Quantum communication: The requirement, essential resources, new protocols and the effect of noise on them

Anirban Pathak

Department of Physics and Materials Sciences & Engineering

JIIT, Noida, India

S. N. Bose National Centre for Basic Sciences, Kolkata, India, January 30, 2018

International Symposium on New Frontiers in Quantum Correlations (ISNFQC18)

Expectations from quantum communication is very high

as it provides unconditional security

What led to this expectation?

1976- Whitfield Diffie and Martin E. Hellman, protocol based on discrete logarithmic problem.

1978 -(**RSA**) Ronald Rivest, Adi Shamir and Leonard Adleman invented key distribution protocol based on large prime factor problem.

Security of these schemes are not unconditional as that depends on the complexity of a computational task(s)

Complexity theory: Longer security would require larger key

IOP Publishing Quantum Sci. Technol. 2 (2017) 020502 https://doi.org/10.1088/2058-9565/aa69cd

Quantum Science and Technology

CrossMark

PERSPECTIVE

Quantum cryptography: a view from classical cryptography

Johannes Buchmann[1], Johannes Braun, Denise Demirel and Matthias Geihs

PUBLISHED

Table 1. Security of instances of the discrete logarithm problem according to Lenstra and Verheul [10, 11].

Bit length of prime number instance	Secure until year
2048	2040
3106	2065
4096	2085
5120	2103
6144	2116

Implications of Shor's algorithm

- **1994- Peter Shor** introduced a **quantum algorithm** that can be used to quickly factorize large numbers.
- Shor's algorithm **solve both prime factorization** and **discrete logarithm.**
- RSA is based **on the assumption** that factoring large numbers is computationally intractable.
- Shor's algorithm **proves that RSA based cryptosystems are not secure if a scalable quantum computer can be built**

Recent success stories of building relatively big quantum computers is a serious threat to RSA and DF based systems. **Further, in 2017, D Wave processor factorised 200099; and Li et al., factorized 291311=> Li et al., used only 3 qubits.**

Analysis of security of banks

Owner(Payment Bank)	Website	Issues in Protocol support	insecure SSL ciphers suported by the server
Allahabad Bank	www.allahabadbank.in	Supports TLS 1.0, SSL 3.0, but SSL 3.0 is an outdated protocol version with known vulnerabilities.	TLS_RSA_WITH_RC4_128_SHA TLS_RSA_WITH_RC4_128_MD5
Andhra Bank	www.onlineandhrabank.net.in	OK	OK
Vijaya Bank	www.vijayabankonline.in	OK	TLS_RSA_WITH_RC4_128_SHA TLS_RSA_WITH_RC4_128_MD5
Central Bank of India	www.centralbank.net.in	Supports TLS 1.2, TLS 1.1, TLS 1.0, SSL 3.0, but SSL 3.0 is an outdated protocol version with known vulnerabilities.	TLS_RSA_WITH_RC4_128_SHA [insecure]TLS_RSA_WITH_RC4_128_MD5
Bank Of Baroda	www.bobibanking.com	OK	TLS_RSA_WITH_RC4_128_SHA TLS_RSA_WITH_RC4_128_MD5

Analysis of security of banks contd…

CORPORATION BANK	www.corpretail.com		TLS_DH_anon_WITH_AES_256_GCM_SHA384 TLS_DH_anon_WITH_AES_128_GCM_SHA256 TLS_DH_anon_WITH_SEED_CBC_SHA TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA TLS_DH_anon_WITH_AES_256_CBC_SHA256 TLS_DH_anon_WITH_AES_128_CBC_SHA256 TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA TLS_DH_anon_WITH_AES_256_CBC_SHA TLS_DH_anon_WITH_AES_128_CBC_SHA TLS_DH_anon_WITH_3DES_EDE_CBC_SHA TLS_DH_anon_WITH_DES_CBC_SHA TLS_DH_anon_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA TLS_RSA_WITH_RC4_128_MD5
Dena Bank	www.denaiconnect.co.in		TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 TLS_RSA_WITH_RC4_128_SHA TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_EXPORT_WITH_RC4_40_MD5

Similarly, we studied the security of 41 banks and have found most of them support insecure SSL ciphers.

Analysis of security of banks contd..

Owner(Payment Bank)	Website	Server Grade	Issues that reduced the grade
Allahabad Bank	www.allahabadbank.in	C	This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. This server accepts RC4 cipher, but only with older protocols. Grade capped to B
Andhra Bank	www.onlineandhrabank.net.in	A	
Vijaya Bank	www.vijayabankonline.in	B B	This server accepts RC4 cipher, but only with older protocols. Grade capped to B The server does not support Forward Secrecy with the reference browsers
Bank Of India	starconnectcbs.bankofindia.com	B	This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. The server does not support Forward Secrecy with the reference browsers

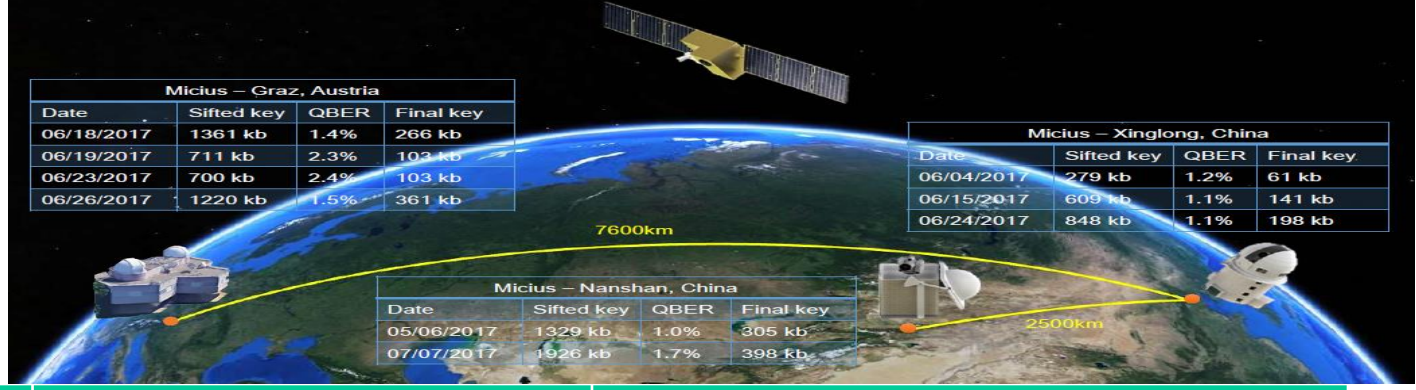
Poodle attack: Padding Oracle on Downgraded Legacy Encryption. SHA: Secure Hash algorithm; RC4 is a stream encryption algorithm.

Analysis of security of banks contd…

Bank Of Baroda	www.bobibanking.com	C	The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C This server accepts RC4 cipher, but only with older protocols. Grade capped to B. The server does not support Forward Secrecy with the reference browsers.
Canara Bank	netbanking.canarabank.in	F	This server is vulnerable to MITM attacks because it supports insecure renegotiation. Grade set to F The server does not support Forward Secrecy with the reference browsers.
Central Bank of India	www.centralbank.net.in	C	This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C This server accepts RC4 cipher, but only with older protocols. Grade capped to B. The server does not support Forward Secrecy with the reference browsers

Similarly, we studied security of 41 banks and have found 7 banks with grade F, 9 with C, 8 B, and remaining 17 A grade.

What has further enhanced the expectation:



Company	Website	Interesting products
Id Quantique	http://www.idquantique.com/	Network encryption, random number generator, photon counting device, single photon source, etc.
Toshiba	http://www.toshiba.eu/eu/Cambridge-Research-Laboratory/Quantum-Information-Group/Quantum-Key-Distribution/Toshiba-QKD-system/	Room temperature single photon detector, QKD system usingT12 protocol
Mitshubishi Electric	http://www.mitsubishielectric.com/company/rd/research/highlights/communications/quantum.html	World's first QKD-based one-time pad mobile phone software
QuNu labs	http://qunulabs.in/	Quantum cryptographic solutions

Expectation is even higher in cases where security is not needed. Classically impossible things may happen in the quantum world.

Actually we don't teleport an object. What we teleport is the informati on associated with it.

Cartoons used in this talk are from: Elements of Quantum Computation and Quantum Communication, **A Pathak**, CRC Press, Boca Raton, USA, (2013).

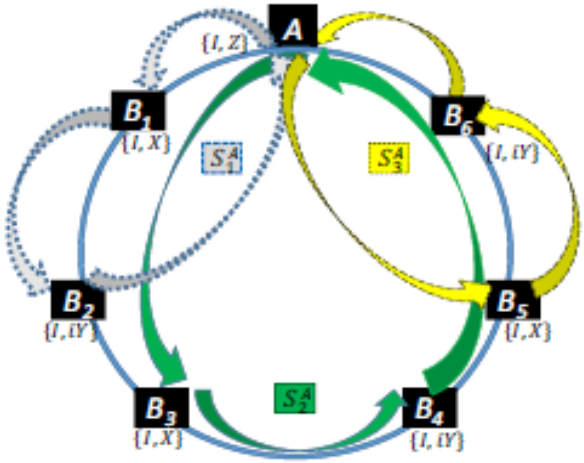
Can we do things beyond QKD?

Teleportation QINP 16, 76 (2017) & QINP 16, 292 (2017) & Controlled teleportation QINP 14, 2599 (2015) & QINP 14, 4601 (2015)

Hierarchical quantum communication QINP 16, 205 (2017)

Direct secure quantum communication QINP 16, 115 (2017) & Asymmetric quantum dialogue QINP 16, 49 (2017)

Quantum voting IJQI 15, 1750007 (2017) & Decoy qubits QINP 15, 1703 (2016) & QINP 15, 4681 (2016)



Quantum key distribution arxiv:1609.07473v1 (2016) & Quantum conference arxiv:1702.00389v1 (2017) & Quantum e-commerce QINP 16, 295 (2017)

Controlled direct secure quantum communication QINP 16, 115 (2017)

Quantum sealed bid auction QINP 16, 169 (2017)

Quantum private comparison arxiv:1608.00101v1 (2016)

Optically implementable MDI-DSQC

Entangled & nonclassical states, PRA, 93 (2016) 022107, 93 (2016) 012340, 91 (2015) 042309, 90 (2014) 013808, 89 (2014) 033812, 89 (2014) 033628, 87 (2013) 022325, Ann. Phys. 366 (2016) 148, 362 (2015) 261

Resources required: Nonclassical states

To perform classically impossible tasks, we definitely need some features that is not present in a classical theory. A state that depicts such a feature is nonclassical.

Informal definition: A state, which does not have any classical analogue, is called nonclassical.

Formal definition used by quantum optics community:

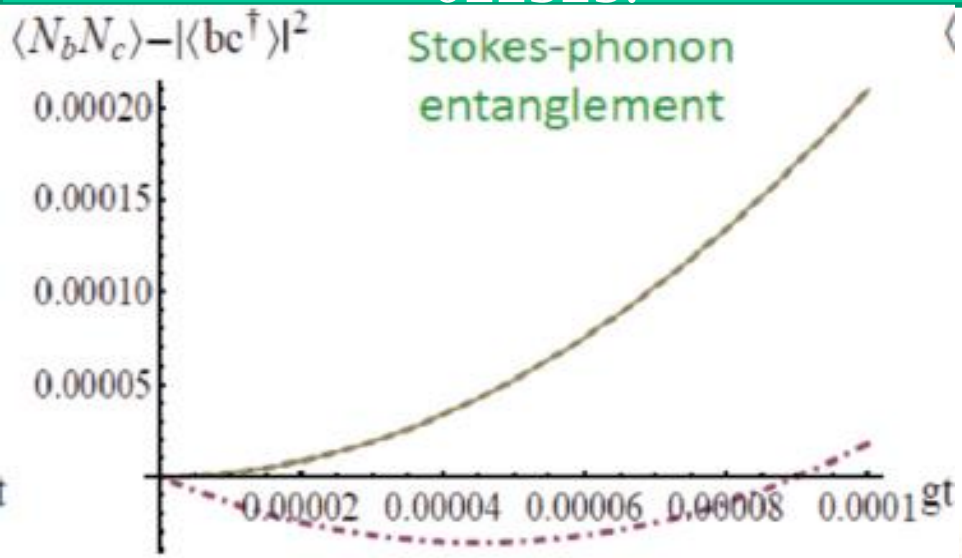
For which Glauber-Sudarshan P function is not a classical probability density function

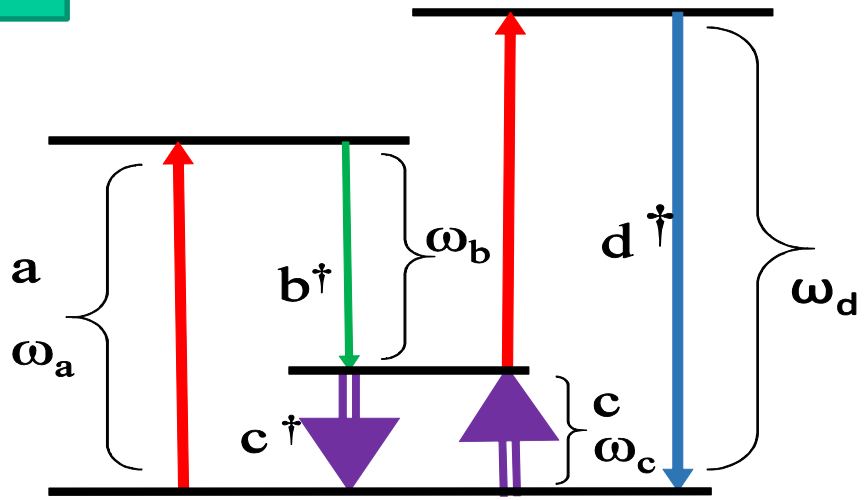
$$\rho = \int P(\alpha) |\alpha\rangle\langle\alpha| d^2\alpha. \qquad (A)$$

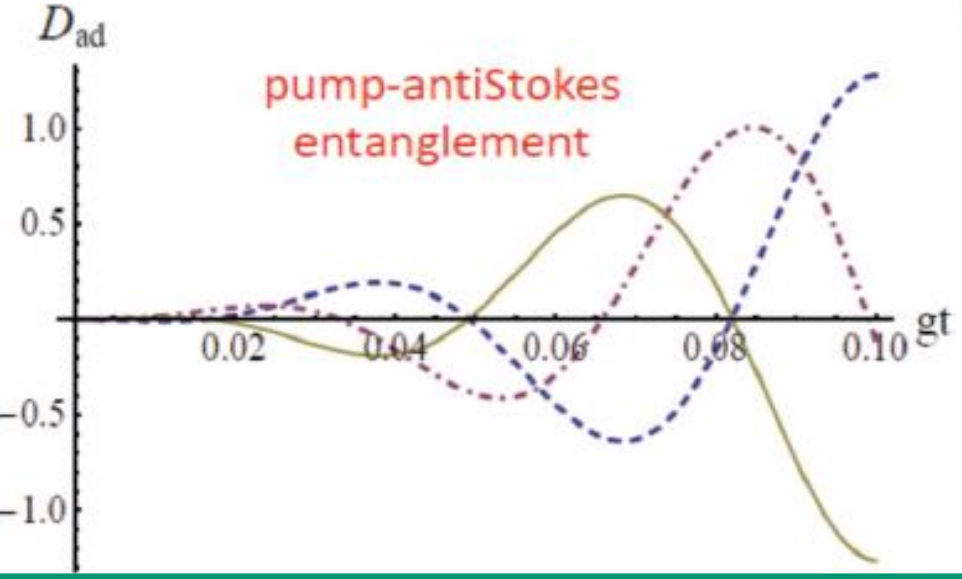
Specific quantum communication task requires specific type of nonclassical states: 2 sided MDIQKD, 1 Sided MDIQKD, QKD (BB84 and Ekert's protocol), CV-QKD=> All have different requirements

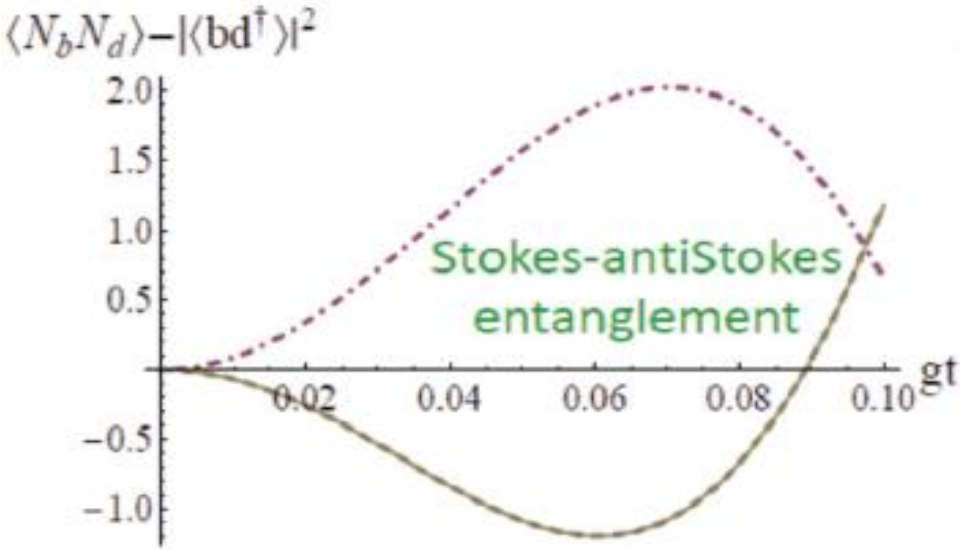
B. Sen, S. K. Giri, S. Mandal, C. H. R. Ooi, and A. Pathak, PRA **87** (2013) 022325.

$$H = \omega_a a^\dagger a + \omega_b b^\dagger b + \omega_c c^\dagger c + \omega_d d^\dagger d + g\left(ab^\dagger c^\dagger + \text{H.c.}\right) + \chi\left(acd^\dagger + \text{H.c.}\right)$$





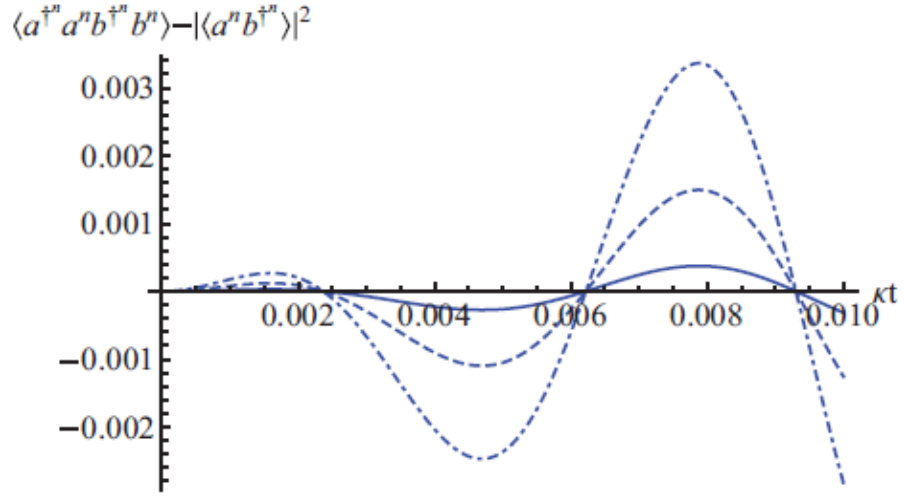


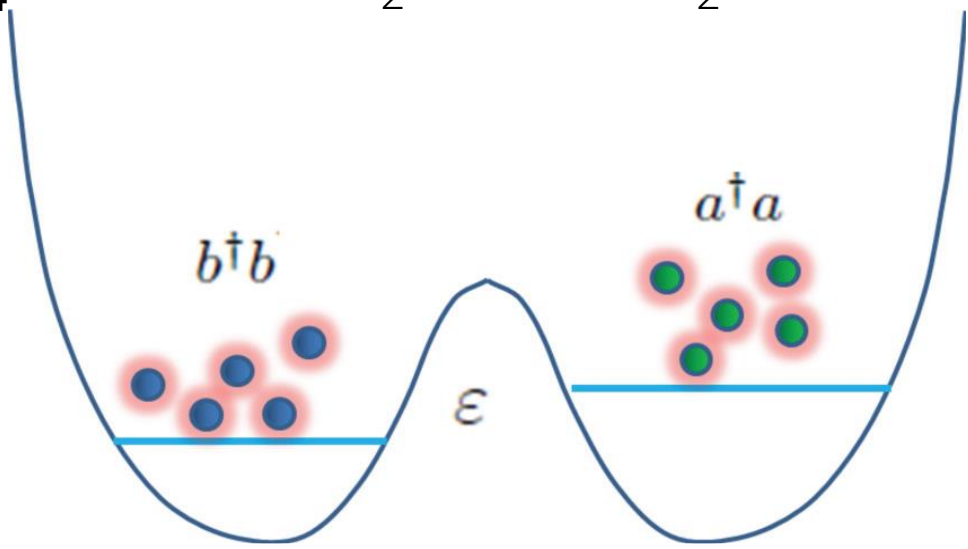


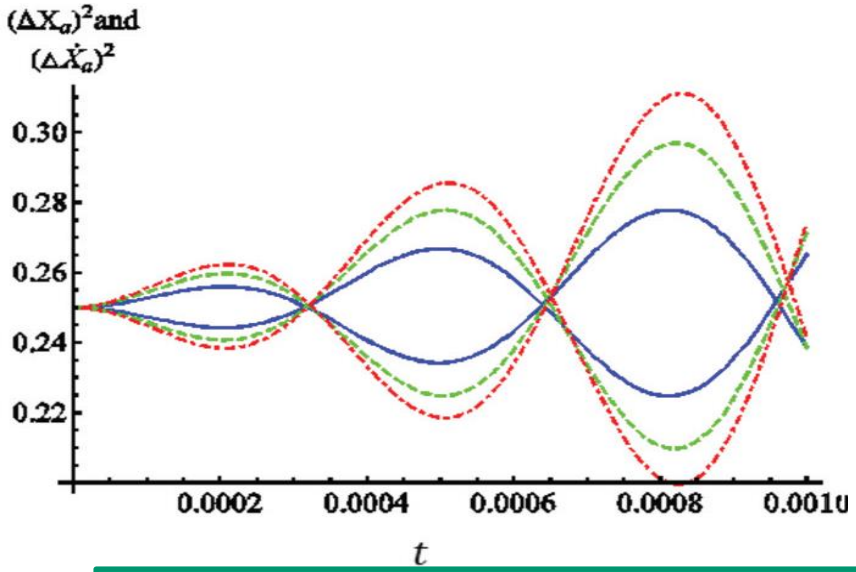
Similar result in: A. Pathak, J. Krepelka and J. Perina, Phys. Lett. A 377 (2013) 2692

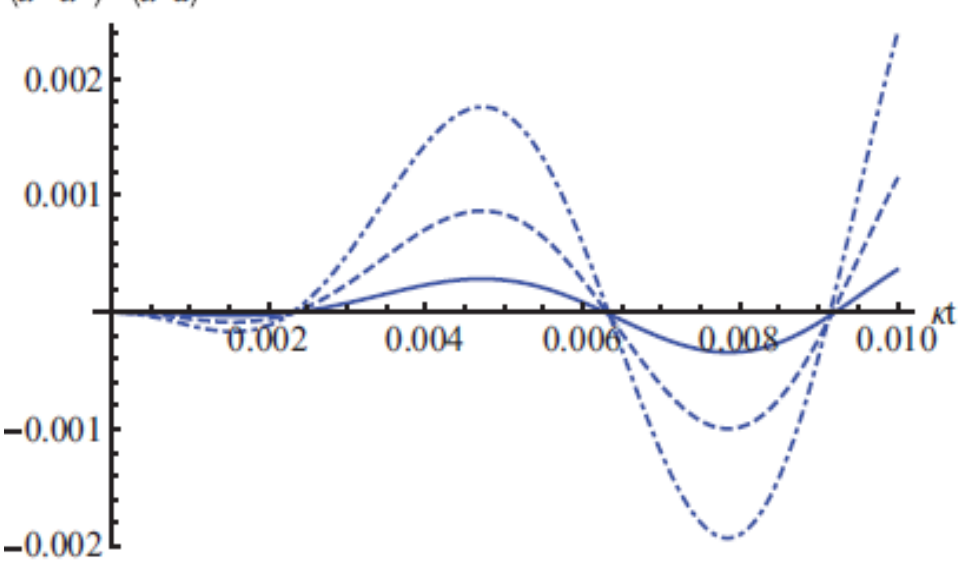
S. K. Giri, B. Sen, C. H. R. Ooi, and A. Pathak, PRA **89** (2014) 033628.

$$H = \frac{\kappa}{4}\left(a^{\dagger 2}a^{2} + b^{\dagger 2}b^{2}\right) + \frac{\Delta\mu}{2}\left(a^{\dagger}a - b^{\dagger}b\right) - \frac{\varepsilon}{2}\left(a^{\dagger}b - b^{\dagger}a\right)$$





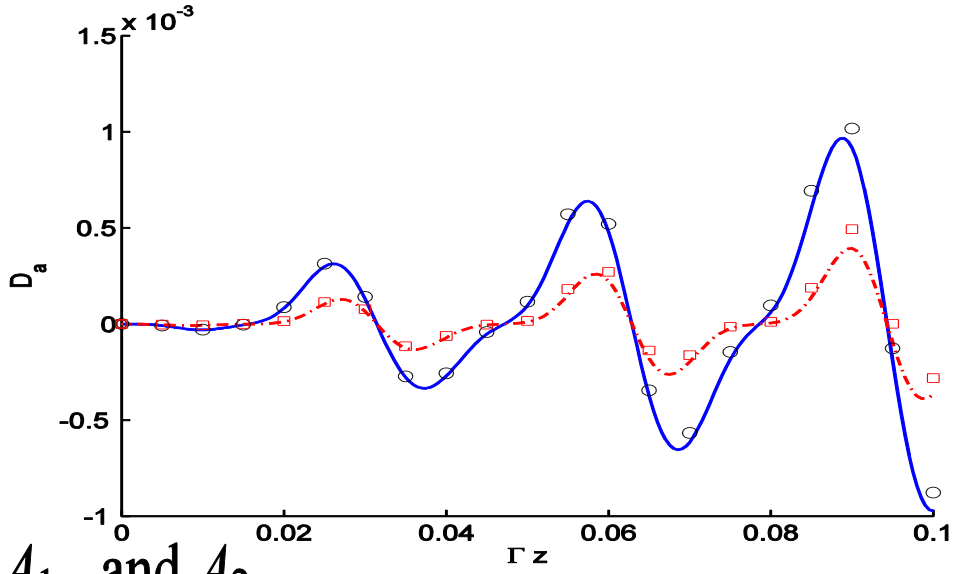


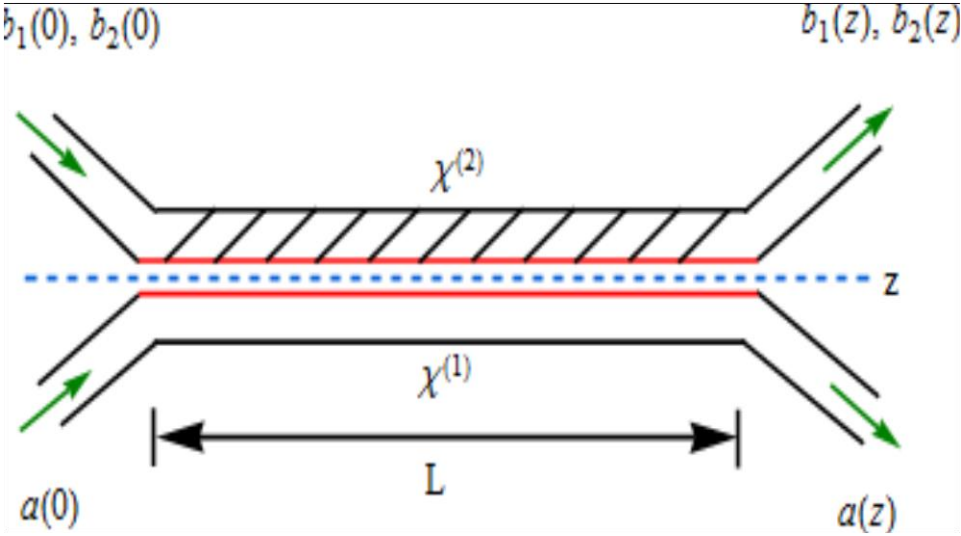


This results are for atom-atom BEC. Similar result for atom-molecule BEC in: S. K. Giri, K. Thapliyal, B. Sen, and A. Pathak arXiv:1407

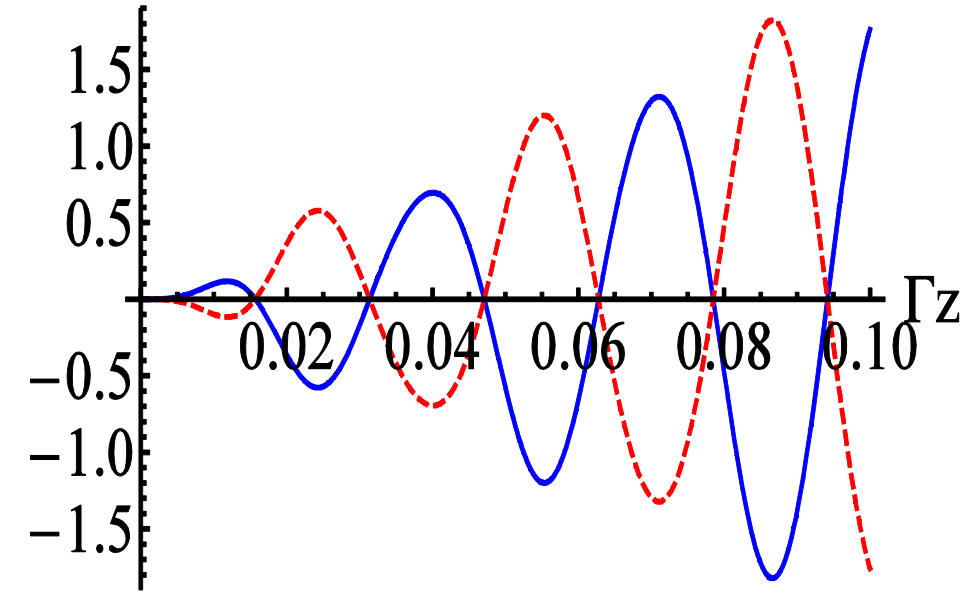
K. Thapliyal, A. Pathak, B. Sen, and J. Perina, PRA 90 (2014) 013808.

$$G_{\text{int}} = -\hbar k a b_1^{\dagger} - \hbar\Gamma b_1^2 b_2^{\dagger} \exp(i\Delta k z) + \text{H.c.}$$

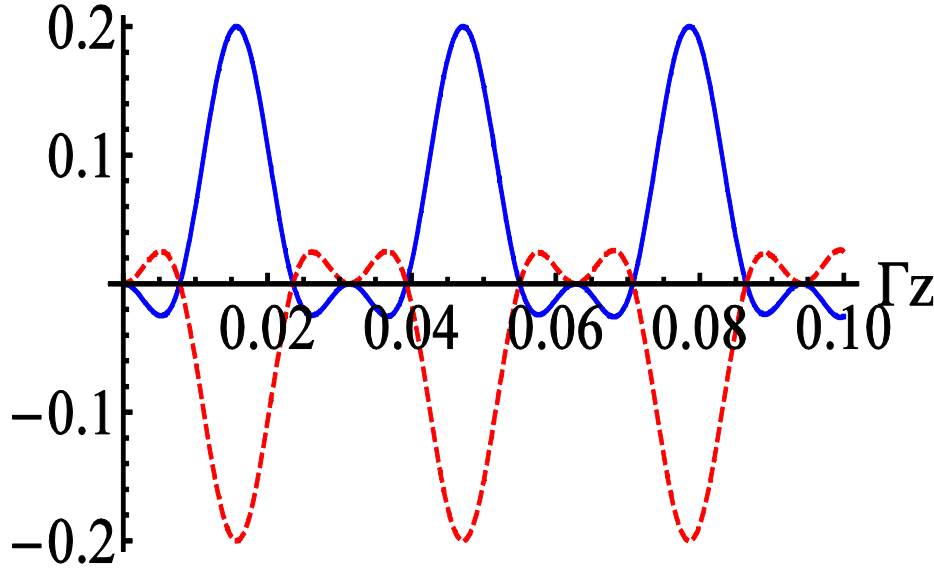




$A_{1,a}$ and $A_{2,a}$

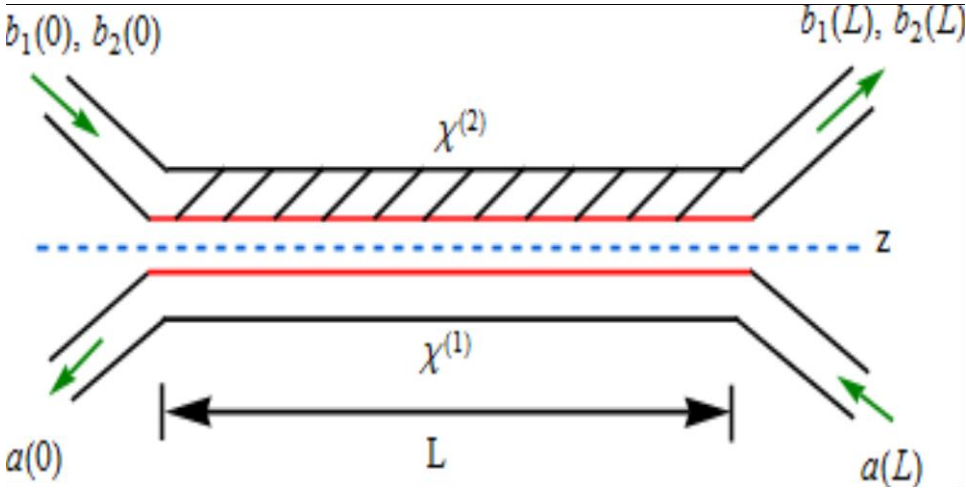


$E^{1,1}_{ab_1}$ and $E'^{1,1}_{ab_1}$

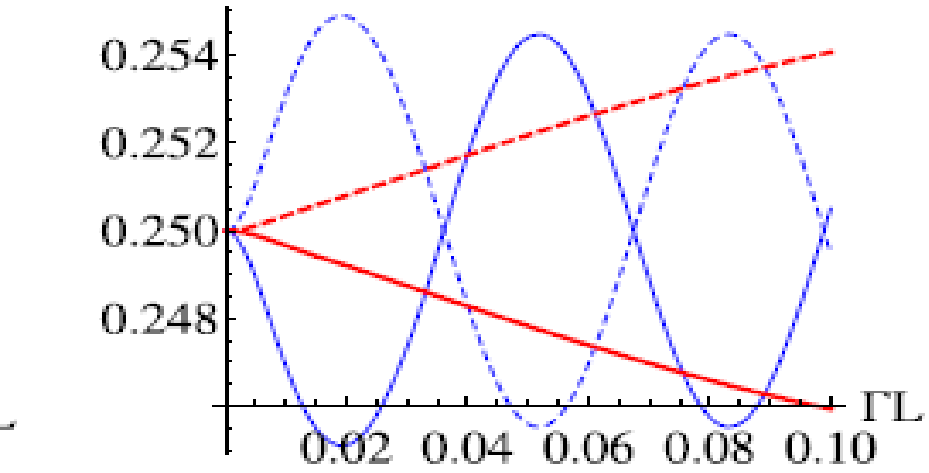


K. Thapliyal, A. Pathak, B. Sen, and J. Perina, PLA 378 (2014) 3431.

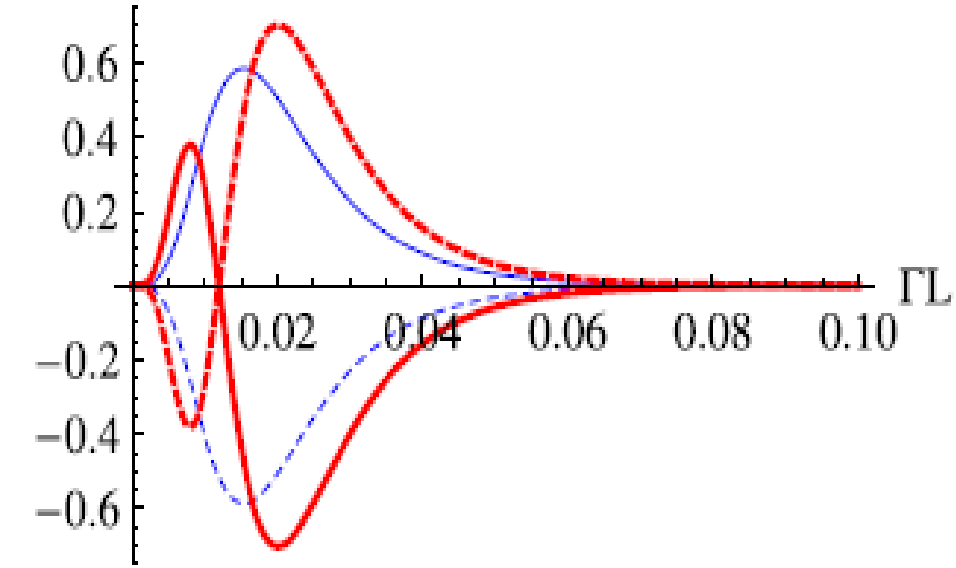
$$G_{\text{int}} = -\hbar k a b_1^{\dagger} - \hbar\Gamma b_1^2 b_2^{\dagger} \exp(i\Delta k z) + \text{H.c.}$$



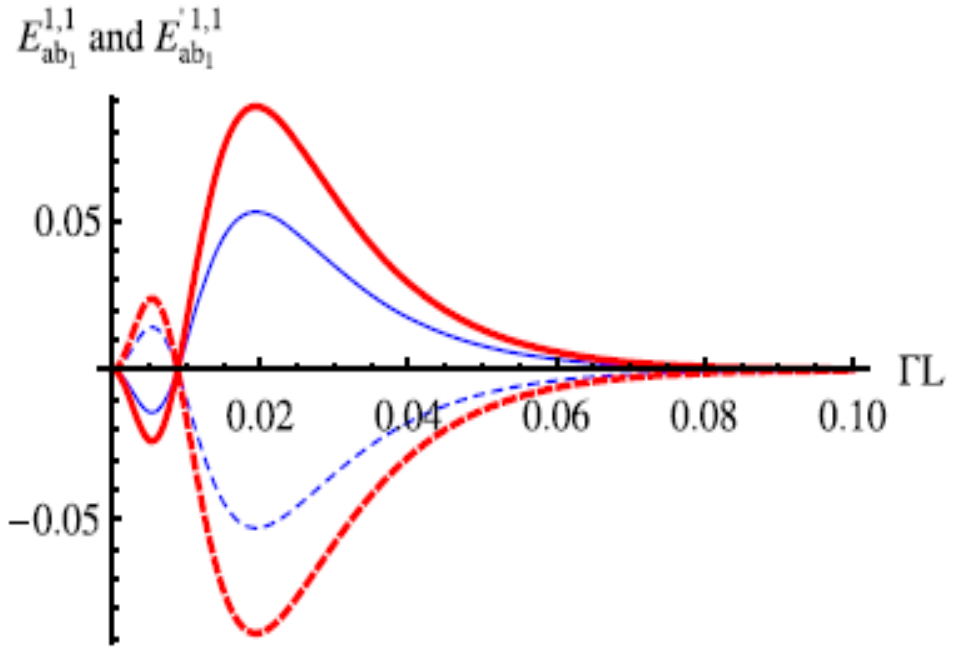
$(\Delta X_{b_1})^2$ and $(\Delta Y_{b_1})^2$



$A_{1,a}$ and $A_{2,a}$



$E_{\text{ab}_1}^{1,1}$ and $E_{\text{ab}_1}^{'1,1}$



Fundamental question: What is purely quantum in quantum mechanics?

We propose to rewrite the postulates of QM as:

1. **(C1) Linearity:** gives superposition (satisfied by: any theory positing wave nature)
2. **(C2) Tensor product space:** C1+C2 gives **classical entanglement** (as pointed out by Simon et al.)
3. **(C3) Norm preserving evolution:** (gives: **unitarity**; satisfied by any theory with rotational invariance and satisfying C1 and C2)
4. **(C4) No-signaling:**
5. **(Q1) Measurement with probabilistic outcomes according to Born rule:** (gives: **non-realism (non-determinism)**, wave-particle duality; Gleason's theorem; sufficient to protect orthogonal-state crypto-protocols like Goldenberg-Vaidman)
6. **(Q2) Non-commutativity** (gives: Kochen-Specker and Bell theorems; uncertainty relations and CV-QKD, BB-84, Ekert, B-92, Deng, LM-05, Ping-Pong protocols)
7. **(Q3) Indistinguishability of identical particles:** -- gives Bosonic and Fermionic symmetrisation

Fundamental question: What is purely quantum in quantum mechanics?

- **C1-C4 are classical; only Q1, Q2 and Q3 are Quantum mechanical**
- **Q1, Q2, Q3 are purely quantum in QM.**
- **Q3 is not usually used in quantum cryptography.**
- **Q1 (non-realism) is sufficient for GV class of protocol.**
- **Q1+Q2 is required for BB-84 class of protocols.**

Wave-particle duality from Q1:
Measuring |+> in X basis gives definite answer (wave nature), whereas measuring in Z basis gives either |0> or |1> probabilistically (particle nature). If it were not probabilistic, it would be just like a classical system where waves and particles can both be seen simultaneously.

This is a crude view for a proper framework see: On the origin of nonclassicality in single systems, S. Aravinda, R. Srikanth, **A. Pathak**, J. Phys. A **50** (2017) 465303.

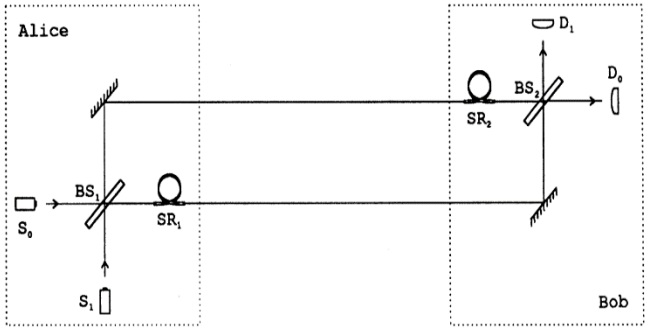
On the origin of security

Our views on the origin of security

- Quantum theory evinces a complex and cryptographically pertinent interplay of local and global properties, as has become evident from the study of general correlation theories. In particular, non-signaling nonlocal correlations imply intrinsic randomness and privacy of shared randomness.
- Nonlocality is known to be bound by uncertainty. Yet, protocols like BB84 require only the incompatibility of conjugate observables, seemingly independent of the non-signaling and nonlocal features of quantum mechanics.
- **Uncertainty via disturbance in the local theory, suffices to guarantee the security.**
- **A secure theory need not be nonlocal. However, if it is, then it should be sufficiently non-signaling to allow the possibility of extracting shared secret bits.**

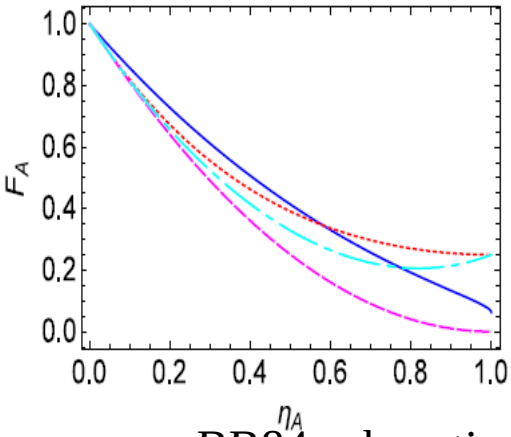
Open problem: Tomograms are not well studied in open quantum systems but environment plays an important role

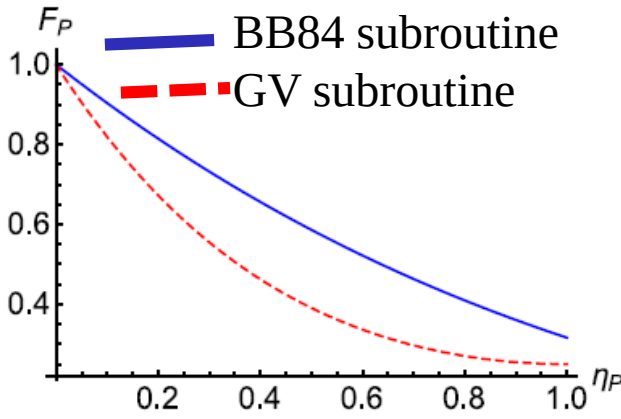
Decoy qubits and Eavesdropping check contd.



In the absence of noise

BB84 subroutine = GV subroutine





The variation of fidelity with decoherence rate for the BB84 subroutine (smooth blue line) and remaining all cases of GV subroutine (dashed red line), when subjected to Phase Damping noise.

BB84 subroutine

GV subroutine: $|\psi^{\pm}\rangle$ $|\phi^{\pm}\rangle$ Cluster state

In noisy channels

BB84 subroutine ≠ GV subroutine

C. Shukla, **A. Pathak** and R. Srikanth, Int. J. Quant. Info., **10** (2012) 1241009; R. D. Sharma, K. Thapliyal, **A. Pathak**, A. K. Pan, and A. De. Quantum Inf. Process. **15** (2016) 1703–1718.

Controlled quantum dialogue protocol of Ba An type

Step 1:

Charlie prepares n copies of a Bell state $|\phi^+\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$. He prepares two sequences: the first sequence P_{B1} is prepared with all the first qubits of Bell pairs and the second sequence P_{B2} is prepared with all the second qubits.

Step 2:

Charlie applies n-qubit permutation operators Π_n on P_{B1} to create a new sequence $P_{B1}' = \Pi_n P_{B1}$ and sends both P_{B1}' and P_{B2} to Bob.

K. Thapliyal and A. Pathak, Quantum Inf. Process. 14, 2599-2616 (2015)

Controlled quantum dialogue protocol of Ba An type

Step 3:

Bob uses the qubits of P_{B1}' (P_{B2}) as home (travel) qubits. He encodes his 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 (i.e., on the qubits of sequence P_{B2}). Without loss of generality, we may assume that $U_0 = I$, $U_1 = \sigma_x = X$, $U_2 = i\sigma_y = iY$ and $U_3 = \sigma_z = Z$, where σ_i are Pauli matrices. Further, we assume that after the encoding operation the sequence P_{B2} transforms to Q_{B2}.

Step 4:

Bob first prepares n decoy qubits in a random sequence of $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$, i.e., the decoy qubit state is $\otimes_{j=1}^{n}|P_j\rangle$, $|P_j\rangle \in \{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$. Bob then randomly inserts the decoy qubits in Q_{B2} to obtain an enlarged new sequence R_{B2} and sends that to Alice and confirms that Alice has received the entire sequence.

K. Thapliyal and A. Pathak, Quantum Inf. Process. 14, 2599-2616 (2015)

Controlled quantum dialogue protocol of Ba An type

Step 5:

Bob discloses the positions of decoy qubits, and applies BB84 subroutine in collaboration with Alice and thus computes the error rate. If the error rate exceeds the tolerable limit, then Alice and Bob abort this communication and repeat the procedure from the beginning. Otherwise, they go on to the next step.

All the intercept-resend attacks are detected in this step. Any attack by Eve will not provide her any meaningful information about the encoding operation executed by Bob as Eve's access to the Bell state is limited to a single qubit.

K. Thapliyal and A. Pathak, Quantum Inf. Process. 14, 2599-2616 (2015)

Controlled quantum dialogue protocol of Ba An type

Step 6:

Alice encodes her secret message by using the same set of encoding operations as was used by Bob and subsequently randomly inserts a set of n decoy qubits in her sequence and returns the new sequence R_{B3} obtained by this method to Bob.

Step 7:

After Bob confirms that he has received R_{B3}, Alice discloses the positions of the decoy qubits, and Alice and Bob follow Step 5 to check eavesdropping. If no eavesdropping is found they move to the next step.

Step 8:

Charlie announces the exact sequence of P_{B1}.

K. Thapliyal and A. Pathak, Quantum Inf. Process. 14, 2599-2616 (2015)

Controlled quantum dialogue protocol of Ba An type

Step 9:

Bob uses the information obtained from Charlie to create n Bell pairs and performs Bell measurements on them. Subsequently, he announces the outcomes of his Bell measurements. As Bob knows the initial Bell state, final Bell state and his own encoding operation he can decode Alice’s bits. Similarly, Alice uses the results of Bell measurements announced by Bob, knowledge of the initial state and her own encoding operation to decode Bob's bits.

K. Thapliyal and A. Pathak, Quantum Inf. Process. 14, 2599-2616 (2015)

The quantum cryptographic switch revisited

1. After receiving Alice's request, Charlie prepares *n* Bell states (not all the same) and sends the first qubits of all the Bell states to Alice and the second qubits to Bob. Charlie does not disclose which Bell state, he has prepared.
2. After receiving the qubits from Charlie, Alice understands that she has been permitted to send the information to Bob.
3. Alice uses dense coding to encode two bits of classical information on each qubit and transmits her qubits to Bob.
4. When Charlie plans to allow Bob to know the secret information communicated to him, he discloses the Bell state he had prepared.
5. Since the initial Bell state is known, by measuring his qubits in the Bell basis, Bob obtains the information encoded by Alice.

N. Srinatha, S. Omkar, R. Srikanth, S. Banerjee and **A. Pathak,** Quant. Infor. Process. **13** (2014) 59-70

Quantum online shopping: Alice (buyer), Bob: online store, Charlie: Bank

CLZ protocol:

CLZ 1: Alice informs Charlie, that she wants to purchase something online. After receiving this information, Charlie prepares and sends a sequence of $2n$ qubits that is randomly prepared in {0,1,+,-}. However, Charlie does not disclose which qubit is prepared in which basis. Out of these $2n$ qubits, n will be used as decoy qubits.

Note: In CLZ protocol, Charlie sends $n + \delta$ qubits, out of which δ were decoy qubits, but unconditional security demands $\delta = n$.

CLZ 2: Alice randomly selects n of the $2n$ qubits received by him and in collaboration with Charlie, applies BB84 subroutine on those n qubits. If the computed error rate is found to be lesser than the tolerable limit they continue to the next step otherwise they quit the protocol.

Note: After the eavesdroping check is performed using BB84 subroutine the qubits used for the same are discarded and Alice is left with n qubits which she uses as message qubits in the next step.

Y.-H. Chou, F.-J. Lin, G.-J. Zeng, Electron Commer Res 14, 349–367 (2014)

Quantum online shopping

CLZ 3: Alice encodes her shopping information (M) on the *n* qubits of her possession using following rule: to encode 0 (1) she does nothing (applies iY operator). Subsequently, she randomly inserts *n* decoy qubits that are randomly prepared in {0, 1, +,-} into the message encoded sequence and sends that to Bob.

Note: The encoding operation here is the same as that used in LM05 protocol of QSDC.

CLZ 4: After receiving authenticated acknowledgment of receipt of 2*n* qubits from Bob, Alice discloses the position of *n* decoy qubits and Alice and Bob applies a BB84 subroutine on the decoy qubits. If no eavesdropping is found they go to the next step, otherwise they restart the protocol.

CLZ 5: Bob asks Charlie, for the initial states of the *n* message qubits available with him and Charlie provides that information. With the encoded qubits and their initial states, merchant deduces the shopping information of the customer.

Y.-H. Chou, F.-J. Lin, G.-J. Zeng, Electron Commer Res **14**, 349–367 (2014)

Quantum online shopping

HYZ protocol:

This protects buyer's personal information (what is he/she buying) from the bank.

HYZ 1: Same as CLZ 1.

HYZ 2: Same as CLZ 2.

HYZ 3: Same as in CLZ 3 with a difference that Alice prepares a random key K and instead M she sends $M_0 = K \oplus M$ to Bob and keeps K secret.

HYZ 4: Same as CLZ 4.

HYZ 5(a): Alice announces K and Bob uses that to obtain $K \oplus M_0 = M$

HYZ 5(b): Same as CLZ 5.

W. Huang, Y. H. Yang, H.-Y. Jia, Quantum Inf. Process. DOI 10.1007/s11128-015-0958-4 (2015)

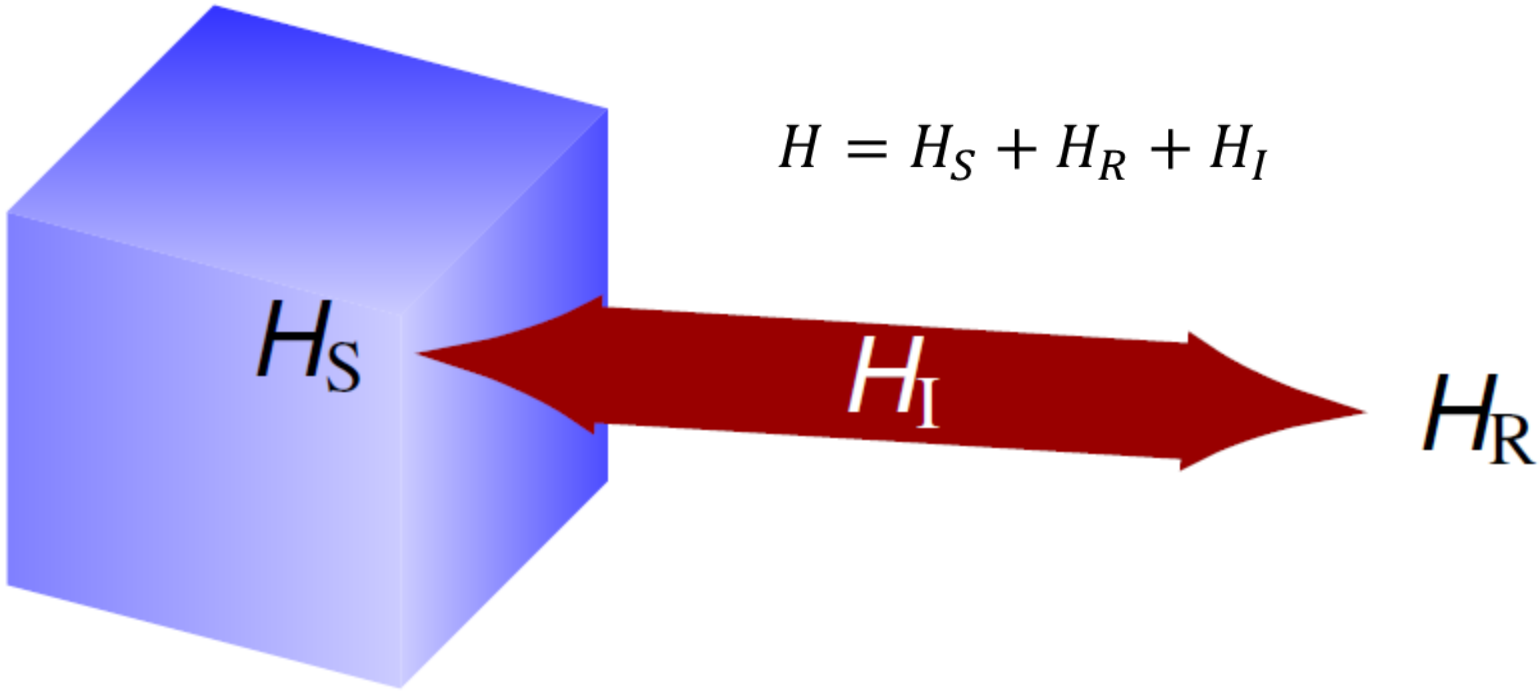
PoP based protocol:

PoP 3: Same as in CLZ 3 with a difference that Alice applies a permutation operator Π on her message encoded sequence before random insertion of the decoy qubits, but keeps the actual sequence secret.

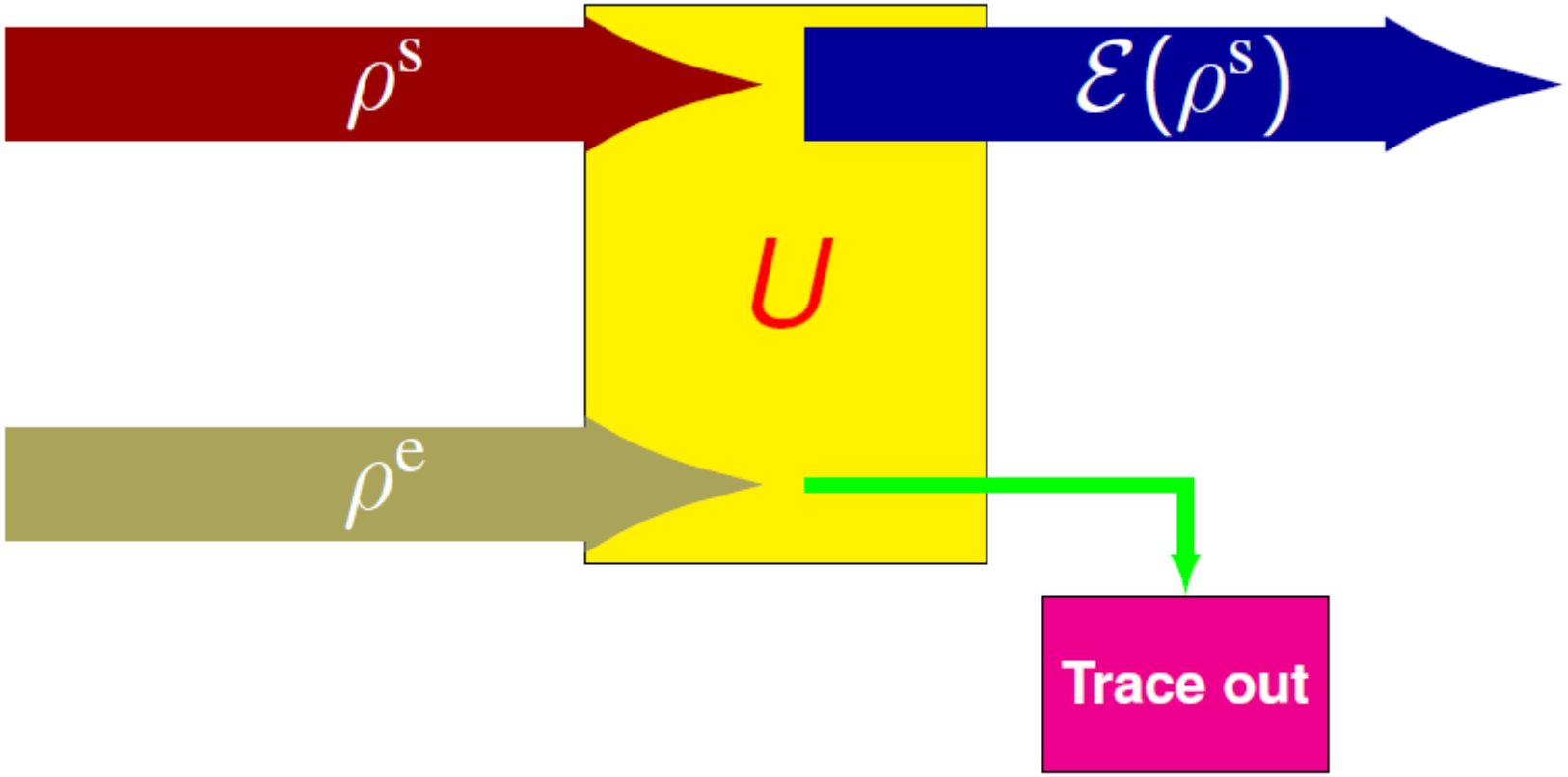
PoP 5(a): Alice announces Π and Bob uses that to obtain M.

A. Pathak: Under preparation

Environment matters



Here H_S is the system Hamiltonian, H_I is the system-reservoir interaction Hamiltonian and H_R is the reservoir Hamiltonian.



Evolution of the system-bath combination is unitary and is given by Liouville-von Neumann equation as $\dot{\rho}(t) = -i[H, \rho(t)]$, where $\rho = \rho^S \otimes \rho^{\mathrm{e}}$ is the quantum state in combined Hilbert space $H^S \otimes \mathrm{H}^{\mathrm{e}}$.

Tracing over the environment degrees of freedom, one can obtain $\dot{\rho}^S(t) = \mathcal{L}[\rho^S(t)]$, where $\mathcal{L}$ is the superoperator acting on the system state.

In operator-sum (or Kraus representation), a superoperator $\mathcal{E}$ acting on a system due to interaction with ambient environment is given by $\rho \to \mathcal{E}(\rho) = \sum_k \langle e_k | U(\rho \otimes |f_0\rangle\langle f_0|)U^\dagger | e_k \rangle = \sum_j E_j \rho E_j^\dagger$, where U is the unitary operator for free evolution of system, reservoir and interaction between them. Here, $|f_0\rangle$ is the environment's initial state, and $\{|e_k\rangle\}$ is a basis of enviroment.
This gives $E_j = \langle e_k | U | f_0 \rangle$ are the Kraus operators satisfying completeness condition $E_j^\dagger E_j = \mathbb{I}$.

The construction of most general form of generator $\mathcal{L}$ leads to the Lindblad equation.

Writing Lindblad form of master equation following assumptions are involved:

1. Born approximation: Weak coupling between system (S) and reservoir (R).
2. Markov approximation: Memoryless (when the time scale associated with the reservoir correlations is much smaller than the time scale over which the state varies appreciably, which is easily justified for weak S − R coupling and high T).

3. Rotating wave approximation: Fast system dynamics compared to the relaxation time.

Non-Markovian channels

Typically, this is due to the fact that the relevant environmental correlation times are not small compared to the system's relaxation or decoherence time, rendering the standard Markov approximation impossible.

The violation of this separation of time scales can occur, for example, in the cases of strong system-environment couplings, structured or finite reservoirs, low temperatures, or large initial system environment correlations.

Markovian channels

Examples of Kraus operators

Type of noise model	Kraus operators
Amplitude damping	
$H_I = a^\dagger b + a b^\dagger$	$E_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-p} \end{bmatrix}, E_1 = \begin{bmatrix} 0 & \sqrt{p} \\ 0 & 0 \end{bmatrix}.$

Here, a is system mode and b is reservoir mode.

Phase damping	
$H_I = \chi a^\dagger a (b + b^\dagger)$	$E_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-p} \end{bmatrix}, E_1 = \begin{bmatrix} 0 & 0 \\ 0 & \sqrt{p} \end{bmatrix}.$

Turchette et al., Phys. Rev. A **62**, 053807 (2000); M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information (2008)

Markovian channels

Generalized amplitude damping (GAD)

$$E_0 = \sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\eta} \end{bmatrix}, \quad E_1 = \sqrt{p}\begin{bmatrix} 0 & \sqrt{\eta} \\ 0 & 0 \end{bmatrix},$$

$$E_2 = \sqrt{1-p}\begin{bmatrix} \sqrt{1-\eta} & 0 \\ 0 & 1 \end{bmatrix}, \quad E_3 = \sqrt{1-p}\begin{bmatrix} 0 & 0 \\ \sqrt{\eta} & 0 \end{bmatrix}.$$

These are generalization of AD to thermal and squeezed thermal reservoir.

Squeezed generalized amplitude damping (SGAD)

$$E_0 = \sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\eta} \end{bmatrix}, \quad E_1 = \sqrt{p}\begin{bmatrix} 0 & \sqrt{\eta} \\ 0 & 0 \end{bmatrix},$$

$$E_2 = \sqrt{1-p}\begin{bmatrix} \sqrt{1-\nu} & 0 \\ 0 & \sqrt{1-\mu} \end{bmatrix},$$

$$E_3 = \sqrt{1-p}\begin{bmatrix} 0 & \sqrt{\mu}e^{-i\xi} \\ \sqrt{\nu} & 0 \end{bmatrix}.$$

Markovian channels

Bit flip

$$E_0 = \sqrt{1-p}\, I_2, \quad E_1 = \sqrt{p}\, X.$$

Phase flip

$$E_0 = \sqrt{1-p}\, I_2, \quad E_1 = \sqrt{p}\, Z.$$

Depolarizing channel

$$E_0 = \sqrt{1-p}\, I_2, \quad E_1 = \sqrt{\frac{p}{3}}\, X,$$

$$E_1 = \sqrt{\frac{p}{3}}\, Y, \quad E_1 = \sqrt{\frac{p}{3}}\, Z.$$

Some collective noises

Collective rotation

$$U_r = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}.$$

Collective dephasing

$$U_p = \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\phi) \end{bmatrix}.$$

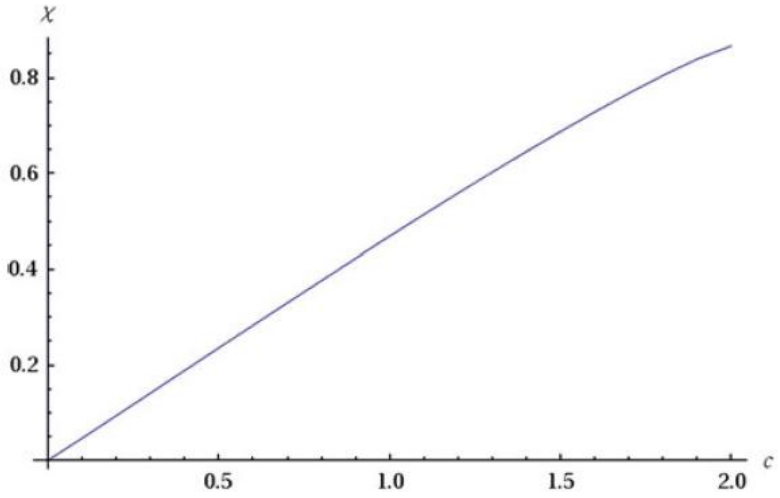
AD vs PD channels

Consider an arbitrary density matrix $\rho = \begin{bmatrix} a & b \\ b^* & c \end{bmatrix}$ evolving under AD channel becomes

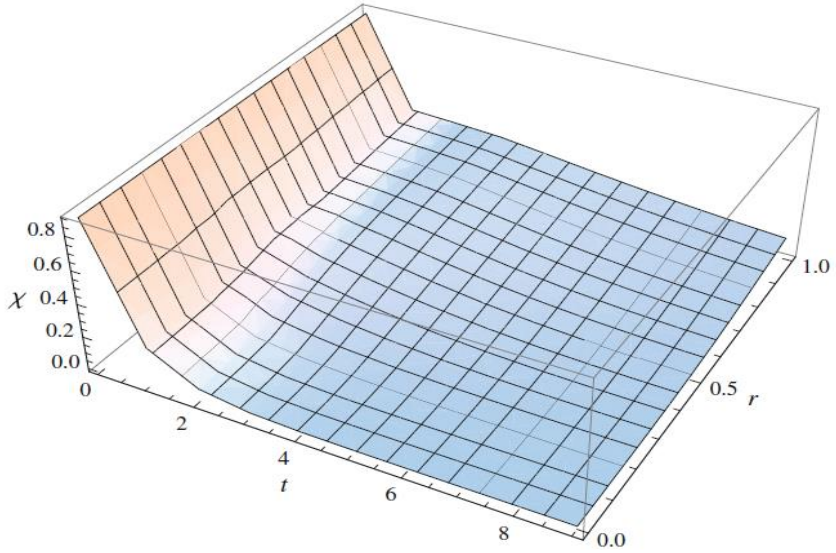
$$\rho' = \begin{bmatrix} a + pc & b\sqrt{1-p} \\ b^*\sqrt{1-p} & (1-p)c \end{bmatrix}.$$

Similarly, the state evolving under PD noise becomes $\rho' = \begin{bmatrix} a & b\sqrt{1-p} \\ b^*\sqrt{1-p} & c \end{bmatrix}$.

The quantum cryptographic switch in the presence of squeezed generalized amplitude damping (SGAD) noise



Information recovered by Bob, quantified by the Holevo quantity χ, as a function of the key information c communicated by Charlie, in the noiseless case.



Information recovered by Bob, quantified by the Holevo quantity χ, as a function of the SGAD channel parameters r (squeezing) and t (time of evolution), assuming Charlie communicates one bit of information. We note that, for sufficiently early times, squeezing fights thermal effects (T = 0.1) to cause an increase in the recovered information

R. Srikanth and S. Banerjee, Phys. Rev. A 77, 012318 (2008);
N. Srinatha, S. Omkar, R. Srikanth, S. Banerjee and **A. Pathak,** Quant. Infor. Process. **13** (2014) 59-70

BCST in the presence of noise

Assumption: Both the qubits sent to Alice (i.e., S_1 and R_2 here)
Both the qubits sent to Bob (i.e., R_1 and S_2 here)
Charlie's qubit is unaffected by Kraus operators.

Under these assumption both BCST schemes (of general structure and cryptographic switch based) have same effect of noise on them.

Alice wishes to teleport

$$|\zeta_1\rangle_{S_1'} = a_1|0\rangle + b_1 \exp(i\phi_1)|1\rangle$$

Bob wants to send

$$|\zeta_2\rangle_{S_2'} = a_2|0\rangle + b_2 \exp(i\phi_2)|1\rangle$$

Suppose Charlie prepares initial 5-qubit Brown state and sends S_1, R_2 to Alice and R_1, S_2 to Bob

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\psi^+\rangle_{S_1R_1}|\psi^+\rangle_{S_2R_2}|0\rangle_{C_1} - |\psi^-\rangle_{S_1R_1}|\phi^-\rangle_{S_2R_2}|1\rangle_{C_1}).$$

Equivalently, Charlie can prepare two Bell states and sends S_1, R_2 to Alice and R_1, S_2 to Bob. In which case the combined state of the system is

$$|\psi'\rangle_{S_1R_1S_2R_2S_1'S_2'} = |\psi_1\rangle_{S_1R_1} \otimes |\psi_2\rangle_{S_2R_2} \otimes |\zeta_1\rangle_{S_1'} \otimes |\zeta_2\rangle_{S_2'}.$$

Corresponding density matrix is

$$\rho = |\psi\rangle_{S_1 S_1' R_1 S_2 S_2' R_2 C_1 S_1 S_1' R_1 S_2 S_2' R_2 C_1} \langle\psi|$$

The effect of noise can be modeled as

$$\rho_k = \sum_{i,j} E^k_{i,S_1} \otimes I_{2,S_1'} \otimes E^k_{j,R_1} \otimes E^k_{j,S_2} \otimes I_{2,S_2'} \otimes E^k_{i,R_2} \otimes I_{2,C_1} \rho$$
$$(E^k_{j,R_1} \otimes I_{2,S_1'} \otimes E^k_{j,R_1} \otimes E^k_{j,S_2} \otimes I_{2,S_2'} \otimes E^k_{i,R_2} \otimes I_{2,C_1})^\dagger$$

We can write the measurement operator

$$U = (|00\rangle_{S_1 S_1' S_1 S_1'} \langle 00|) \otimes I_{2,R_1} \otimes (|00\rangle_{S_2 S_2' S_2 S_2'} \langle 00|) \otimes I_{2,R_2} \otimes (|0\rangle_{C_1 C_1} \langle 0|)$$

assuming all the measurement outcomes as

$$\text{Alice measures} S_1, S_1' \; in \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\} \rightarrow |00\rangle$$
$$\text{Bob measures} S_2, S_2' \; in \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\} \rightarrow |00\rangle$$
$$\text{Charlie measures} C_1 \; in \{|0\rangle, |1\rangle\} \rightarrow |0\rangle$$

K. Thapliyal and **A. Pathak**, Quant. Info. Process **14** (2015) 2599–2616.

Applying this U on ρ_k

$$\rho_{k_1} = U \rho_k U^{\dagger}$$

and renormalizing ρ_{k_1}

$$\rho_{k_2} = \frac{\rho_{k_1}}{Tr(\rho_{k_1})}$$

After tracing out the measured qubits, the final density matrix (i.e., left with R_1, R_2) is

$$\rho_{k,out} = Tr_{S_1 S_1' S_2 S_2' C_1}(\rho_{k_2})$$

Final quantum state the **noisy environment**

While, in an ideal situation,

$$|T\rangle_{R_1 R_2} = |\zeta_1\rangle_{S_1'} \otimes |\zeta_2\rangle_{S_2'}$$
$$= (a_1|0\rangle + b_1 \exp(i\phi_1)|1\rangle) \otimes (a_2|0\rangle + b_2 \exp(i\phi_2)|1\rangle$$

At Bob's end — At Alice's port

Final quantum state in the **absence of noise**

The effect of noise can be calculated using Fidelity

$$F = \langle T | \rho_{k,out} | T \rangle$$

Fidelity under Amplitude damping and Phase damping noise is calculated as

$$F_{AD} = \frac{1}{16\left(2-4\eta_A+5\eta_A^2-4\eta_A^3+2\eta_A^4+\eta_A^2\cos2\theta_1\cos2\theta_2+\eta_A\left(2-3\eta_A+2\eta_A^2\right)(\cos2\theta_1+\cos2\theta_2)\right)} \times \Big[32-164\eta_A+57\eta_A^2-26\eta_A^3+10\eta_A^4+\eta_A\left(34-51\eta_A+30\eta_A^2\right)(\cos2\theta_1+\cos2\theta_2) + \eta_A^2\left(3-2\eta_A+2\eta_A^2\right)(\cos4\theta_1+\cos4\theta_2)+4\eta_A^3\left(3-2\eta_A+2\eta_A^2\right)(\cos2\theta_1\cos4\theta_2+\cos4\theta_1\cos2\theta_2) + 16\eta_A^2\left(2-2\eta_A+\eta_A^2\right)\cos2\theta_1\cos2\theta_2+\eta_A^2\left(1-2\eta_A+2\eta_A^2\right)\cos4\theta_1\cos4\theta_2\Big].$$

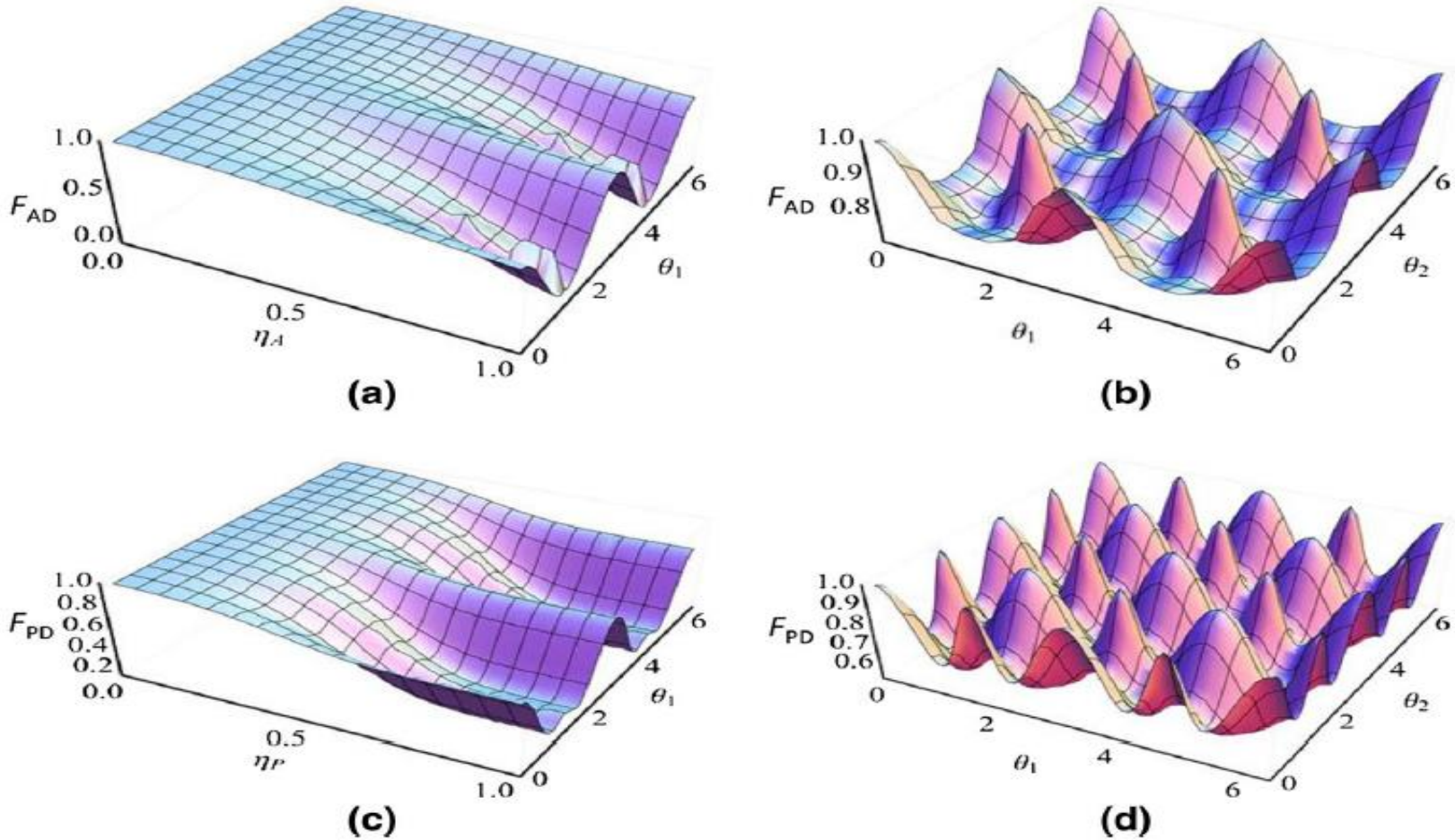
and

$$F_{PD} = \frac{32-128\eta_P+210\eta_P^2-164\eta_P^3+59\eta_P^4+\eta_P^2\left\{2-4\eta_P+3\eta_P^2\right\}(16\cos2\theta_1\cos2\theta_2+\cos4\theta_1\cos4\theta_2+3(\cos4\theta_1+\cos4\theta_2))}{16\left(2-8\eta_P+14\eta_P^2-12\eta_P^3+5\eta_P^4+\eta_P^2\left\{2-4\eta_P+3\eta_P^2\right\}\cos2\theta_1\cos2\theta_2\right)}.$$

respectively. Here, for computational convenience, we have considered $a_i = Sin\theta_i,\ b_i = Cos\theta_i,$ where $i \in \{1,2\}.$

We can observe that $F_{AD/PD}$ depend on the decoherence rate $\eta_{A/P}$ and amplitude information a_i, b_i and are free from phase .

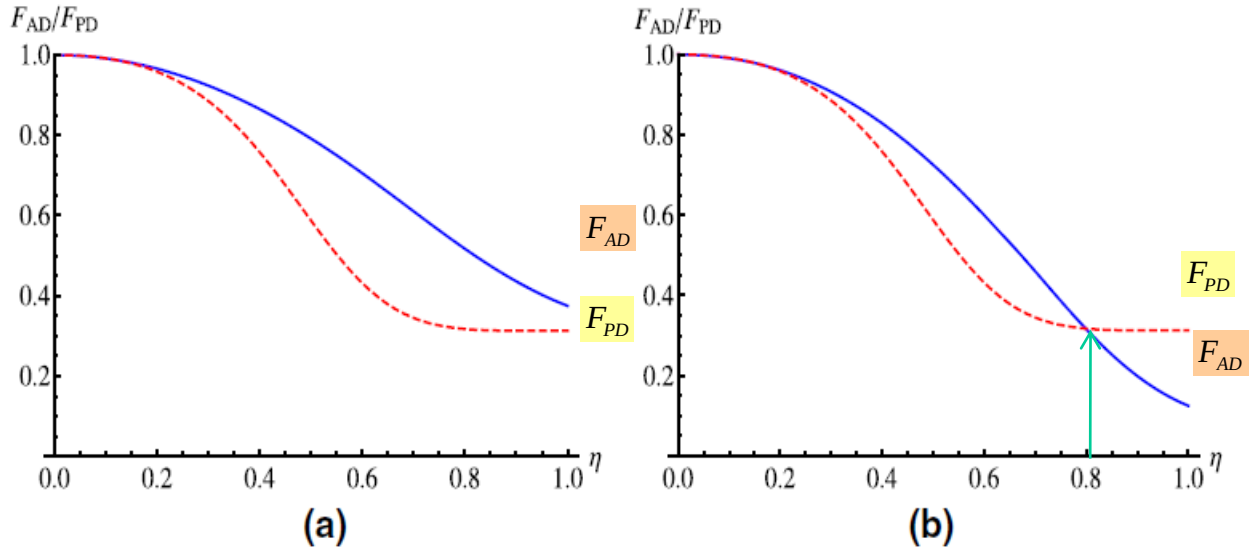
K. Thapliyal and **A. Pathak**, Quant. Info. Process **14** (2015) 2599–2616.



Effect of noise on BCST scheme is visualized through variation of fidelity F_{AD} and F_{PD} with respect to amplitude information of the states to be teleported (i.e., η_i) and decoherence rates (i.e., θ_i)

(a)Amplitude-damping noise with $\theta_2 = \frac{\pi}{6}$, (b) Amplitude-damping noise with $\eta_A = 0.5$

(c) Phase-damping noise with $\theta_2 = \frac{\pi}{6}$, (d) Phase-damping noise with $\eta_P = 0.5$



Comparison of the effect of amplitude-damping noise (solid line) with phase damping noise (dashed line) by assuming $\eta_A = \eta_P = \eta$ and (a) with $\theta_1 = \frac{\pi}{4}, \theta_2 = \frac{\pi}{6}$ (b) with $\theta_1 = \frac{\pi}{4}, \theta_2 = \frac{\pi}{3}$.

(a)$F_{AD} > F_{PD}$ for the same value of decoherence rate η. Whereas;

(b) $F_{AD} < F_{PD}$ for the same value of decoherence rate η after certain value of η, i.e., for $\eta > 0.8$

CBRSP in noisy environment

Similarly, the effect of noise on CBRSP schemes (based on the general structure or cryptographic switch) can be visualized.

We consider here a 5-qubit quantum channel to visualize AD, PD noise models

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\psi^+\rangle_{S_1R_1}|\psi^+\rangle_{S_2R_2}|0\rangle_{C_1} + |\phi^-\rangle_{S_1R_1}|\phi^-\rangle_{S_2R_2}|1\rangle_{C_1}).$$

Fidelity of quantum state prepared using the CBRSP under Amplitude damping and Phase damping noise are given by

$$F_{\mathrm{AD}} = \frac{64 - 128\eta_A + 66\eta_A^2 - 2\eta_A^2\cos 4\theta_1 + \eta_A^2\cos\left(4(\theta_1-\theta_2)\right) - 2\eta_A^2\cos 4\theta_2 + \eta_A^2\cos\left(4(\theta_1+\theta_2)\right)}{16\left(4 - 8\eta_A + 6\eta_A^2 + 2\eta_A^2\cos 2\theta_1 + \eta_A^2\cos\left(2(\theta_1-\theta_2)\right) + 2\eta_A^2\cos 2\theta_2 + \eta_A^2\cos\left(2(\theta_1+\theta_2)\right)\right)}$$

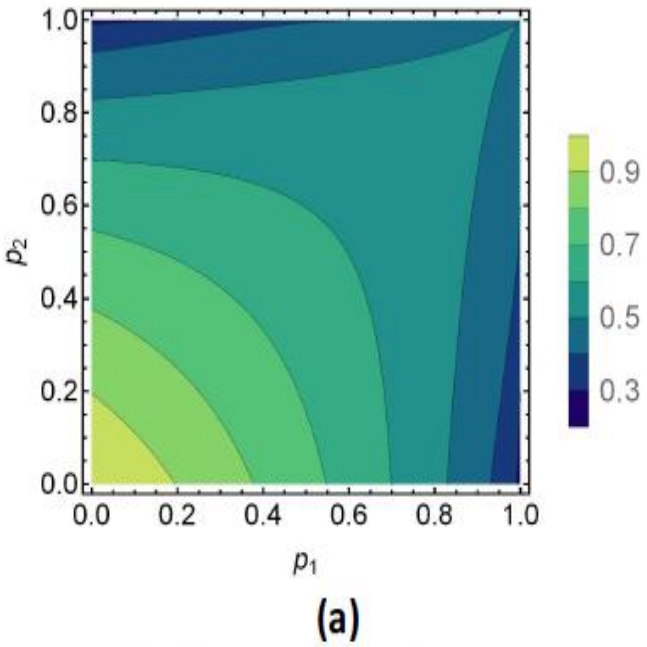
and

$$\begin{aligned} F_{\mathrm{PD}} &= \frac{1}{32\left\{2-8\eta_A+14\eta_A^2-12\eta_A^3+5\eta_A^4+\eta_A^2\left(2-4\eta_P+3\eta_P^2\right)\cos 2\theta_1\cos 2\theta_2\right\}} \\ &\times \left[64 - 256\eta_P + 420\eta_P^2 - 328\eta_P^3 + 118\eta_P^4 + \left(2 - 4\eta_P + 3\eta_P^2\right)\left\{6\eta_P^2\cos 4\theta_1 - 16\eta_P^2\cos\left(2(\theta_1-\theta_2)\right)\right\}\right. \\ &+ 2\eta_P^2\cos\left(4(\theta_1-\theta_2)\right) - 4\eta_P^3\cos\left(4(\theta_1-\theta_2)\right) + 3\eta_P^4\cos\left(4(\theta_1-\theta_2)\right) + 12\eta_P^2\cos 4\theta_2 - 24\eta_P^3\cos 4\theta_2 \\ &+ 18\eta_P^4\cos 4\theta_2 - 32\eta^2\cos\left(2(\theta_1+\theta_2)\right) + 64\eta_P^3\cos\left(2(\theta_1+\theta_2)\right) - 48\eta_P^4\cos\left(2(\theta_1+\theta_2)\right) \\ &\left. + 2\eta_P^2\cos\left(4(\theta_1+\theta_2)\right) - 4\eta_P^3\cos\left(4(\theta_1+\theta_2)\right) + 3\eta_P^4\cos\left(4(\theta_1+\theta_2)\right)\right]. \end{aligned}$$

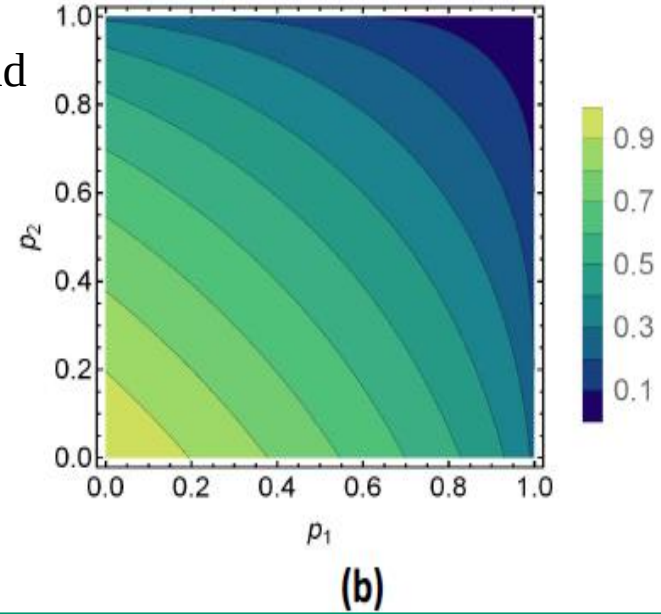
A similar behavior (regarding dependence on only amplitudes and free from phase terms) to BCST scheme is observed here.

V. Sharma, C, Shukla, S. Banerjee and **A.Pathak**, Quant. Info. Process. **14** (2015) 3441–3464.

QPC protocols subjected to AD channels, i.e., both the qubits evolve under AD noise. In (a) and (b), the choice of the initial Bell state by TP is $|\psi^{\pm}\rangle$ and $|\phi^{\pm}\rangle$, respectively.

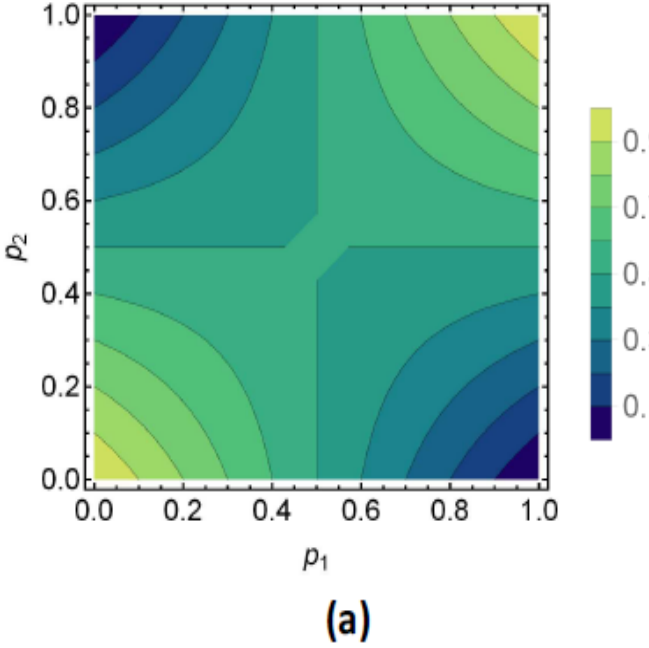


(a)

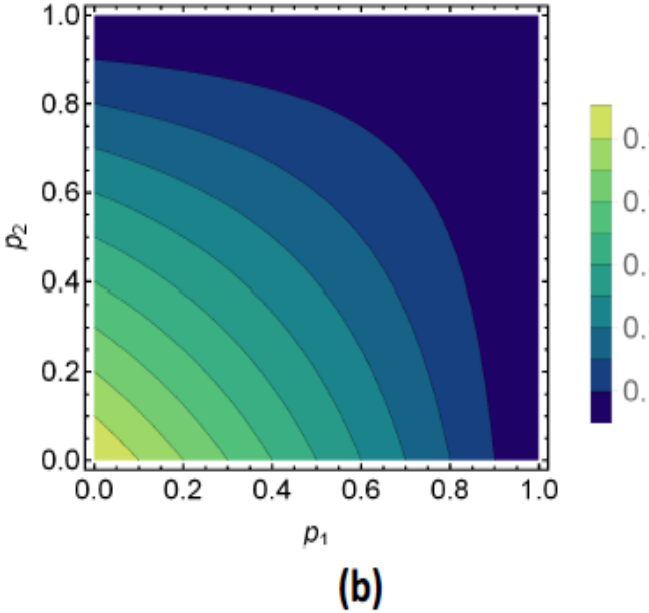


(b)

QPC protocols subjected to noisy environment, when the first qubit of the Bell state (Alice's qubit) is subjected to BF, while the second (Bob's) qubit evolves under different noisy channels. In (a), (b) Bob's qubits is affected by BF, PF.



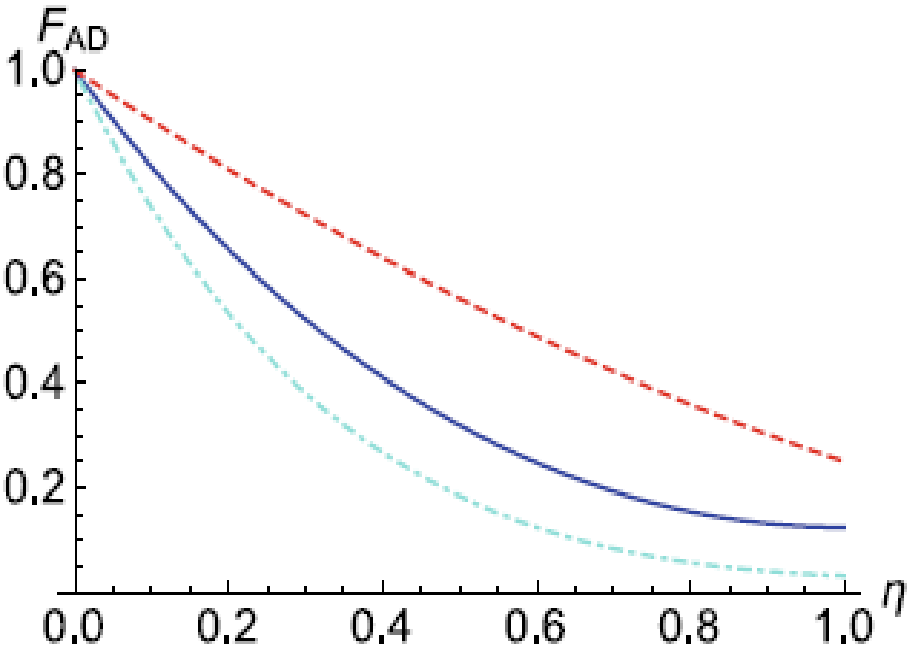
(a)



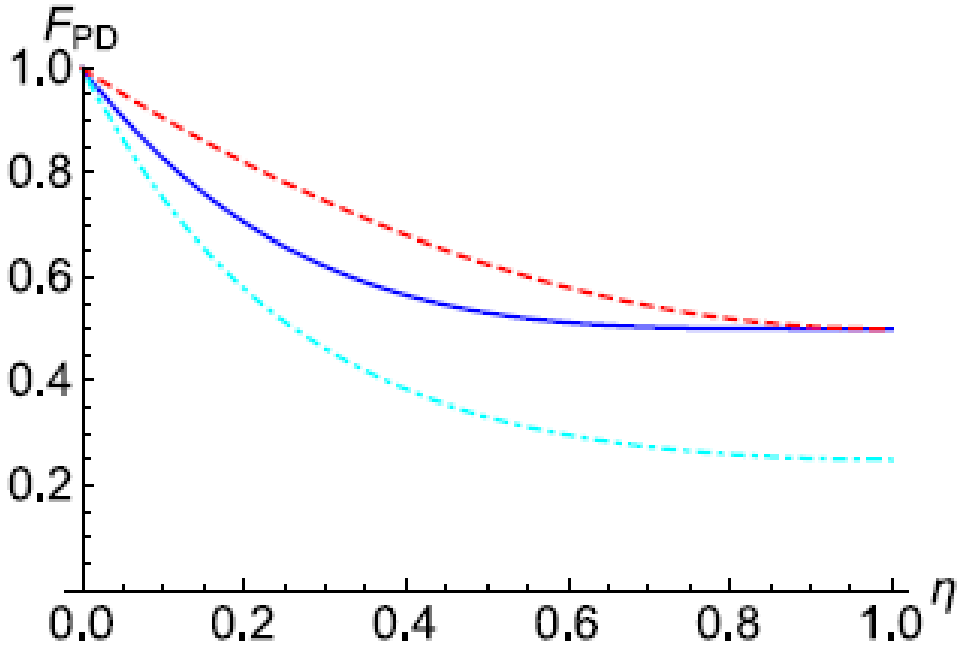
(b)

K. Thapliyal, R. D. Sharma and A. Pathak, arxiv:1608.00101 **(2016)**

Effect of noise on Asymmetric QD



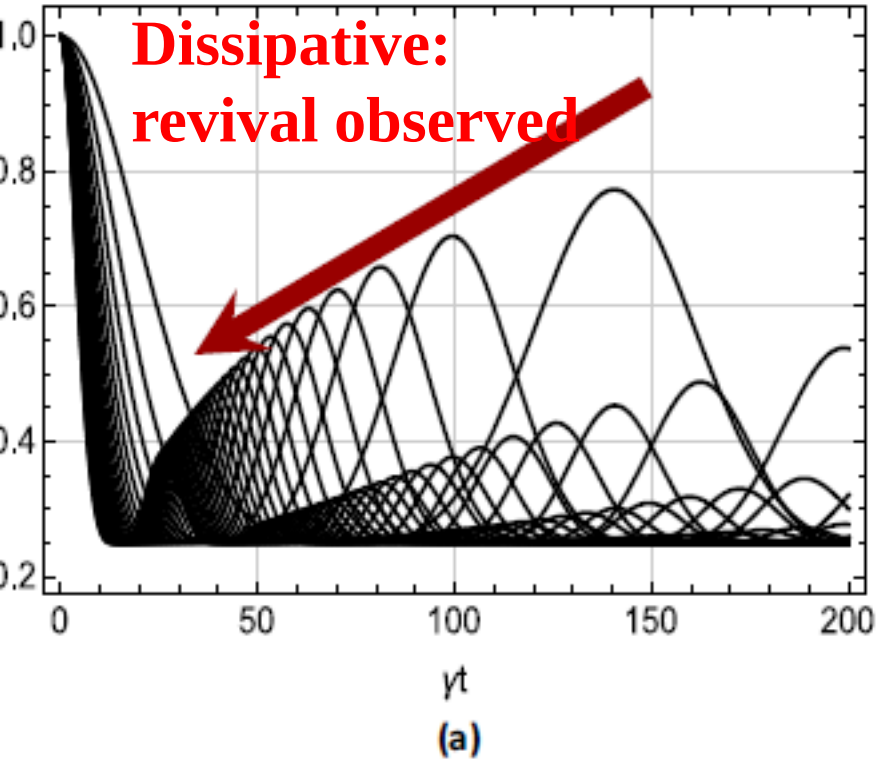
AD channel

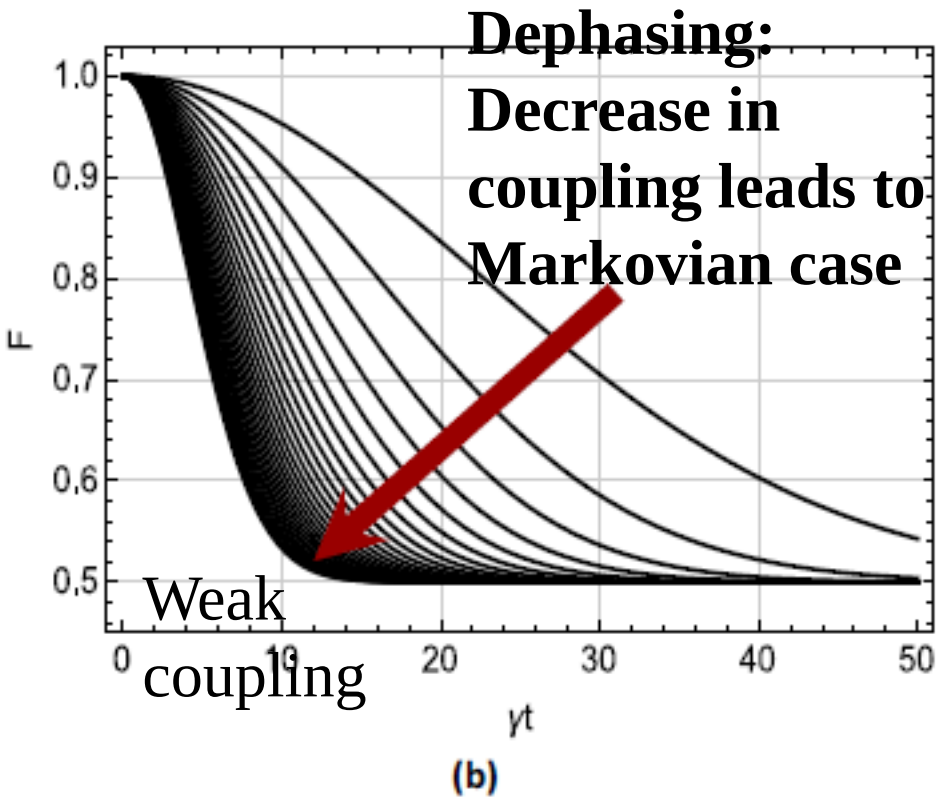


PD channel

Channel used: 4-qubit cluster state.
Decreasing fidelity from AQD to QD and least for 2 QSDCs.

A. Banerjee, C. Shukla, K. Thapliyal, A. Pathak, and P.K. Panigrahi, **Quantum Inf. Process. 14, 2599-2616 (2016)**

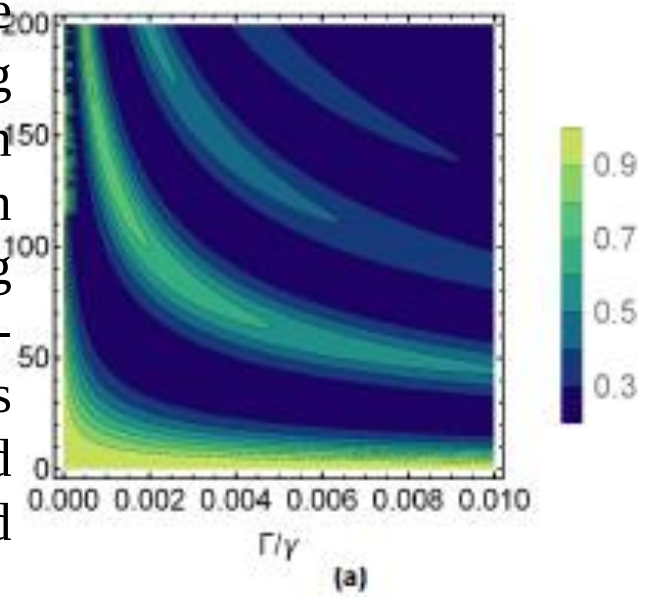


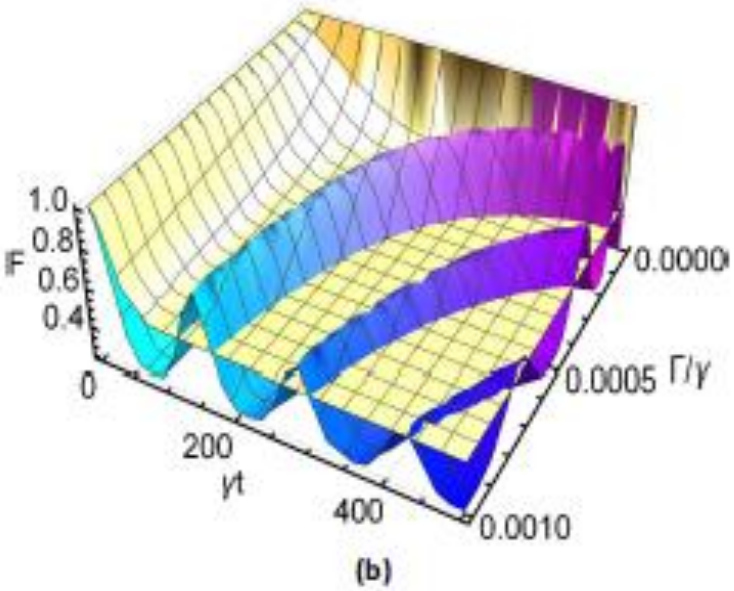


The effect of a change in the coupling strength on the fidelity is illustrated here with a set of plots for damping and dephasing non-Markovian noise in (a) and (b), respectively. Specifically, the parameter of the coupling strength Γ/γ varies from 0.001 to 0.03 in steps of 0.001 in both the plots.

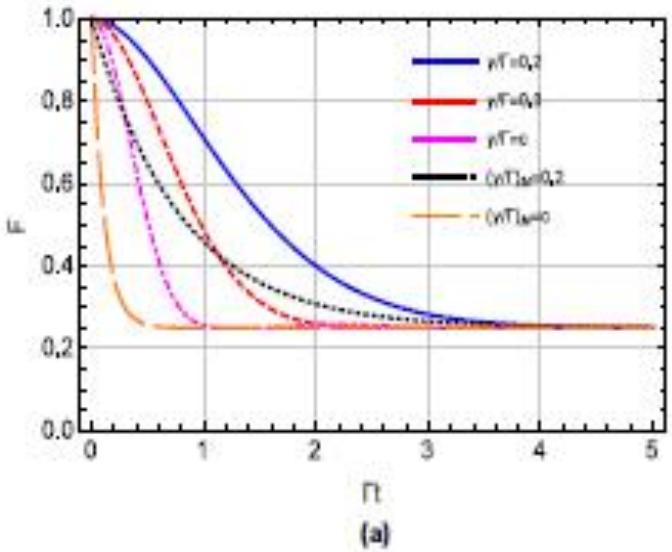
K. Thapliyal, **A. Pathak,** S. Banerjee, Quant. Infor. Process. 16, 115 (2017)

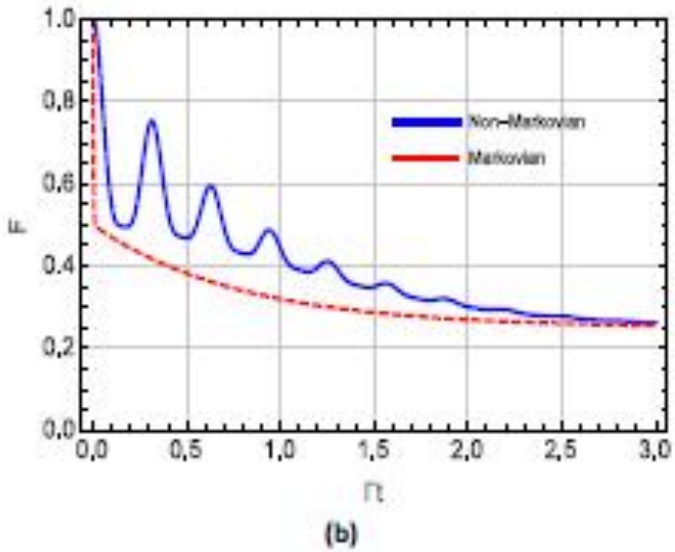
Variation of the fidelity for varying coupling strength and time for both purely dephasing and damping non-Markovian channels in light (yellow) and dark (blue) colored surface plots, respectively.



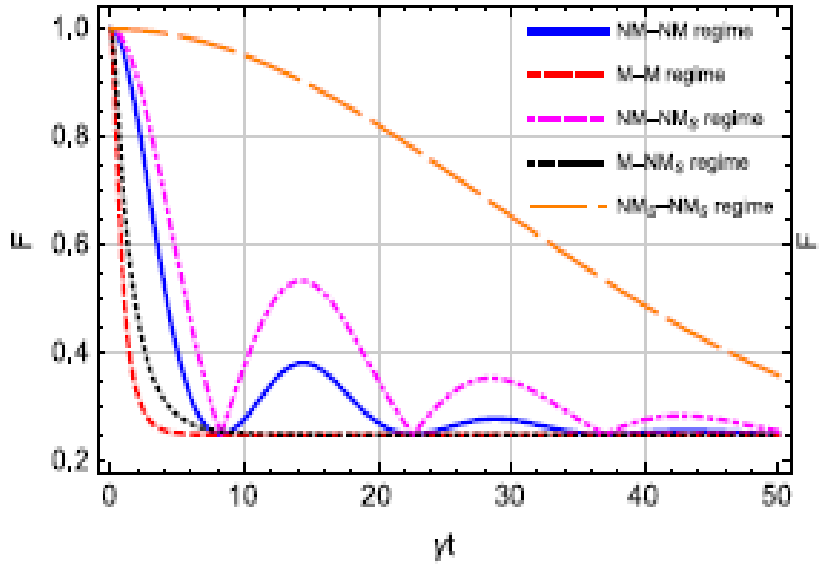


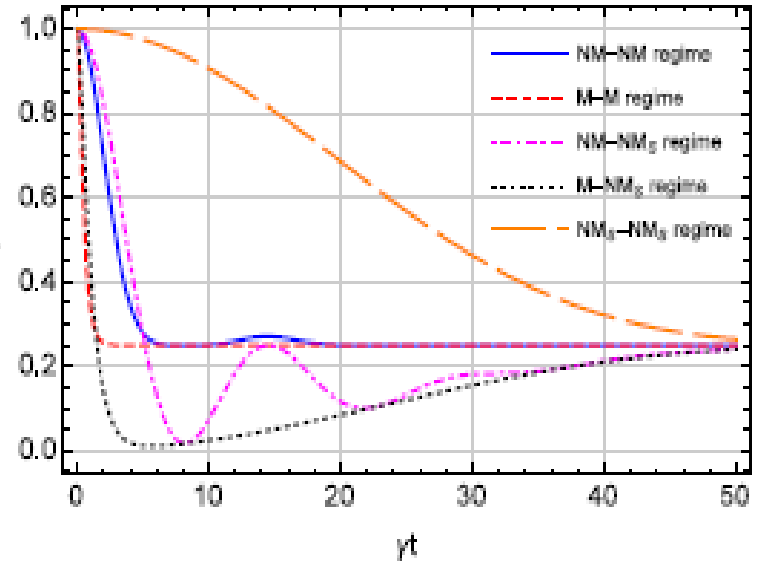
The effect of non-Markovian depolarizing channel on the CQD scheme.

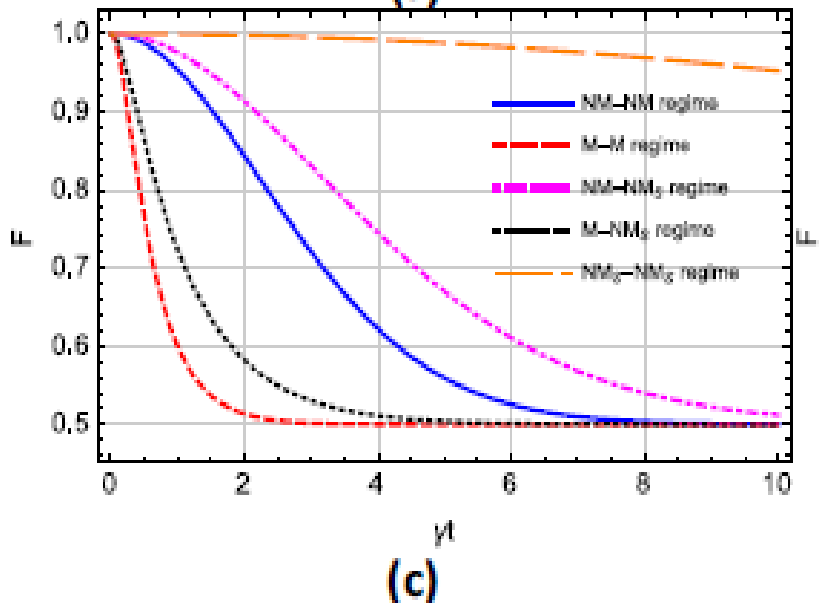


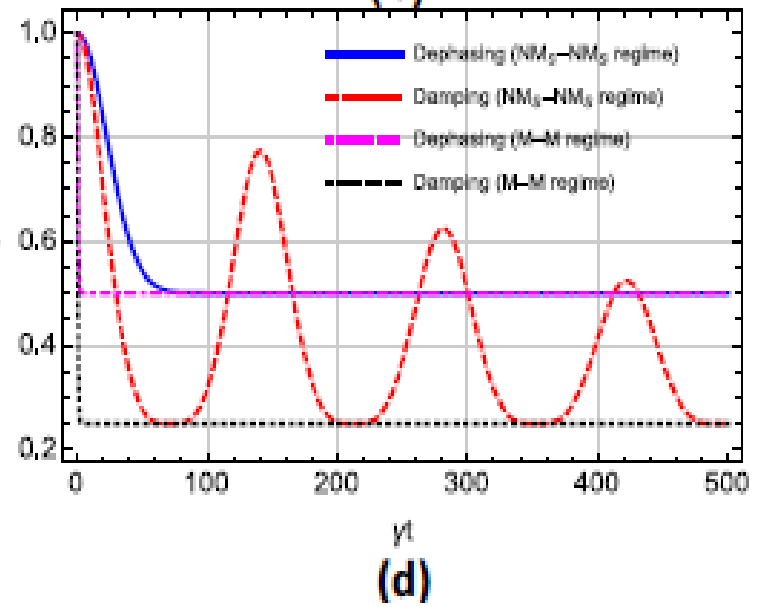


K. Thapliyal, **A. Pathak,** S. Banerjee, Quant. Infor. Process. 16, 115 (2017)



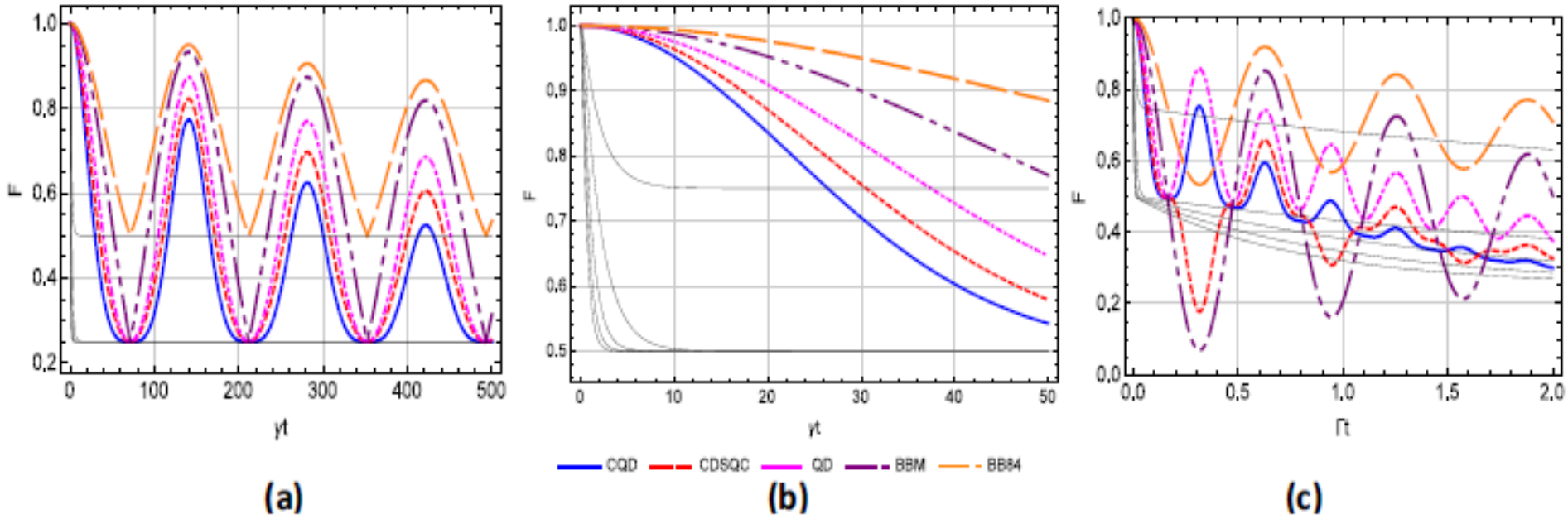






In (a) and (b), the choice of initial Bell states by Charlie is $|\psi^{\pm}\rangle$ and $|\phi^{\pm}\rangle$, respectively. (c) Shows similar cases over the dephasing channels. In (d), both purely dephasing and damping effects are shown.

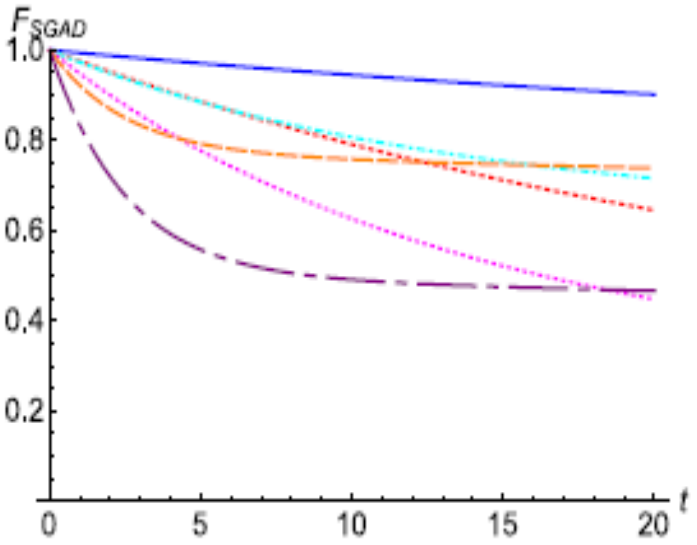
K. Thapliyal, **A. Pathak,** S. Banerjee, Quant. Infor. Process. 16, 115 (2017)



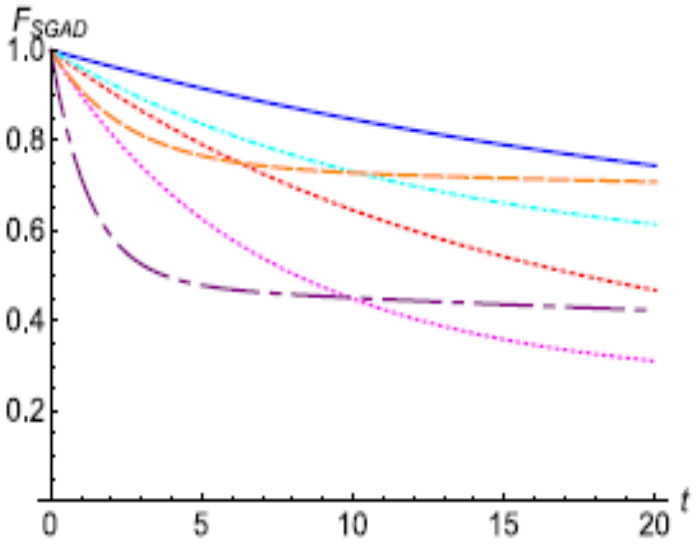
A comparative analysis of all the quantum cryptographic schemes discussed so far over the non-Markovian channels. Each line in all three plots corresponds to the different cryptographic scheme mentioned in the plot legend at the bottom of the figure. The light black lines in all three plots represent the corresponding Markovian cases, and the black lines from bottom to top show **the average fidelity for CQD, CDSQC, QD, BBM QKD, and BB84 QKD protocols.** The fidelity obtained for QSDC, DSQC, and QKA schemes is exactly the same as that of the QD protocol.

K. Thapliyal, **A. Pathak,** S. Banerjee, Quant. Infor. Process. 16, 115 (2017).

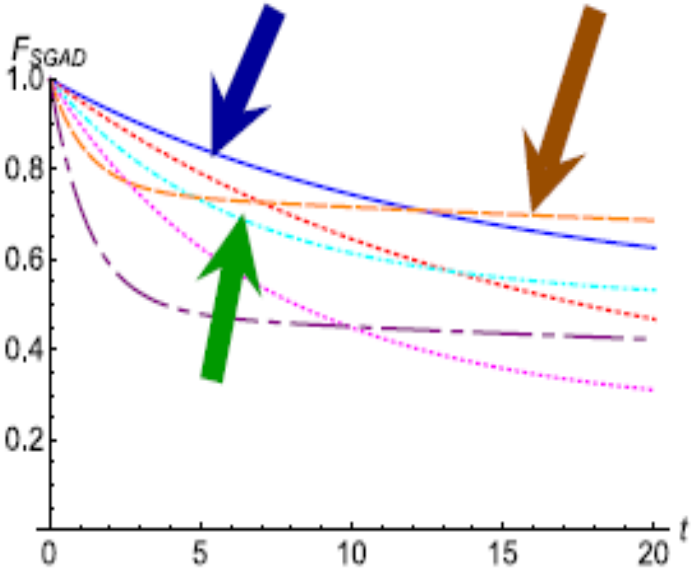
QKD



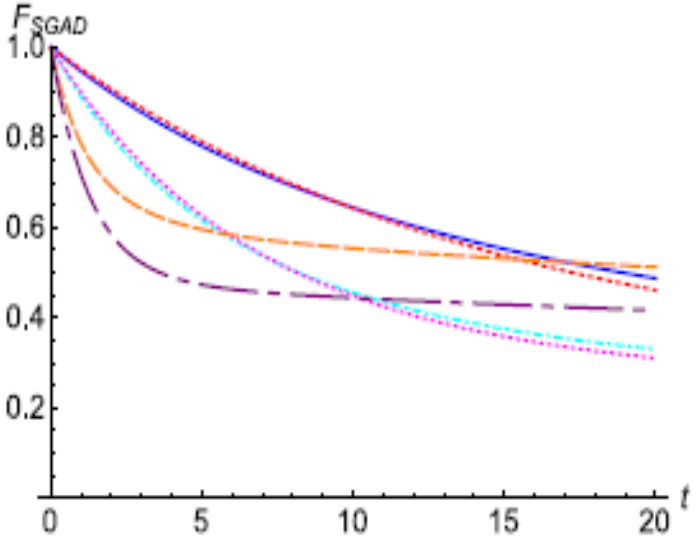
QKA



QSDC



QD



AD → **GAD** → **SGAD**

V. Sharma, K. Thapliyal, **A. Pathak,** S. Banerjee, Quant. Infor. Process. 15 (2016) 4681.

Some of recent publications

1. Design and experimental realization of an optimal scheme for teleportation of an n-qubit quantum state, M Sisodia, A Shukla, K Thapliyal, **A Pathak**, Quant. Infor. Proc. (2017) DOI: 10.1007/s11128-017-1744-2
2. Experimental realization of nondestructive discrimination of Bell states using a five-qubit quantum computer, M. Sisodia, A. Shukla, **A. Pathak**, Phys. Lett. A (2017) DOI 10.1016/j.physleta.2017.09.050.
3. On the origin of nonclassicality in single systems, S. Aravinda, R. Srikanth, **A. Pathak**, J. Phys. A (2017) In Press.
4. Semi-quantum communication: Protocols for key agreement, controlled secure direct communication and dialogue, C. Shukla, K. Thapliyal, **A. Pathak**, Quant. Infor. Process. (2017) DOI: 10.1007/s11128-017-1736-2. Comparison of lower- and higher-order nonclassicality in photon added and subtracted squeezed coherent states, K. Thapliyal, N. L. Samantray, J. Banerji, **A. Pathak**, Phys. Lett. A 381 (2017) 3178-3187.
5. Hierarchical Joint Remote State Preparation in Noisy Environment, C. Shukla, K. Thapliyal, **A. Pathak**, Quant. Infor. Proces. **16** (2017) 205.
6. Quantum cryptography: key distribution and beyond, A. H. Shenoy, **A. Pathak**, R. Srikanth Quanta **6** (2017) 1-47.

7. Quantum sealed-bid auction using a modified scheme for multiparty circular quantum key agreement, R. D. Sharma, K. Thapliyal and **A. Pathak**, Quant. Infor. Proces. **16** (2017) 169.
8. Quantum cryptography over non-Markovian channels, K. Thapliyal, **A. Pathak,** S. Banerjee, Quant. Infor. Process. **16** (2017) 115. Teleportation of a qubit using entangled non-orthogonal states: A comparative study, M. Sisodia, V. Verma, K. Thapliyal, **A. Pathak**, Quant. Infor. Process. (2017) In press; DOI 10.1007/s11128-017-1526-x
9. Protocols for quantum binary voting, K. Thapliyal, R. D. Sharma, **A. Pathak**, **15** (2017) 1750007
10. Asymmetric quantum dialogue in noisy environment, A. Banerjee, C. Shukla, K. Thapliyal, **A. Pathak**, P. K. Panigrahi, Quant. Infor. Proc. (2017) In Press.
11. Higher-order nonclassical properties of atom-molecule Bose-Einstein Condensate, S. K. Giri, K. Thapliyal, B. Sen, and **A. Pathak**, Physica A **466** (2017) 140-152.
12. A comparative study of protocols for secure quantum communication under noisy environment: single-qubit-based protocols versus entangled-state-based protocols, V. Sharma, K. Thapliyal, **A. Pathak**, S. Banerjee, Quant. Info. Proc. (2016) DOI: 10.1007/s11128-016-1396-7.
13. Secure quantum communication with orthogonal states, C. Shukla, A, Banerjee, **A. Pathak** and R. Srikanth, Int. J. Quant. Info. **14** (2016) 1640021.
14. Linear and nonlinear quantum Zeno and anti-Zeno effects in a nonlinear optical coupler, K. Thapliyal, **A. Pathak** and J. Perina, Phys. Rev. A **93** (2016) 22107.

15. Tomograms for open quantum systems: in(finite) dimensional optical and spin systems, K. Thapliyal, S. Banerjee and **A. Pathak**, Annals of Physics **366** (2016) 148-167.
16. Higher order two-mode and multi-mode entanglement in Raman processes, S. D. Giri, B. Sen, **A. Pathak,** and P. K. Jana, Phys. Rev. A **93** (2016) 012340.
17. Which verification qubits perform best for secure communication in noisy channel? R. D. Sharma, K. Thapliyal, **A. Pathak**, A. K. Pan, and A. De. Quant. Infor. Process. **15** (2016) 1703–1718.
18. Maximal entanglement concentration for (n+1)-qubit states, A. Banerjee, C. Shukla and A. **Pathak**, Quant. Infor. Process. **14** (2015) 4523-4536.
19. A General Method for Selecting Quantum Channel for Bidirectional Controlled State Teleportation and Other Schemes of Controlled Quantum Communication, K. Thaliyal, A. Verma and **A. Pathak**, Quant. Infor. Process. **14** (2015) 4601-4614.
20. Quasiprobability distributions in open quantum systems: spin-qubit systems, K. Thapliyal, S. Banerjee, **A. Pathak**, S. Omkar, V. Ravishankar, Annals of Physics **362** (2015) 261-286.
21. Controlled bidirectional remote state preparation in noisy environment: A generalized view, V. Sharma, C, Shukla, S. Banerjee and **A.Pathak**, Quant. Info. Process. **14** (2015) 3441–3464.
22. Applications of quantum cryptographic switch: Various tasks related to controlled quantum communication can be performed using Bell states and permutation of particles, K. Thapliyal and **A. Pathak**, Quant. Info. Process **14** (2015) 2599–2616.

23. Statistical mixtures of states can be more quantum than their superpositions: Comparison of nonclassicality measures for single-qubit states, A. Miranowicz., K. Bartkiewicz, **A. Pathak**, J. Perina Jr, Y. N. Chen and F. Nori, Phys. Rev. A **91** (2015) 042309.
24. Efficient protocols for unidirectional and bidirectional controlled deterministic secure quantum communication: Different alternative approaches, **A. Pathak**, Quant. Info. Process. **14** (2015) 2195-2210.
25. Protocols and quantum circuits for implementing entanglement concentration in cat state, GHZ-like state and 9 families of 4-qubit entangled states, C. Shukla, A. Banerjee and **A. Pathak**, Quant. Info. Process. **14** (2015) 2077-2099.
26. An integrated hierarchical dynamic quantum secret sharing protocol, S. Mishra, C. Shukla, **A. Pathak**, R. Srikanth, A. Venugopalan, Int. J. Theor, Phys. **54** (2015) 3143–3154.
27. Orthogonal-state-based cryptography in quantum mechanics and local post-quantum theories, S. Aravinda, A. Banerjee, **A. Pathak**, R. Srikanth, Int. J. Quant. Info. **12** (2014) 1560020
28. Nonclassical properties of a contradirectional nonlinear optical coupler, K. Thapliyal, **A. Pathak**, B. Sen, J. Perina, Phys. Lett. A 378 (2014) 3431-3440.
29. Two-step orthogonal-state-based protocol of quantum secure direct communication with the help of order-rearrangement technique, P. Yadav, R. Srikanth and **A. Pathak**, Quant. Info. Process. **13** (2014) 2731–2743.


THANK
YOU