Quantum Key Distribution and the Uncertainty Principle

David Wyde

October 7, 2025

Abstract

An attacker who intercepts qubits can break certain classes of quantum key distribution protocols. The idea is to record classical bits for outcomes in each of the small set of allowed measurement bases, for each qubit sent during the key exchange, using a sequence of simple quantum circuits. That approach also seems to enable predicting the future results of non-commuting measurements, which the uncertainty principle forbids.

1 Introduction

This paper describes attacks on a certain class of quantum key distribution protocols, when an eavesdropper, Eve, intercepts each qubit X that Alice sends to Bob as part of a quantum key exchange.

The idea is for Eve to repeatedly apply gates to every X, in each basis that Bob can choose, so that a measurement in the z basis corresponds to a measurement in that basis, CNOT from X to a target qubit so that they agree in the z basis, measure the target, record the outcome in a classical bit, zero the target, then put X back to its previous state. Section 2 describes the algorithm in more detail.

For every X, Eve only has to get correct results for each of a finite number of possible bases, and thus does not need to violate the no-cloning theorem.

Section 3 shows that the attack has applications to the uncertainty principle. If Eve records what Bob will measure in the x basis and in the z basis, for the same qubit, that seems to allow her to predict the results of two non-commuting measurements.

2 Quantum Key Distribution

2.1 Algorithm Sketch

If Alice and Bob do a quantum key exchange that involves roughly the following steps:

1. Alice sends n qubits to Bob,
2. Bob measures each qubit in one of a small number of different bases,
3. Alice and Bob announce over a public channel which basis each qubit should be measured in and which qubits will form the key,

an eavesdropper, Eve, might take the following approach:

1. Start with:
    - (a) One extra qubit, Y, set to $|0\rangle$.
    - (b) A way of storing one classical bit for each basis Bob might measure in, for each qubit Alice will send.
        - i. If a protocol sends n qubits and allows measuring each of them in any of m bases, that will require nm classical bits.
2. For each qubit X that Alice sends to Bob:
    - (a) For each basis B that Bob might measure in:
        - i. Apply a gate to change X into B.
        - ii. Apply the gate CNOT(X, Y).
        - iii. Measure Y in the $|0\rangle$, $|1\rangle$ basis, which corresponds to a measurement in B.
        - iv. Record the classical bit for that measurement outcome.
        - v. Zero Y.
        - vi. Apply the inverse matrix for changing into B, to change X out of B, restoring X to its original basis.
    - (b) Pass X, which is back in its original state, to Bob.

2.2 Algorithm Description

The CNOT(X, Y) gates change $a|00\rangle + b|10\rangle$ to $a|00\rangle + b|11\rangle$, where a is the probability amplitude that X is measured $|0\rangle$ and b is the probability amplitude that it is measured $|1\rangle$. Then, X and Y are guaranteed to agree with each other in the z basis. Each change of basis means that $|0\rangle$ and $|1\rangle$ correspond to a measurement in the desired basis.

When Bob picks a basis for each qubit, the resulting measurement will agree with Eve's corresponding measurement for that qubit and basis. As Alice and Bob announce which qubits and bases form the key, Eve can look up the corresponding values that are stored in classical bits.

The idea seems similar to a parity measurement[1]: CNOT(A, C), CNOT(B, C), and check if C is measured as $|0\rangle$ or $|1\rangle$, to see if A and B agree in the z basis. If C has been flipped 0 or 2 times, C is $|0\rangle$, and A and B agree; otherwise C has been flipped once, and A and B disagree.

In some cases, it may be better for Eve to copy all of the n bases to n target qubits (Y_i), pass Bob's X along, then measure each of the n targets. That may lead to less of a delay between Alice sending a qubit and Bob receiving it.

It seems harder to model the latter approach, since a CNOT from X to Y_2 changes some of the probabilities for Y_1, when X, Y_1, and Y_2 are all viewed as one subsystem. That issue is discussed more in [2].

2.3 Assumptions about Circuits

The algorithm above assumes that certain things are possible, including:

1. For any measurement basis, there is a quantum logic gate that corresponds to changing the qubit X into that basis, and an associated unitary matrix.
2. A gate corresponding to the matrix inverse of 1) will restore X to its original basis.
3. CNOT gates are possible.
4. Zeroing a qubit is possible and does not affect other qubits.
5. Measuring one qubit does not affect other qubits.

If the measurement basis vectors are orthogonal, 1) will be possible. The idea is to take the first basis vector to $|0\rangle$ and the second basis vector to $|1\rangle$.

Then, 2) follows because unitary matrices are invertible.

CNOT gates have been demonstrated, including for qubits based on photon polarization[3].

Zeroing a qubit is not unitary or reversible, which means it cannot be achieved with a standard quantum logic gate. It is still something that makes sense for quantum circuits, since it is common to start a run of a program with all qubits in $|0\rangle$. The quantum computing library *Qiskit* provides a `reset(qubit)` function on a `QuantumCircuit`, which allows zeroing a qubit as part of a circuit[4].

When measuring or zeroing a qubit, the state vector may change, but other qubits are not physically changed, with or without any amount of entanglement. [2] discusses some counterintuitive details.

2.4 Existing Protocols

Some existing quantum key distribution protocols seem to have the structure described above, including BB84[5] and several of its variants[6]. BB84 involves measurements of photons in the $|0°\rangle$, $|90°\rangle$ basis or the $|45°\rangle$, $|-45°\rangle$ basis.

3 The Uncertainty Principle

The preceding ideas on quantum key distribution seem relevant to the uncertainty principle, which claims that it should be impossible to know the results of multiple non-commuting measurements[7].

Eve should then be unable to know what Bob will measure in both the x basis and the z basis, for the same X: those two measurements do not commute. The algorithm described in Section 2 seems to allow that to happen.

It feels a bit extreme to claim that a few changes of basis and CNOT gates are enough to show that quantum mechanics is incomplete[8], but it does look like Eve can store 1 classical bit for a measurement in the x basis, 1 classical bit for a measurement in the z basis, then have those outcomes agree with whichever of those two bases Bob measures in.

References

[1] Sainan Huai, Kunliang Bu, Xiu Gu, Zhenxing Zhang, Shuoming An, Xiaopei Yang, Yuan Li, Tianqi Cai, and Yicong Zheng. Fast joint parity measurement via collective interactions induced by stimulated emission. *Nature Communications*, 15, 2024. Article number: 3045.

[2] David Wyde. Quantum State Vectors. `https://davidwyde.com/thoughts/quantum-state/`. Accessed: 2025-10-07.

[3] Andrea Crespi, Roberta Ramponi, Roberto Osellame, Linda Sansoni, Irene Bongioanni, Fabio Sciarrino, Giuseppe Vallone, and Paolo Mataloni. Integrated photonic quantum gates for polarization qubits. *Nature Communications*, 2, 2011. Article number: 566.

[4] Qiskit documentation. QuantumCircuit class. `https://quantum.cloud.ibm.com/docs/en/api/qiskit/qiskit.circuit.QuantumCircuit#reset`. Accessed: 2025-10-07.

[5] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[6] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74:145–195, 2002.

[7] Jan Hilgevoord and Jos Uffink. The Uncertainty Principle. In Edward N. Zalta and Uri Nodelman, editors, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, Spring 2024 edition, 2024.

[8] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Physical Review*, 47:777–780, 1935.