Security in a Quantum World

Vladimir Zamdzhiev

Department of Computer Science
Tulane University

November 7 2017

Physical Theories

Currently, there are three main physical theories:

- Classical Mechanics – describes the moderately sized world.

Physical Theories

Currently, there are three main physical theories:

- Classical Mechanics – describes the moderately sized world.
- General Relativity – works for moderately sized and macro world (stars, galaxies, black holes, etc.).

Physical Theories

Currently, there are three main physical theories:

- Classical Mechanics – describes the moderately sized world.
- General Relativity – works for moderately sized and macro world (stars, galaxies, black holes, etc.).
- Quantum Mechanics – describes the micro world (photons, electrons, etc.).

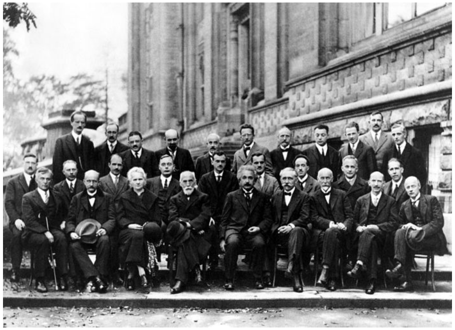


Figure: The 1927 Solvay Conference in Brussels

Classical Computing

- Classical computers (laptops, phones, etc.) manipulate classical information (bits) in order to perform computation.
- Classical information is described using classical information theory which is a mathematical model that assumes the world is explained using classical physics.
- This is a reasonable assumption to make for our current hardware.

Quantum Computing

- Consider computational hardware which can manipulate simple quantum systems called qubits (quantum bits).
- The underlying mathematical model is now different as it is based on quantum physics.
- Processing of quantum information (qubits) is as a result fundamentally different.
- The speed of certain computations is also provably faster in some cases.

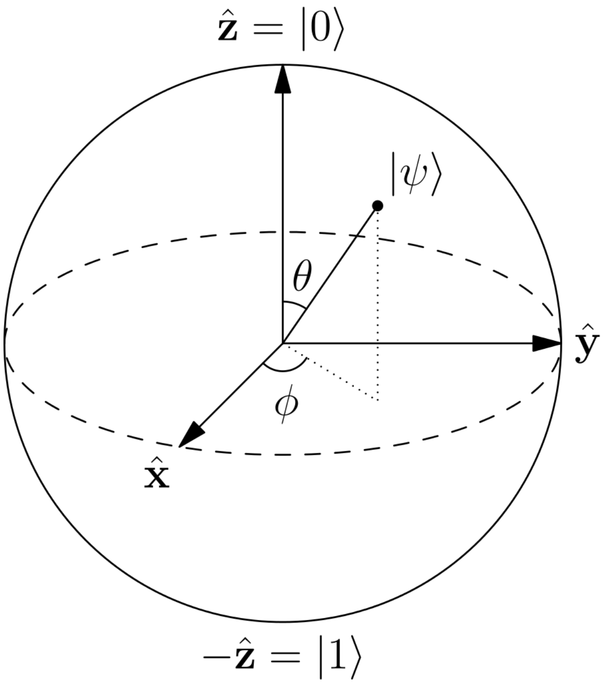


Figure: Bloch-sphere representation of a qubit state

Quantum Entanglement – important resource

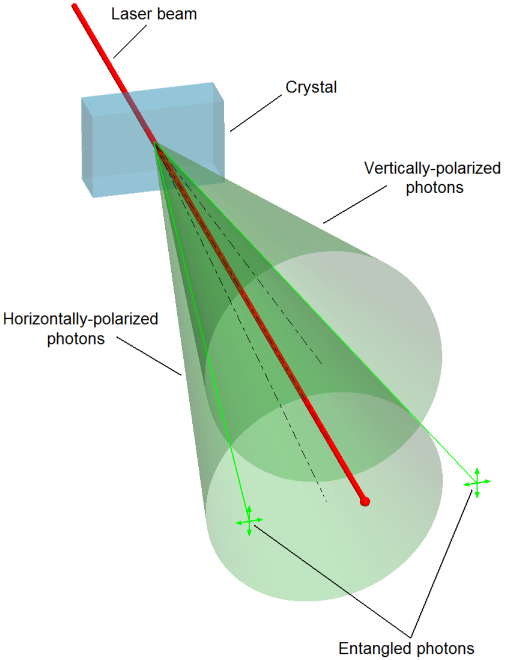
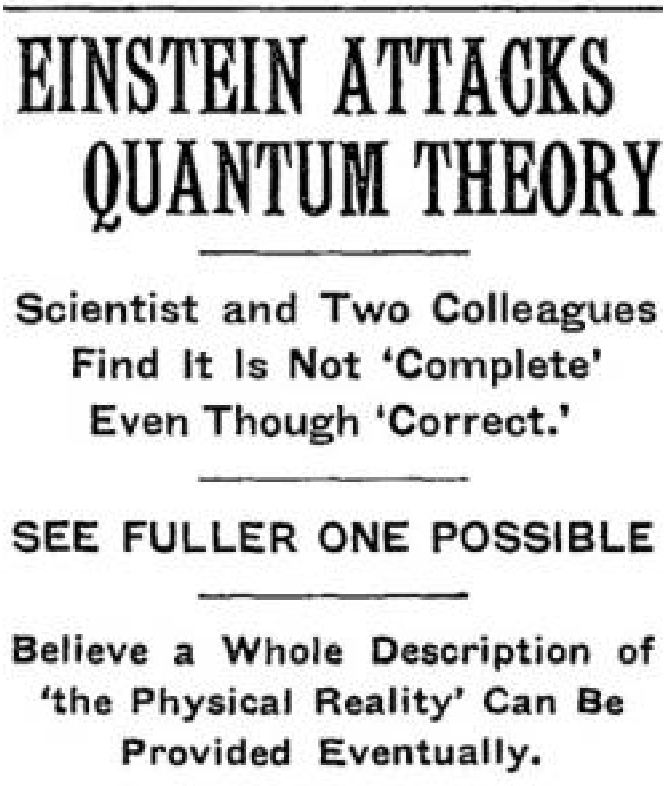


Figure: Illustration of quantum optics experiment which produces entanglement.

Quantum Entanglement – important resource



EINSTEIN ATTACKS
QUANTUM THEORY

Scientist and Two Colleagues
Find It Is Not 'Complete'
Even Though 'Correct.'

SEE FULLER ONE POSSIBLE

Believe a Whole Description of
'the Physical Reality' Can Be
Provided Eventually.

Figure: May 4, 1935 *New York Times* article headline regarding the imminent EPR paper

Quantum Entanglement – important resource

- Quantum entanglement is a special kind of correlation between systems which allows them to exhibit similar properties, even when space-time seperated.
- Einstein famously referred to it as: "Spooky action at a distance".
- Schrödinger described it as: "I would not call entanglement one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought.".
- Quantum entanglement is a crucial resource for quantum computing and also for many quantum information security protocols.

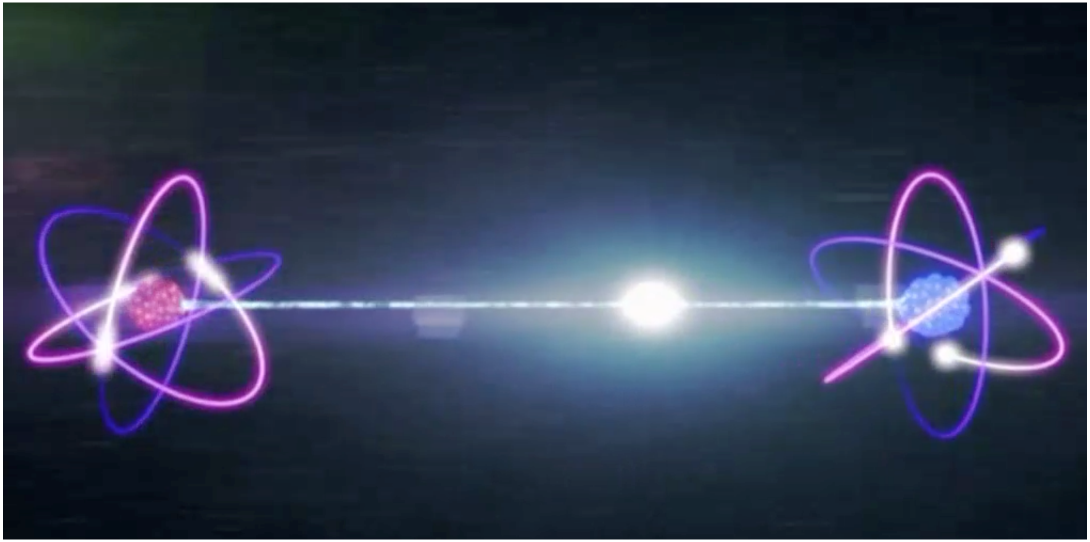


Figure: A most likely inaccurate illustration of quantum entanglement

Security, Classical and Quantum Communication

One of the most important problems in communication security is "Key Distribution".

- The problem involves two parties agreeing on a key in such a way that any third party is unable to obtain it under reasonable assumptions.

Security, Classical and Quantum Communication

One of the most important problems in communication security is "Key Distribution".

- The problem involves two parties agreeing on a key in such a way that any third party is unable to obtain it under reasonable assumptions.
- Two kinds of security for this problem:

Security, Classical and Quantum Communication

One of the most important problems in communication security is "Key Distribution".

- The problem involves two parties agreeing on a key in such a way that any third party is unable to obtain it under reasonable assumptions.
- Two kinds of security for this problem:
  - Computational security – the two parties have a (severe) computational advantage over any third party, but the third party is guaranteed to recover their secrets given enough time.

Security, Classical and Quantum Communication

One of the most important problems in communication security is "Key Distribution".

- The problem involves two parties agreeing on a key in such a way that any third party is unable to obtain it under reasonable assumptions.
- Two kinds of security for this problem:
  - Computational security – the two parties have a (severe) computational advantage over any third party, but the third party is guaranteed to recover their secrets given enough time.
  - Unconditional security (or information-theoretic security) – any third party does not have enough information to recover the secret (regardless of computational power) and can at best guess what it is.

Security, Classical and Quantum Communication

One of the most important problems in communication security is "Key Distribution".

- The problem involves two parties agreeing on a key in such a way that any third party is unable to obtain it under reasonable assumptions.
- Two kinds of security for this problem:
  - Computational security – the two parties have a (severe) computational advantage over any third party, but the third party is guaranteed to recover their secrets given enough time.
  - Unconditional security (or information-theoretic security) – any third party does not have enough information to recover the secret (regardless of computational power) and can at best guess what it is.
- In the classical case where all actors have classical computers and use classical communication channels, we get computational security (public-key encryption).

Security, Classical and Quantum Communication

One of the most important problems in communication security is "Key Distribution".

- The problem involves two parties agreeing on a key in such a way that any third party is unable to obtain it under reasonable assumptions.
- Two kinds of security for this problem:
  - Computational security – the two parties have a (severe) computational advantage over any third party, but the third party is guaranteed to recover their secrets given enough time.
  - Unconditional security (or information-theoretic security) – any third party does not have enough information to recover the secret (regardless of computational power) and can at best guess what it is.
- In the classical case where all actors have classical computers and use classical communication channels, we get computational security (public-key encryption).
- In the quantum case where all actors have quantum computers and use quantum communication channels, we get unconditional security.

Security, Classical and Quantum Communication

One of the most important problems in communication security is "Key Distribution".

- The problem involves two parties agreeing on a key in such a way that any third party is unable to obtain it under reasonable assumptions.
- Two kinds of security for this problem:
    - Computational security – the two parties have a (severe) computational advantage over any third party, but the third party is guaranteed to recover their secrets given enough time.
    - Unconditional security (or information-theoretic security) – any third party does not have enough information to recover the secret (regardless of computational power) and can at best guess what it is.
- In the classical case where all actors have classical computers and use classical communication channels, we get computational security (public-key encryption).
- In the quantum case where all actors have quantum computers and use quantum communication channels, we get unconditional security.
- In the quantum case eavesdropping can be detected, but in the classical case it cannot.

Quantum Superposition – important resource

A quantum system may be in many different states at the same time.

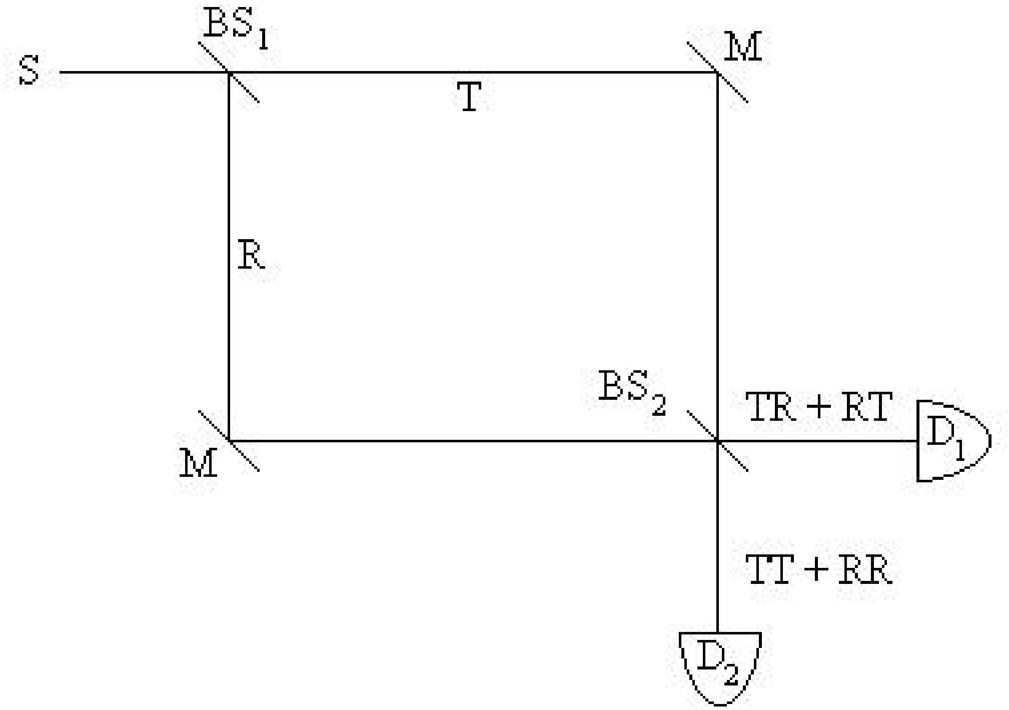


Figure: single-photon interference performed with a Mach-Zehnder interferometer

- Very rough analogy: allows for exponential parallelism.
- Crucial for computational speedup.

Computational advantages

Quantum computing has attracted a lot of interest because it offers computational speedups over some of the best known classical algorithms for important problems.

Computational advantages

Quantum computing has attracted a lot of interest because it offers computational speedups over some of the best known classical algorithms for important problems.

- Grover's algorithm:
  - An algorithm which can search an unsorted database with a quadratic speedup over the best classical algorithm.
  - Decent speedup, but not mind-blowing.
  - This results in improved computational complexity for many practical problems.
  - Symmetric-key cryptography still safe (e.g. AES).

Computational advantages

Quantum computing has attracted a lot of interest because it offers computational speedups over some of the best known classical algorithms for important problems.

- Grover's algorithm:
    - An algorithm which can search an unsorted database with a quadratic speedup over the best classical algorithm.
    - Decent speedup, but not mind-blowing.
    - This results in improved computational complexity for many practical problems.
    - Symmetric-key cryptography still safe (e.g. AES).
- Shor's algorithm:
    - Exponential speedup compared to fastest known classical algorithm for solving the Hidden Subgroup Problem for finite abelian groups.

Computational advantages

Quantum computing has attracted a lot of interest because it offers computational speedups over some of the best known classical algorithms for important problems.

- Grover's algorithm:
    - An algorithm which can search an unsorted database with a quadratic speedup over the best classical algorithm.
    - Decent speedup, but not mind-blowing.
    - This results in improved computational complexity for many practical problems.
    - Symmetric-key cryptography still safe (e.g. AES).
- Shor's algorithm:
    - Exponential speedup compared to fastest known classical algorithm for solving the Hidden Subgroup Problem for finite abelian groups.
    - This destroys all of the widely used public-key encryption systems (RSA, Diffie-Hellman, elliptic curves, etc.).
    - New encryption systems will be needed to protect against adversaries with quantum resources ("post-quantum cryptography").

Computational advantages

Quantum computing has attracted a lot of interest because it offers computational speedups over some of the best known classical algorithms for important problems.

- Grover's algorithm:
  - An algorithm which can search an unsorted database with a quadratic speedup over the best classical algorithm.
  - Decent speedup, but not mind-blowing.
  - This results in improved computational complexity for many practical problems.
  - Symmetric-key cryptography still safe (e.g. AES).
- Shor's algorithm:
  - Exponential speedup compared to fastest known classical algorithm for solving the Hidden Subgroup Problem for finite abelian groups.
  - This destroys all of the widely used public-key encryption systems (RSA, Diffie-Hellman, elliptic curves, etc.).
  - New encryption systems will be needed to protect against adversaries with quantum resources ("post-quantum cryptography").
- Many other faster algorithms are known, but the above two are the most important.

How soon will quantum computers be able to crack encryption?

Here's what the Information Assurance Directorate (IAD) of the National Security Agency (NSA) of the United States has to say on the matter:

- "IAD will initiate a transition to quantum resistant algorithms in the not too distant future. Based on experience in deploying Suite B, we have determined to start planning and communicating early about the upcoming transition to quantum resistant algorithms. Our ultimate goal is to provide cost effective security against a potential quantum computer...
- ...Until this new suite is developed and products are available implementing the quantum resistant suite, we will rely on current algorithms. For those partners and vendors that have not yet made the transition to Suite B elliptic curve algorithms, we recommend not making a significant expenditure to do so at this point but instead to prepare for the upcoming quantum resistant algorithm transition."

Thank you for your attention!