Quantum Secure Communication–Theory and Practices

Arpita Maitra

IAI, TCG CREST, Kolkata
[arpita.maitra@tcgcrest.org]

1st April, 2025

Quantum Communication

Basics of Communication Technologies

- Classical communication: Transmission of bits
- Quantum Communication : Transmission of qubits

Preliminaries: Qubit

- Bit (0 or 1): basic element of a classical computer
- The quantum bit (called the qubit): the main mathematical object in the quantum paradigm (physical counterpart is a photon)

Physical support	Name	Information support	$\|0\rangle$	$\|1\rangle$
Photon	Polarization	Polarization	Horizontal	Vertical
Electrons	Electronic spin	Spin	Up	Down

Qubit and Measurement

- A qubit (quantum counterpart of 0, 1):

$$\alpha|0\rangle + \beta|1\rangle,$$

  $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$.

- Measurement in $\{|0\rangle, |1\rangle\}$ basis: we will get $|0\rangle$ with probability $|\alpha|^2$, $|1\rangle$ with probability $|\beta|^2$.
  The original state gets destroyed.

- Example:

$$\frac{1+i}{2}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle.$$

  After measurement: we will get
  $|0\rangle$ with probability $\frac{1}{2}$,
  $|1\rangle$ with probability $\frac{1}{2}$.

Information content in a Qubit

- One may theoretically pack infinite amount of information in a single qubit
- A single qubit may contain huge information compared to a bit
- It is not clear how to extract such information
- In actual implementation of quantum circuits, it might not be possible to perfectly create a qubit for any α, β
- Technology is still at early stage, lot of problems in computation, storage and communication

More on Quantum Communication (QC)

- Nicely explained in MIT Technology Review

  https://www.technologyreview.com/s/612964/what-is-quantum-communications/

- It is more related to secure communication than usual communication.

- "Quantum communication takes advantage of the laws of quantum physics to protect data. These laws allow particles typically photons of light for transmitting data along optical cables to take on a state of superposition, which means they can represent multiple combinations of 1 and 0 simultaneously. The particles are known as quantum bits, or qubits."

- "The beauty of qubits from a cyber-security perspective is that if a hacker tries to observe them in transit, their super-fragile quantum state collapses to either 1 or 0. This means a hacker can't tamper with the qubits without leaving behind a telltale sign of the activity."

Cloning: Possible in classical domain, not in quantum

Possible to copy a classical bit

Not possible for an unknown quantum bit

No cloning

- A result of quantum mechanics
- Not possible to create identical copies of an arbitrary unknown quantum state
- It was stated by Wootters, Zurek, and Dieks in 1982
- W. K. Wootters and W. H. Zurek. A Single Quantum Cannot be Cloned, Nature 299 (1982), pp. 802–803.
- D. Dieks. Communication by EPR devices, Physics Letters A, vol. 92(6) (1982), pp. 271–272.
- Huge implications in quantum computing, quantum information, quantum cryptography and related fields.

No cloning (contd.)

- Consider a quantum slot machine with two slots labeled A and B
- A is the data slot set in a pure unknown quantum state $|\psi\rangle$ whereas B is target slot set in a pure state $|s\rangle$ where A will be copied
- It is not possible to copy an unknown Quantum state $|\psi\rangle$

No Cloning (contd.)

- The advantages are in the domain of quantum cryptography, where by the laws of physics copying an unknown qubit is not possible
- However, in terms of copying or saving unknown quantum data, this is actually a problem
- Clarification: given a known quantum state, it is always possible to copy it; this is because, for a known quantum state, we know how to create it deterministically and thus it is possible to reproduce it with the same circuit

Orthogonal quantum states: distinguishable

Possible to distinguish two orthogonal states only

- Given two orthogonal states $\{|\psi\rangle, |\psi_\perp\rangle\}$, it is possible to distinguish them with certainty.

- For example,

$$\{|0\rangle, |1\rangle\};$$

$$\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$$

$$\{\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\}$$

Distinguishability of Nonorthogonal quantum states

Not possible to distinguish two nonorthogonal quantum states with certainty

- Given two nonorthogonal states $\{|\psi_0\rangle, |\psi_1\rangle\}$, it is not possible to distinguish them with probability 1.

- Example: it is given that the two states are $|0\rangle$, $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, two nonorthogonal states. Then it is not possible to exactly identify each one.

Benefits of QC over traditional communication methodologies

- Speed & Security
- "Entanglement makes it possible to communicate instantly across arbitrarily large distances in principle" – not that simple, we need quantum repeater
- Possible to "transmit highly sensitive data based on a process called quantum key distribution, or QKD. In theory, at least, these networks are ultra-secure" – needs more careful study for actual implementation

Basic Idea of QKD Protocol

- To transmit 0 or 1 securely.
- Choose some basis:

$$\{|0\rangle, |1\rangle\};$$

$$\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$$

$$\{\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\}$$

- Take any basis. Encode 0 to one qubit and 1 to another qubit.
- If we use only a single basis, then anybody can measure in that basis, get the information and reproduce.
- Thus Alice needs to encode randomly with more than one bases.
- Bob will also measure in random basis.
- Basis will match in a proportion of cases and from that key will be prepared.

An Example: BB84 QKD

$+$: $\{\uparrow = |0\rangle, \rightarrow = |1\rangle\}$, i.e., Z basis

$\times$: $\{\nearrow = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \nwarrow = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$, i.e., X basis

a	0	1	1	0	1	0	0	1
b	0	0	1	0	1	1	1	0
Basis	$+$	$+$	$\times$	$+$	$\times$	$\times$	$\times$	$+$
Polarization	$\uparrow$	$\rightarrow$	$\nwarrow$	$\uparrow$	$\nwarrow$	$\nearrow$	$\nearrow$	$\rightarrow$
Bob's Basis	$+$	$\times$	$\times$	$\times$	$+$	$\times$	$+$	$+$
Bob's measurement	$\uparrow$	$\nearrow$	$\nwarrow$	$\nearrow$	$\rightarrow$	$\nearrow$	$\rightarrow$	$\rightarrow$
Public Discussion	M		M			M		M
Shared Key	0		1			0		1

Security

- The protocol is provably secure (Theoretically).
- Based on no cloning theorem.
- The proof comes from the quantum property that information gain is only possible at the expense of disturbing the signal.
- If the two states we are trying to distinguish are not orthogonal, it is not possible to distinguish them with certainty.
- The protocol is a method of securely communicating a private key from Alice to Bob.

QKD Commercial Products

A partial list:

- Quantum Key Distribution Equipment Provider. ID Quantique (IDQ).
  `http://www.idquantique.com/`
- Quantum Key Distribution System (Q-Box) Provider. MagiQ Technologies Inc. `http://www.magiqtech.com`

QKD Security in Practice

Unconditional Security Vs,. Practical Implementation

- Theoretically, any QKD system provides unconditional security
- Even if the adversary has unbounded power of computation, still he/she can not extract the final key
- However, inherent imperfections of the devices or deviations from the security models can result potential security breach in practice
- Example: Laser damping attack, PNS attack etc.
- Like conventional cryptographic modules or network devices, QKD modules are expected to have strict security testing
- Intensive and strict evaluation is an essential step before QKD is widely accepted by our Government

What should be done?

- In this direction, the ISO/IEC [1] 23837 series defines a set of rigorous and common security specifications for QKD modules
- It is expected that the manufacturers should follow the standard procedure to design and implement IT products that use QKD
- Evaluators should also follow the standard procedure to test and evaluate the security of QKD modules, reducing the risk of being vulnerable

[1] ISO: International Organization for Standarization, IEC: International Electrotechnical Commission

QKD Classifications

- The QKD protocols can be classified into two categories based on the decoding method of quantum states:
  - DV-QKD
  - CV-QKD

DV and CV-QKD

- DV-QKD:
  - The transmitter encodes information with discrete variables such as phase, polarization or time-bin
  - To decode information, the receiver uses single-photon detectors
- CV-QKD:
  - The transmitter encodes information using conjugate variables (quadratures) of a quantized electromagnetic field in an infinite dimensional Hilbert space (eg. coherent optical states)
  - The receiver uses a coherent detection technique (eg. homodyne or heterodyne detection)

Classification by architecture

- Classification of QKD protocols by the architecture of the protocols:
  - PM-QKD,
  - MDI-QKD,
  - EM-QKD

Threats Exploiting Device Imperfections

- Optical source flaws: PNS attack, Phase Remapping attack, Wavelength-Dependent attack
- Optical detection vulnerabilities: Efficiency mismatch of two single-photon detectors in a QKD receiver modules
- Parameter adjustment vulnerabilities: Time-mismatch vulnerability between transmitter module and receiver module
- Classical post processing vulnerabilities: vulnerabilities in classical cryptographic primitives like ECC and PA

Partial list of possible attacks in QKD

Physical tampering scenarios	TSF devices/elements
Trojan horse attack	Encoder, Decoder
Laser damaging attack	Encoder, Decoder
Laser seeding attack	Encoder
Phase-remapping attack	Encoder
Pulse energy monitor attack	Encoder
Wavelength-dependent attack	Decoder
Detector blinding attack	Detector
Detector efficiency attacks	Detector
After-gate attack	Detector
Detector superlinearity attack	Detector
Dead time attack	Detector
Double-click attack	Detector
Parameter adjustment attack	QKD module
Local oscillator attack	QKD module

What to evaluate?

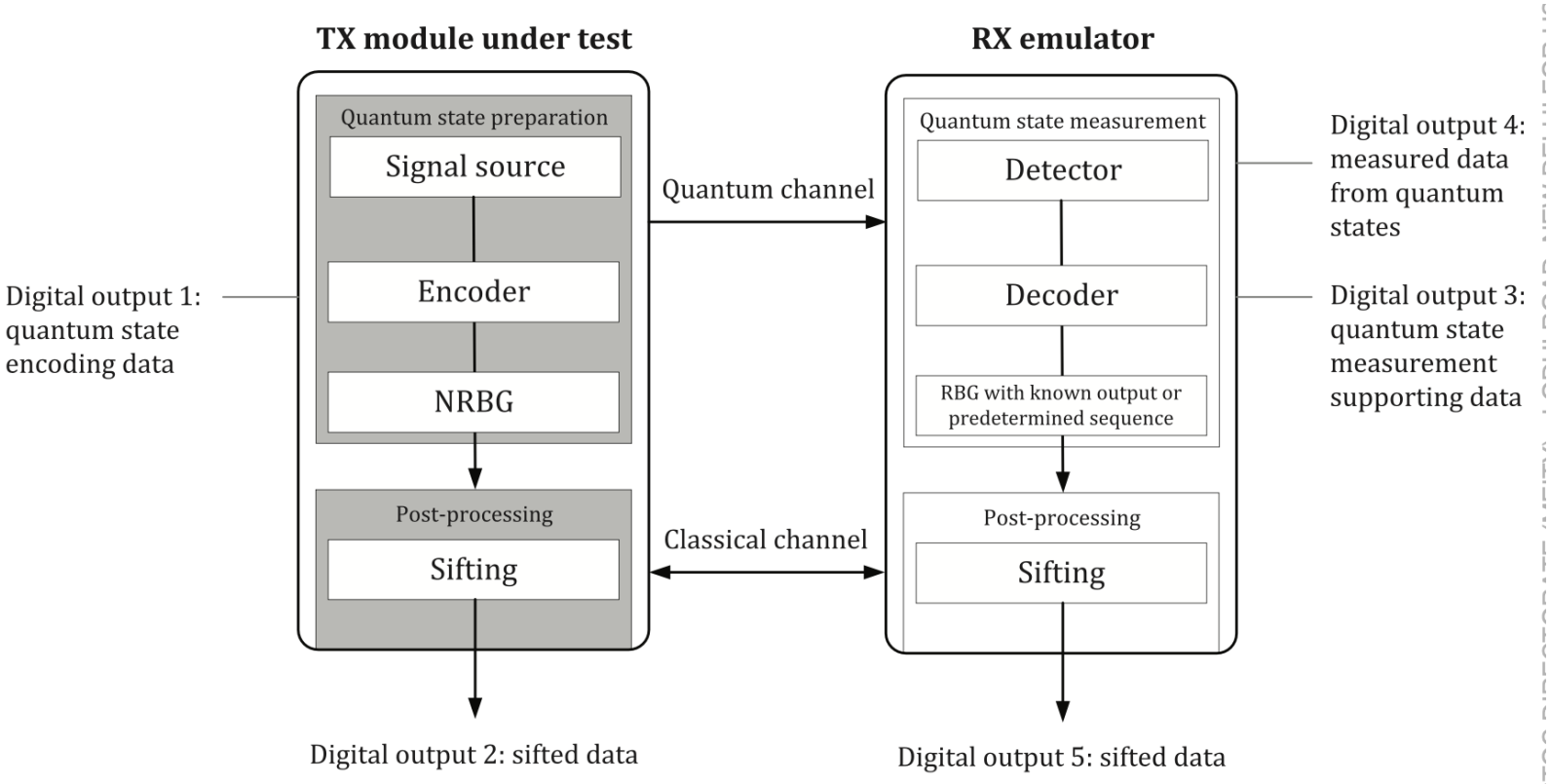
Evaluation activity	Description
Test quantum state transmission and sifting procedures	Test the correctness of functionality of the related generation of raw data between the TX module and the RX module, and the functionality of sifting of the resulting data when sifting is part of the QKD protocol.
Test other post-processing procedures	Test the correctness of the implementation of the post-processing procedures in TOE (target of evaluation), subsequent to any sifting that forms part of the QKD protocol.
Test parameter adjustment procedure(s)	Test the correctness of the implementation of the parameters in TOE.

TX stands for transmitter and RX stands for receiver.

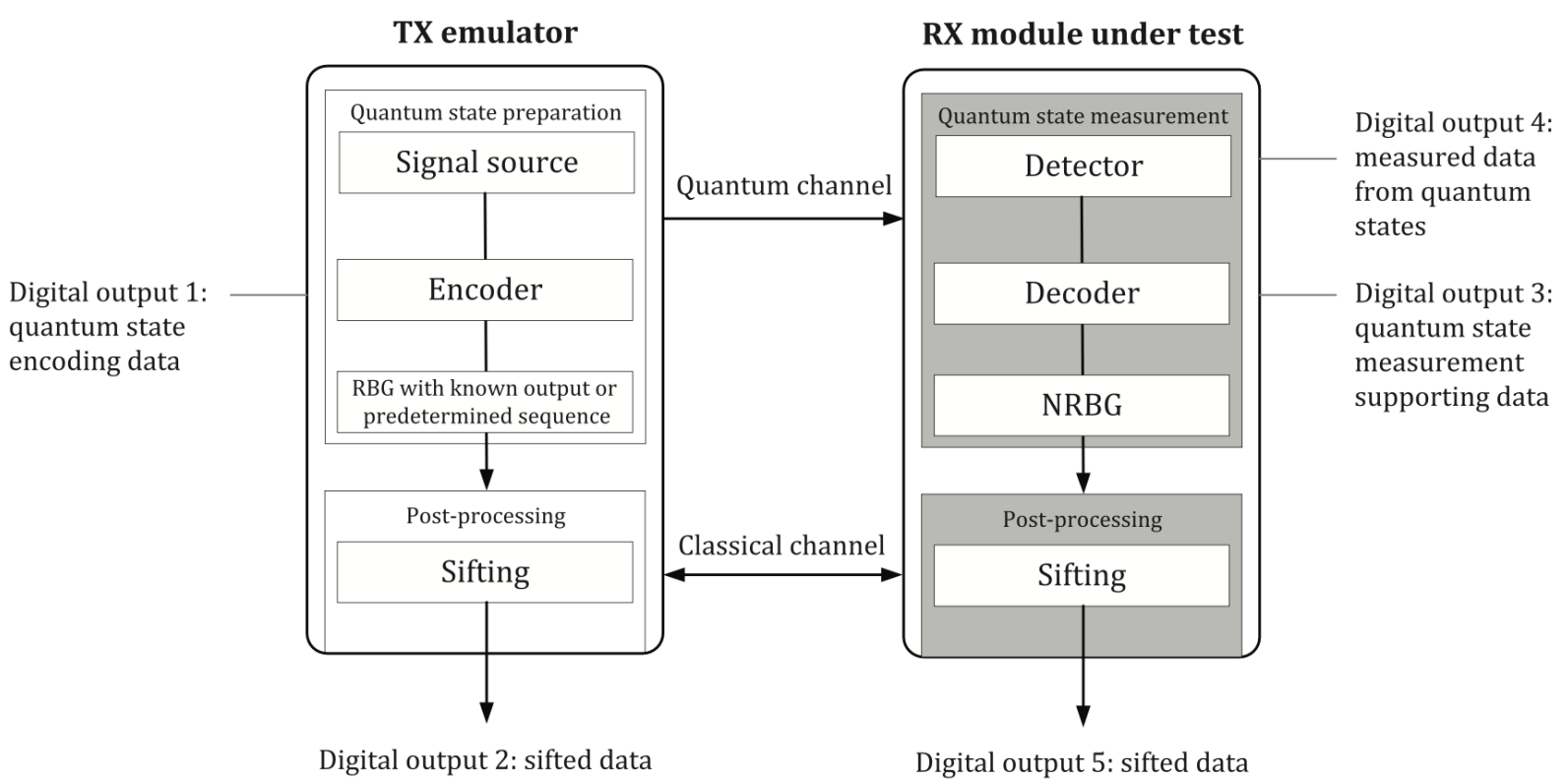
How to evaluate?

- If the module under test is a QKD transmitter, an RX emulator with known characteristics is required to be available and working well
- Similarly, if the module under test is a QKD receiver, a TX emulator with known characteristics is required to be available and working well

Setup for testing encoding and sifting functionalities of a TX module



Setup for testing quantum state measurement and sifting functionalities of an RX module



In a nutshell

- Many companies, research laboratories are claiming QKD hardware
- However, without proper evaluation it is very risky to deploy those devices in the network
- It may cause potential information leakage if not evaluated properly even if the QKD protocol has robust security proof
- We need to keep in mind that there is a non negligible gap between the theory and practical implementation
- When QKD demands the detection of the footprint of the eavesdropper if he/she tries to extract the information, there are several examples where eavesdropper can steal significant amount of information without being detected

Fynman first principle: You must not fool yourself, and you are the easiest person to fool.

QKD as a Black Box: Device Independent Security

Concept of Device Independence

- The security of any QKD protocols usually based on three main assumptions:
  - validity of Quantum Mechanics.
  - assumption of no-information leakage from the honest parties' labs.
  - fact that the honest parties have a sufficiently good knowledge of their devices.
- All the three assumptions are necessary for the security of standard protocols. For example, Alice and Bob may unknowingly use multi-photon source in BB84. It causes Photon Number Splitting (PNS) attack.
- Removing the third assumption is the additional requirement for Device Independent Security.

Device Independent Quantum Key Distribution

- A QKD protocol whose security can be proven without making any assumptions on the devices.
- These protocols, that are named Device Independent, offer a stronger form of security since they require the minimal assumptions.
- Security follows from some input-output statistics of devices, for example testing Bell inequality or CHSH inequality (John Clauser, Michael Horne, Abner Shimony, and Richard Holt)
- Clauser was awarded the 2022 Nobel Prize in Physics, jointly with Alain Aspect and Anton Zeilinger "for experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science".

CHSH game

- Two versions of the solution: Classical and Quantum.
- Alice is given an input x and Bob is given an input y.
- The rule of the game is that after receiving the input they can not communicate between themselves.
- Alice outputs a; Bob outputs b.
- They win when $a \oplus b = x \wedge y$.
- Best classical strategy: Alice outputs 0, Bob outputs 0 (Same for 1), Probability of success: 0.75.
- Quantum Strategy outperforms Classical Strategy, Probability of success: $\frac{1}{2}(1 + \frac{1}{\sqrt{2}}) = 0.853$, requires sharing of Maximally entangled states between Alice and Bob.

CHSH Game (Contd.)

- Best classical strategy: Alice outputs 0, Bob outputs 0 (Same for 1).
- Probability of success: 0.75.

(a, b)	(x, y)	$a \oplus b$	$x \wedge y$	$\Pr((a \oplus b = x \wedge y)\|(a, b))$	$\Pr((a \oplus b \neq x \wedge y)\|(a, b))$
(0, 0)	(0, 0)	0	0	$\frac{1}{4}$	0
	(0, 1)	0	0	$\frac{1}{4}$	0
	(1, 0)	0	0	$\frac{1}{4}$	0
	(1, 1)	0	1	0	$\frac{1}{4}$
(1, 1)	(0, 0)	0	0	$\frac{1}{4}$	0
	(0, 1)	0	0	$\frac{1}{4}$	0
	(1, 0)	0	0	$\frac{1}{4}$	0
	(1, 1)	0	1	0	$\frac{1}{4}$

CHSH Game (Contd.)

In quantum domain,

- Alice and Bob share a maximally entangled state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
- If $x = 0$, Alice measures her qubit in $\{0, 1\}$ basis, if $x = 1$, she measures her qubit in $\{+, -\}$ basis.
- If Alice gets $|0\rangle$ or $|+\rangle$, considers $a = 0$.
- If she gets $|1\rangle$ or $|-\rangle$, considers $a = 1$.
- If $y = 0$, Bob measures his qubit in $\{\pi/8, -\pi/8\}$ basis, if $y = 1$, he measures his qubit in $\{3\pi/8, -3\pi/8\}$, where

$$|\pi/8\rangle = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle, |-\pi/8\rangle = -\sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle,$$
$$|3\pi/8\rangle = \sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle, |-3\pi/8\rangle = -\cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle.$$

- If Bob gets $|\pi/8\rangle$ or $|3\pi/8\rangle$, considers $b = 0$.
- If Bob gets $|-\pi/8\rangle$ or $|-3\pi/8\rangle$, considers $b = 1$.

CHSH Game (Contd.)

(x, y)	(a, b)	$\Pr((a, b) \mid (x, y))$	$\Pr((a \oplus b = x \wedge y) \mid (x, y))$	$\Pr((a \oplus b \neq x \wedge y) \mid (x, y))$
$(0, 0)$	$(0, 0)$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	0
	$(0, 1)$	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$	0	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$
	$(1, 0)$	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$	0	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$
	$(1, 1)$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	0
$(0, 1)$	$(0, 0)$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	0
	$(0, 1)$	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$	0	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$
	$(1, 0)$	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$	0	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$
	$(1, 1)$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	0
$(1, 0)$	$(0, 0)$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	0
	$(0, 1)$	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$	0	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$
	$(1, 0)$	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$	0	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$
	$(1, 1)$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	0
$(1, 1)$	$(0, 0)$	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$	0	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$
	$(0, 1)$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	0
	$(1, 0)$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	0
	$(1, 1)$	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$	0	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$

$$\Pr(a \oplus b = x \wedge y) = \frac{1}{2}(1 + \frac{1}{\sqrt{2}}) = 0.853.$$

Fully Device Independent QKD

- U. Vazirani and T. Vidick, Fully device independent quantum key distribution, **Phys. Rev. Lett.**, 113, 140501, Published 29 September 2014.
- Exploiting quantum CHSH game, the authors proposed a new QKD protocol and proved its device-independent security with tolerance of a constant noise rate and guaranteed generation of a linear amount of key.

Pseudo-Telepathy Game

- Pseudo-Telepathy game is another qnauntum game which can be exploited to certify the device independence of the devices.
- This is a n players game, where $n \geq 3$.
- Each player A_i receives a single input bit x_i and is requested to produce an output bit y_i.
- The bit string $x_1 \ldots x_n$ contains even number of 1's.

Pseudo-Telepathy Game (Contd.)

- $x_1 \ldots x_n$ is the questions and $y_1 \ldots y_n$ is the answers.
- The game G_n will be won by this team of n players if

$$\sum_{i=1}^{n} y_i \equiv \frac{1}{2} \sum_{i=1}^{n} x_i (\text{mod } 2).$$

- For winning collectively, if $\text{HW}(x_1 \ldots x_n) = 0$ mod 4, (resp. 2 mod 4), then $\text{HW}(y_1 \ldots y_n)$ should be even (resp. odd).

Multi Party Pseudo Telepathy (Contd.)

- No communication is allowed among the n participants after receiving the inputs and before producing the outputs.
- It has been proved that no classical strategy for the game G_n can be successful with a probability better than $\frac{1}{2} + 2^{-\lceil n/2 \rceil}$.
- Quantum entanglement serves to eliminate the classical need to communicate and it is shown that there exists a perfect quantum protocol where the n parties will always win the game.
- Thus, the probability difference is $1 - \frac{1}{2} - 2^{-\lceil n/2 \rceil}$; increases with the number of the players.
- Stronger distinguisher than CHSH game.

Pseudo Telepathy (the set up)

- Define

$$|\Phi_n^+\rangle = \frac{1}{\sqrt{2}}|0^n\rangle + \frac{1}{\sqrt{2}}|1^n\rangle$$

and

$$|\Phi_n^-\rangle = \frac{1}{\sqrt{2}}|0^n\rangle - \frac{1}{\sqrt{2}}|1^n\rangle.$$

- H denotes Hadamard transform. S denotes the unitary transformation $S|0\rangle \mapsto |0\rangle,\ S|1\rangle \mapsto i|1\rangle$.
- If S is applied to any two qubits of $|\Phi_n^+\rangle$ leaving the other qubits undisturbed then the resulting state is $|\Phi_n^-\rangle$ and vice versa.

Pseudo Telepathy (the set up, (Contd.))

- If $|\Phi_n^+\rangle$ is distributed among n players and if exactly m of them apply S to their qubit, then the resulting global state will be $|\Phi_n^+\rangle$ if $m \equiv 0 \bmod 4$ and $|\Phi_n^-\rangle$ if $m \equiv 2 \bmod 4$.
- Note that

$$(H^{\otimes n})|\Phi_n^+\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{wt(y)\equiv 0 \bmod 2} |y\rangle$$

and

$$(H^{\otimes n})|\Phi_n^-\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{wt(y)\equiv 1 \bmod 2} |y\rangle.$$

Pseudo Telepathy (the quantum algorithm)

The players are allowed to share a prior entanglement, the state $|\Phi_n^+\rangle$.

1. If $x_i = 1$, A_i applies transformation S to his qubit; otherwise he does nothing.
2. He applies H to his qubit.
3. He measures his qubit in order to obtain y.
4. He produces y_i as his output.

The game G_n is always won by the n distributed parties without any communication among themselves.

Device Independent QKD Exploiting Pseudo-Telepathy Game

- J. Basak, **A. Maitra** and S. Maitra, Device Independent Quantum Key Distribution using Three-Party Pseudo-Telepathy, Pages 456–471, **Progress in Cryptology - INDOCRYPT 2019**, Hyderabad, India, December 15-18, 2019. Lecture Notes in Computer Science, Springer.
- In this protocol, Pseudo-Telepathy game is exploited to certify the device independence.

Challenges Associated

- Locality Loophole: The entanglement can not be generated locally, i.e., there must be sufficient distance between the boxes.
- Memory Loophole: All the rounds must be i.i.d. There should not be any memory which can store the information of the earlier events.
- Freedom of Choice: The dimension of the sub-systems must be two dimensional, i.e., qubit.
- Loophole free Bell Test or CHSH Test is still a challenge. Though in some recent papers, the loophole free Bell test has been reported[2]
- The commercial product for DIQKD is still not reported.

[2] Y. Liu, Q. Zhao, M.-H. Li, J.-Y. Guan, Y. Zhang, B. Bai,W. Zhang, W.-Z. Liu, C. Wu, X. Yuan, et al., Nature **562**, pp. 548–551, 2018.

Summary

- Quantum computer: a real threat to RSA and ECC based cryptography.
- Post Quantum Cryptography: Code based and Lattice based; believed to be hard in quantum domain.
- Alternative solution: Quantum Cryptography.
- Quantum key distribution has been proven secure.
- QKD and QRNG devices are available in the international market.
- To the best of my knowledge, no DIQKD or DIQRNG devices are available in the commercial domain because of the difficulty to achieve loophole free CHSH or Bell test.