Hands-On Workshop on Quantum Cryptography

Mohammad Saidur Rahman Ph.D.
Jesus R. Lopez Viviana Cadena

https://rahmanmsaidur.com/



UTEP
Computer Science

Learning objectives

- Explain the key-establishment problem and the quantum threat to RSA/ECC.
- Distinguish post-quantum cryptography (PQC) from quantum cryptography.
- Use polarization states and measurement probabilities to explain BB84.
- Derive the ideal intercept–resend quantum bit error rate (QBER).
- Perform four optical/key-distribution exercises and interpret their limitations.

Why do we need cryptography?

Security goals

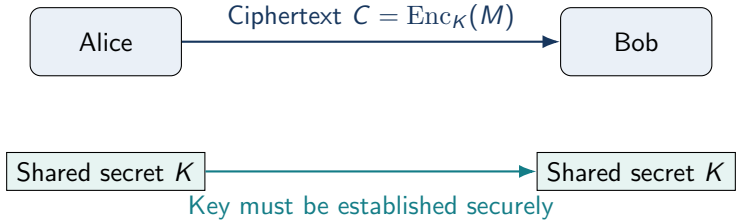
- Confidentiality: prevent unauthorized reading.
- Integrity: detect unauthorized modification.
- Authentication: establish who is communicating.

A recurring challenge

Alice and Bob want to communicate securely over an insecure network.

Encryption is only useful if keys can be established and managed securely.

Symmetric encryption: one shared key



Examples: AES-GCM for authenticated encryption; the main challenge is securely obtaining K.

Public-key cryptography: two related keys

Key pair

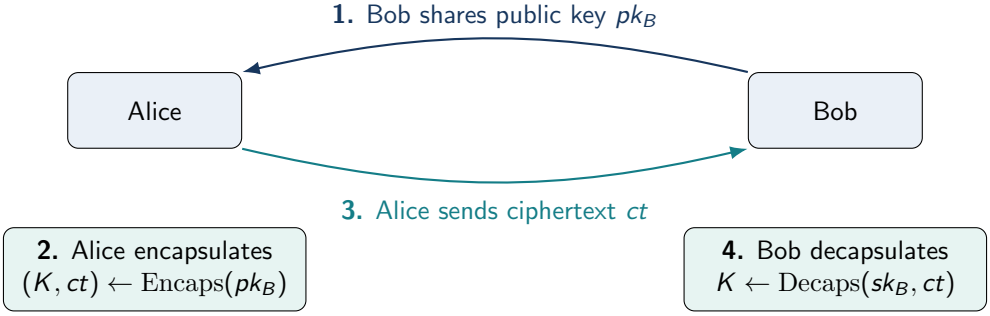
- Public key pk: may be distributed.
- Private key sk: must remain secret.
- Public-key encryption, key encapsulation, and signatures serve different purposes.

Basic idea

$$C = \mathrm{Enc}_{pk}(M), \quad M = \mathrm{Dec}_{sk}(C)$$

In practice, hybrid encryption establishes a symmetric session key, then uses AES or another symmetric cipher for data.

How public-key key establishment works



Security requirement: Bob's public key must be authenticated to prevent man-in-the-middle attacks.

Why RSA was considered secure

RSA mathematical structure

Choose primes p, q and compute $N = pq$. Public parameters include (N, e); private exponent d satisfies $ed \equiv 1 \pmod{\varphi(N)}$.

Classical hardness assumption

For properly generated large RSA moduli, recovering the private key is computationally infeasible using known classical attacks.

Factoring N reveals p, q and hence $\varphi(N)$.

Elliptic-curve cryptography (ECC)

Core operation	Security assumption
Given point P and secret integer x, compute $Q = xP$. $$\underbrace{P + P + \cdots + P}_{x \text{ times}} = Q$$	Recovering x from P, Q is the elliptic-curve discrete logarithm problem. ECDH uses related operations to establish shared secrets; ECDSA uses elliptic-curve signatures.

What protects RSA and ECC today?

- Their security is based on the difficulty of specific mathematical problems for known feasible classical computers.
- RSA: integer factorization is closely related to recovering the private key.
- ECC: elliptic-curve discrete logarithms.
- A cryptosystem can fail when a faster algorithm or new computing model changes the attack cost.

Question

What happens if an adversary can run a sufficiently powerful fault-tolerant quantum computer?

Quantum computing changes the attack model

Classical attack model

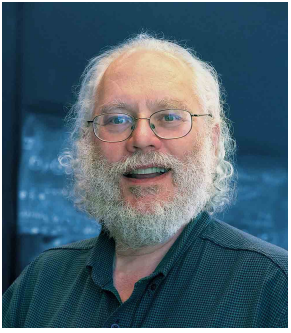
Best known practical classical methods
do not efficiently solve RSA/ECC problems

Quantum attack model

Shor's algorithm solves factoring and
discrete logarithms in polynomial time

Note: A quantum algorithm is not simply a faster implementation of a classical algorithm.

1994: Shor's Algorithm Changed Cryptography



Peter W. Shor

MIT

quant-ph/9508027v2 25 Jan 1996

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

Keywords: algorithmic number theory, prime factorization, discrete logarithms, Church's thesis, quantum computers, foundations of quantum mechanics, spin systems, Fourier transforms

Shor's Landmark Paper

FOCS 1994; proceedings published 1995

A sufficiently powerful quantum computer can factor integers and solve discrete logarithms efficiently.

Shor's algorithm: the main public-key threat

- Shor's algorithm gives polynomial-time quantum algorithms for factoring and discrete logarithms.
- A sufficiently large, fault-tolerant quantum computer would undermine widely deployed RSA, finite-field DH, and ECC.
- Current quantum devices are not capable of breaking properly sized deployed RSA/ECC at scale.
- The relevant uncertainty is when cryptographically relevant quantum computers become available.

Security consequence

Public-key encryption/key exchange and signatures need quantum-resistant replacements.

Grover's algorithm and symmetric cryptography

Unstructured search

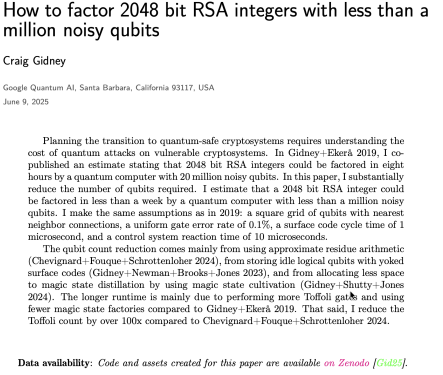
Grover gives a quadratic query speedup in the ideal black-box model.

Classical: $O(2^k)$ Quantum: $O(2^{k/2})$

Practical interpretation

- It does not break AES in the same way Shor threatens RSA/ECC.
- Larger symmetric key sizes help maintain security margins.
- Resource costs and parallelization matter.

How Close Are Quantum Computers to Breaking RSA?



How to factor 2048 bit RSA integers with less than a million noisy qubits

Craig Gidney

Google Quantum AI, Santa Barbara, California 93117, USA

June 9, 2025

Planning the transition to quantum-safe cryptosystems requires understanding the cost of quantum attacks on vulnerable cryptosystems. In Gidney+Ekerå 2019, I co-published an estimate stating that 2048 bit RSA integers could be factored in eight hours by a quantum computer with 20 million noisy qubits. In this paper, I substantially reduce the number of qubits required. I estimate that a 2048 bit RSA integer could be factored in less than a week by a quantum computer with less than a million noisy qubits. I make the same assumptions as in 2019: a square grid of qubits with nearest neighbor connections, a uniform gate error rate of 0.1%, a surface code cycle time of 1 microsecond, and a control system reaction time of 10 microseconds.

The qubit count reduction comes mainly from using approximate residue arithmetic (Chevignard+Fouque+Schrottenloher 2024), from storing idle logical qubits with yoked surface codes (Gidney+Newman+Brooks+Jones 2023), and from allocating less space to magic state distillation by using magic state cultivation (Gidney+Shutty+Jones 2024). The longer runtime is mainly due to performing more Toffoli gates and using fewer magic state factories compared to Gidney+Ekerå 2019. That said, I reduce the Toffoli count by over 100x compared to Chevignard+Fouque+Schrottenloher 2024.

Data availability: *Code and assets created for this paper are available on Zenodo [Gid25].*

Craig Gidney, Google Quantum AI (2025)

RSA-2048: Estimated Quantum Attack Cost

- **2019 estimate:** 20 million physical qubits, 8 hours.
- **2025 estimate:** Fewer than 1 million physical qubits, less than one week.
- **Key insight:** Algorithmic and error-correction advances substantially reduce required resources.

These are theoretical resource estimates, not demonstrated RSA-2048 breaks.

Harvest now, decrypt later (HNDL)



An attacker may collect encrypted sessions now and decrypt them later if the recorded key establishment becomes vulnerable.

Long-lived secrets require protection before a cryptographically relevant quantum computer exists.

Which cryptographic functions are affected?

Function	Typical current approach	Quantum-era response
Key establishment	RSA / (EC)DH	Quantum-resistant KEM; QKD in specialized settings
Digital signatures	RSA / ECDSA	Quantum-resistant signatures
Bulk encryption	AES	Maintain adequate symmetric key strength
Hash functions	SHA-2 / SHA-3	Review output lengths and threat models

Key point: replacing key establishment does not automatically replace authentication or digital signatures.

2026: U.S. Executive Order on Quantum Security



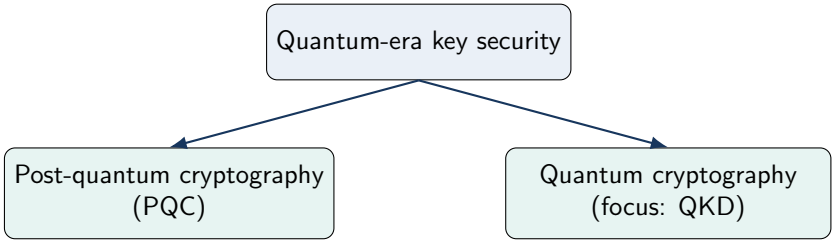
Executive Order 14412

June 22, 2026

- Recognizes the threat of quantum computers to existing cryptography.
- Highlights **harvest-now, decrypt-later** attacks.
- Directs federal migration to **NIST-approved PQC standards**.
- Prioritizes sensitive information and critical infrastructure.

Quantum-safe cryptography is now a national cybersecurity priority.

Two approaches to quantum-resistant key establishment



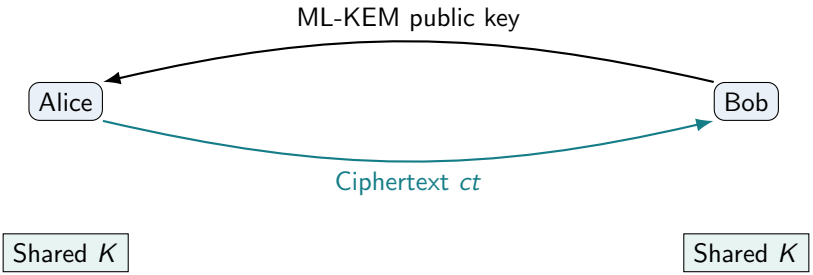
What is post-quantum cryptography?

- PQC consists of classical cryptographic algorithms designed to resist known classical and quantum attacks.
- It runs on ordinary computers and classical networks.
- Security remains computational and depends on mathematical assumptions and correct implementation.
- NIST standards include ML-KEM (FIPS 203), ML-DSA (FIPS 204), and SLH-DSA (FIPS 205).

Important distinction

PQC does not require transmitting qubits or using quantum hardware.

PQC: what happens during key establishment?



Both sides derive the same symmetric secret using classical messages. Public-key authentication and protocol integration are still necessary.

What is quantum cryptography?

- Quantum cryptography uses quantum-information phenomena in cryptographic protocols.
- Quantum key distribution (QKD) is its best-known application.
- In QKD, Alice sends quantum states; Bob measures them; both use an authenticated classical channel for post-processing.
- QKD establishes shared key material; it does not itself encrypt application data.

Focus of this workshop

We study prepare-and-measure BB84 QKD using photon polarization as the intuitive encoding.

PQC versus QKD: what is actually different?

Property	PQC	QKD
Medium	Classical networks	Quantum + authenticated classical
Equipment	Conventional hardware	Quantum optical hardware
Security model	Computational assumptions	Information-theoretic under defined device/channel assumptions
Primary function	KEMs, signatures, etc.	Key distribution
Deployment	Broad software migration	Specialized physical infrastructure

Neither approach removes the need for authentication, correct implementations, or sound key management.

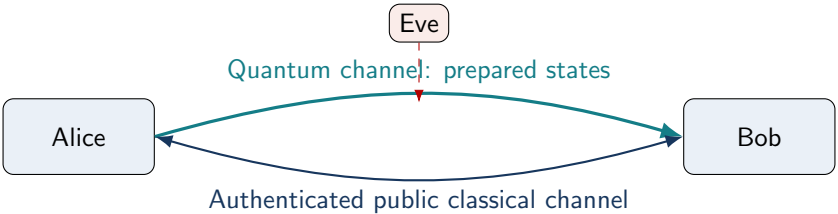
Why study QKD if PQC already exists?

- QKD provides a distinct security model for key establishment: information leakage can be bounded using quantum observations.
- It is a concrete application of quantum mechanics to a security protocol.
- It reveals how incompatible measurements and no-cloning constrain an eavesdropper.
- It also exposes important engineering tradeoffs: losses, detector behavior, authentication, distance, and cost.

Balanced perspective

PQC is the principal general-purpose migration path; QKD can be appropriate in selected high-assurance link scenarios.

The key-distribution problem revisited



Eve may observe, block, replace, or manipulate quantum signals; authenticated classical discussion prevents undetected impersonation.

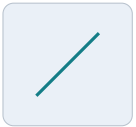
The four BB84 polarization states



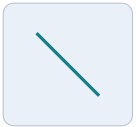
Horizontal $|0\rangle$



Vertical $|1\rangle$



Diagonal $|+\rangle$



Anti-diagonal $|-\rangle$

$$Z = \{|0\rangle, |1\rangle\}, \qquad X = \{|+\rangle, |-\rangle\}$$

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Qubit states and polarization

State representation

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$|\alpha|^2 + |\beta|^2 = 1$$

Polarization provides one physical encoding of a qubit.

Measurement

In the Z basis, outcomes $0, 1$ occur with probabilities $|\alpha|^2, |\beta|^2$.

A measurement generally changes the post-measurement state.

Why the choice of basis matters

If Alice prepares $|0\rangle$ but Bob measures in the X basis,

$$|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}}$$

$$P(+ \mid |0\rangle) = |\langle +|0\rangle|^2 = \tfrac{1}{2}, \quad P(- \mid |0\rangle) = \tfrac{1}{2}.$$

Interpretation

Matching preparation and measurement bases yield the intended bit ideally; mismatched bases produce unbiased random outcomes.

Predict the measurement outcome



1. Can Bob deterministically infer Alice's bit?
2. What are the two possible outcomes?
3. What is the probability of each outcome?

The No-Cloning Theorem

Suppose a universal unitary cloner could copy arbitrary quantum states:

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle,$$
$$U|\phi\rangle|0\rangle = |\phi\rangle|\phi\rangle.$$

Since unitary operations preserve inner products,

$$\boxed{\langle\psi|\phi\rangle = \langle\psi|\phi\rangle^2}$$

Thus the overlap must be 0 or 1.

But distinct nonorthogonal states have

$$0 < |\langle\psi|\phi\rangle| < 1.$$

Orthogonal states



Possible for a known orthogonal set

Nonorthogonal states



Perfect universal cloning is impossible

An unknown arbitrary quantum state cannot be perfectly copied by a universal device.

BB84 state preparation: the encoding rule

Alice bit	Basis	State	Polarization
0	Z	$\|0\rangle$	Horizontal (0°)
1	Z	$\|1\rangle$	Vertical (90°)
0	X	$\|+\rangle$	Diagonal (45°)
1	X	$\|-\rangle$	Anti-diagonal (135°)

Alice independently chooses a random bit and random basis for each signal. Bob independently chooses a measurement basis.

BB84 overview: five logical steps



1. Prepare states with random bits and bases.
2. Send quantum signals; Bob measures in random bases.
3. Publicly compare bases and retain matches.
4. Estimate errors on a sample.
5. Reconcile errors, authenticate discussion, and apply privacy amplification.

Worked example: Alice prepares eight signals

Position	1	2	3	4	5	6	7	8
Alice bit	0	1	1	0	1	0	0	1
Alice basis	Z	X	Z	X	X	Z	X	Z
Prepared state	$\|0\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$

The bases and bit values are independently and randomly chosen. The prepared states are transmitted through the quantum channel.

Worked example: Bob measures

Position	1	2	3	4	5	6	7	8
Alice bit	0	1	1	0	1	0	0	1
Alice basis	Z	X	Z	X	X	Z	X	Z
Bob basis	Z	Z	Z	X	Z	X	X	Z
Bob outcome	0	0	1	0	1	1	0	1

Mismatched-basis outcomes are illustrative random realizations. Matching-basis outcomes agree in this ideal, no-noise example.

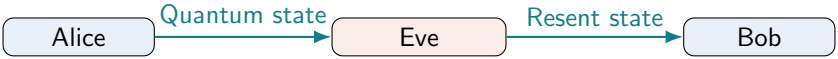
Worked example: public basis sifting

Position	1	2	3	4	5	6	7	8
Alice basis	Z	X	Z	X	X	Z	X	Z
Bob basis	Z	Z	Z	X	Z	X	X	Z
Keep?	Yes	No	Yes	Yes	No	No	Yes	Yes
Alice retained	0	–	1	0	–	–	0	1
Bob retained	0	–	1	0	–	–	0	1

$$\text{Sifted strings} = 01001$$

This toy string is not yet a secure final key: parameter estimation, reconciliation, and privacy amplification are still required.

Why eavesdropping changes the statistics



Eve chooses a basis
and measures

When Eve measures in the wrong basis, she disturbs the state. If Bob uses Alice's original basis, his result can disagree with Alice's bit.

Deriving the ideal intercept–resend QBER

Condition on a sifted position: Bob's basis matches Alice's.

$$P(\text{Eve chooses wrong basis}) = \frac{1}{2}$$

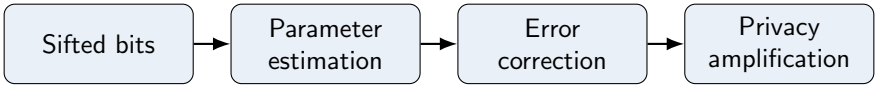
$$P(\text{Bob error} \mid \text{Eve wrong}) = \frac{1}{2}$$

$$\boxed{\text{QBER} = \frac{1}{2} \times \frac{1}{2} = \frac{1}{4} = 25\%}$$

Scope of the result

This is the expected QBER for an ideal, full intercept–resend attack with random Eve bases and otherwise noiseless equipment. It is not a universal eavesdropping signature.

From sifted bits to a usable secret key



Error correction reconciles Alice's and Bob's strings but leaks some information through public messages. Privacy amplification compresses the reconciled string to limit Eve's information.

Abort if the observed statistics do not support a secure key length.

What QKD security does not guarantee

- QKD does not eliminate the need for authenticated classical communication.
- Real implementations can leak information through sources, detectors, side channels, and imperfect random number generators.
- Losses, finite-key effects, and calibration errors limit achievable key rates.
- Classical polarization intensity demonstrations illustrate optics, not full single-photon QKD security.

Lecture takeaway

QKD security is a protocol-level statement under explicit physical, device, and adversary assumptions.

Quantum Key Distribution Protocols

Quantum Key Distribution is based on the **principles of quantum mechanics** to generate a shared secret between two parties through a quantum channel. It relies on the **no-cloning** theorem which any attempt at **eavesdropping** introduces detectable disturbances.

Quantum Key Distribution Protocols

QKD protocols generally consist of two main phases:

- **Quantum transmission phase**: Quantum states are transmitted and measured by the communicating parties.
- **Post-processing phase**: The raw bit strings obtained from the quantum transmission phase are processed using classical algorithms for error correction and privacy amplification. Ultimately producing a pair of identical and secure cryptographic keys.

Polarization Bases in Quantum Key Distribution

The polarization of photons forms the foundation for encoding information in Quantum Key Distribution. Information is represented using the polarization states of individual photons. Two primary polarization bases are used.

Rectilinear Basis (+)

This basis includes horizontal (0°) and vertical (90°) polarizations.

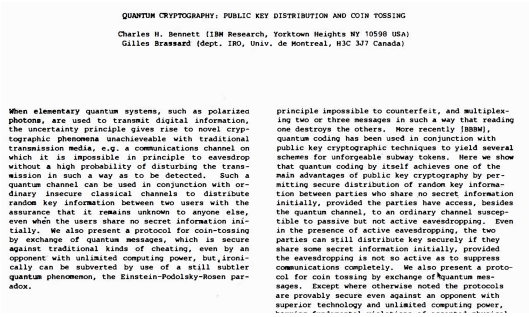
Diagonal Basis (X)

This basis includes polarizations at 45° and 135° angles.

Types of QKD Protocols

- **Discrete-variable protocols:** These include BB84, B92, E91 and SARG04, where individual quantum states are used to encode information.
- **Continuous-variable protocols (CV-QKD):** These protocols use continuous properties of lights such as the quadratures of the electromagnetic field, to encode key information.
- **Distributed-phase-reference protocols:** Examples include coherent One-Way (COW) and Differential Phase shift (DPS), which rely on the phase differences between pulses rather than individual quantum states.

BB84: Introduction

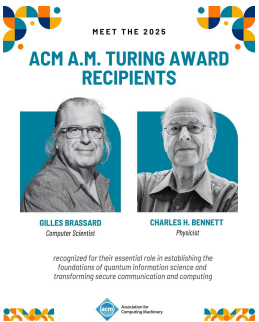


QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING

Charles H. Bennett (IBM Research, Yorktown Heights NY 10598 USA)
Gilles Brassard (dept. IRO, Univ. de Montreal, H3C 3J7 Canada)

When elementary quantum systems, such as polarized photons, are used to transmit digital information, the uncertainty principle gives rise to novel cryptographic phenomena unachieveable with traditional transmission media, e.g. a communications channel on which it is impossible in principle to eavesdrop without a high probability of disturbing the transmission in such a way as to be detected. Such a quantum channel can be used in conjunction with ordinary insecure classical channels to distribute random key information between two users with the assurance that it remains unknown to anyone else, even when the users share no secret information initially. We also present a protocol for coin-tossing by exchange of quantum messages, which is secure against traditional kinds of cheating, even by an opponent with unlimited computing power, but ironically can be subverted by use of a still subtler quantum phenomenon, the Einstein-Podolsky-Rosen paradox.

principle impossible to counterfeit, and multiplexing two or three messages in such a way that reading one destroys the others. More recently [BBBW], quantum coding has been used in conjunction with public key cryptographic techniques to yield several schemes for unforgeable subway tokens. Here we show that quantum coding by itself achieves one of the main advantages of public key cryptography by permitting secure distribution of random key information between parties who share no secret information initially, provided the parties have access, besides the quantum channel, to an ordinary channel susceptible to passive but not active eavesdropping. Even in the presence of active eavesdropping, the two parties can still distribute key securely if they share some secret information initially, provided the eavesdropping is not so active as to suppress communications completely. We also present a protocol for coin tossing by exchange of quantum messages. Except where otherwise noted the protocols are provably secure even against an opponent with superior technology and unlimited computing power,



BB84 Protocol (1984) **2025 ACM A.M. Turing Award**

- Proposed by **Charles Bennett and Gilles Brassard** in 1984.
- The most widely recognized QKD protocol.
- Uses quantum states to establish a shared secret key and detect eavesdropping-induced disturbances.

BB84: How does it work?

1. **Alice Sends Qubits**
   Alice randomly selects a bit value (0 or 1)for each qubit and randomly chooses a basis for encoding each qubit: rectilinear or diagonal. Using these selections she prepares and send a stream of quibits to bob over a quantum channel.
2. **Bob Measures the Qubits**
   Bob independently and randomly selects basis to measure the incoming qubit.
3. **Public Basis Comparison**
   After the qubits are measured, Alice and Bob compare only the bases they used. They discard all bits where their bases did not match and the remaining bits form a raw key.

BB84: How does it work? (cont.)

4. **Error checking**
   Alice and bob publicly compare a random subset of their raw key to check for discrepancies. If an eavesdropper attempted to intercept and measure the qubits, her actions would introduce detectable errors due to the no-cloning theorem and measurement disturbance.
5. **Post-Processing**
   - **Error correction:** Alice and Bob apply classical error correction techniques to resolve any remaining discrepancies.
   - **Privacy amplification:** They apply privacy amplification methods to distill a final secret key.

BB84

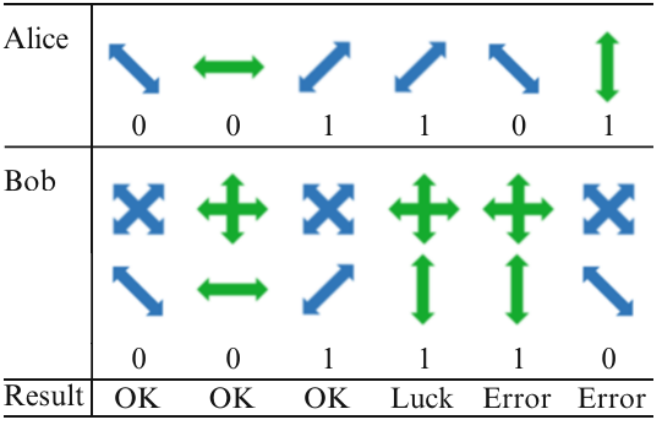


Figure from the book Quantum Key Distribution Networks: A Quality of Service Perspective

BB84: Eavesdropping

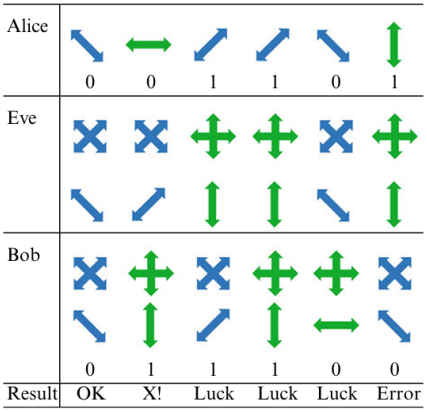


Figure from the book Quantum Key Distribution Networks: A Quality of Service Perspective

Laboratory activities: Thorlabs demonstration kit

1. **Simulating BB84 Protocol** — Generate a sifted key on paper; encrypt and decrypt two letters using bitwise XOR.
2. **Introduction to Polarization and Bases** — Change Alice's and Bob's polarizer angles and observe transmitted light.
3. **Simulating BB84 Protocol with Hardware** — Generate a key with the optical kit, transmit encrypted bits, and recover two letters.
4. **Eavesdropping Experiment** — Introduce Eve's intercept–resend measurements and compare Alice's and Bob's sifted bits.

Follow the separate laboratory handout for procedures and recording tables.

Activities

4 activities in total for both days at lab.
A couple of reminders:

- **Use gloves at all time** when operating lab equipment.
- If you have any question do not hesitate to **ask** Jesus or Dr. Rahman.
- **Do not touch the lenses** only the rings.

Activity: Introduction to Polarization and Bases

Objective

Understand how polarization represents quantum states and how measurement in different bases affect results

Instructions (Alice)

1. Set Alice lens to 0°.

3. Repeat, but now change Alice lens from 0° to 45°

Instructions (Bob)

2. Set Bob lens at:
   - 0°
   - 90°
   - 45°

Activity: Simulating BB84 Protocol

Objective

Simulate Key generation using the BB84 quantum key distribution protocol.

Instructions

1. We are going to be tracing the encryption of two letters using basis and bits.
2. Follow the instructions on the hands-on
3. Answer the questions that are at the end of the activity.

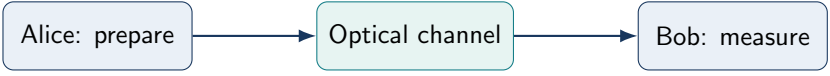
Activity: Simulating BB84 with hardware

Objective

Simulate Key generation using the BB84 quantum key distribution protocol.

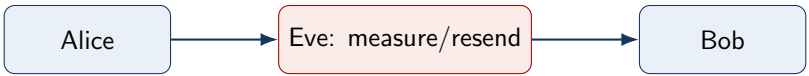
Instructions

1. We are going to be tracing the encryption fo two letters using basis and bits with the hardware.
2. Follow the instructions on the hands-on.
3. Answer the questions that are at the end of the activity.



Activity: Eavesdropping Experiment

- Use the supplied Alice and Eve basis choices to simulate Eve's intercept–resend measurements.
- Record Bob's outcomes and compare the sifted bits with Alice's original bits.
- Identify mismatches and assess whether the observed errors indicate disturbance.



Key Takeaways

1. **Quantum Threat:** Shor's algorithm threatens RSA and ECC, motivating quantum-safe cryptography.
2. **Quantum Key Distribution:** BB84 uses quantum states and measurement disturbance to establish secret keys securely.
3. **Hands-on Experience:** We explored polarization, BB84 key exchange, and the effects of eavesdropping.

Thank You!

Questions & Discussion

Mohammad Saidur Rahman, Ph.D.

Jesus Lopez Viviana Cadena

Intelligent and Quantum Secure Advanced Cyber Defense Research (IQSeC) Lab
University of Texas at El Paso

rahmanmsaidur.com