Unconditional security of quantum cryptographic protocols: A myth or reality?

Anirban Pathak

Jaypee Institute of Information Technology, Noida

QIPA-18, HRI, December 2, 2018

Purpose of this talk

- Certain things are strongly believed in computer science, specially in the complexity theory (say $\mathrm{P} \neq NP$). Such believes/confidence are dangerous for cryptography.
- **Purpose of the talk:** Not to become religious and start trusting your (quantum) protocols and devices; keep questioning!
- **Declaration:**

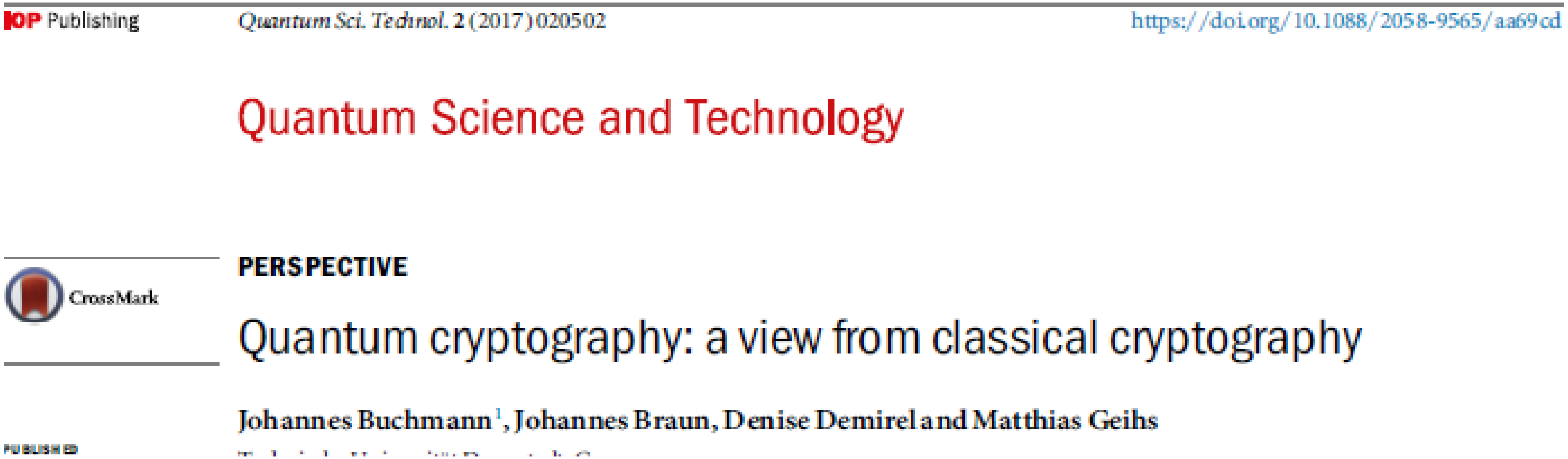
1. I'll not talk much on security proofs. This talk will be more on physical aspects. Specifically, on- what happens in reality, specially when devices used are not perfect and noise is present?
2. A broader meaning of the word "unconditional" will be used.
3. The problem is deeper than the problems associated with SPS and SPD.

Let’s understand the difference between conditional and unconditional security via some examples

- Remote coin tossing: Alice and Bob wants to toss a coin, but Alice is at JIIT and Bob is at HRI, and they neither trust a third party (a common friend) nor they want to see each other.
- RSA and DH also provide conditional security.

Longer key corresponds to more difficult problem and we assume that Eve will take more time to break it and the key will remain secure for longer time.

The assumption about Eve’s computational power makes the scheme conditionally secure.



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

Quantum Science and Technology

PERSPECTIVE

Quantum cryptography: a view from classical cryptography

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

PUBLISHED

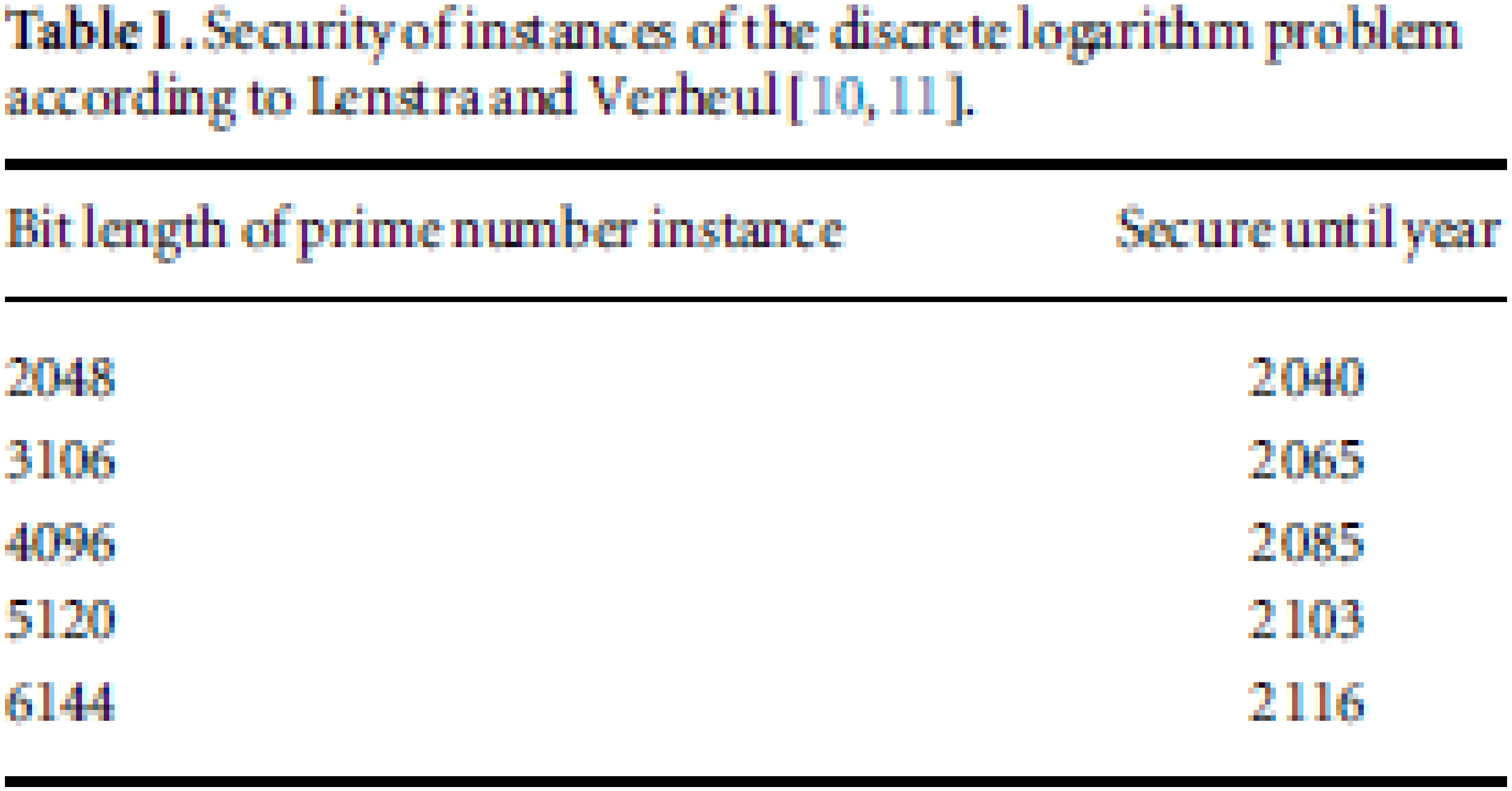


Table 1. Security of instances of the discrete logarithm problem according to Lenstra and Verheul [10, 11].

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 DH based systems. **Further, in 2017, D Wave processor factorised 200099; and Li et al., factorized 291311=> Li et al., used only 3 qubits. Panigrahi et al. claimed=>90L+**

Krichoff's principle to QKD

- A cryptosystem would remain secure even if everything about the system, except the key is a public knowledge. Thus, it would be impossible to break (unlock) the cryptogram without a key. Once the key is secure the communication using that key will also be secure.

- Alice and Bob may meet privately and share a key, but that may not be possible in every occasion.
- When Alice and Bob cannot meet, we would require a mechanism for key distribution (KD).
- When a KD scheme is implemented using quantum resources, it is referred to as QKD.

What a QKD protocol is?

- A scheme for key amplification.
- A scheme that exploits uncertainty principle (noncommutativity leading to nocloing and inability to perform simultaneous measurement in the non-orthogonal bases), nonlocality, etc.
- It’s actually art of utilizing negative results of early quantum mechanics for a meaningful (positive) purpose.

BB84, B92, Ekert, GV,….What leads to security?

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

MERMAID!
GIVE AN EXAMPLE OF QUANTUM SUPERPOSITION
BUT NOBODY HAS SEEN IT!
THAT'S SIMPLE, THE MOMENT YOU OBSERVE A MERMAID, IT GETS COLLAPSED TO EITHER FISH OR GIRL

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

Some observations

Notes:

(1) Nocloning may be applicable for orthogonal states, too.

(2) Conjugate coding is not essential for quantum cryptography!

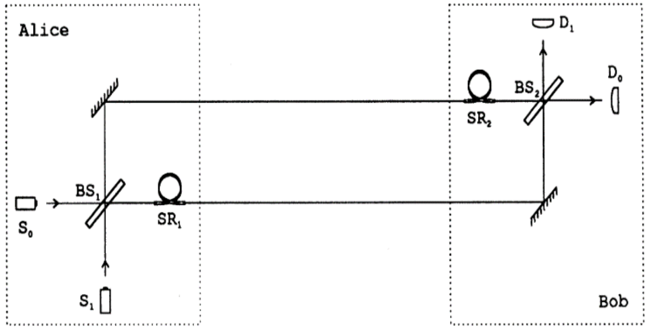
(3) Everything that can be done using conjugate code can also be done with orthogonal states based scheme, and they are equivalent in noiseless situation. Noise destroys the equivalence.

- **Orthogonal state based protocols:**

QKD: **GV, N09**

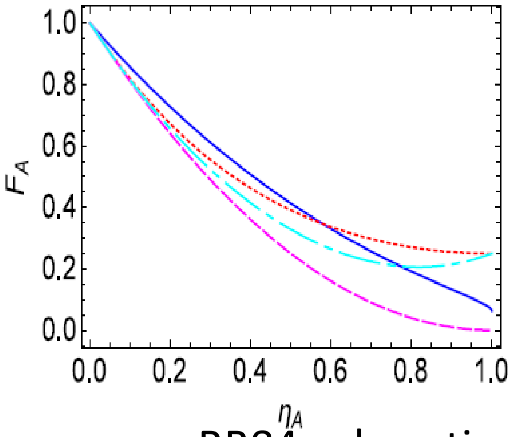
1. P. Yadav, R. Srikanth and **A. Pathak**, "Two-step orthogonal-state-based protocol of quantum secure direct communication with the help of order-rearrangement technique", Quant. Info. Process. (2014).
2. C. Shukla, **A. Pathak** and R. Srikanth, "Beyond the Goldenberg-Vaidman protocol: Secure and efficient quantum communication using arbitrary, orthogonal, multi-particle quantum states", Int. J. Quant. Info., **10** (2012) 1241009.
3. C. Shukla and **A. Pathak**, "Orthogonal-state-based secure direct quantum communication without actual transmission of the message qubits", Quant. Info. Process **13** (2014) 2099-2113.
4. C. Shukla, N. Alam and **A. Pathak,** "Protocols of quantum key agreement solely using Bell states and Bell measurement", Quant. Info. Process. **13** (2014) 2391-2405.
5. K. Thapliyal, R. D. Sharma and **A. Pathak**, Int. J. Quant. Inf. 16, 1850047 (2018)

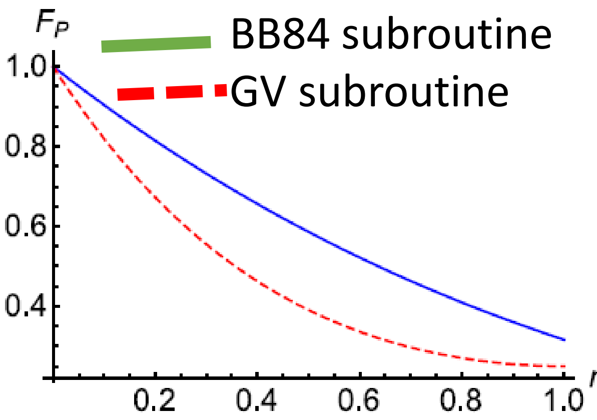
Equivalence of GV and BB84 is not valid in noisy environment



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.

“Quantum phenomena do not occur in a Hilbert space. They occur in a laboratory”-- Asher Peres

⇒Quantum cryptography utilizes quantum phenomena and that do happens in the laboratory and the limitations of the devices create windows for side channel attacks or hacking.

⇒Imperfection of the devices leads to a possibility of hacking and probably puts a question mark on the claimed unconditional security.

⇒Presence of noise provides an opportunity to Eve to hide behind the noise or to exploit it by replacing a lossy channel by a better channel, say a Markovian channel by a non-Markovian channel.

Quantum hacking and post-quantum cryptography

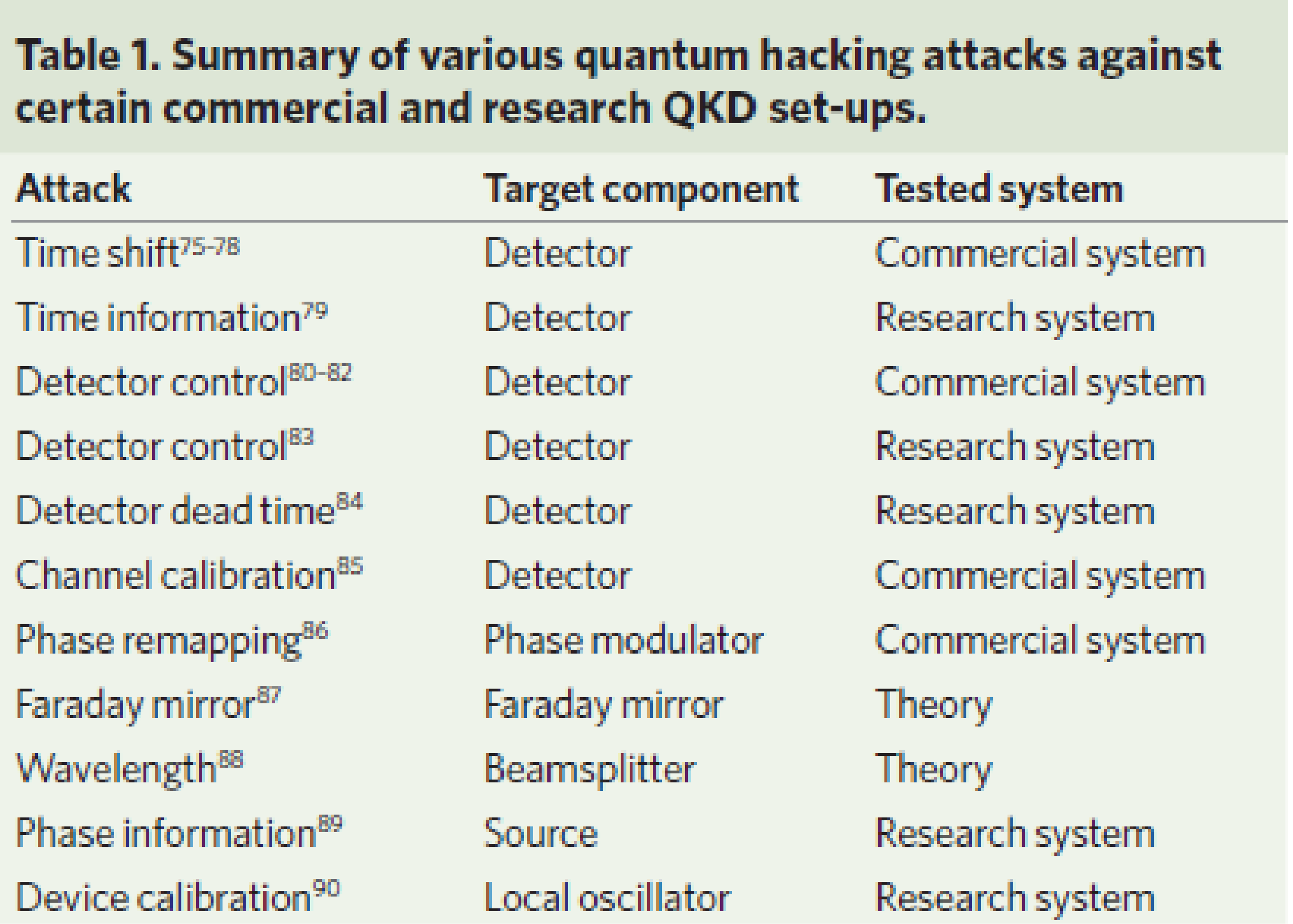


Table 1. Summary of various quantum hacking attacks against certain commercial and research QKD set-ups.

Attack	Target component	Tested system
Time shift[75–78]	Detector	Commercial system
Time information[79]	Detector	Research system
Detector control[80–82]	Detector	Commercial system
Detector control[83]	Detector	Research system
Detector dead time[84]	Detector	Research system
Channel calibration[85]	Detector	Commercial system
Phase remapping[86]	Phase modulator	Commercial system
Faraday mirror[87]	Faraday mirror	Theory
Wavelength[88]	Beamsplitter	Theory
Phase information[89]	Source	Research system
Device calibration[90]	Local oscillator	Research system

1. Lattice-based cryptography
2. Code-based cryptography
3. Multivariate polynomial cryptography
4. Hash-based signatures
5. Secret-key cryptography, such as Advanced Encryption Standard (AES)

Note: Security provided by post-quantum cryptographic schemes are not unconditional.

H.-K. Lo, Nature Photonics 8, 595 (2014);
A. Shenoy-Hejamadi, A. Pathak, S. Radhakrishna. Quanta **6**, 1 (2017).

A bit of computing: We can solve problems of BQP complexity class

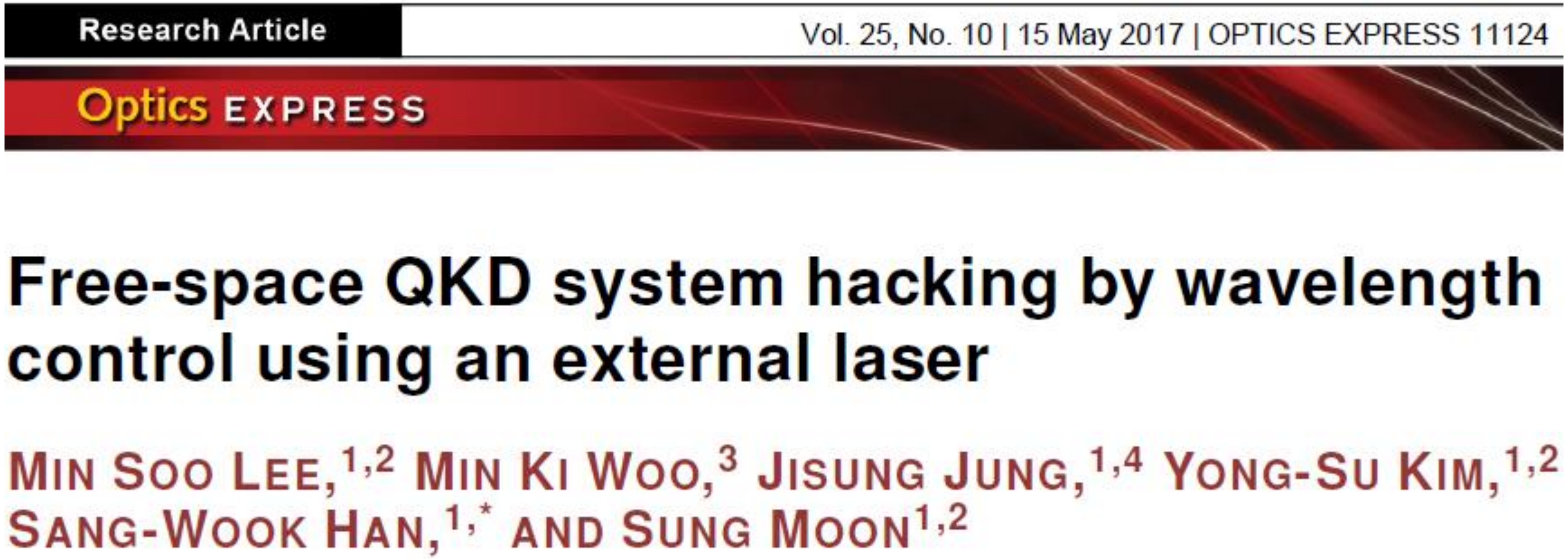
BOB, YOU GET AN F GRADE, AS YOU CANNOT SOLVE ANY PROBLEM IN 3 HOURS !!
IT IS NOT MY FAULT. THE PROBLEMS WERE IN NP WITH RESPECT TO THE ALGORITHMS I KNOW.
IF YOU DON'T STUDY THEN ALL PROBLEMS WILL APPEAR IN NP-COMPLETE !!

Shor’s Algorithm is dangerous for classical cryptography

Grover’s Algorithm

IF I GIVE YOU A PHONE NUMBER FROM A TELEPHONE DIRECTORY HAVING 10^6 NAMES, THEN HOW MANY SEARCHES YOU NEED TO FIND THE NAME OF THE TELEPHONE OWNER?
ONLY SINGLE QUERY, I'LL JUST CALL HIM AND ASK HIS NAME!

Quadratic saving does not do much harm to classical cryptographic protocols. Key size gets doubled and we have post-quantum schemes

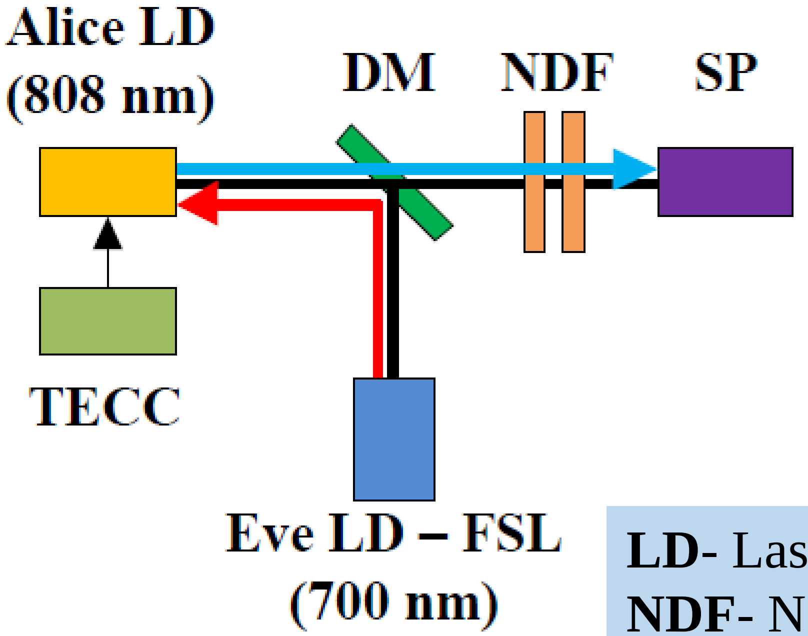


Research Article Vol. 25, No. 10 | 15 May 2017 | OPTICS EXPRESS 11124

Optics EXPRESS

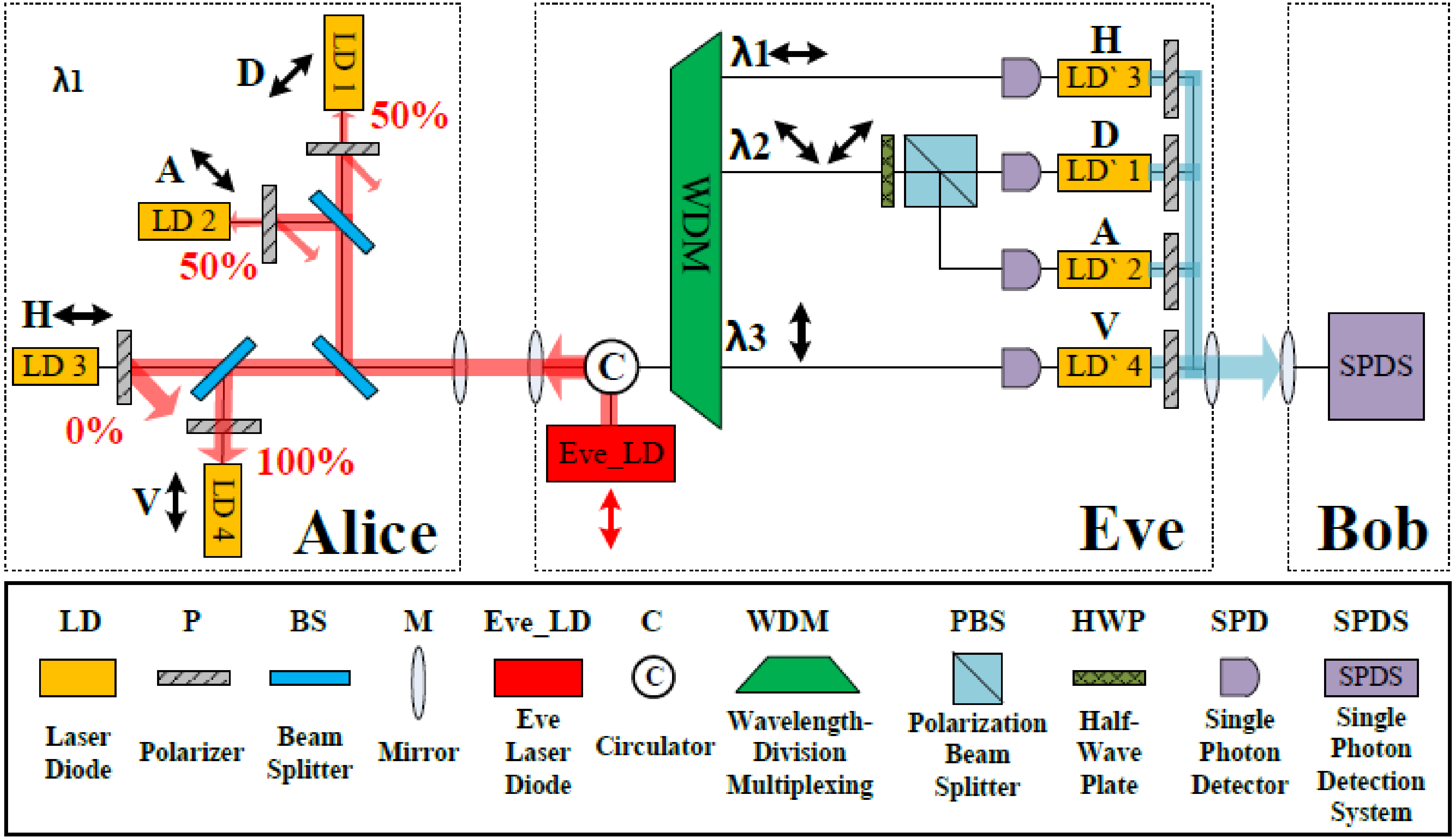
Free-space QKD system hacking by wavelength control using an external laser

MIN SOO LEE,[1,2] MIN KI WOO,[3] JISUNG JUNG,[1,4] YONG-SU KIM,[1,2] SANG-WOOK HAN,[1,*] AND SUNG MOON[1,2]



LD- Laser diode, **DM**- Dichroic mirror
NDF- Neutral-density-filter, **SP**- Spectrometer
TECC- Thermoelectric cooler controller
FSL- Femtosecond laser

A simple attack on BB84 subroutine



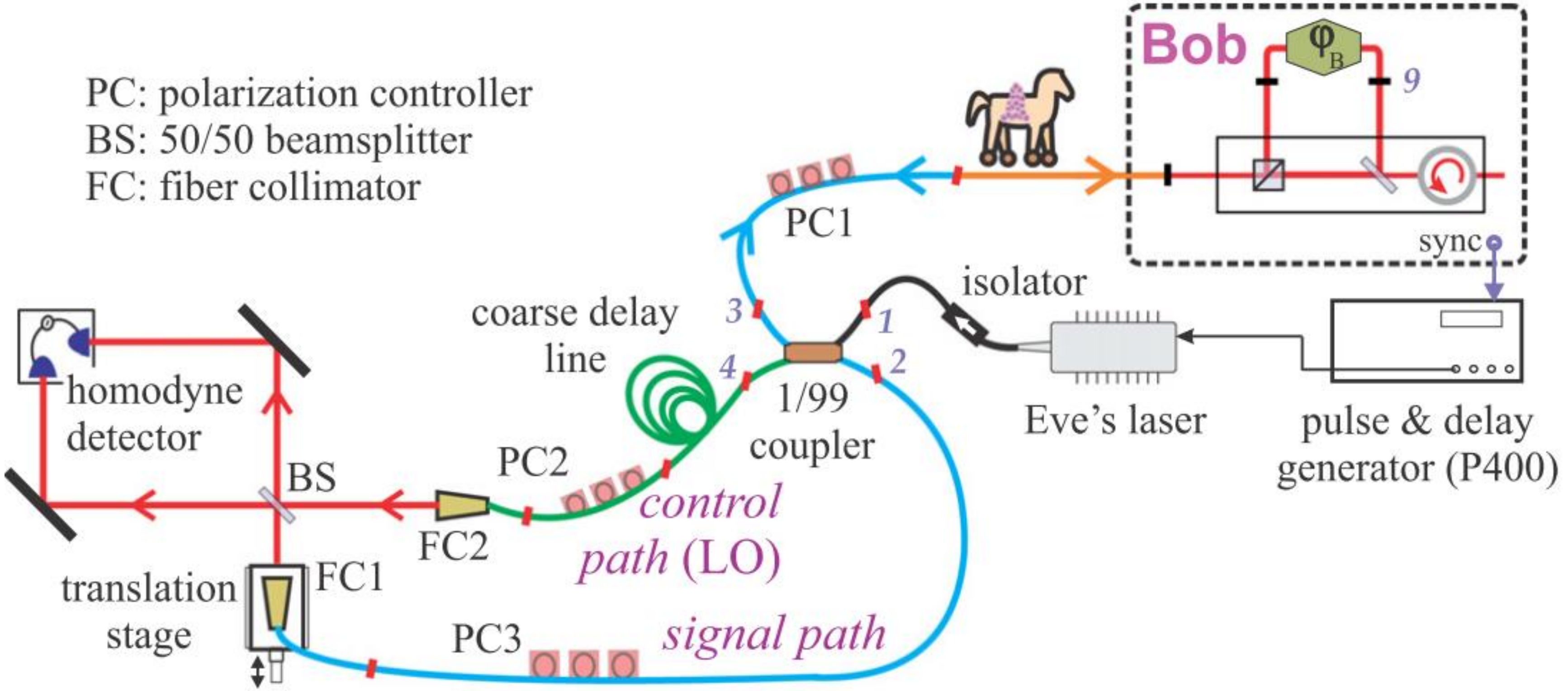
How to prevent the attack:

(1) An external strong laser monitoring unit can detect Eve’s attempt.

(2) Random variations in the LD wavelength under Alice’s control can be a second solution.

(3) Alice can insert a circulator at the end of his Box.

An attack on Clavis2 which implements SARG04



Schematic of a Trojan-horse eavesdropper

1. Eve may send a bright light from the quantum channel and analyzing the back-reflections she may know Bob's secret basis choice with more than 90% probability (Even when the number of back-reflected photons is not high).

N. Jain, et al. "Trojan-horse attacks threaten the security of practical quantum cryptography." *New Journal of Physics* 16, 123030 (2014).

Does Kirchoff’s principle implies that unconditional security of a QKD protocol (say, BB84) implies unconditional security for every other cryptographic tasks?

- At least not in a direct manner.
    - Look at the remote coin tossing scheme
        - Alice and Bob cannot use QKD to pre-generate a key.
- Similar problem exists in two party bit commitment & oblivious transfer.

Main concepts and practices that can be questioned in view of the claim of unconditional security

- **Concept 1: Nocloning**=> What about partial cloning? Imperfect cloning is allowed. Usually, that would leave a trace and we can get a trace under a broader class of measurement induced errors, but we need to consider it.
- **Concept 2: Nonlocality leading to device independence**=> Are the tests performed to check quantum correlation loophole free? In most cases it's not.
- **Concept 2.1: Complete device independence:** 100% efficient detector is required which does not seem realistic.
- **Concept 2.2: Measurement device independent QKD:** Protects from the detector side channel attacks only. What about other device use? If we assume that the other devices are not prone to side channel attacks, we are imposing conditions and loosing the beauty of unconditional security in a broader sense.

Little more on partial cloning and its connection to quantum cryptography

1996: Buzek and Hillery (PRA **54**, 1844 (1996)) introduced the **Universal Quantum Cloning Machine** which can clone any arbitrary d-dimensional quantum state with fidelity F$=\frac{1}{2}+\frac{1}{1+d}$

⇒This expression leads to a question what is the optimal value of *d* in QKD?

1998: Duan and Guo [PRL **80**, 4999 (1998)] invented the **Probabilistic Quantum Cloning Machine** where a quantum state, randomly chosen from a certain set, can be probabilistically cloned with positive cloning efficiencies iff all the states in the set are linearly independent.

2000: Bruß, Cinchetti, et al [PRA **62**, 012302 (2000)] invented best state dependent quantum cloning machine known as the **"phase covariant," quantum cloning machine.**

Little more on partial cloning and its connection to quantum cryptography

- **2002**: N. J. Cerf, et al. [PRL **88**, 127902 (2002)], and in 2004 Durt et al., [PRA **69**, 032313 (2004).] considered different qudit-based quantum cryptographic schemes and **computed the upper bound on the error rate that ensures unconditional security against a cloning-based individual attack**

- **2012**: A. Ferenczi and N. Lutkenhaus [PRA **85**, 052310 (2012)] have investigate the connection between the optimal collective eavesdropping attack and the optimal cloning attack where the **eavesdropper employs an optimal cloner to attack the quantum key distribution (QKD) protocol for discrete variable protocols in *d*-dimensional Hilbert spaces.**

Even device independent schemes can be attacked

- A critical weakness of device-independent protocols that rely on public communication between secure laboratories -- Untrusted devices may record their inputs and outputs and reveal information about them via publicly discussed outputs during later runs. Reusing devices thus compromises the security of a protocol and risks leaking secret data.

Composability issue is in general present in all protocols beyond QKD.

Barrett, Jonathan, Roger Colbeck, and Adrian Kent. "Memory attacks on device-independent quantum cryptography." *Physical Review Letters* 110 (2013) 010503.

Usual practices followed in designing new protocols

- **Usual practice 1:** We often write- Alice and Bob compare the result of measurements on the verification (decoy) qubits and compute error rate. If the error is found to be smaller than the tolerable limit, we move to the next step, otherwise we discard the protocol (or go back to first step).

Question: Do we really know a tight bound on tolerable error rate for any arbitrary attack?

No! In most cases tolerable error rate is computed for a set of attacks. **Are we assuming that Eve will perform only one of those attacks?**

Is that a compromise with the claim of unconditional security?

Usual practices followed in designing new protocols

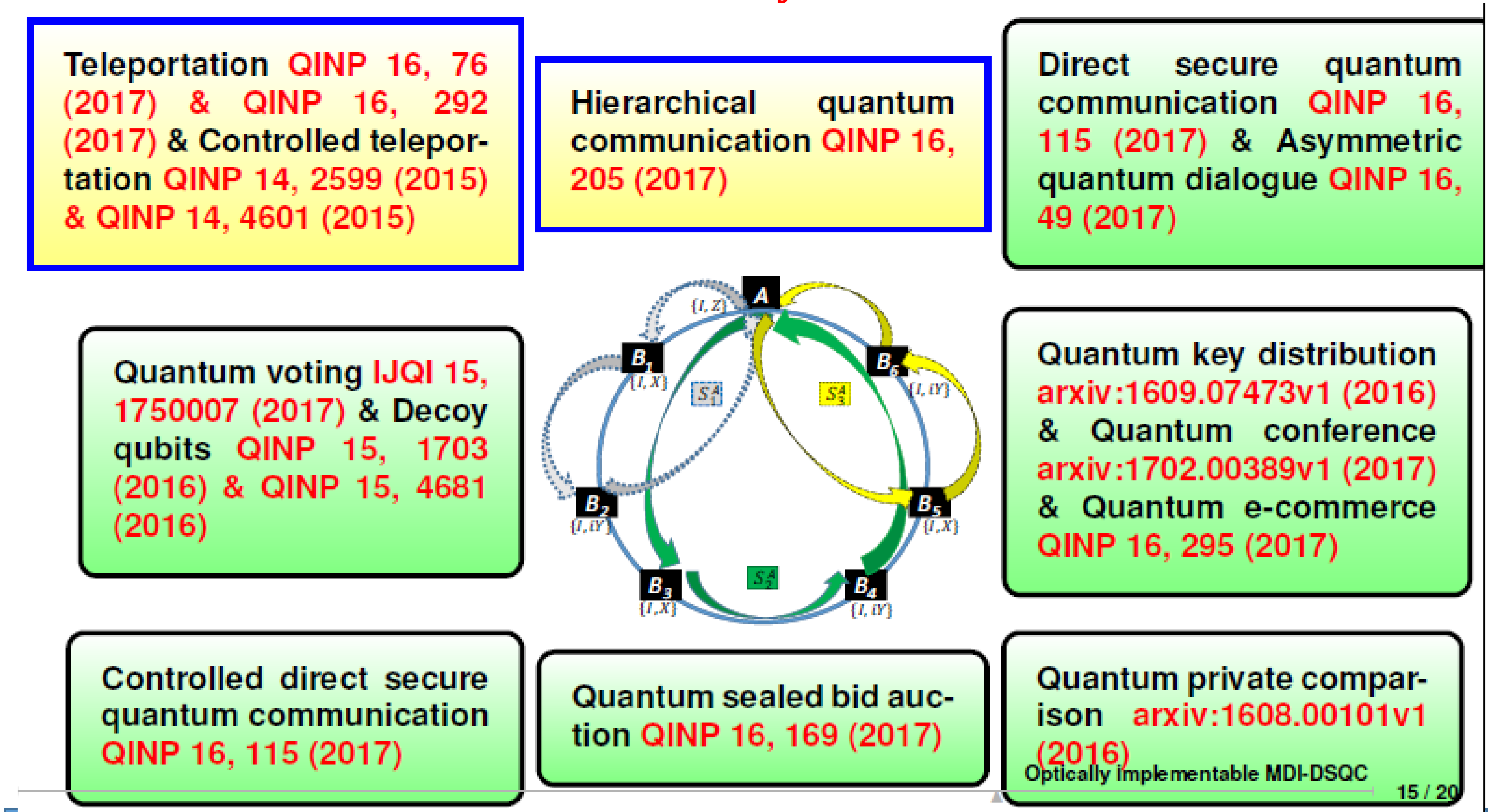
- **Usual practice 1:** We often write- After receiving an ***authentic*** acknowledgement or receipt from Bob, Alice discloses …..
- In such statements and to start the protocol you need a kind of authentication which in turn requires a pre-shared key.

How can that be done in a public key crypto system?

Often Hash function is used for authentication but is not unconditionally secure. Only our confidence is high on them.

Note: Trust and confidence is dangerous for cryptography.

Quantum cryptography is not all about QKD: Are these protocol unconditionally secure



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)

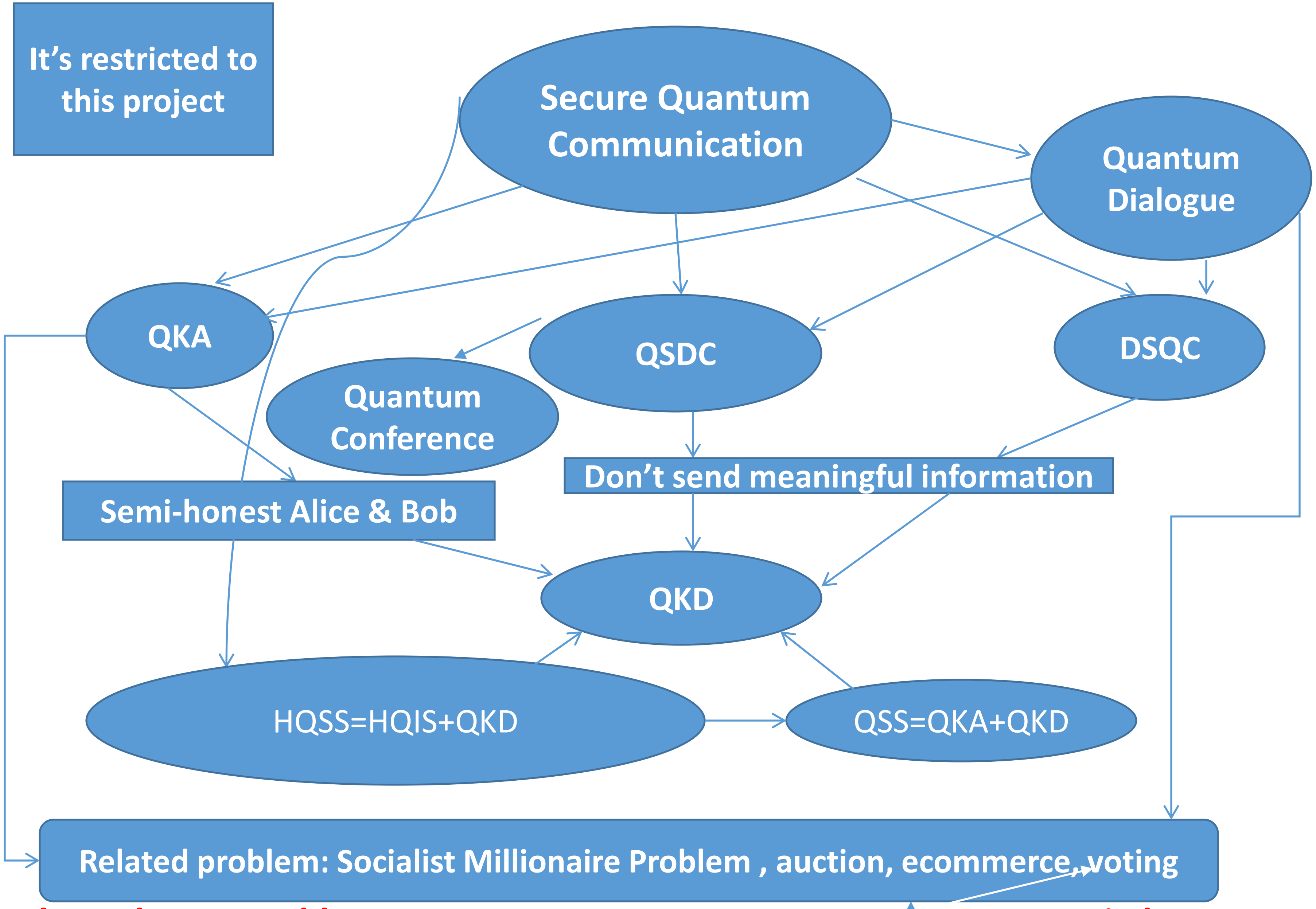
Controlled direct secure quantum communication QINP 16, 115 (2017)

Quantum sealed bid auction QINP 16, 169 (2017)

Quantum private comparison arxiv:1608.00101v1 (2016)

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

Many facets of secure direct quantum communication



It's restricted to this project

Secure Quantum Communication

Quantum Dialogue

QKA

QSDC

DSQC

Quantum Conference

Don't send meaningful information

Semi-honest Alice & Bob

QKD

HQSS=HQIS+QKD

QSS=QKA+QKD

Related problem: Socialist Millionaire Problem , auction, ecommerce, voting

Other relevant problems: HQSS, HDQSS, C-QSDC, C-DSQC, Crypto-Switch, etc.

In the schemes of controlled quantum communication, what happens if Alice and Bob are not semi-honest?

- A semi-honest user is one who follows the protocol honestly, but tries to get more information (more than what he is authorized to receive) or prior information or to cheat.
- All schemes of controlled-teleportation (does not require security), controlled-QSDC, controlled-DSQC, controlled-QKD assumes that Alice and Bob are semi-honest.
- Is not it a strong assumption, which essentially weakens unconditional security?

Quantum Protocols for online shopping or e-commerce are essentially CDSQC protocol

Examples of controlled cryptographic schemes

- Srinatha, N., Omkar, S., Srikanth, R., Banerjee, S., & Pathak, A. (2014). The quantum cryptographic switch. *Quantum information processing*, *13*(1), 59-70.
- Thapliyal, K., & Pathak, A. (2015). Applications of quantum cryptographic switch: various tasks related to controlled quantum communication can be performed using Bell states and permutation of particles. *Quantum Information Processing*, *14*(7), 2599-2616.
- Thapliyal, K., Pathak, A., & Banerjee, S. (2017). Quantum cryptography over non-Markovian channels. *Quantum Information Processing*, *16*(5), 115.
- Shukla, C., Thapliyal, K., & Pathak, A. (2017). Semi-quantum communication: protocols for key agreement, controlled secure direct communication and dialogue. *Quantum Information Processing*, *16*(12), 295.
- Thapliyal, K., & Pathak, A. (2018). Quantum e-commerce: A comparative study of possible protocols for online shopping and other tasks related to e-commerce. *arXiv preprint arXiv:1807.08199*.

Quantum Protocols for online shopping or e-commerce are essentially CDSQC protocol

QUANTUM DIALOGUE: BA AN PROTOCOL

1. Bob prepares large number of copies of a Bell state $\left|\phi^{+}\right\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$. 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.

Nguyen, Ba An. "Quantum dialogue." *Physics Letters A* 328.1 (2004): 6-10.

SUFFICIENT CONDITION FOR QUANTUM DIALOGUE

- If we have a mutually orthogonal set of n-qubit states $\{|\phi_0\rangle, |\phi_1\rangle, \cdots, |\phi_i\rangle, \cdots, |\phi_{2^n-1}\rangle\}$ and a set of m-qubit $(m \leq n)$ unitary operators $\{U_0, U_1, U_2, ..., U_{2^n-1}\} : U_i|\phi_0\rangle = |\phi_i\rangle$ and $\{U_0, U_1, U_2, ..., U_{2^n-1}\}$ forms a group under multiplication then it would be sufficient to construct a quantum dialogue protocol of Ba-An-type using this set of quantum states and this group of unitary operators.

Rearrangement of order of the particles and insertion of decoy photons make the protocol unconditionally secure.

C. Shukla, V. Kothari, A. Banerjee and **A. Pathak**, Phys. Lett. A, **377** (2013) 518.

How to form groups of unitary operators?

$G_1=\{I,X,iY,Z\}$ forms a group of order 4 under multiplication

$\therefore G_n=G_1^{\otimes n}=\{I,X,iY,Z\}^{\otimes n}$ forms a group of order $2^{2^n}=4^n$

Example: G_2 is the group of order 16.

$$\begin{aligned} G_2 &= G_1\otimes G_1=\{I,X,iY,Z\}\otimes\{I,X,iY,Z\}\\ &= \{I\otimes I, I\otimes X, I\otimes iY, I\otimes Z, X\otimes I, X\otimes X,\\ &\quad X\otimes iY, X\otimes Z, iY\otimes I, iY\otimes X, iY\otimes iY,\\ &\quad iY\otimes Z, Z\otimes I, Z\otimes X, Z\otimes iY, Z\otimes Z\} \end{aligned}$$

Pauli Operators	I	X	iY	Z
I	I	X	iY	Z
X	X	I	Z	iY
iY	iY	Z	I	X
Z	Z	iY	X	I

Group multiplication table

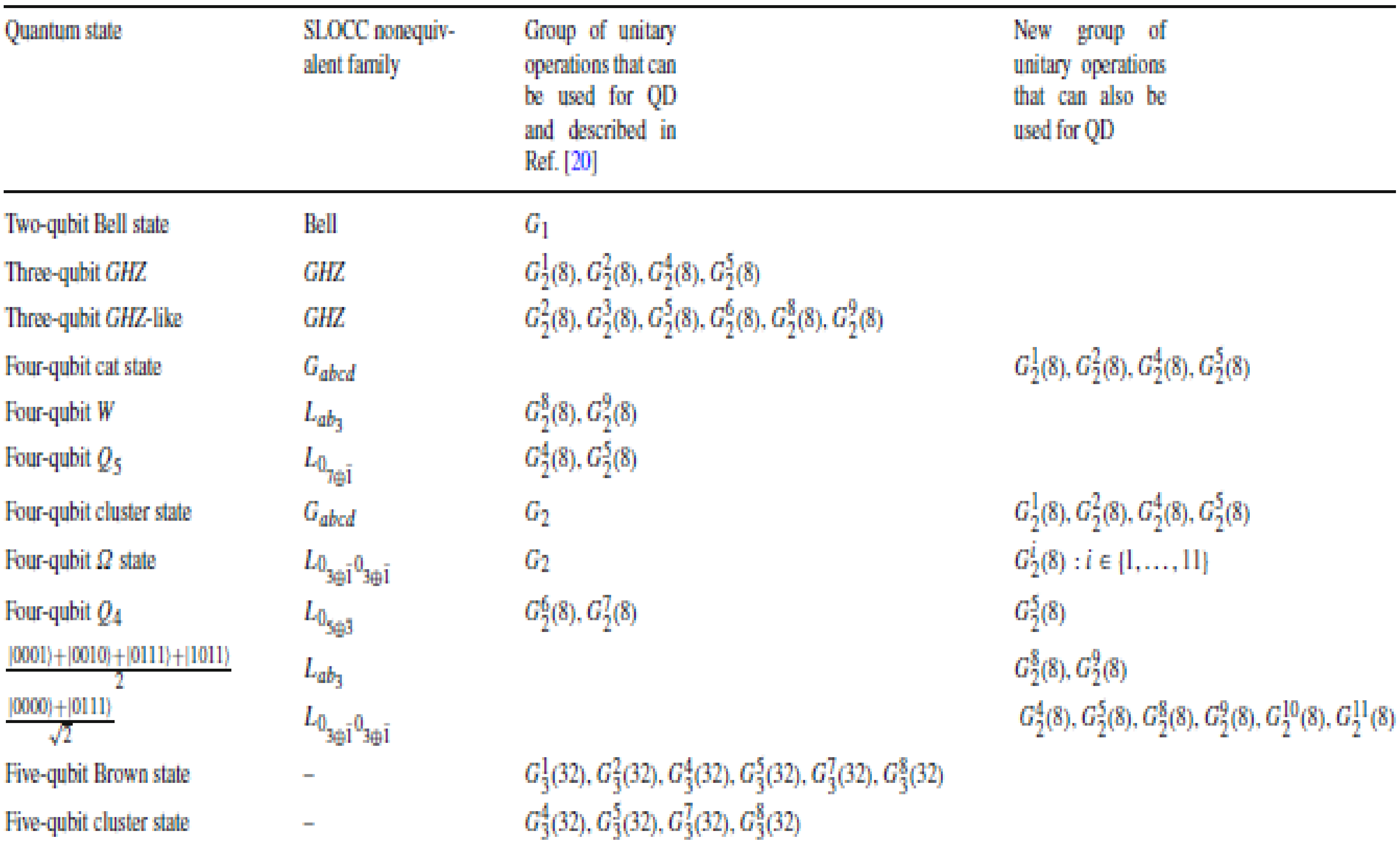
$G_1=G_1^{\otimes 1}(order\ 2^{2^1}=4^1=4)$

$G_2=G_1^{\otimes 2}=G_1\otimes G_1(order\ 2^{2^2}=4^2=16)$

$G_3=G_1^{\otimes 3}=G_1\otimes G_1\otimes G_1=G_2^{\otimes 2}\otimes G_1(order\ 2^{2^3}=4^3=64)$

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

Table 1 List of useful quantum states and corresponding operators that may be used to implement protocols for AQD and QD



Quantum state	SLOCC nonequivalent family	Group of unitary operations that can be used for QD and described in Ref. [20]	New group of unitary operations that can also be used for QD
Two-qubit Bell state	Bell	G_1	
Three-qubit *GHZ*	*GHZ*	$G_2^1(8), G_2^2(8), G_2^4(8), G_2^5(8)$	
Three-qubit *GHZ*-like	*GHZ*	$G_2^2(8), G_2^3(8), G_2^5(8), G_2^6(8), G_2^8(8), G_2^9(8)$	
Four-qubit cat state	G_{abcd}		$G_2^1(8), G_2^2(8), G_2^4(8), G_2^5(8)$
Four-qubit W	L_{ab_3}	$G_2^8(8), G_2^9(8)$	
Four-qubit Q_5	$L_{0_{7\oplus\bar{1}}}$	$G_2^4(8), G_2^5(8)$	
Four-qubit cluster state	G_{abcd}	G_2	$G_2^1(8), G_2^2(8), G_2^4(8), G_2^5(8)$
Four-qubit Ω state	$L_{0_{3\oplus\bar{1}}0_{3\oplus\bar{1}}}$	G_2	$G_2^i(8) : i \in \{1, \ldots, 11\}$
Four-qubit Q_4	$L_{0_{5\oplus 3}}$	$G_2^6(8), G_2^7(8)$	$G_2^5(8)$
$\frac{\|0001\rangle+\|0010\rangle+\|0111\rangle+\|1011\rangle}{2}$	L_{ab_3}		$G_2^8(8), G_2^9(8)$
$\frac{\|0000\rangle+\|0111\rangle}{\sqrt{2}}$	$L_{0_{3\oplus\bar{1}}0_{3\oplus\bar{1}}}$		$G_2^4(8), G_2^5(8), G_2^8(8), G_2^9(8), G_2^{10}(8), G_2^{11}(8)$
Five-qubit Brown state	–	$G_3^1(32), G_3^2(32), G_3^4(32), G_3^5(32), G_3^7(32), G_3^8(32)$	
Five-qubit cluster state	–	$G_3^4(32), G_3^5(32), G_3^7(32), G_3^8(32)$	

Asymmetric quantum dialogue in noisy environment, A. Banerjee, C. Shukla, K. Thapliyal, A. Pathak, P. K. Panigrahi, Quantum Inf. Process. 14, 2599-2616 (2016)

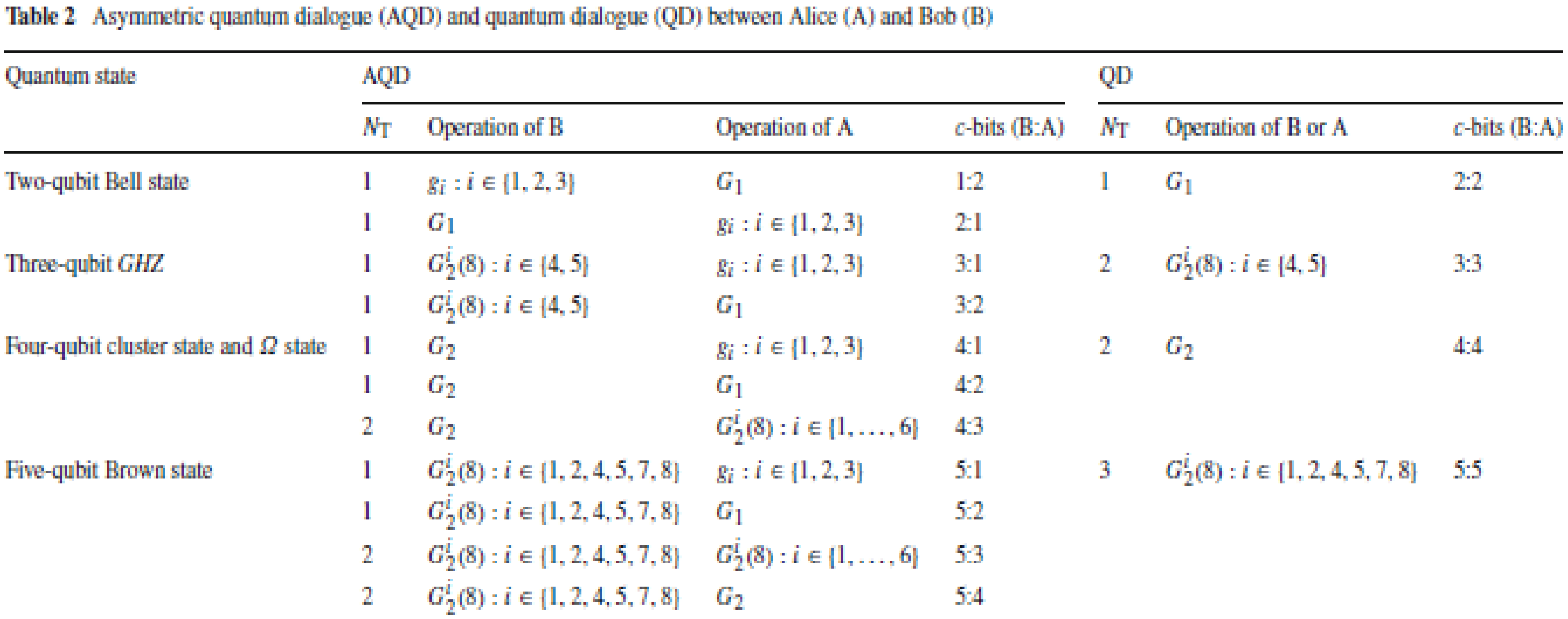


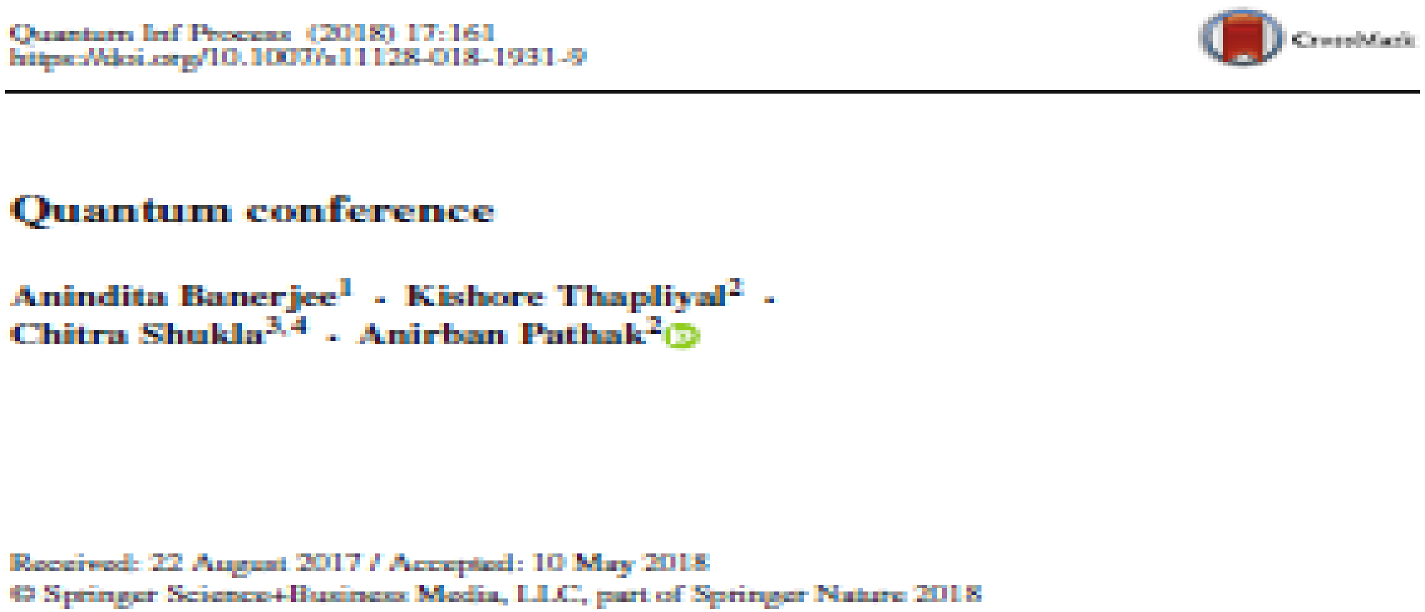
Table 2 Asymmetric quantum dialogue (AQD) and quantum dialogue (QD) between Alice (A) and Bob (B)

Quantum state	AQD				QD		
	N_T	Operation of B	Operation of A	c-bits (B:A)	N_T	Operation of B or A	c-bits (B:A)
Two-qubit Bell state	1	$g_i : i \in \{1, 2, 3\}$	G_1	1:2	1	G_1	2:2
	1	G_1	$g_i : i \in \{1, 2, 3\}$	2:1			
Three-qubit *GHZ*	1	$G_2^i(8) : i \in \{4, 5\}$	$g_i : i \in \{1, 2, 3\}$	3:1	2	$G_2^i(8) : i \in \{4, 5\}$	3:3
	1	$G_2^i(8) : i \in \{4, 5\}$	G_1	3:2			
Four-qubit cluster state and Ω state	1	G_2	$g_i : i \in \{1, 2, 3\}$	4:1	2	G_2	4:4
	1	G_2	G_1	4:2			
	2	G_2	$G_2^i(8) : i \in \{1, \ldots, 6\}$	4:3			
Five-qubit Brown state	1	$G_2^i(8) : i \in \{1, 2, 4, 5, 7, 8\}$	$g_i : i \in \{1, 2, 3\}$	5:1	3	$G_2^i(8) : i \in \{1, 2, 4, 5, 7, 8\}$	5:5
	1	$G_2^i(8) : i \in \{1, 2, 4, 5, 7, 8\}$	G_1	5:2			
	2	$G_2^i(8) : i \in \{1, 2, 4, 5, 7, 8\}$	$G_2^i(8) : i \in \{1, \ldots, 6\}$	5:3			
	2	$G_2^i(8) : i \in \{1, 2, 4, 5, 7, 8\}$	G_2	5:4			

Asymmetric quantum dialogue in noisy environment, A. Banerjee, C. Shukla, K. Thapliyal, A. Pathak, P. K. Panigrahi, Quantum Inf. Process. 14, 2599-2616 (2016)

Quantum Conference: Another member in the family of two-way quantum communication

Two novel multiparty quantum communication schemes where prior generation of key is not required are proposed. However, these schemes naturally reduce to the schemes for multiparty key distribution if the parties send random bits instead of meaningful messages.



Quantum Inf Process (2018) 17:161
https://doi.org/10.1007/s11128-018-1931-9

Quantum conference

Anindita Banerjee[1] · Kishore Thapliyal[2] ·
Chitra Shukla[3,4] · Anirban Pathak[2]

Received: 22 August 2017 / Accepted: 10 May 2018
© Springer Science+Business Media, LLC, part of Springer Nature 2018

Scheme A: multiparty QSDC-type scheme

This scheme can be viewed as the generalization of ping-pong protocol to a multiparty scenario, where multiple senders can simultaneously send their information to a receiver. In a similar way, if all the senderswish to send and receive the same amount of information, then all of them can also choose to prepare their initial state $|\psi\rangle$ independently and send it to all other parties in a sequential manner. Subsequently, all of them may follow the scheme described below to perform N simultaneous multiparty QSDC protocols. Let us consider a case, where $(N-1)$ parties send their message to N th

party. This can be thought of as a multiparty QSDC. Suppose all the parties decide to encode or communicate k-bit classical messages. In this case, each user would require a subgroup of operators to encode his message with at least 2^k operators. In other words, each party would need at least a subgroup gi of order 2^k of a group G. Here, we would like to propose one such multiparty QSDC scheme.

A. Banerjee, K. Thapliyal, C. Shukla, **A. Pathak,** Quant. Infor. Process. 17, 161 (2018).

- **Step 1** First party Alice be given one subgroup $g_{\mathrm{A}} = \{A_1, A_2, . . . , A_{2k} \}$ to encode her k- bit information. Similarly, other parties (say Bob and Charlie) can encode using subgroups $g_{\mathrm{B}} =\{ B_1, B_2, . . . , B_{2k}\}$, and $g_{\mathrm{C}} = \{C_1,C_2, . . . ,C_{2k}\}$, and so on for $(N - 1)$th party Diana, whose encoding operations are $g_D =\{ D_1, D_2, . . . , D_{2k} \}$.

- **Step 2** Nathan (the Nth party) prepares an n-qubit entangled state $|\psi\rangle$ (with $n \geq (N - 1)\ k$).It is noteworthy that maximum information that can be encoded on the $(N - 1)\ k$-qubit quantum channel is $(N - 1)\ k$ bits and here $(N - 1)$ parties are sending k bits each. In other words, after encoding operation of all the $(N - 1)$ parties, the quantum states should be one of the $2(N-1)k$ possible orthogonal states.

A. Banerjee, K. Thapliyal, C. Shukla, **A. Pathak,** Quant. Infor. Process. 17, 161 (2018).

- **Step 3** Nathan sends m qubits ($m < n$) of the entangled state $|\psi\rangle$ to Alice in a secure manner,2 who applies one of the operations A_i (which is an element of the subgroup of operators available with her) on the travel qubits to encode her message. This will transform the initial state to $|\psi_A\rangle = Ai|\psi\rangle$. Subsequently, Alice sends all these encoded qubits to the next user Bob.
- **Step 4** Bob encodes his message which will transform the quantum state to $|\psi_B\rangle = BjAi|\psi\rangle$ Finally, he also sends the encoded qubits to Charlie in a secure manner.
- **Step 5** Charlie would follow the same strategy as followed by Alice and Bob. In the end, Diana receives all the encoded travel qubits, and she also performs the operation corresponding to her message to transform the state into $|\psi_{i,j,k,\ldots l}\rangle = Dl \ldots Ck, Bj, Ai|\psi\rangle$ She returns all the travel qubits to Nathan.

A. Banerjee, K. Thapliyal, C. Shukla, **A. Pathak,** Quant. Infor. Process. 17, 161 (2018).

- **Step 5.6** Nathan can extract the information sent by all $(N-1)$ parties by measuring the final state using an appropriate basis set. It may be noted that Nathan can decode messages sent by all $(N-1)$ parties, if and only if the set of all the encoding operations gives orthogonal states after their application on the quantum state, i.e., $\{|\psi'_{i,j,k,\ldots l}\rangle\}$ are orthogonal for all $\{i, j, k, \ldots, l \in 1, . . . 2^{k}\}$. In other words, after the encoding operation of all the $(N-1)$ parties the quantum states should be a part of a basis set with $2^{(N-1)k}$orthogonal states for unique decoding of all possible encoding operations.

A. Banerjee, K. Thapliyal, C. Shukla, **A. Pathak,** Quant. Infor. Process. 17, 161 (2018).

Scheme B: multiparty QD-type scheme

- The scheme which will be followed by a prescription to obtain the set of operations for *N*th party, assuming a working scheme designed for the multiparty QSDC scheme. This scheme is a generalized QD scheme. In analogy of the Ba-An-type QD scheme, we will need the set of encoding operations for the *N*th party (Nathan).

A. Banerjee, K. Thapliyal, C. Shukla, **A. Pathak,** Quant. Infor. Process. 17, 161 (2018).

- **Step 1** Same as that of Step 1 of Scheme A with a simple modification that provides Nathan a subgroup $g_N = \{N_1, N_2, . . . , N_{2k}\}$, which enables him to encode a k-bit message at a later stage. The mathematical structure of this subgroup will be discussed after the implementation procedure.
- **Step 2** Same as Step 2 of Scheme A.
- **Step 3** Same as Step 3 of Scheme A.
- **Step 4** Same as Step 4 of Scheme A.
- **Step 5** Same as Step 5 of Scheme A.
- **Step 6** Nathan applies unitary operation Nm to encode his secret and the resulting state would be $|\psi''_{i,j,k\ldots l,m}\rangle = Nm, Dl \ldots Ck, Bj, Ai|\psi\rangle$.

A. Banerjee, K. Thapliyal, C. Shukla, **A. Pathak,** Quant. Infor. Process. 17, 161 (2018).

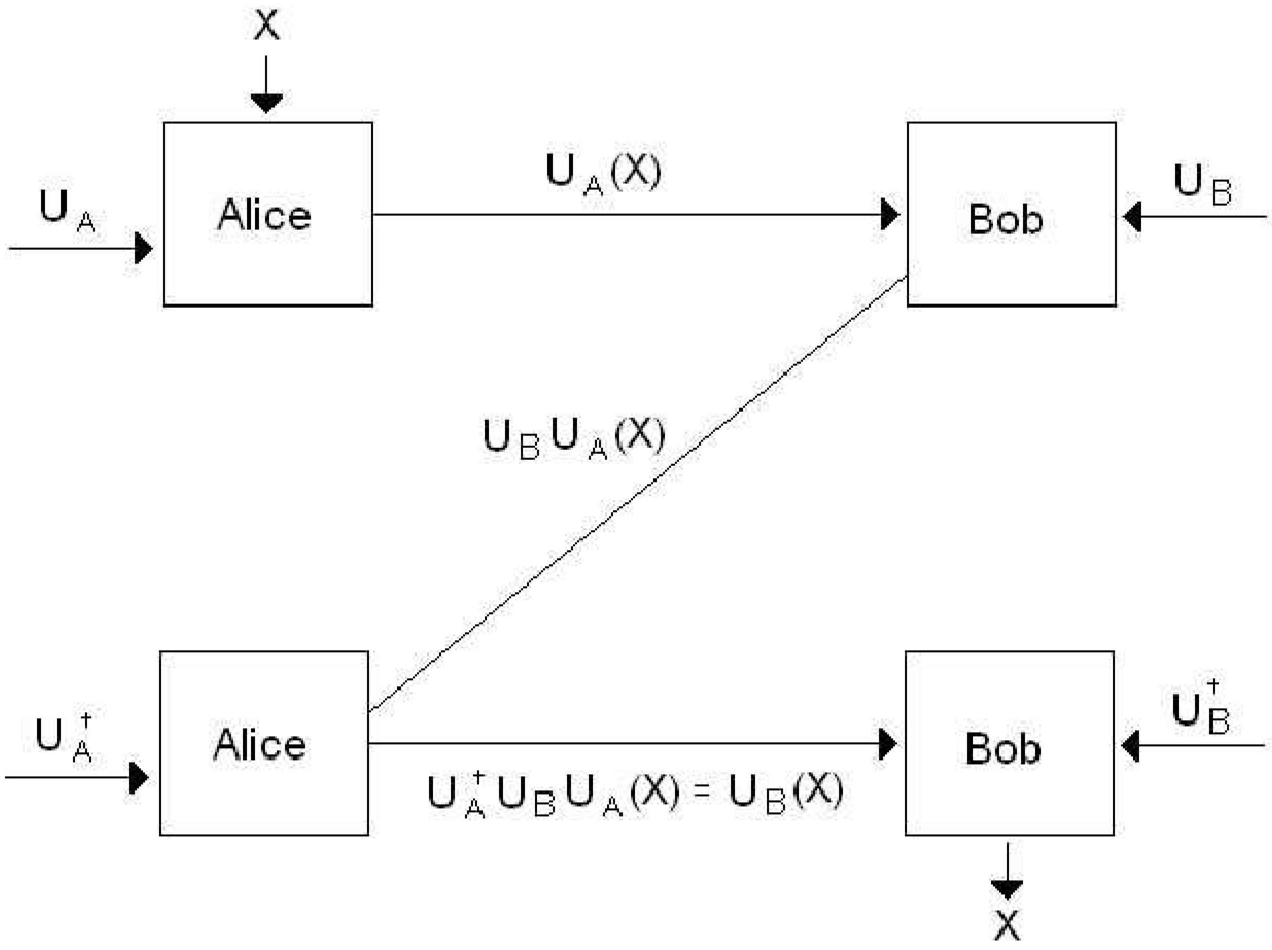
- **Step 7** Nathan measures $|\psi''_{i,j,k,..l,m}\rangle$ using the appropriate basis as was done in Step 1.6 of Scheme A and announces the measurement outcome. Now, with the information of the initial state, final state and one's own encoding, all parties can extract the information of all other parties. It is to be noted that the information can be extracted only if the set of all the encoding operations gives orthogonal states after their application on the quantum state, i.e., all the elements of $\{|\psi''_{i,j,k,..l,m}\rangle\}$ are required to be mutually orthogonal for $i,j,k,..l,m \in \{1,\ldots.2^{k}\}$. In other words, after the encoding operation of all the N parties the set of all possible quantum states should form a $2^{(N-1)k}$ dimensional basis set.

A. Banerjee, K. Thapliyal, C. Shukla, **A. Pathak,** Quant. Infor. Process. 17, 161 (2018).

Is QD of Ba An type (and its variants) is (are) unconditionally secure in its original form

- No there is a problem of information leakage!

Kak’s protocol and Noise



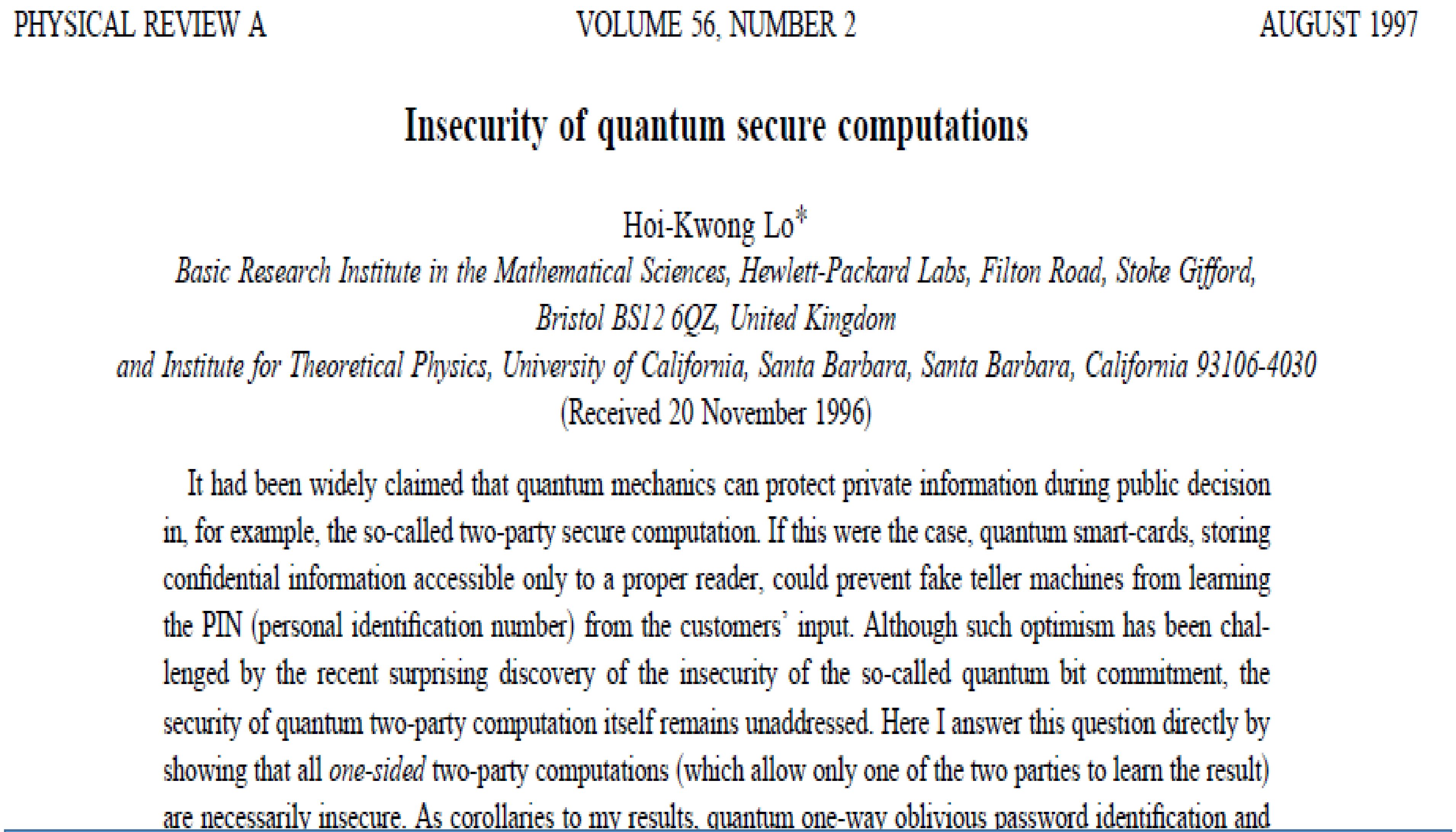
The rotation operator (*U_i*) do not commute with Kraus operators in general. Thus, three stage scheme fails in noise.

S. Kak, *Foundations of Physics Letters* 19.3 (2006) 293-296.
K. Thapliyal and A. Pathak, Quantum Inf. Process. 17 (2018) 229.

Quantum Computation Vs Communication

- Quantum computation: We compute a function *f(x,y,z,…)* for various values of the variables *x, y, z,…* (Recall: What is done in Deutsch, DJ and Grover algorithm) using quantum resources.
- Note: Every gate and circuit computes a function, which maps an input state to an output state according to a rule.
- Communication: Involves transmission of the state, but may include computation of functions, too (cf. application of Pauli gates in teleportation or dense coding or in DLL protocol and RSA Scheme based on complexity of computation).
- Not to infer much from statements like- "Quantum communication is ready for use, but quantum computing is far away.

The paper that first claimed that quantum cryptography is not omnipotent



PHYSICAL REVIEW A VOLUME 56, NUMBER 2 AUGUST 1997

Insecurity of quantum secure computations

Hoi-Kwong Lo*

Basic Research Institute in the Mathematical Sciences, Hewlett-Packard Labs, Filton Road, Stoke Gifford,
Bristol BS12 6QZ, United Kingdom
and Institute for Theoretical Physics, University of California, Santa Barbara, Santa Barbara, California 93106-4030

(Received 20 November 1996)

It had been widely claimed that quantum mechanics can protect private information during public decision in, for example, the so-called two-party secure computation. If this were the case, quantum smart-cards, storing confidential information accessible only to a proper reader, could prevent fake teller machines from learning the PIN (personal identification number) from the customers' input. Although such optimism has been challenged by the recent surprising discovery of the insecurity of the so-called quantum bit commitment, the security of quantum two-party computation itself remains unaddressed. Here I answer this question directly by showing that all *one-sided* two-party computations (which allow only one of the two parties to learn the result) are necessarily insecure. As corollaries to my results, quantum one-way oblivious password identification and

Boundary between computation and communication is very weak.

What is one-sided two-party computation?

- Alice and Bob have secret inputs

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

  $$f(i,j) \in (1,2,\cdots,p)$$

  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).

Lo’s results and arguments 1

- Three conditions for security- (a), (b), and (c) are incompatible in the sense that if (a) and (b) are satisfied, then a cheating strategy can be designed that would allow Bob to learn the values of *f* (*i*, *j*) for *all j*’s, thus violating security requirement (c).

Lo’s work and subsequent works implied impossibility of 2 party secure computation, but did not tell much about secure multi-party computation (SMC)

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*

- 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*

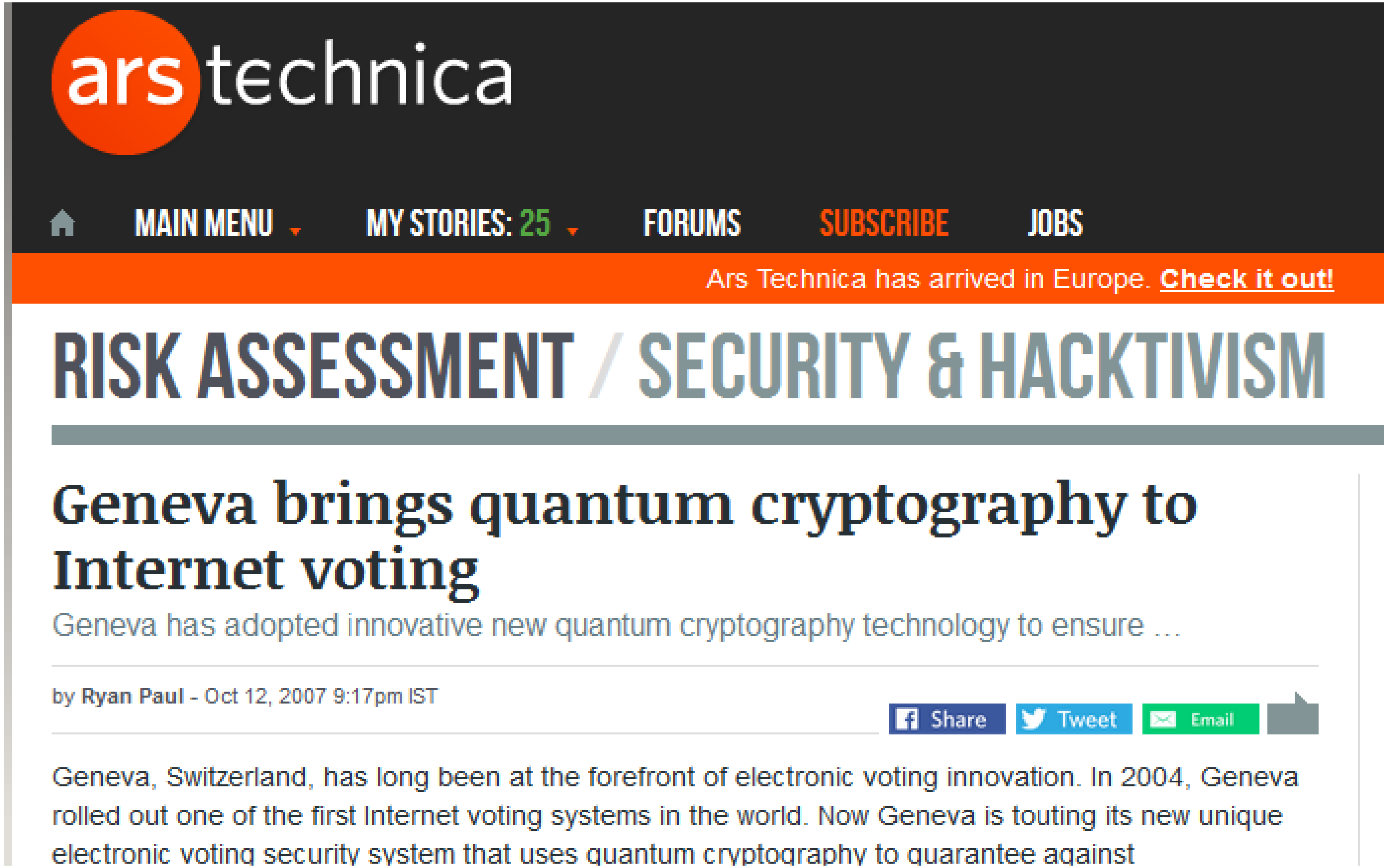
A more general case of two-party secure computation is SMC.

The notion of secure multiparty computation (SMC)

- One of the most important branches of classical and quantum cryptography is SMC.
- SMC is a primitive for distributed computation. It enables the distributed computing of correct output of a function in a situation, where the inputs are given by a group of mutually distrustful users.
- A SMC is required to be fair, and secure. Specifically, it should not leak the secret inputs of the individual players.
- In all the existing protocols of SMC, it is assumed that some of the users follow the protocol honestly (which implies that some of the users are ***semi-honest***).

A. C. Yao, In Foundations of Computer Science. SFCS'08. 23rd IEEE Annual Symposium 160 (1982).

Id Quantique's 2007 success story



Ars Technica has arrived in Europe. **Check it out!**

RISK ASSESSMENT / SECURITY & HACKTIVISM

Geneva brings quantum cryptography to Internet voting

Geneva has adopted innovative new quantum cryptography technology to ensure …

by **Ryan Paul** - Oct 12, 2007 9:17pm IST

Geneva, Switzerland, has long been at the forefront of electronic voting innovation. In 2004, Geneva rolled out one of the first Internet voting systems in the world. Now Geneva is touting its new unique electronic voting security system that uses quantum cryptography to guarantee against

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 $N=3, |\psi_0\rangle = \frac{1}{\sqrt{3}}\left(|00\rangle + |11\rangle + |22\rangle\right)$

Step 2: Charlie keeps one of the qunits (say the second one) and sends the first one to the first voter (say Alice$_1$), 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.

M. Hillery, et al. *Physics Letters A* 349.1-4 (2006): 75-81.

Hillery's (HZBB06) protocol

Step 3: After registering her vote Alice$_1$ sends the qunit to Alice$_2$ who registers her vote by using the same encoding strategy as was adopted by Alice$_1$, and sends the qunit to Alice$_3$, and the process continues until Alice$_N$ casts her vote. Finally, Alice$_N$ sends the qunit to Charlie.

Step 4: Charlie measures her qunits in computational basis to obtain a quantum state $|j+s\rangle\langle j|$ from where he easily obtains the number of "yes" votes *s*. If *s*>*N/2*, then the "yes" option wins and if *s*<*N/2*, then the "no" option wins.

Limitations of HZBB06 protocol and possible ways to circumvent them

Limitation 1 (collusion of voters reveals the voting pattern): If two voters (Alice$_i$ and Alice$_j$) collude, then they can find out how many "yes" votes have been casted by the voters who casted their votes between them. Specifically, Alice$_i$ can measure the qunit available with her to obtain the state of the ballot as a quantum state $|k\rangle$ and subsequently, Alice$_j$ can measure the quantum state again and by comparing their results, easily obtain the number of "yes" votes casted by the voters who voted between them.

Note: This drawback was mentioned in the original HZBB06 paper.

Hillery et al., (Phys. Lett. A 349, 75-81 (2006)) claimed: This collusion attack would lead to a random result of the voting as the measurement of Alice$_i$ would destroy the entanglement and the state of Charlie's qunit would randomly collapse to one of the state $|j\rangle$ completely unknown to colluding voters.

Limitation 2 of HZBB06 protocol

Collusion of voters controlling the final outcome of the voting: If two voters Alice$_i$ and Alice$_j$ such that $j-i \geq \frac{N}{2}$ collude, then they can control the final result. As in the previous colluding attack, Alice$_i$ measures her qunit first and informs the result *|m+l>* Alice$_j$ via secure channel. Now, if the colluding parties wish option "no" ("yes") to win then Alice$_j$ would replace the qunit received by her by *|m+l>|m+l+j-i>).* As $l \leq i \leq \frac{N}{2},$ we must have $j-i \geq \frac{N}{2},$ above replacement strategy ensures that the option favoured by the colluding voters Alice$_i$ and Alice$_j$ such that $j-i \geq \frac{N}{2}$ would always win.

Most recent protocol of quantum voting: TZL protocol (Tian, J.-H., Zhang, J.-H., Li, Y.-P.: A Voting Protocol Based on the Controlled Quantum Operation Teleportation. Int. J. Theor. Phys. 57.10 (2018): 3200-3206.

- Underlying assumptions: There exists zero knowledge quantum authentication method for quantum ID cards, etc.

Kishore Thapliyal, Rishi Dutt Sharma, and Anirban Pathak. *International Journal of Quantum Information* 15.01 (2017): 1750007.

Expected properties of a binary voting scheme

Security:

1. The vote value remains secret until the tally is made,
2. Votes are receipt-free,
3. Voters are anonymous.

Assumptions: Let's make the following assumptions about quantum voting:

1. Anonymity (who made the vote) and secrecy (of the value of the vote) is ensured using nonlocal resources (entanglement).

2. Only the tally person has access to the whole quantum system at the beginning and at the end of the voting.

3. The number of binary votes per voter is restricted by the use of a local subsystem to record the vote that has a state-space dimension of 2. (A binary vote represents a voter choosing 1 or 0.)

4. The tally is the number of 1 votes.

No-go theorem for a binary voting scheme

- **Task in hand:** Given the above definition of security and assumptions, it is impossible to ensure the security of quantum voting by purely physical means. In other words there is an incompatibility between the security and the assumptions.
- In order to accommodate Assumptions 1 and 2 let the quantum voting system be a distributed system where each voter has access to one unique part, and let the tally person have access to the whole system only after all votes have been cast.
- **Let the whole quantum voting system after the nth vote be represented by the pure state *|ψ(n)>.* To analyze the action of one particular voter, divide the whole system into two parts where one is the local subsystem *X* of that voter and the other is the remainder *R* of the voting system (comprising the subsystems of all other voters). We can repeat this subdivision for each voter *(i)* independently.**

No-go theorem for a binary voting scheme

- Let the Schmidt decomposition for this bipartite system be

$$|\psi(n)\rangle = \sum_i c_i(n)|R_i(n)\rangle|X_i(n)\rangle.$$

- Here $c_i(n)$ are the (non-negative real) Schmidt coefficients and $\{|X_i(n)> \ : \ i \in N\}$ and $\mathbf{\{|R_i(n)> \ : \ i \in N\}}$ represent orthonormal sets of states for the local subsystem X and the remainder R of the voting system, respectively.

- Consider the set of states throughout the voting process:

$$\{|\psi(n)\rangle : n = 1,2,3\ldots\}$$

- If the nth voter votes 1, the tally must increase and so *|ψ(n)>* must be orthogonal to *|ψ(n-1)>* in order that the vote value be determined unambiguously. However, if the nth voter votes 0, the tally does not change and so *|ψ(n)>* could be collinear with *|ψ(n-1)>.*

No-go theorem for a binary voting scheme

- Let Q be the local unitary operation (operating on a 2 dimensional space) performed by the nth voter on his/her local subsystem X to record a 1 vote.
- Assume that a 0 vote is recorded by applying the identity operator.
- **When nth voter votes 1:**

$$|\psi(n)\rangle = (I \otimes Q)|\psi(n-1)\rangle = \sum_i c_i(n-1)|R_i(n-1)\rangle|X_i(n-1)\rangle.$$

- **When nth voter votes 0:**

$$|\psi(n-1)\rangle = \sum_i c_i(n-1)|R_i(n-1)\rangle|X_i(n-1)\rangle.$$

- Suppose each voter is assigned a 2 dimensional subsystem.
- Orthonormality ensures

$$\langle\psi(n-1)|\psi(n)\rangle = 0 = c_0^2\langle X_0|Q|X_0\rangle + c_1^2\langle X_1|Q|X_1\rangle,$$

$$\langle\psi(n-1)|\psi(n-1)\rangle = 1 = c_0^2 + c_1^2.$$

No-go theorem for a binary voting scheme

- These equations are satisfied by

$$Q|X_0\rangle = c_1^2|X_0\rangle + \sqrt{1-c_1^4}\,|X_1\rangle \quad \text{and} \quad Q|X_1\rangle = -c_0^2|X_1\rangle + \sqrt{1-c_0^4}\,|X_0\rangle.$$

- The task of the tally person is to determine the number of times the operator *Q* has been applied in the final state.

- If there are *N* voters and m votes of 1 in total, then the dimension of **the subspace needed to contain *{|ψ(n)> : n = 1; 2; …N}* is *m + 1* (the extra dimension is for the initial state *|ψ(0)>).* The actual state space has a dimension of *2^N^*, being the tensor product of *N* 2-dimensional state spaces.** The task of tallying the votes is determining the value of *m*. It is convenient to label the final state *|ψ(N)>* after the last voter has voted in terms of the number of 1 votes it has. There are $^{N}C_{m}$ ways in which the *N* voters can cast m votes of 1. These represent the redundancy in a count of m votes (and provide anonymity of the voter). Let *|ψ(N,m,k)>* be the *k*th way in which *N* voters have cast *m* votes of 1.

No-go theorem for a binary voting scheme

- We can construct an Hermitian tally operator T of the following form

$$T = \sum_{m=0}^{N} m\Pi_m,$$

where Π_m is a $^N C_m$-rank projection operator that projects onto the subspace *{|ψ(N,m,k)>:k=1,2,…, $^N C_m$}*

$$\Pi_m = \sum_{k=1}^{^N C_m} |\psi(N,m,k)\rangle\langle\psi(N,m,k)|.$$

- The expectation value for the final voting state *|ψ(N,m,k)>* is

$$\langle T\rangle = \langle\psi(N,m,k)|T|\psi(N,m,k)\rangle = m \;\; \forall \;\; k = 1,2,\ldots{}^N C_m$$

gives the tally *m* (i.e. the number of 1 votes) without revealing the way in which the individual voters voted (represented by the value of *k*).

No-go theorem for a binary voting scheme

- The value of j and, thus the way in which all voters voted, could subsequently be found by determining the expectation value of the corresponding spy operator

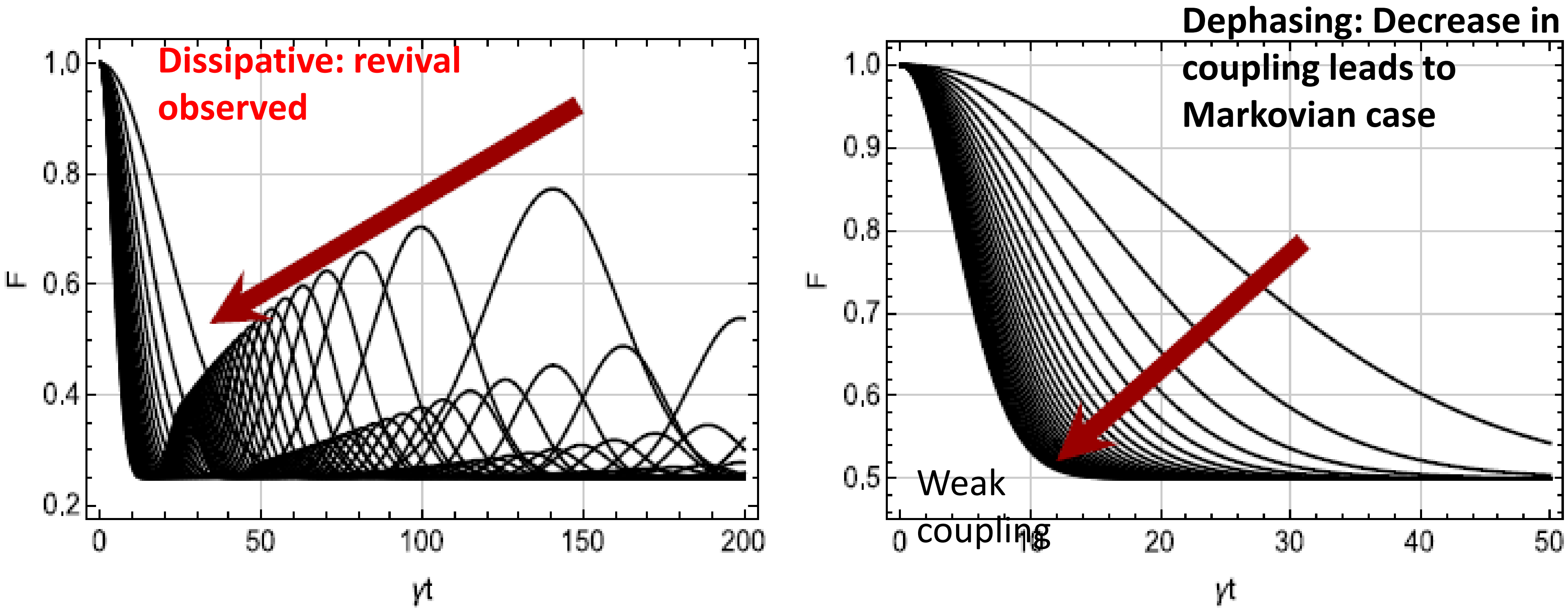
$$S_m = \sum_{k=1}^{{}^N C_m} k \left|\psi(N,m,k)\right\rangle\left\langle\psi(N,m,k)\right|.$$

- That is

$$\langle S_m \rangle = \langle \psi(N,m,k) | S_m | \psi(N,m,k) \rangle = k.$$

- Thus the way in which the voters have voted is not unconditionally secure because the voters need to trust the Tally person not to make a measurement of S_m. Hence the Assumptions are incompatible with the definition of Security.

In this formalism, only Tallyman can apply Spy operator as only he/she has access. We have obtained that allowing each voter a higher dimensional space to encode his information do not provide any advantage against Tallyman.



Dissipative: revival observed

Dephasing: Decrease in coupling leads to Markovian case

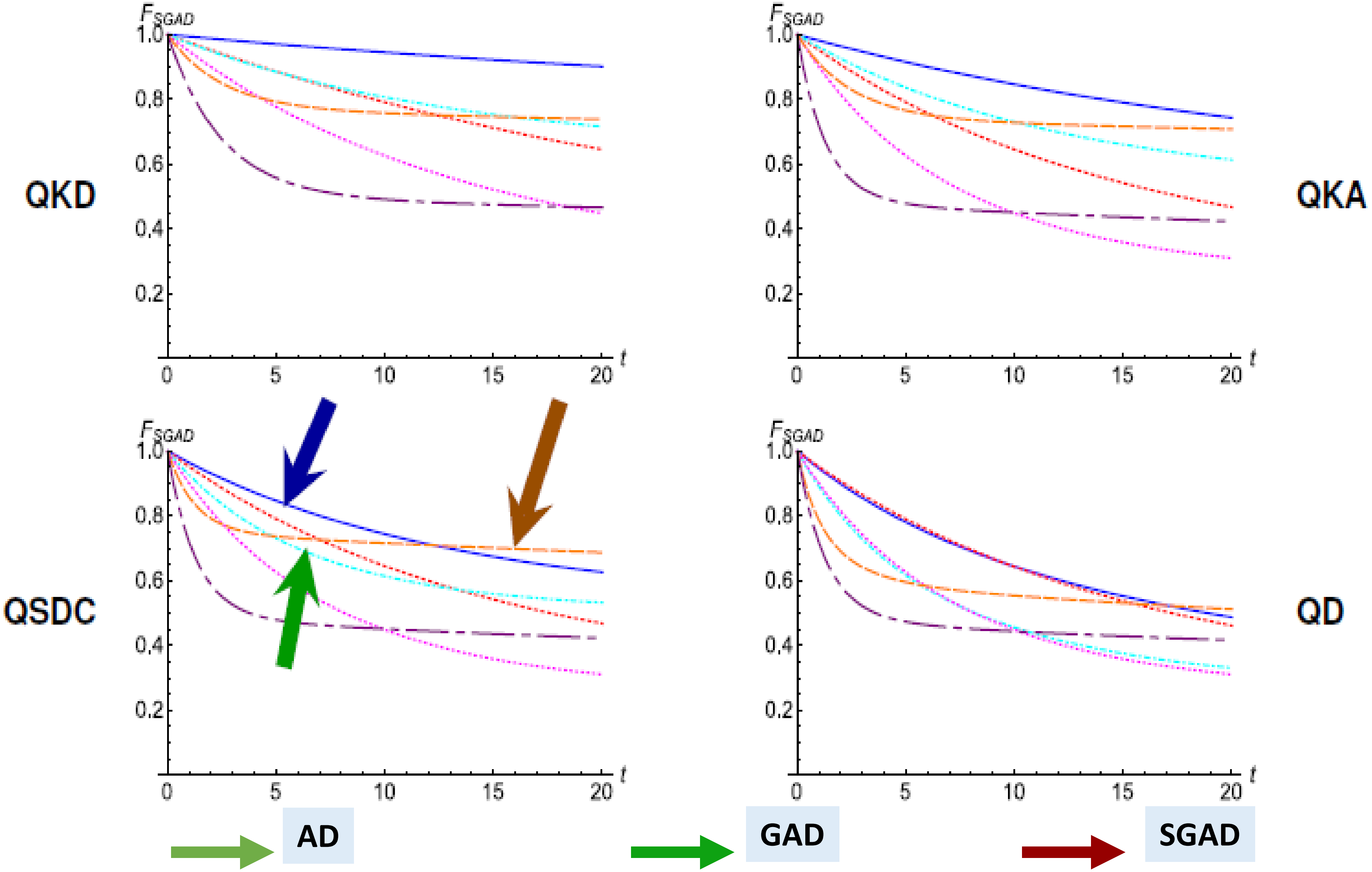
Weak coupling

(a)

(b)

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)



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

Noise is important

CHARLS BENNET TELEPORTATION
NEW DELHI
FASTEST WAY TO GO
12:03:2030 19:30 GMT
NEWYORK
PETER SHOR TELEPORTATION
NEWYORK
12:03:2030 19:35 GMT
SORRY SIR, DUE TO NOISE IN THE TELEPORTATION CHANNEL, WE COULD NOT ACHIEVE UNIT FIDELITY!

We performed proof of principle experiment using IBM and fidelity was low: QINP 16 (2017) 292; PLA 381 (2017) 3860.
QPT also show low gate fidelity arXiv:1805.07185

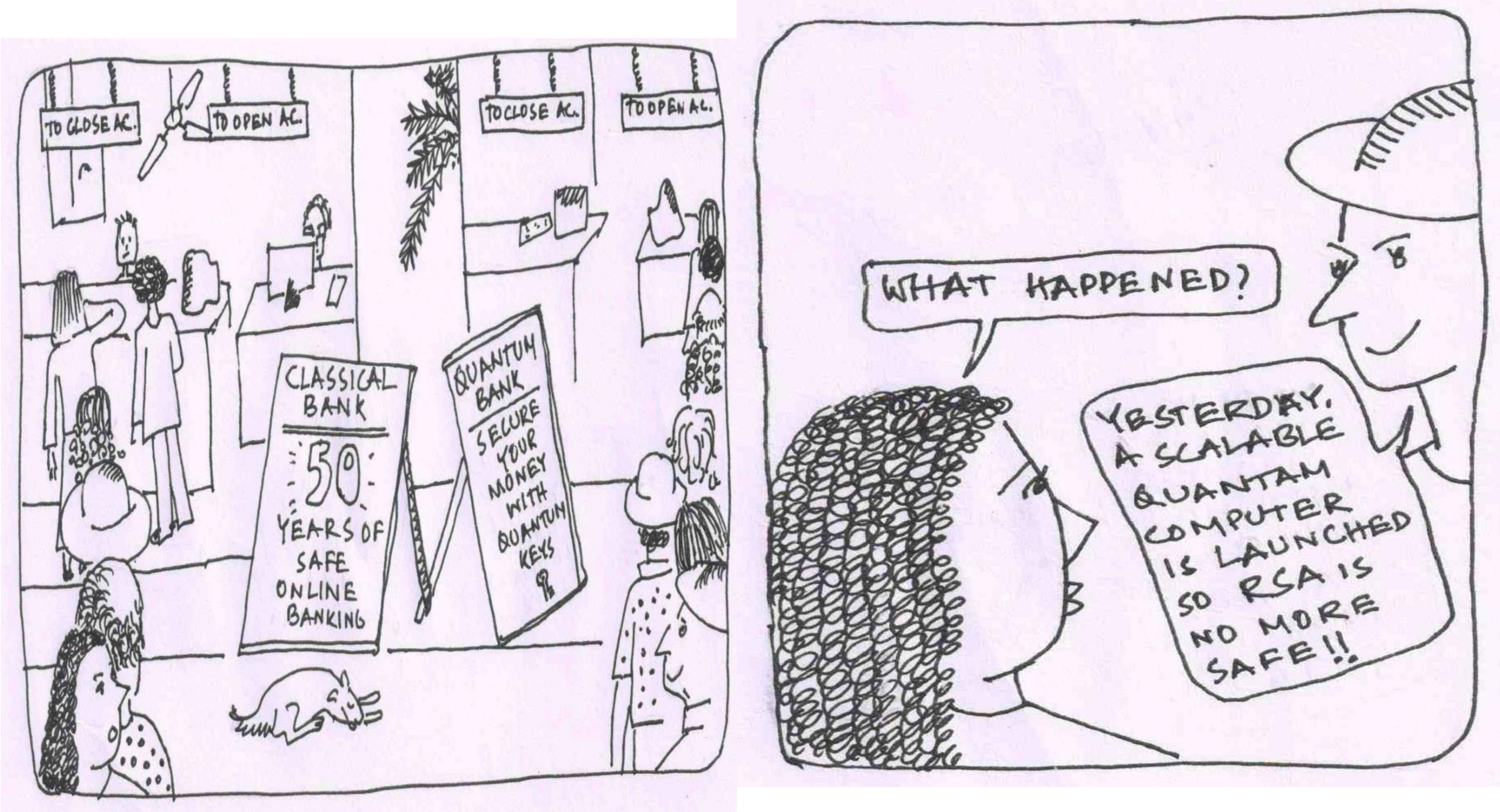
Cartoons used in this talk are from: Elements of Quantum Computation and Quantum Communication, **A Pathak**, CRC Press, Boca Raton, USA, (2013).

Decoherence the villain: Why a scalable quantum computer is not expected in near future?

HAVE YOU MADE ANY CONTRIBUTION TO QUANTUM COMPUTING?
I HAVE PROFOUND INFLUENCE ON ALL THE EXPERIMENTAL REALIZATIONS OF ALL QUANTUM COMPUTERS TILL DATE. I WAS PART OF THE ENVIRONMENT IN ALL OF THEM.
BIO DATA

Note 1: In D-wave's quantum computer (one of which is purchased by NASA and Google) all qubits cannot be addressed independently.

Note 2: You can play with IBM quantum experience and verify it.


TO CLOSE AC.
TO OPEN AC.
TO CLOSE AC.
TO OPEN AC.
CLASSICAL BANK 50 YEARS OF SAFE ONLINE BANKING
QUANTUM BANK SECURE YOUR MONEY WITH QUANTUM KEYS
WHAT HAPPENED?
YESTERDAY, A SCALABLE QUANTAM COMPUTER IS LAUNCHED SO RSA IS NO MORE SAFE!!

We are still hopeful

सत्यमेव जयते
Department of Science and Technology
Ministry of Science and Technology
Government of India

THANK YOU

Supports Received from: DRDO; SERB, DST; CSIR