B92 Protocol: Theory, Simulation, and Error Correction Performance

Charles H. Bennett — IBM Research Division, Yorktown Heights, New York

Sumit Tapas Chongder
Supervisor: Dr. V. Narayanan
M.Tech in Quantum Technologies
Roll No.: M25IQT013

Course: Quantum Cryptography and Coding

Indian Institute of Technology Jodhpur

Introduction to Quantum Key Distribution

Current Cryptographic Systems:

- RSA, ECC and AES are widely used for secure communication.
- Security relies on computational hardness (e.g., factoring large primes).
- Vulnerable to quantum attacks — Shor's algorithm can break RSA and ECC.

Why RSA is Not Reliable in the Quantum Era:

- RSA depends on the difficulty of factoring large numbers.
- Quantum computers can solve this efficiently using Shor's algorithm.
- Post-quantum cryptography is still under development and standardization.

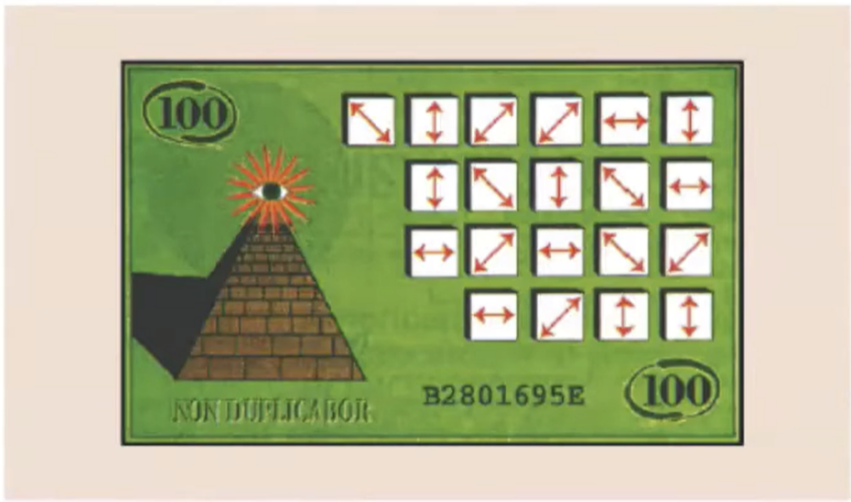
Quantum to the Rescue:

- Needed: A way to securely distribute a random key between two legitimate parties.
- An eavesdropper should not be able to intercept the key.
- Any attempt at intrusion should be detectable!
- **Solution: Quantum Key Distribution!**

A Bit of History: Stephen Wiesner (1970s)

Stephen Wiesner was one of the earliest pioneers in quantum information theory during the 1970s.

- Introduced the concept of **quantum money** — a form of currency that is impossible to counterfeit due to quantum mechanics.
- Contributed to the idea of **superdense coding**, enabling transmission of two classical bits using one qubit.



These ideas were revolutionary and inspired later protocols like BB84 and B92, forming the backbone of quantum communication.

A Bit of History: BB84 Protocol (1984)

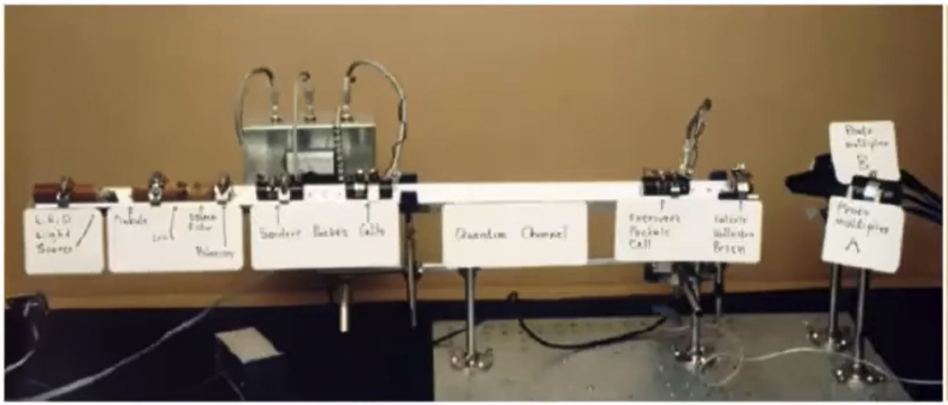
In 1984, **Charles Bennett** and **Gilles Brassard** built on Wiesner's ideas to propose the first quantum cryptography protocol — **BB84**.

- Introduced quantum key distribution using four polarization states.
- Demonstrated how quantum mechanics could ensure secure communication.
- BB84 remains the most widely studied and implemented QKD protocol.

A Bit of History: First QKD Experiment (1989)

In 1989, **Charles Bennett**, **Lee Smolin**, and collaborators conducted the first experimental demonstration of quantum key distribution.

- Demonstrated feasibility of QKD using polarized photons.
- Validated theoretical predictions with real-world hardware.
- Paved the way for future QKD systems and commercial implementations.



A Bit of History: E91 Protocol by Artur Ekert (1991)

Artur Ekert proposed the **E91 protocol** in 1991, introducing quantum entanglement as a resource for secure key distribution.

- Used entangled pairs to detect eavesdropping via Bell inequality violations.
- Provided a fundamentally different approach to QKD compared to BB84.
- Strengthened the connection between quantum cryptography and quantum foundations.

A Bit of History: B92 Protocol (1992)

In 1992, **Charles Bennett** introduced the **B92 protocol**, a simplified version of BB84 using only two non-orthogonal quantum states.

- Reduced complexity in state preparation and measurement.
- Maintained security through non-orthogonality and quantum measurement disturbance.
- Inspired further research into minimalistic and efficient QKD protocols.

B92 Protocol: Original Paper Reference

Original Proposal: Charles H. Bennett, *Quantum cryptography using any two nonorthogonal states*, Phys. Rev. Lett. 68, 3121 (1992)

VOLUME 68, NUMBER 21 PHYSICAL REVIEW LETTERS 25 MAY 1992

Quantum Cryptography Using Any Two Nonorthogonal States

Charles H. Bennett

IBM Research Division, T. J. Watson Research Center, Yorktown Heights, New York 10598

(Received 23 December 1991)

Quantum techniques for key distribution—the classically impossible task of distributing secret information over an insecure channel whose transmissions are subject to inspection by an eavesdropper, between parties who share no secret initially—have been proposed using (a) four nonorthogonally polarized single-photon states or low-intensity light pulses, and (b) polarization-entangled or spacetime-entangled two-photon states. Here we show that in principle any *two* nonorthogonal quantum states suffice, and describe a practical interferometric realization using low-intensity coherent light pulses.

PACS numbers: 03.65.Bz, 42.50.Wm, 89.70.+c

Key distribution is the term applied to techniques allowing two parties to acquire a random bit sequence (the "key") with a high level of confidence that no one else knows it or has significant partial information about it. One party (henceforth "Alice"), for example, might generate the key by a physically random process, make a copy of it, and hand deliver the copy to the other party (henceforth "Bob"). Such shared secret key bits, although random and meaningless in themselves, are a valuable resource because they allow the communicating parties to achieve, with provable security, two of the main goals of cryptography: encrypting a subsequent meaningful message to make it unintelligible to a third party [1], and certifying to the legitimate receiver that a message (plain or encrypted) has not been altered in transit [2].

If two parties share no secret information initially and communicate solely through classical messages monitored by an eavesdropper, it is impossible for them to arrive at a certifiably secret key [3]. However, it becomes possible to do so if they exchange both classical public messages (which can be monitored but not altered or suppressed by the eavesdropper) and quantum transmissions having the property that they can be suppressed or altered, but cannot in principle be monitored without disturbance [4]. Various types of quantum transmissions have been shown to suffice: a random sequence of spin-$\frac{1}{2}$ particles or single photons in four nonorthogonal polarization states

TABLE I. EPR and non-EPR key distribution.

EPR	non-EPR														
1a	–	○	+	○	+	+	+	+	+	○	○	+	○	○	○	+
2a	2b	↺	|	↻	↔	|	|	↔	↔	↻	↺	|	↻	↺	↺	|
3	3	+	○	○	+	+	○	○	+	○	+	○	○	○	○	+
4	4	|		↻	↔	|	↺	↺	↔	↻	|	↻	↻		↺	|
5	5	+		○	+	+	○	○	+	○	+	○	○		○	+	
6	6			√	√	√			√	√			√		√	√	
7	7			↻	↔	|			↔	↻			↻		↺	|	
8	8			1	0	1			0	1			1		0	1	
9	9			1	0				0				1			1	
10	10				0	1			0	1			1		0	1	

[1a] In the EPR version, Alice chooses a random basis for measuring one member of each EPR pair of photons: rectilinear (+), or circular (○). The other photon of each EPR pair is measured by Bob in step 3.

[2a] Alice's measurement results in effect determine, through the EPR correlations, a random sequence of states for Bob's photon: horizontal (↔), vertical (↕), right-circular (↻), and left-circular (↺).

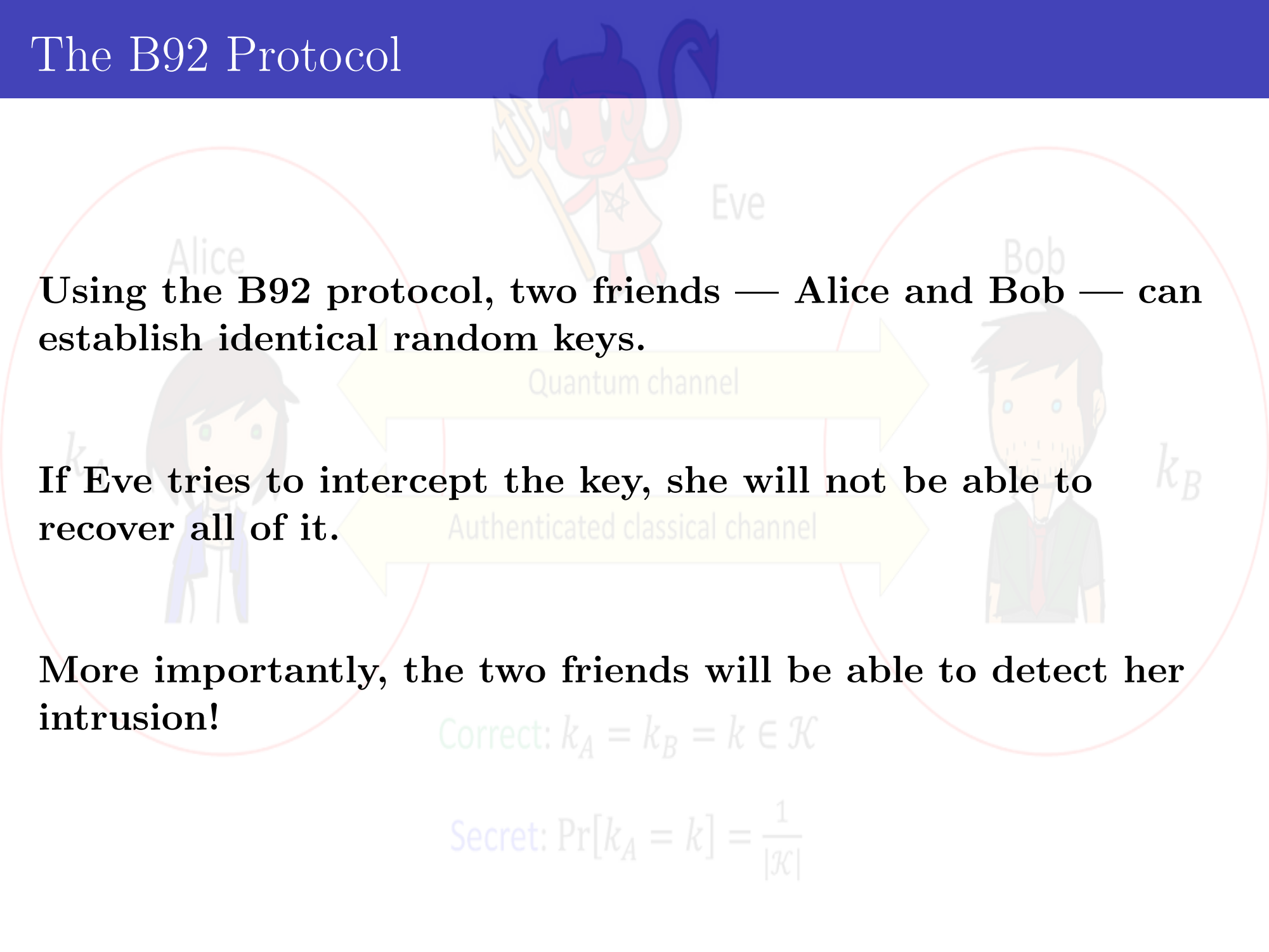
[2b] In the non-EPR version, Alice *prepares* a random sequence of photons polarized ↔, ↕, ↻, and ↺, and sends them to Bob.

[3] Bob measures his photon using a random sequence of bases.

[4] Results of Bob's measurements. Some photons are shown as not having been received owing to imperfect detector efficiency. (Realistic detectors would also generate occasional errors due to dark counts, which can be found and corrected as described in [5].)

Reference Link: Click here to view the original paper on Physical Review Letters

The B92 Protocol

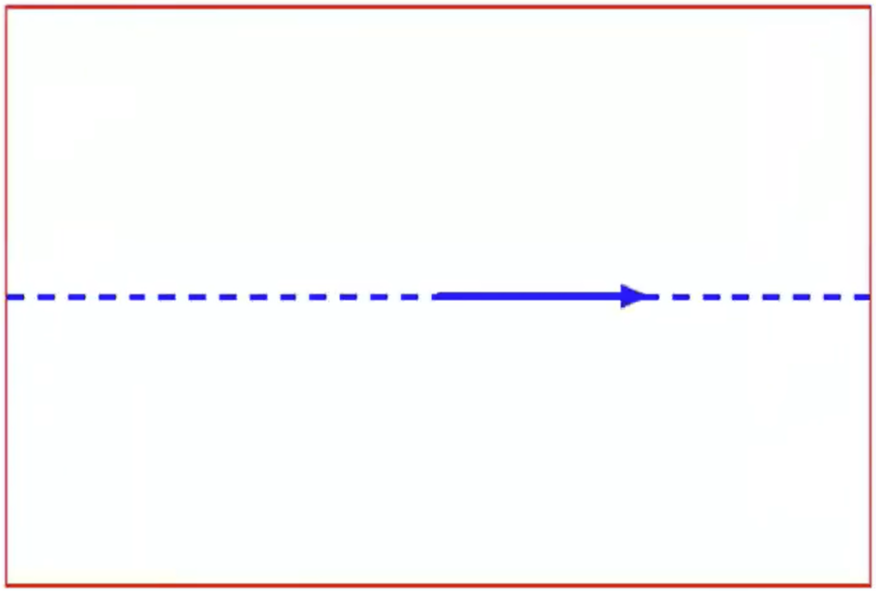


Using the B92 protocol, two friends — Alice and Bob — can establish identical random keys.

If Eve tries to intercept the key, she will not be able to recover all of it.

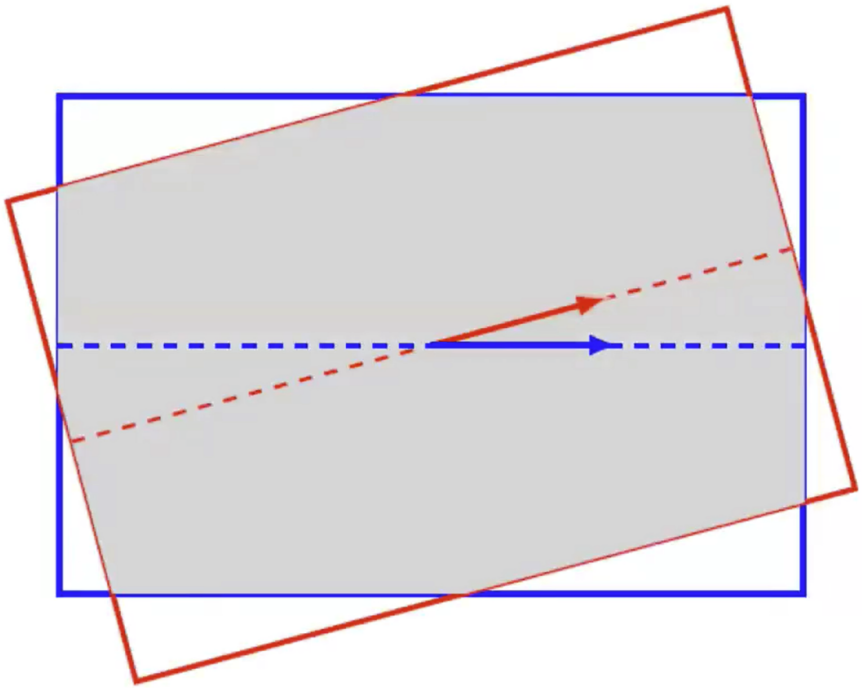
More importantly, the two friends will be able to detect her intrusion!

Background: Polarization of Light



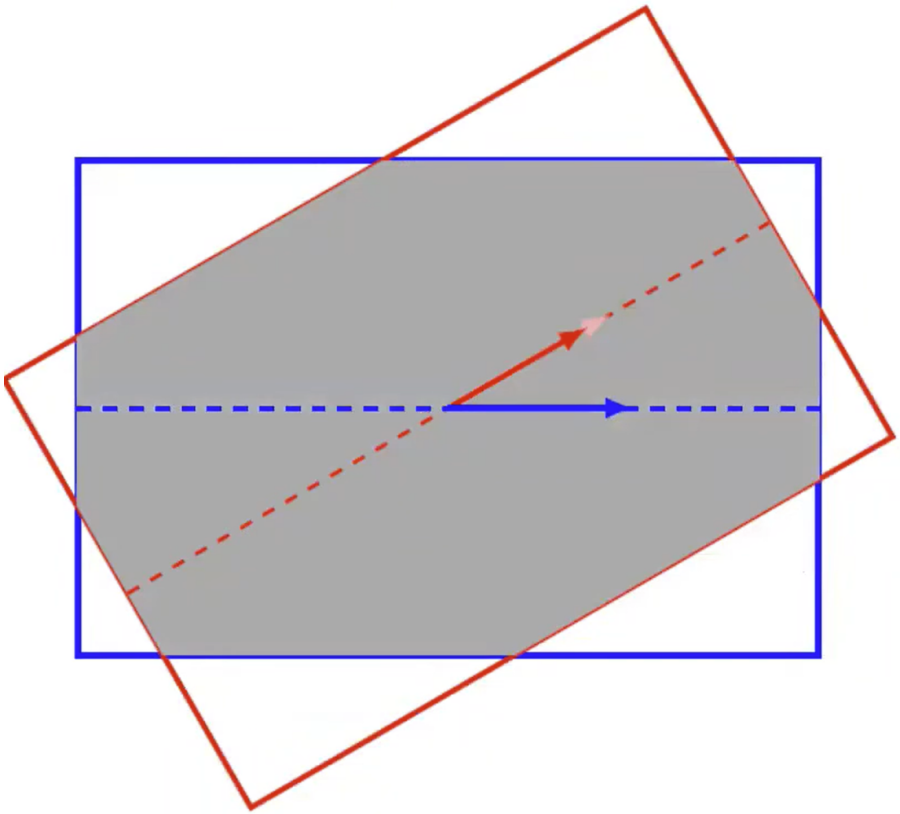
- **After passing through the polarizer, light is horizontally polarized.**

Background: Polarization of Light



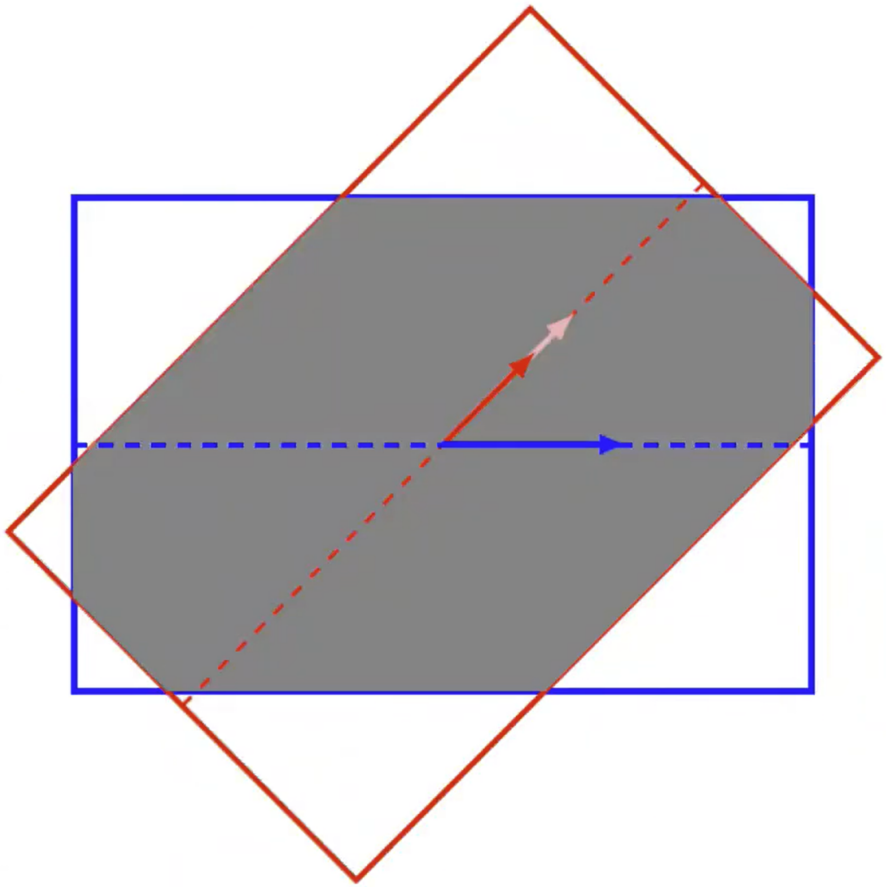
- **After passing through the polarizer, light is horizontally polarized.**
- **Only the component along the analyzer's pass axis gets through.**

Background: Polarization of Light



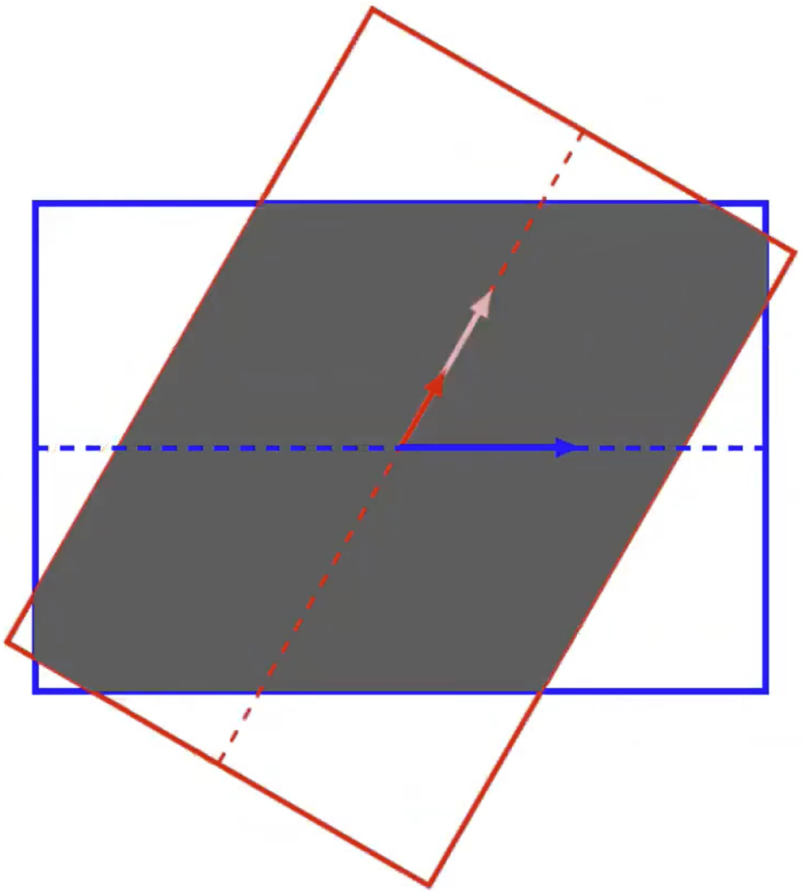
- **After passing through the polarizer, light is horizontally polarized.**
- **Only the component along the analyzer's pass axis gets through.**
- $$E = E_0 \cos\theta$$

Background: Polarization of Light



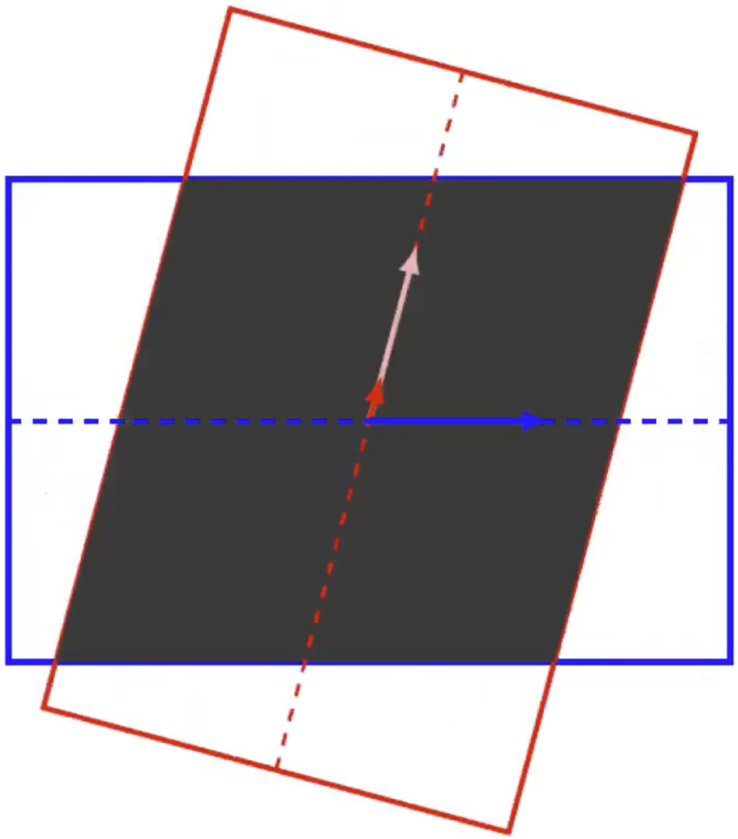
- **After passing through the polarizer, light is horizontally polarized.**
- **Only the component along the analyzer's pass axis gets through.**
- $$E = E_0 \cos\theta$$
- $$I = I_0 \cos^2\theta$$

Background: Polarization of Light



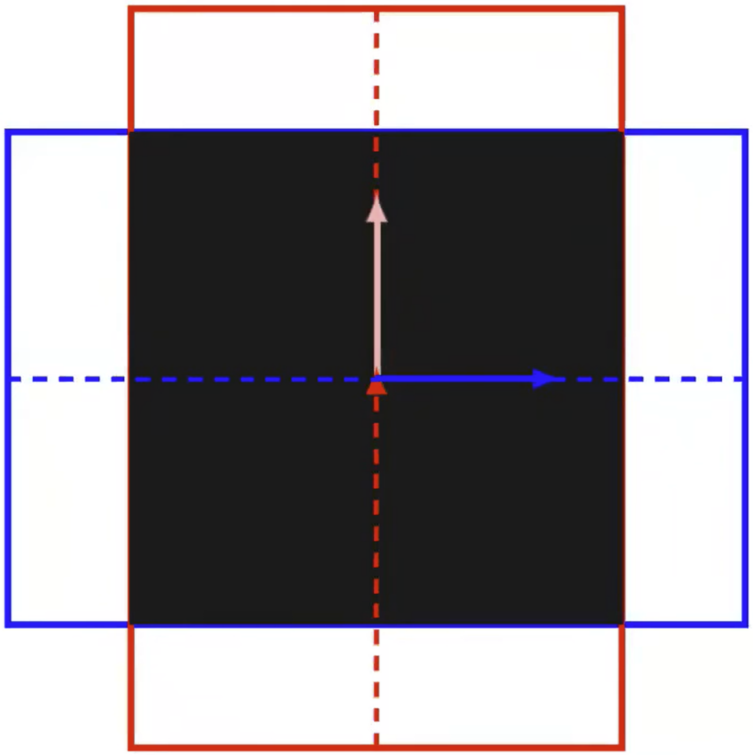
- **After passing through the polarizer, light is horizontally polarized.**
- **Only the component along the analyzer's pass axis gets through.**
- $$E = E_0 \cos\theta$$
- $$I = I_0 \cos^2\theta$$
- **For diagonal polarization:** 50% of the light intensity passes through the polarizer-analyzer combo.

Background: Polarization of Light



- **After passing through the polarizer, light is horizontally polarized.**
- **Only the component along the analyzer's pass axis gets through.**
- $$E = E_0 \cos\theta$$
- $$I = I_0 \cos^2\theta$$
- **For diagonal polarization:** 50% of the light intensity passes through the polarizer-analyzer combo.

Background: Polarization of Light



- **After passing through the polarizer, light is horizontally polarized.**
- **Only the component along the analyzer's pass axis gets through.**
- $$E = E_0 \cos\theta$$
- $$I = I_0 \cos^2\theta$$
- **For diagonal polarization:** 50% of the light intensity passes through the polarizer-analyzer combo.

B92 Quantum Key Distribution Protocol

Alice

1000110101001101...

Bit	State
0	$\rightarrow$
1	$\nearrow$

Bob

0010010101101101...

Bit	Pass Axis
0	$\uparrow$
1	$\nwarrow$

Alice generates either **horizontally polarized** ($\rightarrow$) or **diagonally polarized** ($\nearrow$) photons according to whether her bit is 0 or 1, respectively, and sends them over to Bob.

Bob, in his turn, arranges to detect their state by aligning his analyzer south-west, or vertical, according to whether his bit is **0 or 1**, respectively.

B92 Quantum Key Distribution Protocol

Alice's Bit	Bob's Bit	Photon Sent	Polarizer Status	Transmission	Probability
0	0	$\rightarrow$	$\nwarrow$	Yes	50-50
0	1	$\rightarrow$	$\uparrow$	No	0
1	0	$\nearrow$	$\nwarrow$	No	0
1	1	$\nearrow$	$\uparrow$	Yes	50-50

- A photon will never pass if Bob and Alice have different bits.
- If they have the same bit, there is a 50% chance of success.
- By keeping the bits at which the photon gets through, they can share identical random keys.
- Bob only needs to publicly declare which photons went through.

QBER for B92 Protocol

In the B92 protocol, only one basis state is used to encode each bit. When Bob measures the incoming photon, there's a 50% chance that his basis matches Alice's, allowing correct decoding. The other 50% of the time, mismatched bases lead to discarded bits. As a result, only 25% of the total transmitted bits are usable for key generation.

The Quantum Bit Error Rate (QBER) for B92 is given by:

$$QBER = p_{\text{pol}} + \frac{p_{\text{dark}}}{\mu \cdot T_{\text{chan}} \cdot \eta_{\text{det}}}$$

Where:

- p_{dark}: Probability of a dark count (false detection)
- μ: Average number of photons per pulse
- T_{chan}: Channel transmittance
- η_{det}: Detector quantum efficiency
- $p_{\text{pol}} = \frac{1-V_f}{2}$: Probability of polarization error due to visibility V_f

Key Rate in B92 Protocol

In the B92 protocol, the key rate is determined by the fraction of bits that are successfully transmitted and retained after basis reconciliation and error filtering. Since only non-orthogonal states are used, and Bob only keeps the bits where a photon is detected, the sifted key rate is inherently lower than BB84.

The secure key rate R_{B92} can be approximated by:

$$R_{B92} = \frac{1}{4} \cdot P_{\text{click}} \cdot \left[(1 - \tau') + F(QBER) \cdot h(QBER)\right]$$

Where:

- P_{click}: Probability that a photon is successfully detected by the receiver's single-photon detector.
- τ': Sifting or transmission loss factor due to protocol constraints and inconclusive measurements.
- $F(QBER)$: Fidelity-based correction function that quantifies the usable information after accounting for quantum bit errors.
- $h(QBER)$: Binary entropy function representing the uncertainty or information leakage due to QBER.

The B92 Protocol — Foiling Eve

- What if Eve intercepts the photons midway?
  - She must determine the state of the intercepted photon.
  - She can try to mimic Bob's measurement strategy.
  - She can be certain of the photon's state only if it passes through her analyzer — which occurs only 25% of the time.
  - In those cases, she can forward the photon to Bob without disturbance.
  - In the remaining 75%, she must:
    - guess the state,
    - prepare a copy,
    - and send it onward.
- This means Eve can be certain of only $\frac{1}{16}$ of the actual key bits.
- **But wars have been won on less!**

The B92 Protocol — Foiling Eve

- What if Eve intercepts the photons midway?
  - She must determine the state of the intercepted photon.
  - She can try to mimic Bob's measurement strategy.
  - She can be certain of the photon's state only if it passes through her analyzer — which occurs only 25% of the time.
  - In those cases, she can forward the photon to Bob without disturbance.
  - In the remaining 75%, she must:
    - guess the state,
    - prepare a copy,
    - and send it onward.
- This means Eve can be certain of only $\frac{1}{16}$ of the actual key bits.
- **But wars have been won on less!**

The B92 Protocol — Foiling Eve

- What if Eve intercepts the photons midway?
  - She must determine the state of the intercepted photon.
  - She can try to mimic Bob's measurement strategy.
  - She can be certain of the photon's state only if it passes through her analyzer — which occurs only 25% of the time.
  - In those cases, she can forward the photon to Bob without disturbance.
  - In the remaining 75%, she must:
    - guess the state,
    - prepare a copy,
    - and send it onward.
- This means Eve can be certain of only $\frac{1}{16}$ of the actual key bits.
- **But wars have been won on less!**

The B92 Protocol — Foiling Eve

- What if Eve intercepts the photons midway?
  - She must determine the state of the intercepted photon.
  - She can try to mimic Bob's measurement strategy.
  - She can be certain of the photon's state only if it passes through her analyzer — which occurs only 25% of the time.
  - In those cases, she can forward the photon to Bob without disturbance.
  - In the remaining 75%, she must:
    - guess the state,
    - prepare a copy,
    - and send it onward.
- This means Eve can be certain of only $\frac{1}{16}$ of the actual key bits.
- **But wars have been won on less!**

The B92 Protocol — Foiling Eve

- What if Eve intercepts the photons midway?
  - She must determine the state of the intercepted photon.
  - She can try to mimic Bob's measurement strategy.
  - She can be certain of the photon's state only if it passes through her analyzer — which occurs only 25% of the time.
  - In those cases, she can forward the photon to Bob without disturbance.
  - In the remaining 75%, she must:
    - guess the state,
    - prepare a copy,
    - and send it onward.
- This means Eve can be certain of only $\frac{1}{16}$ of the actual key bits.
- **But wars have been won on less!**

The B92 Protocol — Foiling Eve

- What if Eve intercepts the photons midway?
  - She must determine the state of the intercepted photon.
  - She can try to mimic Bob's measurement strategy.
  - She can be certain of the photon's state only if it passes through her analyzer — which occurs only 25% of the time.
  - In those cases, she can forward the photon to Bob without disturbance.
  - In the remaining 75%, she must:
    - guess the state,
    - prepare a copy,
    - and send it onward.
- This means Eve can be certain of only $\frac{1}{16}$ of the actual key bits.
- **But wars have been won on less!**

The B92 Protocol — Foiling Eve

- What if Eve intercepts the photons midway?
  - She must determine the state of the intercepted photon.
  - She can try to mimic Bob's measurement strategy.
  - She can be certain of the photon's state only if it passes through her analyzer — which occurs only 25% of the time.
  - In those cases, she can forward the photon to Bob without disturbance.
  - In the remaining 75%, she must:
    - guess the state,
    - prepare a copy,
    - and send it onward.
- This means Eve can be certain of only $\frac{1}{16}$ of the actual key bits.
- **But wars have been won on less!**

The B92 Protocol — Foiling Eve

- What if Eve intercepts the photons midway?
  - She must determine the state of the intercepted photon.
  - She can try to mimic Bob's measurement strategy.
  - She can be certain of the photon's state only if it passes through her analyzer — which occurs only 25% of the time.
  - In those cases, she can forward the photon to Bob without disturbance.
  - In the remaining 75%, she must:
    - guess the state,
    - prepare a copy,
    - and send it onward.
- This means Eve can be certain of only $\frac{1}{16}$ of the actual key bits.
- **But wars have been won on less!**

The B92 Protocol — Foiling Eve

- What if Eve intercepts the photons midway?
  - She must determine the state of the intercepted photon.
  - She can try to mimic Bob's measurement strategy.
  - She can be certain of the photon's state only if it passes through her analyzer — which occurs only 25% of the time.
  - In those cases, she can forward the photon to Bob without disturbance.
  - In the remaining 75%, she must:
    - guess the state,
    - prepare a copy,
    - and send it onward.
- This means Eve can be certain of only $\frac{1}{16}$ of the actual key bits.
- **But wars have been won on less!**

The B92 Protocol — Foiling Eve

- What if Eve intercepts the photons midway?
  - She must determine the state of the intercepted photon.
  - She can try to mimic Bob's measurement strategy.
  - She can be certain of the photon's state only if it passes through her analyzer — which occurs only 25% of the time.
  - In those cases, she can forward the photon to Bob without disturbance.
  - In the remaining 75%, she must:
    - guess the state,
    - prepare a copy,
    - and send it onward.
- This means Eve can be certain of only $\frac{1}{16}$ of the actual key bits.
- **But wars have been won on less!**

The B92 Protocol — Foiling Eve

- What if Eve intercepts the photons midway?
  - She must determine the state of the intercepted photon.
  - She can try to mimic Bob's measurement strategy.
  - She can be certain of the photon's state only if it passes through her analyzer — which occurs only 25% of the time.
  - In those cases, she can forward the photon to Bob without disturbance.
  - In the remaining 75%, she must:
    - guess the state,
    - prepare a copy,
    - and send it onward.
- This means Eve can be certain of only $\frac{1}{16}$ of the actual key bits.
- **But wars have been won on less!**

The B92 Protocol — Foiling Eve

- Alice and Bob now share a key which is partially compromised.
- What saves the day for them is that Eve's interference leaves a detectable signature on the final key!
- In the cases she had to guess, Eve will make a number of mistakes!
- Her measurement has changed the state of the photon!
- This will lead to errors in the final key that they decide upon.
- They can share randomly chosen bits from the key to check this.
- Once they are sure that the shared bits are error-free, they can discard them and go ahead.

The B92 Protocol — Foiling Eve

- Alice and Bob now share a key which is partially compromised.
- What saves the day for them is that Eve's interference leaves a detectable signature on the final key!
- In the cases she had to guess, Eve will make a number of mistakes!
- Her measurement has changed the state of the photon!
- This will lead to errors in the final key that they decide upon.
- They can share randomly chosen bits from the key to check this.
- Once they are sure that the shared bits are error-free, they can discard them and go ahead.

The B92 Protocol — Foiling Eve

- Alice and Bob now share a key which is partially compromised.
- What saves the day for them is that Eve's interference leaves a detectable signature on the final key!
- In the cases she had to guess, Eve will make a number of mistakes!
- Her measurement has changed the state of the photon!
- This will lead to errors in the final key that they decide upon.
- They can share randomly chosen bits from the key to check this.
- Once they are sure that the shared bits are error-free, they can discard them and go ahead.

The B92 Protocol — Foiling Eve

- Alice and Bob now share a key which is partially compromised.
- What saves the day for them is that Eve's interference leaves a detectable signature on the final key!
- In the cases she had to guess, Eve will make a number of mistakes!
- Her measurement has changed the state of the photon!
- This will lead to errors in the final key that they decide upon.
- They can share randomly chosen bits from the key to check this.
- Once they are sure that the shared bits are error-free, they can discard them and go ahead.

The B92 Protocol — Foiling Eve

- Alice and Bob now share a key which is partially compromised.
- What saves the day for them is that Eve's interference leaves a detectable signature on the final key!
- In the cases she had to guess, Eve will make a number of mistakes!
- Her measurement has changed the state of the photon!
- This will lead to errors in the final key that they decide upon.
- They can share randomly chosen bits from the key to check this.
- Once they are sure that the shared bits are error-free, they can discard them and go ahead.

The B92 Protocol — Foiling Eve

- Alice and Bob now share a key which is partially compromised.
- What saves the day for them is that Eve's interference leaves a detectable signature on the final key!
- In the cases she had to guess, Eve will make a number of mistakes!
- Her measurement has changed the state of the photon!
- This will lead to errors in the final key that they decide upon.
- They can share randomly chosen bits from the key to check this.
- Once they are sure that the shared bits are error-free, they can discard them and go ahead.

The B92 Protocol — Foiling Eve

- Alice and Bob now share a key which is partially compromised.
- What saves the day for them is that Eve's interference leaves a detectable signature on the final key!
- In the cases she had to guess, Eve will make a number of mistakes!
- Her measurement has changed the state of the photon!
- This will lead to errors in the final key that they decide upon.
- They can share randomly chosen bits from the key to check this.
- Once they are sure that the shared bits are error-free, they can discard them and go ahead.

The No-Cloning Theorem

- Couldn't Eve simply clone Alice's photons before measuring?
- **No!**
- Any non-disruptive operation in Quantum mechanics has to be unitary.
- Since an operation can not clone non-orthogonal states!

The No-Cloning Theorem

- Couldn't Eve simply clone Alice's photons before measuring?
- **No!**
- Any non-disruptive operation in Quantum mechanics has to be unitary.
- Since an operation can not clone non-orthogonal states!

The No-Cloning Theorem

- Couldn't Eve simply clone Alice's photons before measuring?
- **No!**
- Any non-disruptive operation in Quantum mechanics has to be unitary.
- Since an operation can not clone non-orthogonal states!

The No-Cloning Theorem

- Couldn't Eve simply clone Alice's photons before measuring?
- **No!**
- Any non-disruptive operation in Quantum mechanics has to be unitary.
- Since an operation can not clone non-orthogonal states!

B92 Experimental Setup: General Idea

ALICE's operations:

1. **Preparing single photons:** using sources such as weak coherent pulsed (WCP), spontaneous parametric down-conversion (SPDC), etc.
2. **Random selection** of polarization state for each photon — either vertical (V) or anti-diagonal (A).
3. **Record time** stamping and polarization state for each photon.
4. **Send stream of photons to Bob.**

C. H. Bennett, Phys. Rev. Lett. ***68****, 3121 (1992)*

B92 Experimental Setup: General Idea

BOB's operations:

1. **Random selection** of polarization basis for each photon — either horizontal (H) or vertical (V).
2. **Measure** each photon in the selected basis.
3. **Record time** stamping and polarization state for detected photons.
4. **Send time stamping data** to Alice over a classical channel.

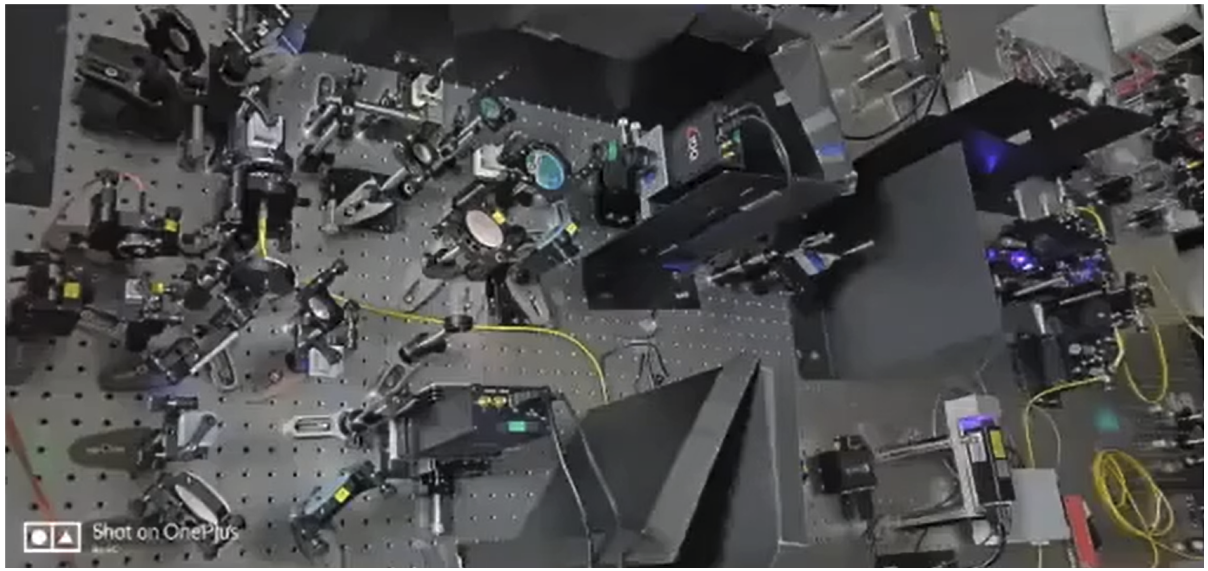
ALICE's operations:

- Compare Bob's time stamping data with her own.
- Retain only correlated events and discard the rest.

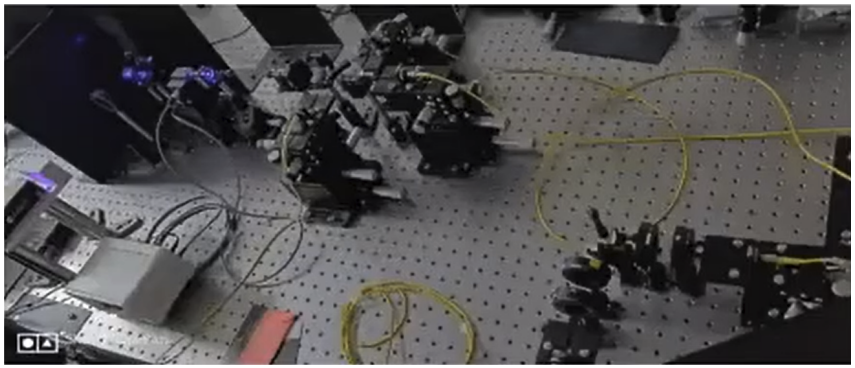
C. H. Bennett, Phys. Rev. Lett. ***68****, 21 (1992)*

Photographs of B92 Experimental Setup

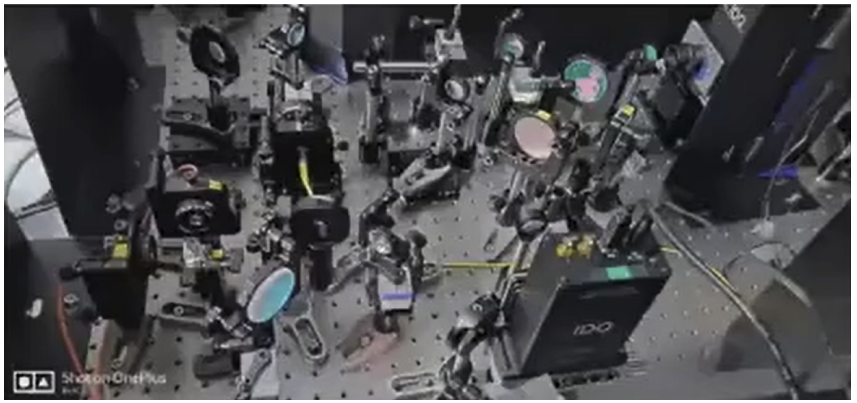
Alice and Bob setup



Alice setup

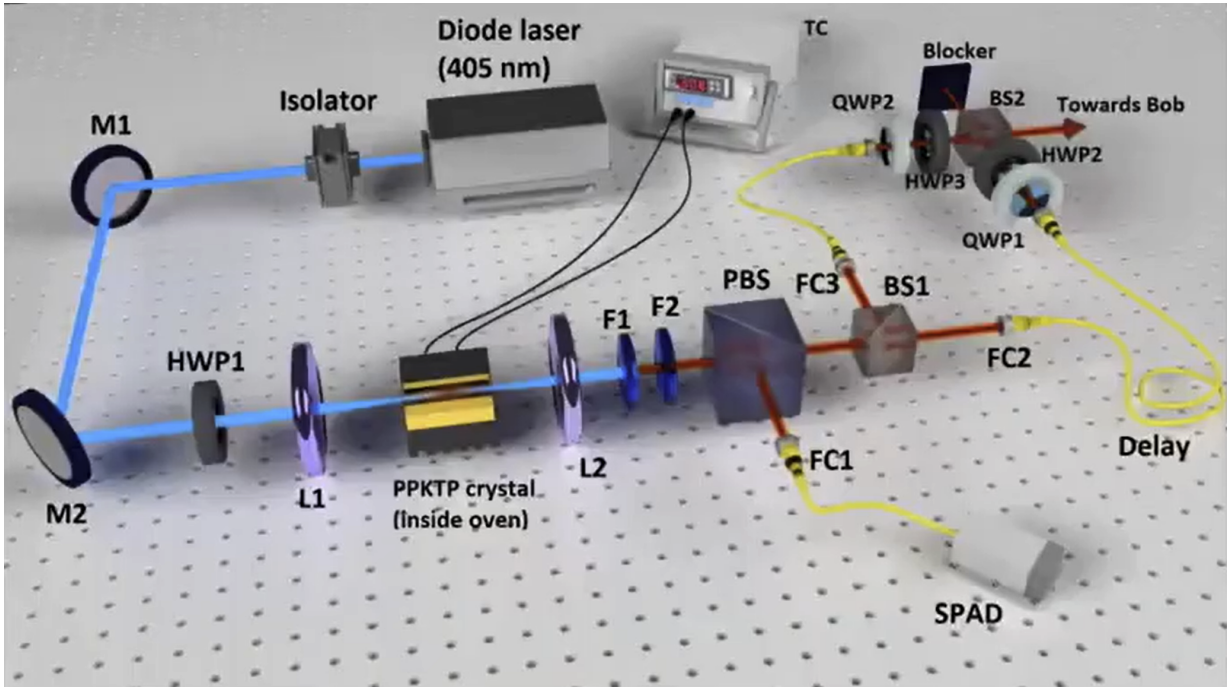


Bob setup



R. Chatterjee, K. Joarder, S. Chatterjee, B. C. Sanders, and U. Sinha, Phys. Rev. Applied ***14****, 024036*

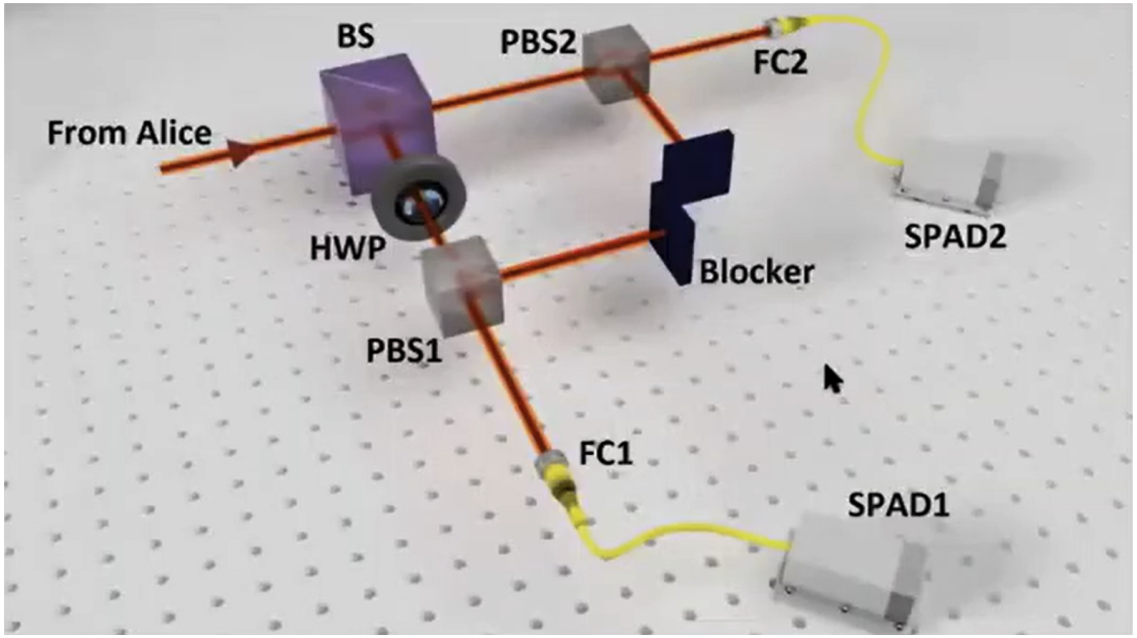
Experimental Demonstration: Alice's Setup



- **L1, L2:** Lens
- **M1, M2:** Mirrors
- **FC1, FC2, FC3:** Fiber couplers
- **HWP1, HWP2, HWP3:** Half-wave plates
- **TC:** Temperature controller
- **F1:** Long-pass filter
- **F2:** Band-pass filter
- **PBS:** Polarizing beamsplitter
- **BS1, BS2:** Beamsplitters (non-polarizing)
- **SPAD:** Single-photon avalanche detector

R. Chatterjee, K. Joarder, S. Chatterjee, B. C. Sanders, and U. Sinha, Phys. Rev. Applied ***14****, 024056*

Experimental Demonstration: Bob's Setup



- HWP: Half-wave plate
- PBS: Polarizing beamsplitter
- BS: Beamsplitter (non-polarizing)
- FC: Fiber coupler
- SPAD: Single-photon avalanche diode detector

Channel length = 2 m | Pump power = 30 mW | Crystal length = 20 mm | Temperature = 50°C

Time of Experiment	**Key Rate (kHz)**	**QBER (%)**	**Asymmetry (%)**
Day	47.8 ± 0.6	4.79 ± 0.01	50.2 ± 0.2
Night	48.1 ± 0.6	4.75 ± 0.01	50.1 ± 0.2

R. Chatterjee, K. Joarder, S. Chatterjee, B. C. Sanders, and U. Sinha, Phys. Rev. Applied ***14****, 024056*

Benchmark for B92 Setup

"To my knowledge, till date, the best available B92 setup (using SPDC source) has reported key rate of 31.6 kHz, and QBER 10.5% for 0.4 meters transmission."

Jeffrey Wilson et al., Free-space quantum key distribution with a high generation rate potassium titanyl phosphate waveguide photon-pair source, Quant. Comm. & Quant. Imag. XIV, Vol. 9980, ISOP, 99800U (2016)

QKD – Science Fiction or Reality?

- In 2009, Cambridge and Toshiba achieved secure key distribution at **1 Mbps over 20 km** of optical fiber.
- In 2017, Pan Jianwei's team distributed entangled photons over **1200 km**.
- The QUESS mission established an international QKD channel between **China and Austria**.
- The first **bank transfer using QKD** was conducted in Vienna in 2004.
- In 2007, Austrian election results were transmitted using **quantum encryption**.
- **Four companies currently offer commercial QKD tools:**
  - Toshiba (Japan)
  - ID Quantique (Switzerland)
  - QuintessenceLabs (Australia)
  - MagiQ Technologies (USA)
- **QKD is already here** — transforming secure communication.

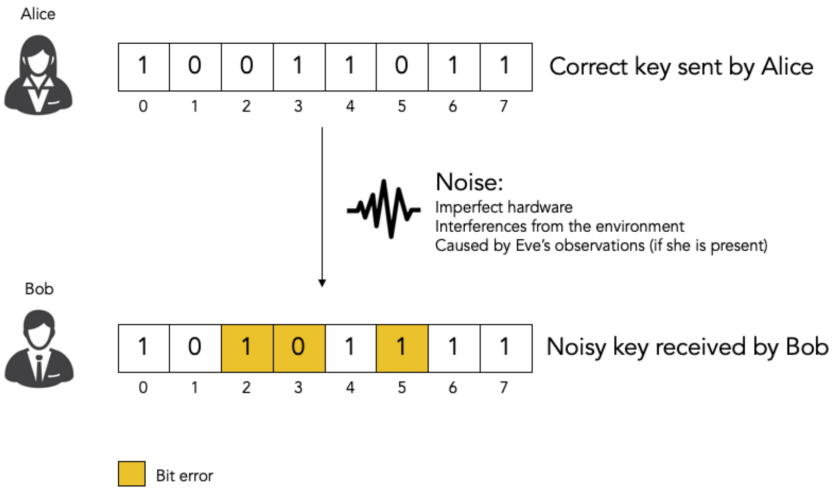
Quantum Key Distribution is no longer theoretical — it's operational.

Contributions

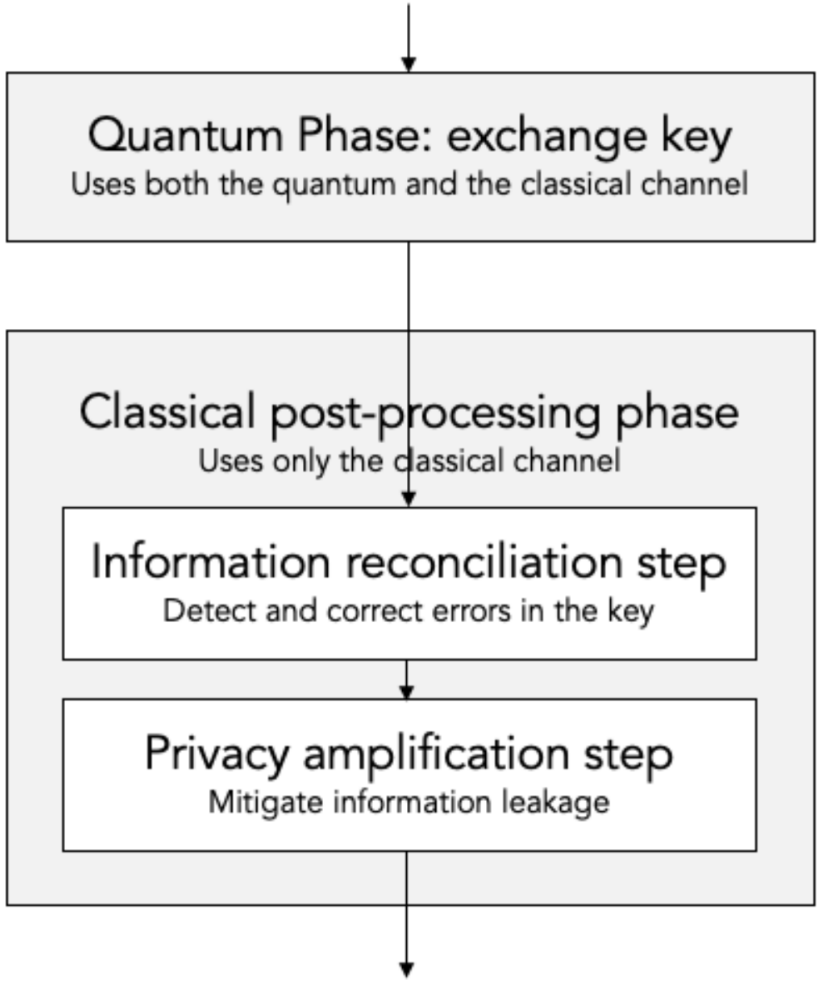
Goal: Demonstrate the B92 Quantum Key Distribution protocol and compare classical error correction schemes.

- **Quantum stage:** Simulated B92 protocol using Qiskit — generation, transmission, measurement, and sifting.
- **Channel modelling:** Added depolarizing and bit-flip noise, plus intercept-resend eavesdropper to study QBER.
- **Post-processing:**
  - Error estimation (QBER)
  - Error correction: Cascade, Hamming (15,11), LDPC
  - Privacy amplification via Toeplitz hashing
- **Performance metrics:** Key rate, residual error rate, and leakage.
- **Visualization:** Plots and tables comparing schemes across QBER levels.

Information Reconciliation in QKD



Bit Errors in Quantum Key Transmission



Error Correction Flowchart

Images adapted from the Cascade protocol documentation

https://cascade-python.readthedocs.io/en/latest/protocol.html#parallelization-and-bulking

Cascade Error Correction

Cascade is an interactive protocol that corrects bit errors using parity checks and iterative refinement.

- Divides the sifted key into blocks and compares parities over a public channel.
- Uses binary search to locate and correct mismatched bits.
- Performs multiple passes to catch residual errors and improve efficiency.

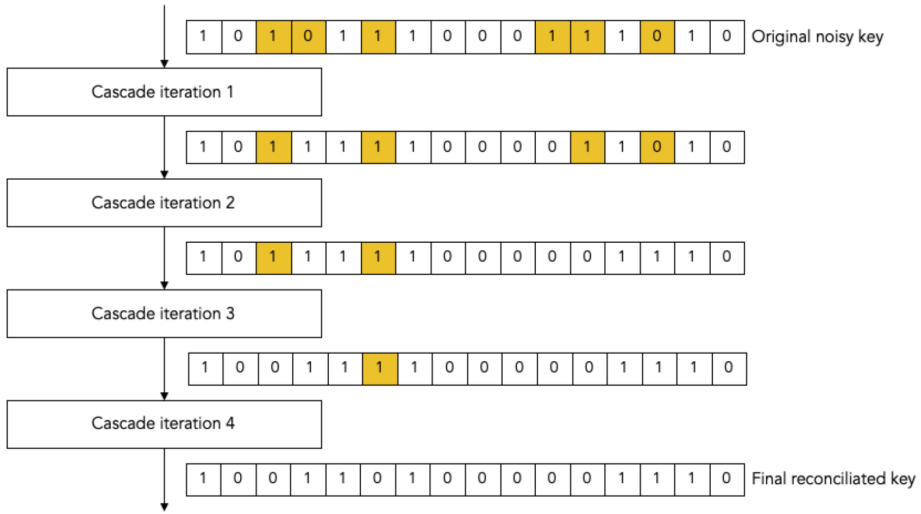


Figure: Cascade protocol correcting bit errors over multiple iterations.

Pros: Reliable for moderate QBER, no need for pre-shared codebooks.
Cons: Communication-heavy and slower for large keys.

Image adapted from the Cascade protocol documentation

https://cascade-python.readthedocs.io/en/latest/protocol.html#parallelization-and-bulking

Hamming (15,11) Error Correction

Hamming (15,11) is a block code that encodes 11 bits into 15, allowing single-bit error correction.

- High-Density Encoding Technique
- Uses parity bits to detect and correct one error per block.
- Fast and lightweight — only ideal for low-noise channels.
- Performs structured parity checks to locate the error position.

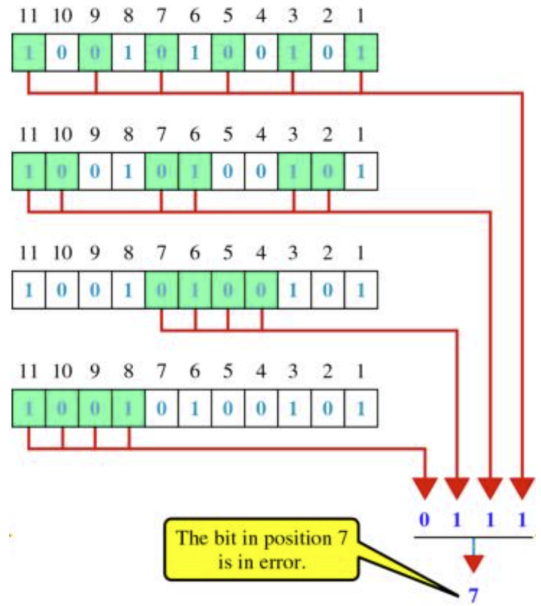


Figure: Hamming code detects and corrects a single-bit error using parity logic.

Pros: Simple, low computational cost, minimal leakage.
Cons: Limited to correcting only one error per block — not suitable for high QBER.

Image adapted from

https://www.slideserve.com/tahir/error-detection-and-correction

LDPC Error Correction

Low-Density Parity-Check (LDPC) codes use sparse matrices and iterative decoding to correct errors.

- Belief-propagation algorithm estimates bit values based on parity constraints.
- Well-suited for high-speed QKD and scalable systems.
- Developed in the 1960s by Robert G. Gallager, LDPC codes regained prominence in the 2000s for outperforming Turbo codes.

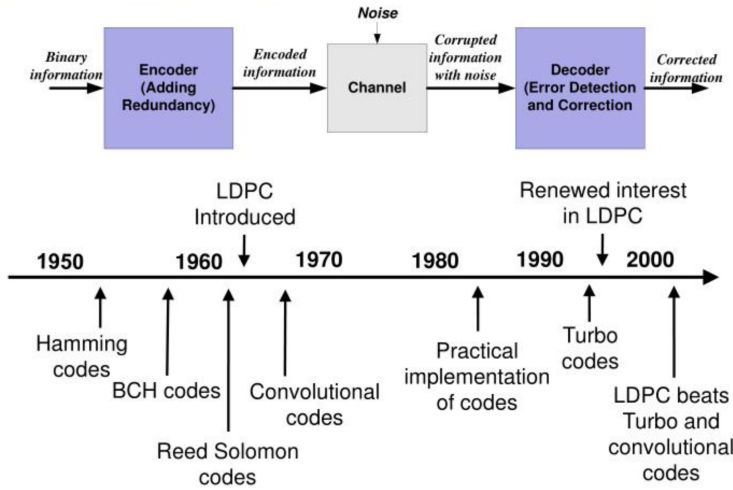


Figure: LDPC codes in communication systems — timeline and decoding flow.

Pros: High correction power, low leakage, efficient for large keys.
Cons: Requires careful matrix design and more computation.

Image adapted from

https://www.slideserve.com/pilis/error-correction-and-ldpc-decoding

LDPC Error Correction

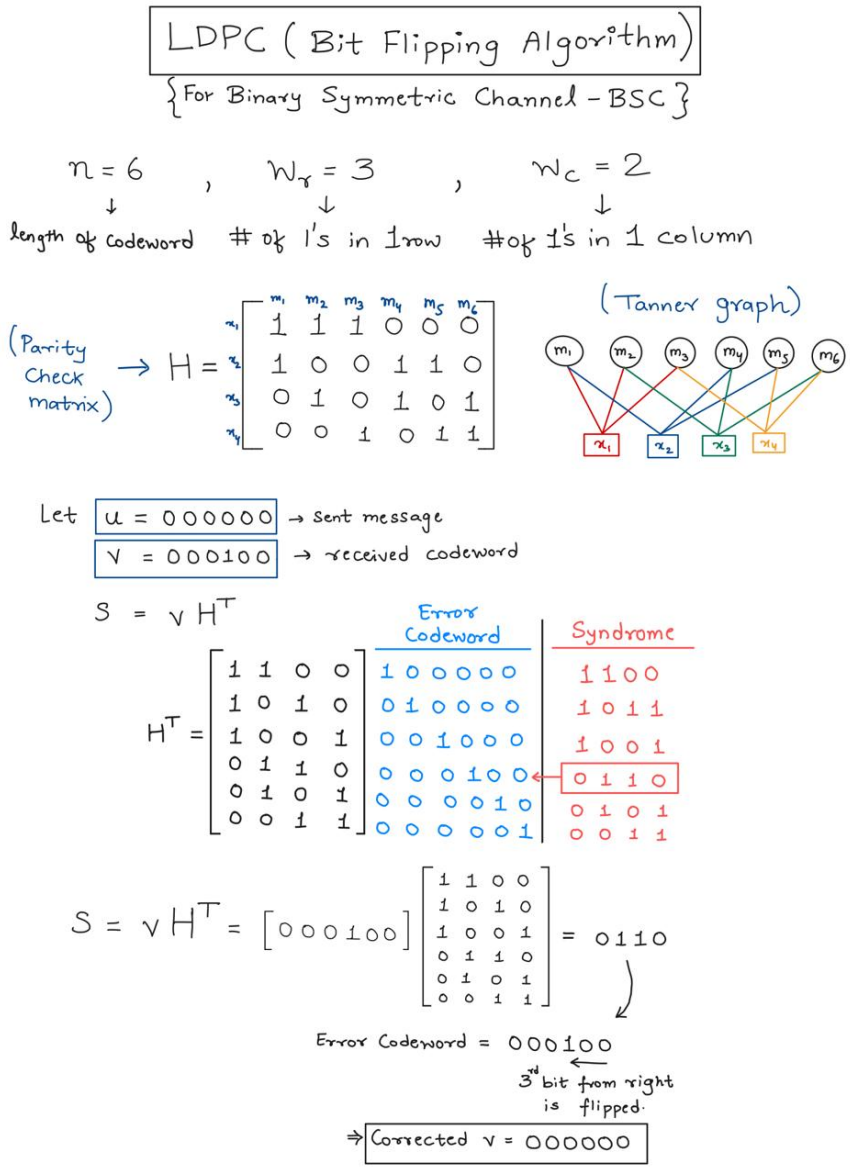
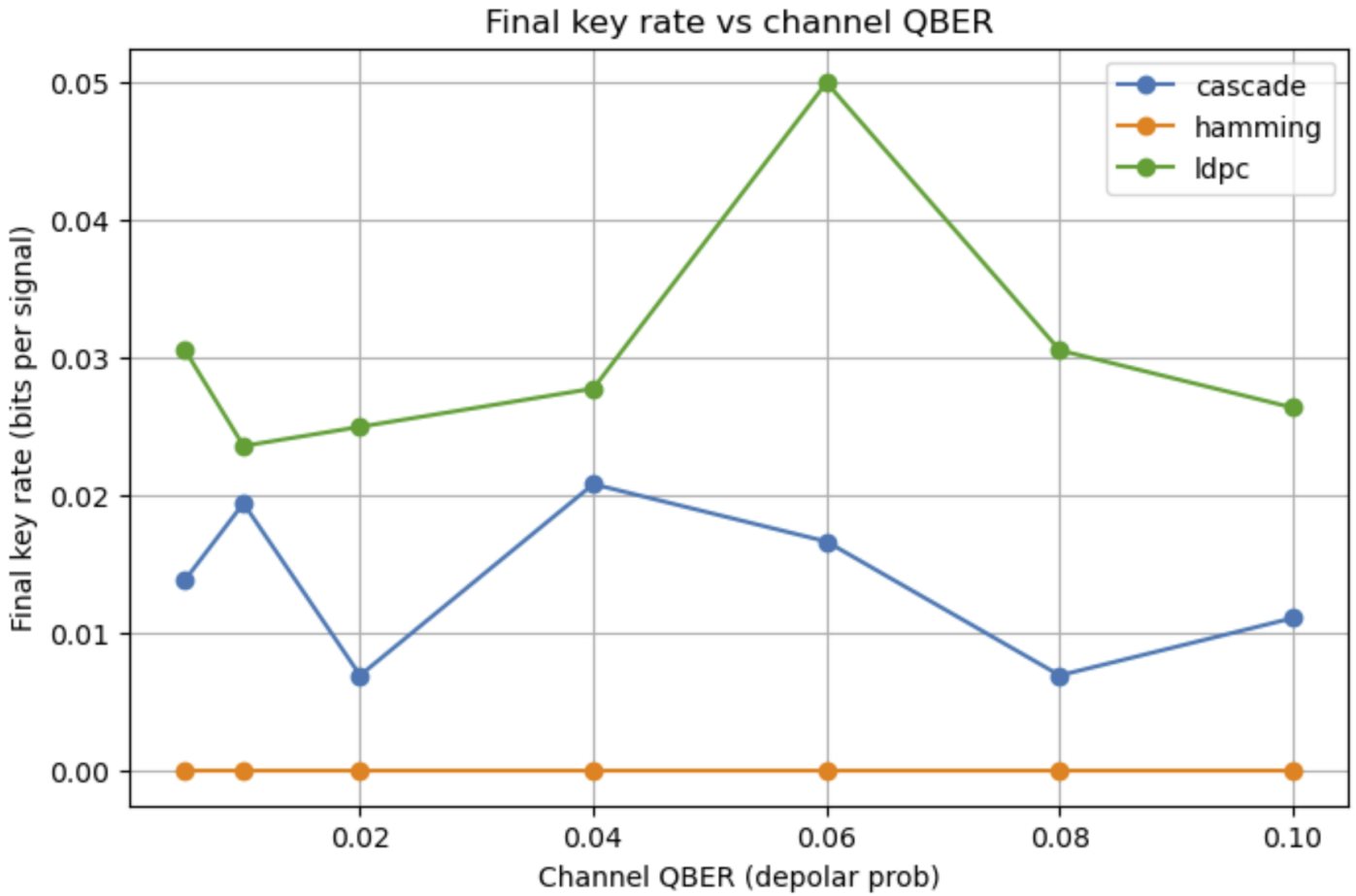


Figure: LDPC decoding using bit-flipping algorithm and parity-check matrix.

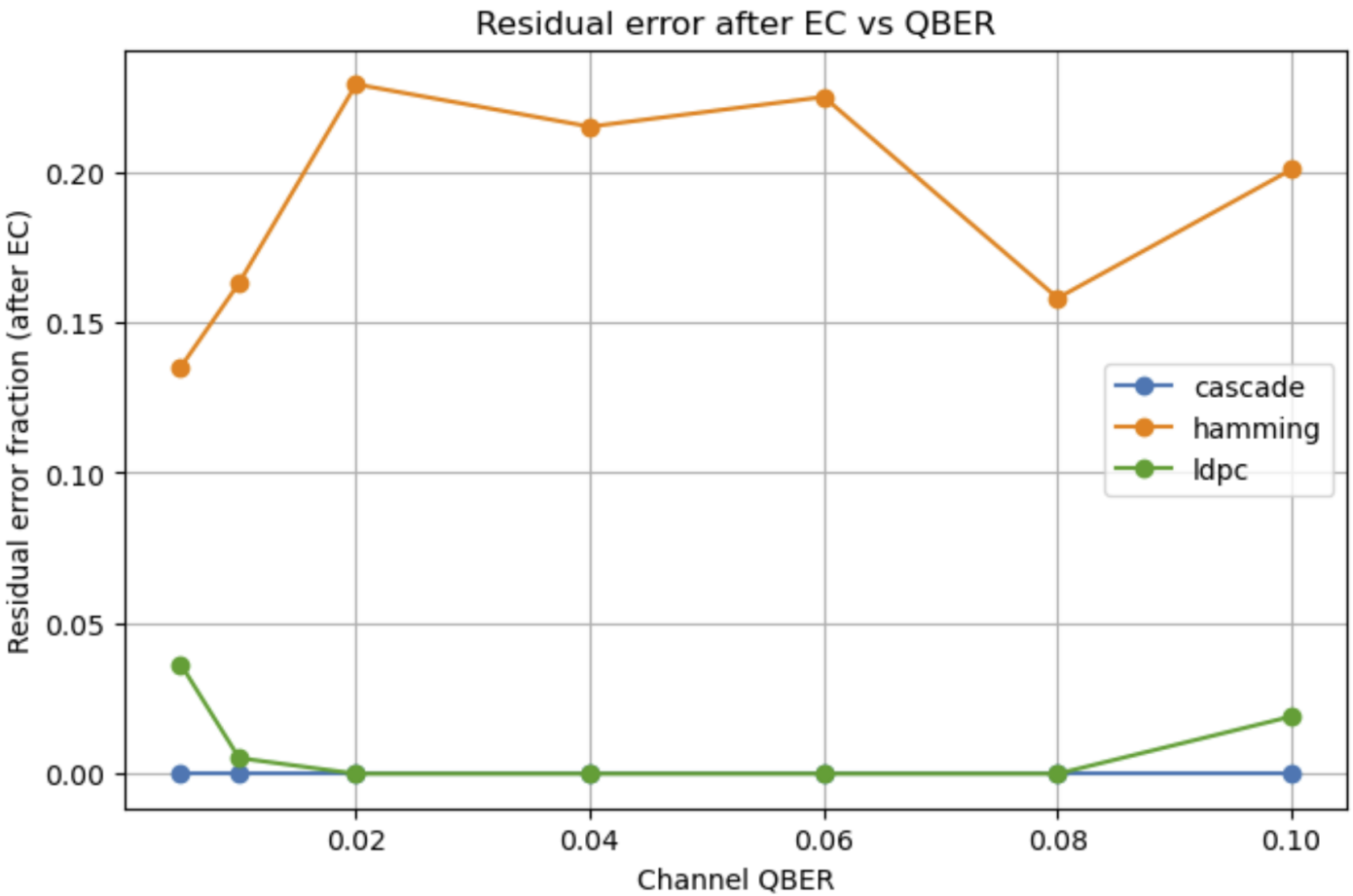
Results: Final Key Rate vs Channel QBER

The graph below compares the performance of the **Cascade, Hamming, and LDPC** error correction protocols across varying channel **QBER** values. **LDPC** consistently achieves the highest final key rate, especially in moderate noise regimes.



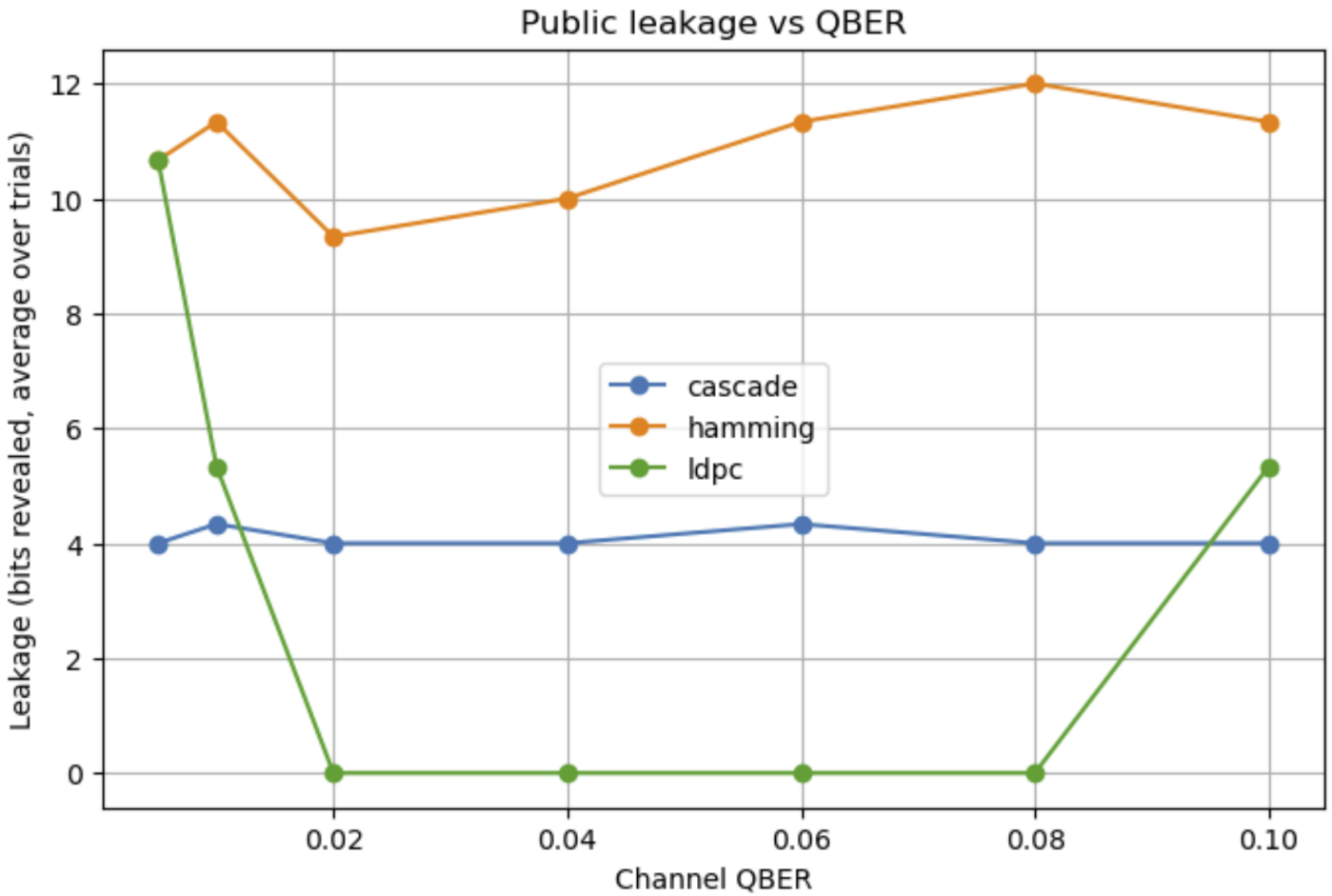
Results: Residual Error vs Channel QBER

The graph below shows how residual error after error correction varies with channel QBER. **LDPC** and **Cascade** protocols maintain low residual error across all QBER levels, while **Hamming** exhibits significantly higher residual error, especially as **QBER** increases.



Results: Public Leakage vs Channel QBER

The graph below illustrates how public leakage varies with channel QBER across different error correction protocols. **LDPC** demonstrates minimal leakage at low QBER, while **Hamming** consistently leaks more information. **Cascade** maintains moderate leakage across all QBER levels.



References

- C. H. Bennett, G. Brassard, and N. D. Mermin, *Quantum cryptography without Bell's theorem*, Phys. Rev. Lett. 68, 3121. `https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.68.3121`
- Jeffrey Wilson et al., *Free-space quantum key distribution with a high generation rate potassium titanyl phosphate waveguide photon-pair source*, Quant. Comm. Quant. Imag. XIV, Vol. 9980, ISOP, 99800U (2016).
- R. Chatterjee, K. Joarder, S. Chatterjee, B. C. Sanders, and U. Sinha, *Experimental demonstration of quantum advantage in communication complexity*, Phys. Rev. Applied 14, 024056.
- R. G. Gallager, *Low-density parity-check codes*, IRE Trans. Inf. Theory, vol. 8, no. 1, pp. 21–28, 1962.
- D. Elkouss, J. Martinez-Mateo, and V. Martin, *Information reconciliation for quantum key distribution*, Quantum Information Computation, vol. 11, no. 3–4, pp. 226–238, 2011.
- M. Tomamichel et al., *Leftover Hashing Against Quantum Side Information*, IEEE Trans. Inf. Theory, vol. 57, no. 8, pp. 5524–5535, 2011.
- H. Xu et al., *Experimental quantum key distribution with LDPC codes*, Optics Express, vol. 20, no. 11, pp. 12366–12373, 2012.
- M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, Cambridge University Press, 2011.
- N. Lütkenhaus, *Security against individual attacks for realistic quantum key distribution*, Phys. Rev. A 61, 052304 (2000).