EQUIANGULAR 3-STATE QKD

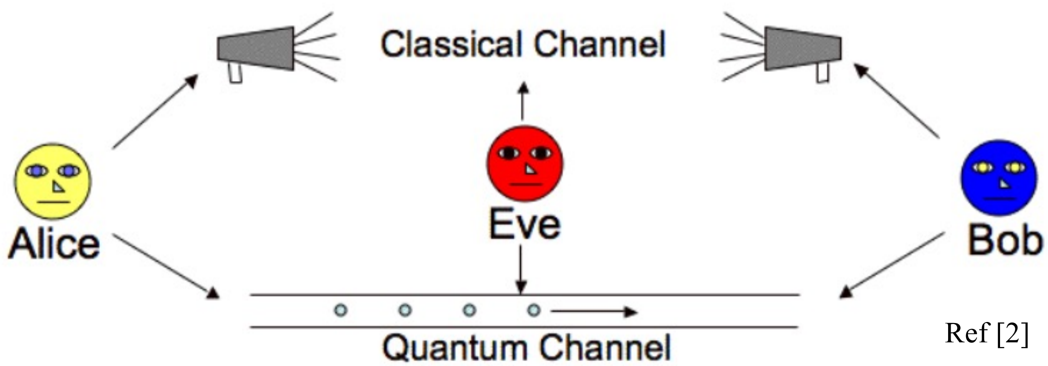
OPTI 646 Final Presentation

By Guillermo Hermoso López

Ref [1]

1. INTRODUCTION

- QKD = Quantum Key Distribution ⟶ Quantum Cryptography.
  - Goal: generate random secure key to encrypt messages.
  - Users: Alice (sender), Bob (receiver), Eve (eavesdropper).
  - Methods:
    - Classical Cryptography Method: Mathematical complexity f.e. **factorization**.
    - Quantum Cryptography: principles of quantum physics, f.e. **entanglement**.



Ref [2]

II. COMPARISON WITH CLASSICAL CHANNEL:

- Conventional public-key cryptography:
  - Long-term confidentiality threatened by **harvest and decrypt attacks**:
    - Encrypted data easily collected and stored.
    - Decrypt later when more powerful (quantum) computers are available.

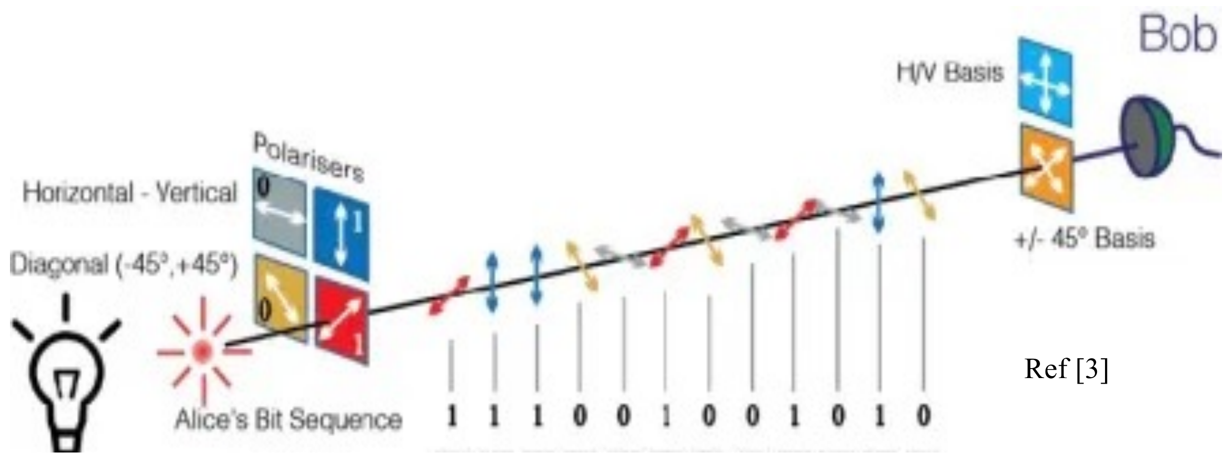
At Risk!!!

- QKD:
  - Detect eavesdropping (measurement must be done).
  - Secret digital keys secure from future advances in cryptoanalysis and computing.

III. PROTOCOL BB84 (BENNETT – BRASSARD)

- Heisenberg's Uncertainty Principle (HUP):
  - **Any 2 pair of conjugate states** can be used, f.e. **polarization** → Horizontal – Vertical basis & Diagonal basis.
  - No possible measurement distinguishes 4 different polarization states, since they are **not all orthogonal**. Measurement in one basis gives random result for bits encoded in the other basis.

- **No Cloning Theorem:** impossible to create identical copies of an arbitrary unknown quantum state.
- Eavesdropper can't measure photons and transmit them on to Bob without disturbing photon's state in a **detectable way.**
- **Random Secret Key Transmission:** bits encoded in the polarization of a string of photons.



Ref [3]

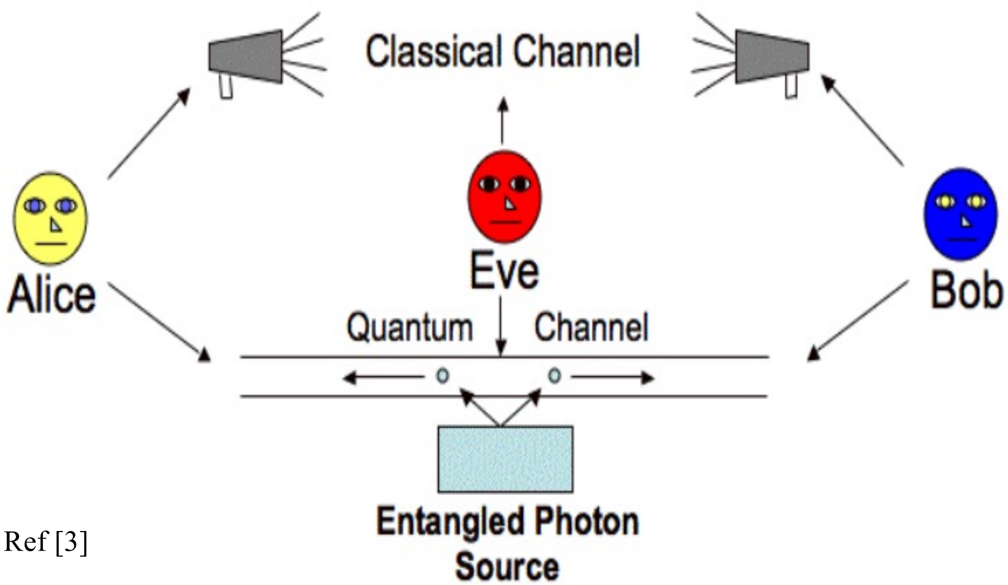
III. BB84 PROTOCOL

- Phase 1:
  - Alice → Random string of bits w/ random basis for each bit & send to Bob.
  - Bob → Random measuring basis for each bit.
- Phase 2:
  - Communication through classical (insecure) channel.
  - Measurement basis (Bob's) shared.
  - ONLY correct bits form key.
- Quantum Channel is secure if no eavesdropping detected.

Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

Ref [3]

IV. PROTOCOL E91 (ECKERT)



Ref [3]

- Single source emits pairs of perfectly correlated entangled particles (polarized photons).
  - Alice and Bob each choose a random basis.
  - Discuss bases in classical channel.
  - Bit measured with same basis: Alice & Bob get opposite results due to entanglement (**binary complements**) → One party inverts key.
- Eavesdropper detection:
  - Examine photons measured w/ different basis in a 3rd basis.
  - Test **Bell's Inequality** → should **not hold for entangled particles.**

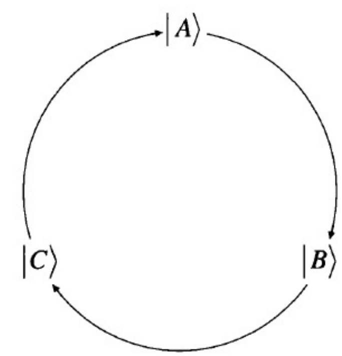
V. PROTOCOL BB92 (BENNETT – BRASSARD)

- Same principle as before but using **only 2 states**: Horizontal polarization and +45°-polarization.
- **Photon Transmission**: Alice randomly sends photons in either the H-polarization state (bit '0') or the +45°-polarization state (bit '1').
- **Bob's Measurement**:
  1. Bob randomly selects between rectilinear and diagonal bases to measure.
  2. In rectilinear basis:
     1. If incident photon is H-polarized, the outcome is H-state with 100% certainty.
     2. If incident photon is +45°-polarized, the outcome is either H-state or V-state with equal probability.
  3. In diagonal basis: Measurement outcome of -45°-state → incident polarization state of the photon is 'H'.
- **Result Announcement**:
  1. After measuring the photons, Bob announces instances where the outcome was either 'V' or '-45°', discarding the rest.
  2. These announced results form the basis for generating a random bit string between Alice and Bob.
- **Verification of Eavesdropping**:
  - For security verification, Bob and Alice publicly share a part of the generated random bit string.
  - If the bit error rate surpasses a tolerable limit, indicating potential eavesdropping, the protocol is aborted.

VI. 3-STATE PROTOCOLS

- BB92's secure key rate strongly affected by losses: Eve can **extract information by increasing the losses** and performing USD attack.
  - **Unambiguous State Discrimination (USD) attack**: uses optimal quantum measurement, type of measurement that aims to obtaining the full information about the state sent from an ensemble of possible states without introducing errors.

- **BB92 three-state protocol**: addition of 3rd state enough for noise-independent unconditional security of the protocol → Drawback: key rates not close to 4-state BB84 protocol.
- **PBC00**: **Optimal 3-state protocol** by Phoenix-Barnett-Chefles.
  - States form equilateral triangle in X-Z plane of Bloch sphere.
  - Symmetry can be exploited to achieve similar rates to BB84.



Ref [4]

VII. PBC00 PROTOCOL

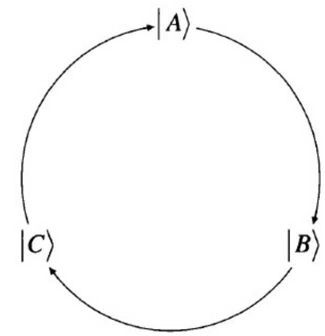
1. **State Preparation (Alice):** Randomly prepares qubits with equal a priori probabilities in states $|A\rangle$, $|B$, and $|C\rangle$ with equal probabilities.
2. **Measurement (Bob):**
   1. Randomly measures qubits using operators P_A, P_B, and P_C with equal probabilities.
   2. Discards timeslots with measurement result zero, tell Alice to discard them too.
3. **Key Establishment:**
   1. Alice announces a **state not sent** for each remaining timeslot.
   2. Bob discards timeslots if Alice's announcement doesn't match his measurement and tells Alice what to discard.

- For example:
  1. Suppose Alice sent (A) for particular timeslot → she would announce either (B) or (C) each with probability 1/2.
  2. Suppose Bob measured P_B (timeslot has not been discarded by him) → Bob would know that either (A) or (C) had been sent by Alice.
     - If Alice announced that she did not send (C), Bob would immediately know that Alice had, in fact sent the state (A).
     - If , however, Alice announced that she did not send the state (B) → Bob would **obtain no further useful information**

VII. PBC00 PROTOCOL

4. **Key Generation:** Binary string created based on the clockwise cyclic arrangement of states. Begin with state transmitted by Alice. If state announced as "**Not Sent**" is:
    1. One-hop away clockwise → Bit value is '0'.
    2. Two hops away clockwise → Bit value is '1'.

5. **Eavesdropping Detection:**
    1. Impossible for Eve to guess which state was sent by Alice.
    2. Eve's intercept-resend strategy results in key bit errors, detectable by Alice and Bob.



Ref [4]

Timeslot	1	2	3	4	5	6	7	8	9	10
Alice prepares	$\|A\rangle$	$\|B\rangle$	$\|C\rangle$	$\|C\rangle$	$\|C\rangle$	$\|B\rangle$	$\|A\rangle$	$\|A\rangle$	$\|B\rangle$	$\|A\rangle$
Bob measures	$\hat{P}_{\bar{A}}$	$\hat{P}_{\bar{A}}$	$\hat{P}_{\bar{B}}$	$\hat{P}_{\bar{A}}$	$\hat{P}_{\bar{C}}$	$\hat{P}_{\bar{C}}$	$\hat{P}_{\bar{C}}$	$\hat{P}_{\bar{B}}$	$\hat{P}_{\bar{C}}$	$\hat{P}_{\bar{B}}$
Result	0	1	1	0	0	1	1	0	1	1
Alice says not		$\|C\rangle$	$\|B\rangle$			$\|A\rangle$	$\|B\rangle$		$\|C\rangle$	$\|C\rangle$
Bob says		✓	×			✓	✓		×	✓
Sequence		BC				BA	AB			AC
Inferred bit		0				1	0			1

VII. PBC00 PROTOCOL

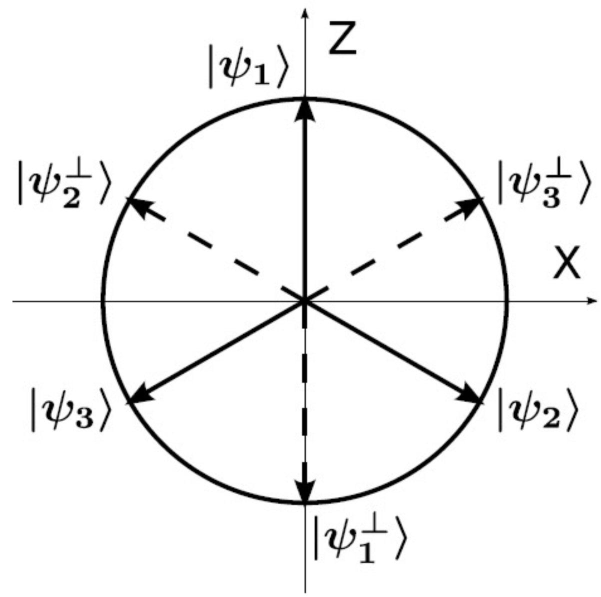
6. **Key Generation:** Binary string created based on the clockwise cyclic arrangement of states. Begin with state transmitted by Alice. If state announced as "**Not Sent**" is:
   1. One-hop away clockwise → Bit value is '0'.
   2. Two hops away clockwise → Bit value is '1'.
7. **Eavesdropping Detection:**
   1. Impossible for Eve to guess which state was sent by Alice.
   2. Eve's intercept-resend strategy results in key bit errors, detectable by Alice and Bob.
8. **Optimum Measurements (POM)→** Two strategies for eavesdropping:
   1. Minimize probability that state is assigned incorrectly.
   2. Maximize mutual information between Alice & Eve.
9. **Optimum Measurements (Probability Operator Measurements) →** Two strategies for eavesdropping:
   1. Minimize probability that state is assigned incorrectly.
   2. Maximize mutual information between Alice & Eve.
10. **Eavesdropper Detection**
    1. Eve's strategy revealed in public discussion.
    2. Intercept-resend strategy induces errors with a probability of 2/7 (QBER=28.6%).
    3. Sending a random state to Bob increases error probability.
11. **Conclusion:**
    1. The protocol allows secure key exchange while detecting eavesdropping attempts.
    2. Still requires public exchange of sifted key on order to estimate the Quantum Bit Error Rate.

VIII. R04 PROTOCOL

- Improvement of PBC00 protocol, estimates QBER from number of inconclusive events → all conclusive events used for key extraction.
- 3 quantum states:
  - $\{|\psi_i\rangle, i = 1,2,3\}$ placed in equilateral triangle in X-Z plane of Bloch sphere.
  - Grouped in set: $S_1 = \{|\psi_1\rangle, |\psi_2\rangle\}$, $S_2 = \{|\psi_2\rangle, |\psi_3\rangle\}$ and $S_3 = \{|\psi_3\rangle, |\psi_1\rangle\}$.
  - 1st state → bit 0, 2nd state → bit 1.
  - No information in each state about associated bit before the information about the used set is disclosed.
- Entanglement version: using polarization-entangle photon pairs in singlet state.

$$|\Psi^-\rangle = \frac{|H\rangle_A|V\rangle_B - |H\rangle_A|V\rangle_B}{\sqrt{2}}$$

- Subscripts indicate photon gong to Alice or Bob, and $|H\rangle$ or $|V\rangle$ are horizontal or vertical polarizations states.
- Photons A & B are anti-correlated in any basis for measurement.



Ref [5]

VIII. R04 PROTOCOL

1. The states relate: $$\begin{cases} |\psi_1^{\perp}\rangle = |V\rangle, |\psi_2^{\perp}\rangle = \frac{\sqrt{3}}{2}|H\rangle - \frac{1}{2}|V\rangle, \psi_3^{\perp} = \frac{\sqrt{3}}{2}|H + \frac{1}{2}|V \\ |\psi_1\rangle = |H\rangle, |\psi_2\rangle = \frac{1}{2}|H\rangle + \frac{\sqrt{3}}{2}|V\rangle, \text{and } |\psi_3\rangle = \frac{1}{2}|H\rangle - \frac{3}{2}|V\rangle \end{cases}$$
2. Alice measures photon A using the POVM:

   $$\left\{\Pi_i \equiv \frac{2}{3}|\psi_i^{\perp}\rangle\langle\psi_i^{\perp}|\right\}$$
3. Anticorrelation: when Alice detects $|\psi_i^{\perp}\rangle$ she has sent Bob the state $|\psi_i\rangle$
4. Bob performs his measurements in the same POVM as Alice $\{\Pi_i\}$.
5. After all measurements, Bob and Alice compare the instants of their events, keeping only those where both have a detection within a fixed coincidence window.
   - Don't share any bit string yet since each state can mean 0 or 1.

VIII. R04 PROTOCOL

6. Alice uses **QRNG to determine bit value** for each symbol → Combination of **state & bit value** unambiguously determines set $\boldsymbol{S_i}$.
   - For example: Alice sends $|\psi 2\rangle$ and the QRNG gives 1, the set used for that event is $S1$).
7. For each event, Alice tells Bob the corresponding set by sending him the **value of the index *i***. Bob uses i to associate 2 (for $i = 1$), 3 (for $i = 2$), and 1 (for $i = 3$) with bit 0, and 1 (for $i = 1$), 2 (for $i = 2$), and 3 (for $i = 3$) with bit 1.
8. All other combinations are marked as **inconclusive**, since Bob is not able to determine the state sent by Alice.
9. Bob tells Alice which events are inconclusive and both discard them. Then estimate QBER from the **fraction of inconclusive events** and use this information to distill the key using error correction and privacy amplification.

- **Sifting procedure:**

1. According to the random bit choice at Alice's side (on the left for 0, on the right for 1).
2. The cell (Ai,Bj) stands for a coincidence between Alice's detector i and Bob's detector j. Inconclusive events are marked as "Inc".
3. The events in the diagonal (Ai,Bi) give an error independently from the bit choice.
4. The other combinations (Ai,Bj), with i ≠ j, are either a "good" conclusive or an inconclusive event, according to Alice's choice.

	Bit = 0			Bit = 1		
	A1	A2	A3	A1	A2	A3
B1	1	Inc	0	0	1	Inc
B2	0	1	Inc	Inc	0	1
B3	Inc	0	1	1	Inc	0

Ref [5]

VIII. R04 PROTOCOL

6. **Secret key** rate

- Post-processing Objective: Transformation of a partially correlated, partially secret key to reduce Eve's information.
- **Quantification of Key Transformation**: Secret fraction "r" represents the **ratio of secure to conclusive bit.** In asymptotic limit of infinitely long key:

$$r = 1 - f_{EC} h(Q) - h\left(\frac{5}{4}Q\right),$$

where $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$

is the binary entropy, Q is the QBER and $f_{EC} = 1.1$ is the efficiency of the error correction protocol.

- The **QBER** is estimated: $Q = \frac{1-2I}{1-I}$, where I is the fraction of inconclusive results.
- # of secure bits is $N_{CONC} * r$, and the **Secret Key Rate is:** $\frac{N_{CONC} * r}{Exposure\ time}$

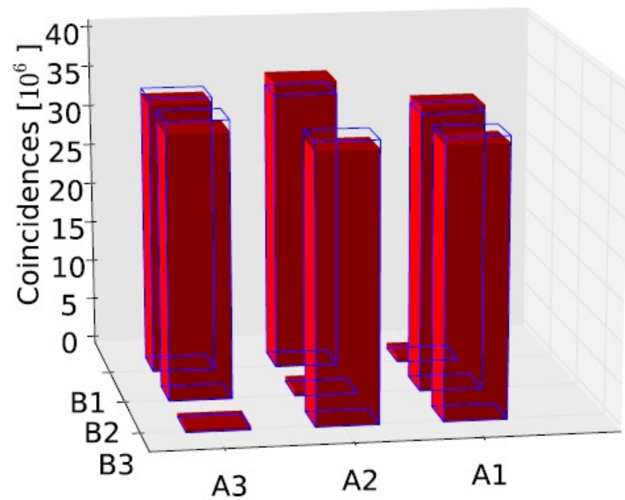
IX. EXPERIMENTAL REALIZATION

- Measured **Heralding efficiency** = 5% → corresponds to a total loss level of 13 dB.
- Loss contribution of 1.5 dB due to the POVM.
- QBER remains almost constant below 2%.
- **Asymptotic Secure Key Rate > 10 kbit/s.**

	A1	A2	A3
B1	0.6	35.8	33.6
B2	35.1	0.6	32.8
B3	33.4	33.2	0.4

Ref [5]

Total number of coincidences at the different detectors (million events). The cell (Ai,Bj) corresponds to a coincidence of Alice's detector *i* and Bob's detector *j*.



Ref [5]

Total number of coincidences at the different detectors. Full (red) bars correspond to detected events and (blue) contours represent the expected number of detection events.

REFERENCES

1. https://governmenttechnologyinsider.com/quantum-key-distribution-podcast-on-securing-future-network-communications/
2. https://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/#fundamentalsLecture slides, course OPTI 541C, prof. R. J. Jones, Lecture 6 Nonlinear Propagation.
3. https://qt.eu/quantum-principles/communication/quantum-key-distribution-qkd Kuriakose, V C & Porsezian, Kuppuswamy. (2010). Elements of optical solitons: An overview. Resonance. 15. 643-666. 10.1007/s12045-010-0048-y.
4. Simon J. D. Phoenix, Stephen M. Barnett & Anthony Chefles (2000) “Three-state quantum cryptography”, Journal of Modern Optics, 47:2-3, 507-516, DOI: 10.1080/09500340008244056
5. Matteo Schiavon, Giuseppe Vallone & Paolo Villoresi (28 July 2016) Experimental realization of equiangular three-state quantum key distribution”, www.nature.com/scientificreports