BB84 Quantum Cryptography Protocol Worksheet

Objective: Understand the world's first quantum cryptography protocol through interactive questions and exercises.

Part A: Understanding Quantum Bases

Questions:

1. Z basis measurements give us ____
   Hint: Think about the standard computational basis
2. X basis measurements give us ____
   Hint: This involves the Hadamard gate
3. Why can't we measure both Z and X bases simultaneously?
   ____
   ____
   Hint: This is a fundamental quantum principle

Part B: Protocol Steps Sequencing

Instructions: Number the steps in the correct chronological order (1-4):

- Step ____: Alice and Bob publicly compare which bases they used
- Step ____: Alice encodes random bits using randomly chosen bases (Z or X)
- Step ____: Bob measures received qubits using randomly chosen bases (Z or X)
- Step ____: They keep only the bits where their bases matched

Correct Sequence: ____ → ____ → ____ → ____

Part C: Security Analysis

Security Questions:

1. If Eve (eavesdropper) measures in the wrong basis, what happens?
   - A) She gets the correct bit with 100% accuracy
   - B) She gets random results (50% 0, 50% 1)
   - C) The qubit is destroyed
   - D) Nothing happens
2. How do Alice and Bob detect Eve's presence?
   - A) By checking if their keys are identical
   - B) By publicly comparing a subset of bits
   - C) By measuring entanglement
   - D) They can't detect Eve
3. What's the approximate maximum safe error rate for BB84?
   - A) 5%
   - B) 11%
   - C) 25%
   - D) 50%

Part D: Code Implementation

Task: Complete the quantum encoding function for BB84:

```python
def encode_qubit(bit, basis):
    """
    Encode a classical bit into a quantum state for BB84 protocol

    Parameters:
    bit (int): 0 or 1
```

```python
    basis (str): 'Z' or 'X'

    Returns:
    QuantumCircuit: Circuit encoding the bit
    """
    qc = QuantumCircuit(1, 1)

    if basis == 'Z':
        # Z basis: |0⟩ for 0, |1⟩ for 1
        if bit == 1:
            qc.______(0)  # Apply which gate to make |1⟩?
    else:  # X basis
        # X basis: |+⟩ for 0, |-⟩ for 1
        if bit == 0:
            qc.______(0)  # Apply which gate to make |+⟩?
        else:
            qc.______(0)  # First make |1⟩
            qc.______(0)  # Then transform to |-⟩

    return qc
```

Missing Gates: Choose from: `h`, `x`, `y`, `z`

Part E: Critical Thinking

Scenario Analysis:

Imagine Eve tries these attacks. What happens in each case?

1. Intercept-Resend Attack: Eve measures all qubits in Z basis and sends new ones.
   Error rate introduced: _________%
2. Partial Attack: Eve measures only 30% of qubits.
   Probability of detection: _________%
3. Basis Guessing: Eve randomly guesses Z or X for each qubit.
   Average information gained per qubit: _________ bits

Part F: Quantum Principles Review

Match each quantum principle with its role in BB84:

Principle	Role in BB84
No-Cloning Theorem	
Uncertainty Principle	
Measurement Collapse	
Superposition	

Options:

- A) Prevents perfect copying of quantum states
- B) Makes wrong-basis measurements random
- C) Disturbs state when Eve measures
- D) Allows encoding in multiple bases

Part G: Short Answer Questions

1. What does "BB84" stand for?
2. Name one real-world implementation of quantum cryptography:
3. How is quantum key distribution different from classical encryption?

4. What happens if Alice and Bob discover high error rates?

Part H: Learning Objectives Checklist

- Understand the difference between Z and X basis measurements
- Sequence the BB84 protocol steps correctly
- Explain how quantum mechanics enables security
- Implement basic quantum encoding in code
- Calculate error rates for eavesdropping detection
- Connect quantum principles to practical cryptography
- Analyze different eavesdropping strategies
- Compare quantum vs classical security approaches

Answer Key Section *(For Teachers/Instructors)*

Part A Answers:

1. $|0\rangle$ or $|1\rangle$ (computational basis states)
2. $|+\rangle$ or $|-\rangle$ (Hadamard basis states)
3. Due to the Heisenberg Uncertainty Principle - Z and X are complementary observables that cannot be measured simultaneously without uncertainty

Part B Answers:

Correct order: 2 → 3 → 1 → 4

Part C Answers:

1. B) She gets random results (50% 0, 50% 1)

2. B) By publicly comparing a subset of bits
3. B) 11%

Part D Answers:

Missing gates in order: `x`, `h`, `x`, `h`

Part E Answers:

1. 25%
2. Depends on sample size, but detectable with probability increasing with sample size
3. 0.5 bits (50% chance of guessing correctly)

Part F Answers:

- No-Cloning Theorem → A
- Uncertainty Principle → B
- Measurement Collapse → C
- Superposition → D

Part G Answers:

1. Bennett & Brassard 1984 (the inventors and year)
2. Examples: ID Quantique systems, Chinese quantum satellite, etc.
3. Quantum uses physics for security, classical uses mathematical complexity
4. They discard the key and start over - high errors indicate possible eavesdropping

---

Scoring Rubric

Section	Max Points	Scoring Criteria
Part A	6	2 points per correct answer
Part B	4	1 point per correct sequence
Part C	6	2 points per correct answer
Part D	4	1 point per correct gate
Part E	6	2 points per correct calculation
Part F	8	2 points per correct match
Part G	8	2 points per correct answer
Total	42	

Grade Scale:

- 38-42: Excellent (A)
- 34-37: Very Good (B)
- 30-33: Good (C)
- 25-29: Satisfactory (D)
- Below 25: Needs Improvement

Additional Resources & References

1. Textbook References:
    - Nielsen & Chuang, "Quantum Computation and Quantum Information"
    - Scarani et al., "The Security of Practical Quantum Key Distribution"
2. Online Resources:

    - Qiskit Textbook: Quantum Cryptography Chapter
    - IBM Quantum Experience Lab
    - MIT OpenCourseWare: Quantum Information Science
3. Software Tools:
    - Qiskit (Python library)
    - IBM Quantum Lab (online platform)
    - Quirk (quantum circuit simulator)
4. Further Reading:
    - Original BB84 Paper: Bennett & Brassard (1984)
    - Quantum Hacking and Countermeasures
    - Post-Quantum Cryptography

Worksheet Information

Course: Quantum Computing Fundamentals
Module: Quantum Cryptography
Duration: 60-90 minutes
Difficulty Level: Intermediate
Prerequisites: Basic quantum mechanics, Python programming
Created: [Date]
Last Updated: [Date]
Version: 1.0

Instructor Notes:

- This worksheet works well for individual or group work
- Code section requires Qiskit installation
- Consider pairing with hands-on quantum simulation
- Discussion of answers enhances learning
