compared to the shortest path protocol.

Our approach performs better, since it considers not just the shortest, but all paths satisfying the definition of a repeater line.



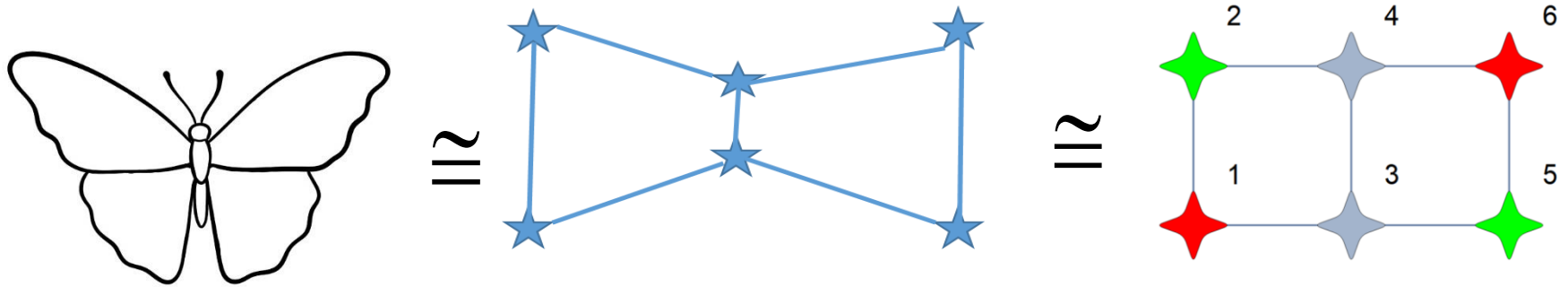
4X
4



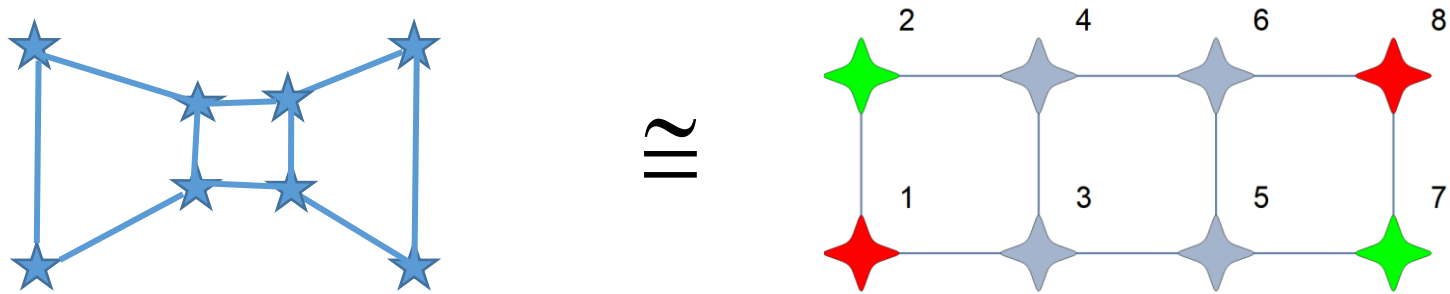
6X6

Our protocol finds over a hundred additional cases where the bottleneck could be resolved

Butterfly and butterfly-like networks

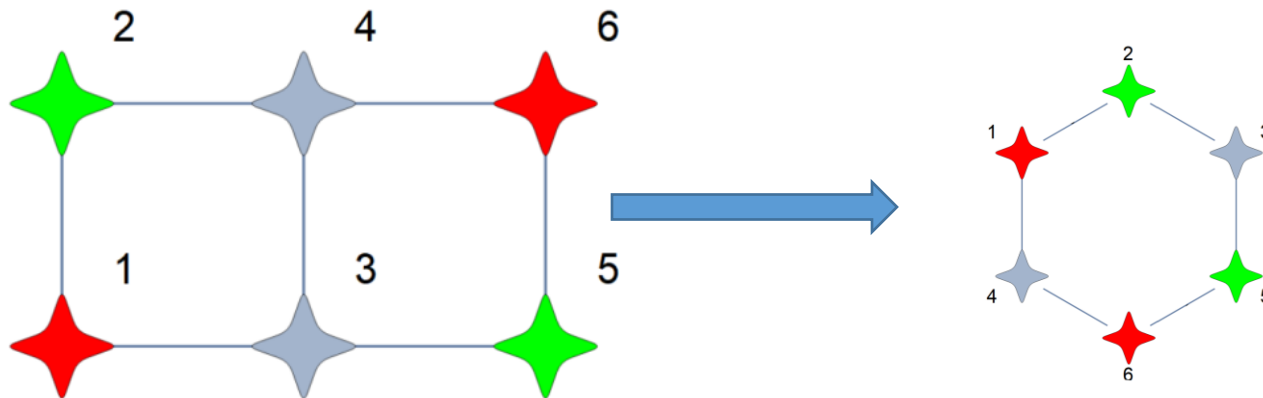
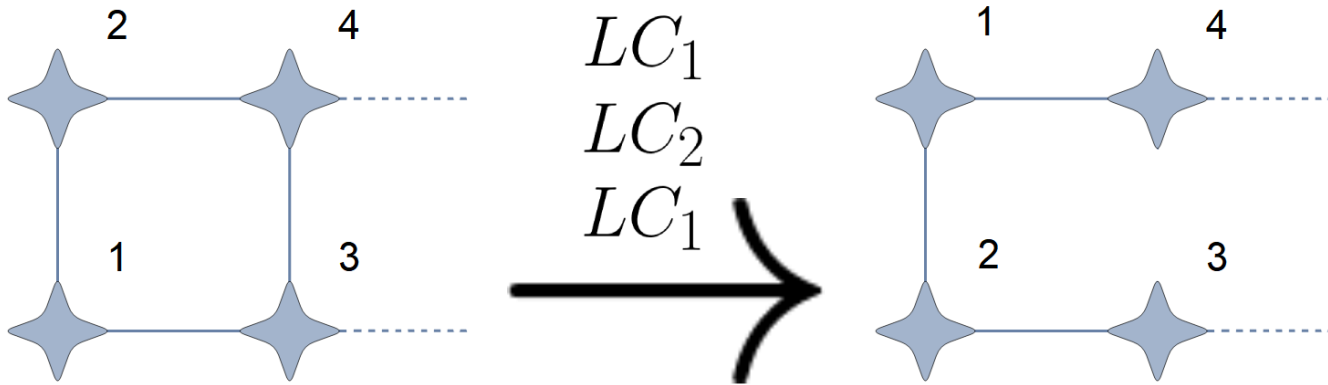


Butterfly networks



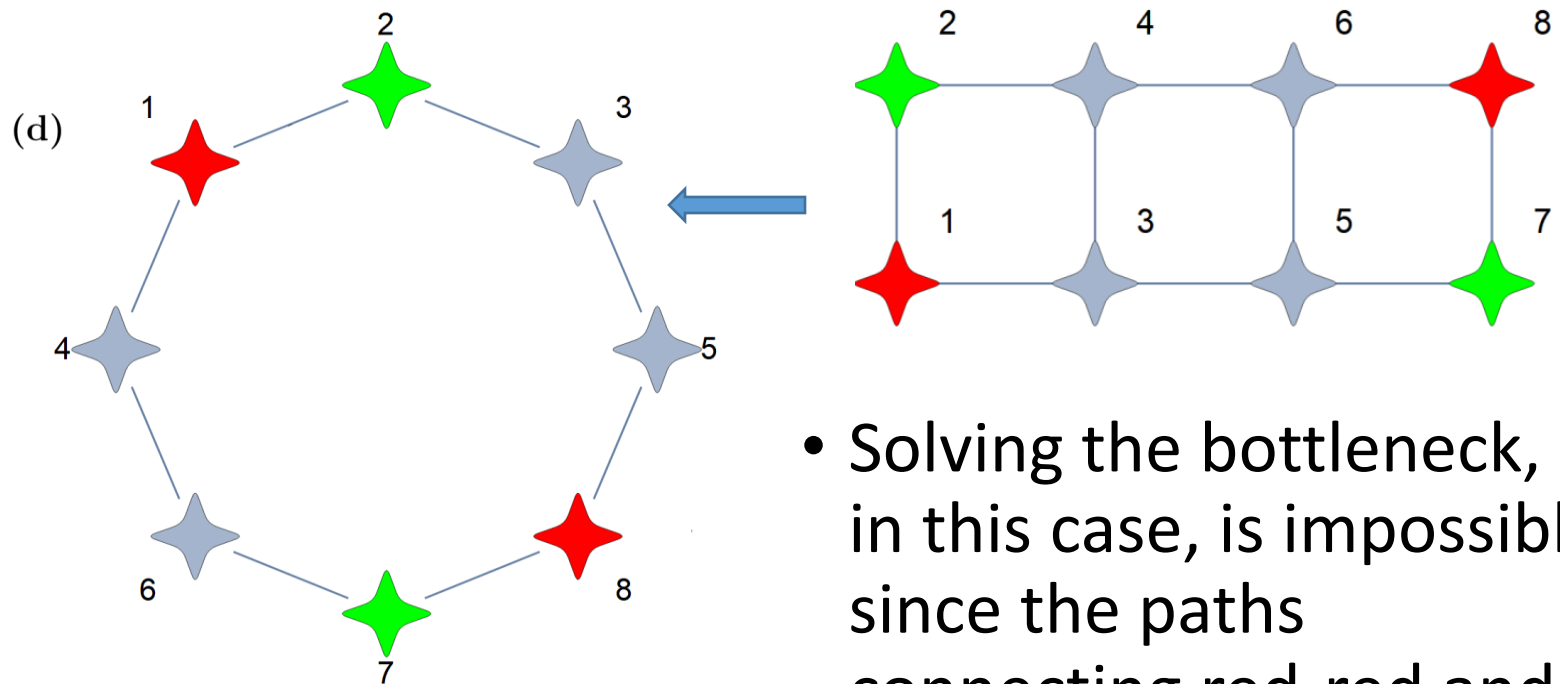
Butterfly-like networks

Advantage of transforming a grid graphs to a ring graph

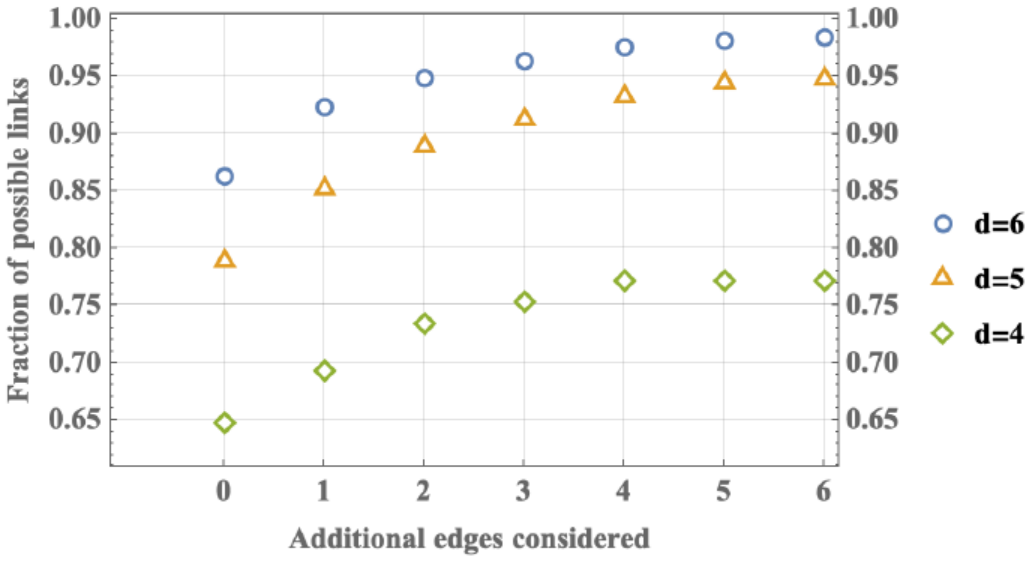


The bottleneck is removed

What happens in a butterfly like network?



- Solving the bottleneck, in this case, is impossible since the paths connecting red-red and green-green always cross.



Thank you

Our activities are supported by



Indo-US partnership 2020

