Comparing Quantum Protocols via PRISM

Gabriele Tedeschi

University of Pisa

June 9, 2022

Motivations

Quantum cryptographic protocols have been proved to be **unconditionally secure**, meaning that every possible attack will fail with probability arbitrarily close to one.

But one would also like to:

- Compare different protocols
- Verify other properties of the protocol
- Compare the behaviour with different parameters

Thats when **model checking** comes in handy!

Table of Contents

Braket Notation

In linear algebra, we write:

- Vector $\mathbf{v}$
- Conjugate transpose
  $\mathbf{v}^* = \mathbf{v}^H = \overline{\mathbf{v}^T}$
- Dot product between $\mathbf{v}$ and $\mathbf{u}$
  $$v^* \cdot u$$
- Norm of $\mathbf{v}$: $\|\mathbf{v}\| = v^* \cdot u$

Braket Notation

In linear algebra, we write:

- Vector $\mathbf{v}$
- Conjugate transpose $\mathbf{v}^* = \mathbf{v}^H = \overline{\mathbf{v}}^T$
- Dot product between $\mathbf{v}$ and $\mathbf{u}$
$$v^* \cdot u$$
- Norm of $\mathbf{v}$: $\|\mathbf{v}\| = v^* \cdot u$

In quantum mechanics, we write:

- Vector $|\psi\rangle$
- conjugate transpose $\langle\psi| = |\psi\rangle^H = \overline{|\psi\rangle}^T$
- dot product between$|\psi\rangle$ and $|\phi\rangle$
$$\langle\psi|\phi\rangle$$
- Norm of $|\psi\rangle$: $\langle\psi|\psi\rangle$

First Postulate: Quantum State

I Postulate

Any **isolated** physical system is completely described by a **unit vector** in a **complex vector space** with inner product (called **Hilbert Space** $\mathcal{H}$)

First Postulate: Quantum State

I Postulate

Any **isolated** physical system is completely described by a **unit vector** in a **complex vector space** with inner product (called **Hilbert Space** $\mathcal{H}$)

- **Complex vector space**: A vector space with coefficients in $\mathbb{C}$, so some possible vectors are:

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} i \\ i \end{pmatrix}, \quad \begin{pmatrix} 5+5i \\ \frac{1}{3}+\frac{1}{5}i \end{pmatrix}, \quad \dots$$

First Postulate: Quantum State

I Postulate

Any **isolated** physical system is completely described by a **unit vector** in a **complex vector space** with inner product (called **Hilbert Space** $\mathcal{H}$)

- **Complex vector space**: A vector space with coefficients in $\mathbb{C}$, so some possible vectors are:

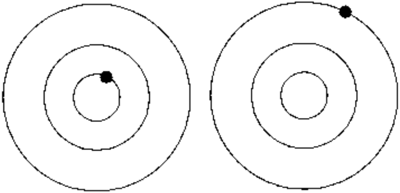
$$\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} i \\ i \end{pmatrix}, \quad \begin{pmatrix} 5+5i \\ \frac{1}{3}+\frac{1}{5}i \end{pmatrix}, \quad \dots$$

- **Unit vector**: a vector $|\psi\rangle$ such that $\langle\psi|\psi\rangle = 1$, like:

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ i \end{pmatrix}, \quad \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}}i \end{pmatrix}, \quad \dots$$

Qubits

Suppose a physical system with only two states: an particle with spin up or spin down, for example, or an electron that can be in an excited state or in the ground state.



Qubits

A system with only two possible state is described by a **qubit**, a unitary vector in the 2-dimensional Hilbert space $\mathcal{H}_2 \equiv \mathbb{C}^2$.

For example, if an electron is in the ground state, we say that is in state

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

while if it is in the excited state, it's in state

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Computational Basis

$|0\rangle$ and $|1\rangle$ form the so called **computational base** of the (bidimensional) Hilbert space. This means that each vector $|\psi\rangle$ can be expressed as

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha\,|0\rangle + \beta\,|1\rangle\,, \text{ with } \alpha, \beta \in \mathbb{C}, \langle\psi|\psi\rangle = 1$$

Quantum Superposition

Since $|0\rangle$ and $|1\rangle$ are vectors in $\mathcal{H}_2$, so it is any **linear combination** of the two, provided it has unitary length.

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}, \quad \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}, \quad \begin{pmatrix} \sqrt{0.9} \\ \sqrt{0.1} \end{pmatrix}$$

Quantum Superposition

Since $|0\rangle$ and $|1\rangle$ are vectors in $\mathcal{H}_2$, so it is any **linear combination** of the two, provided it has unitary length.

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}, \quad \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}, \quad \begin{pmatrix} \sqrt{0.9} \\ \sqrt{0.1} \end{pmatrix}$$

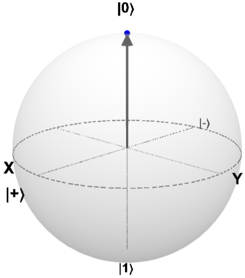
Hadamard basis

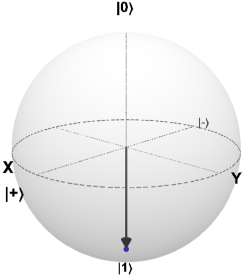
The vector $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle$ is called the $|+\rangle$ state

The vector $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ .1 \end{pmatrix} = \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle$ is called the $|-\rangle$ state

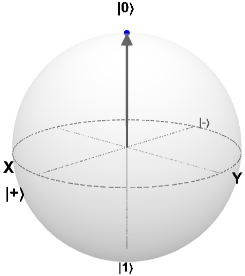
They form the Hadamard Basis of $\mathcal{H}_2$

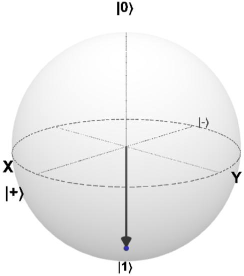
Bloch sphere

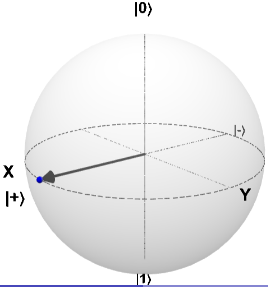




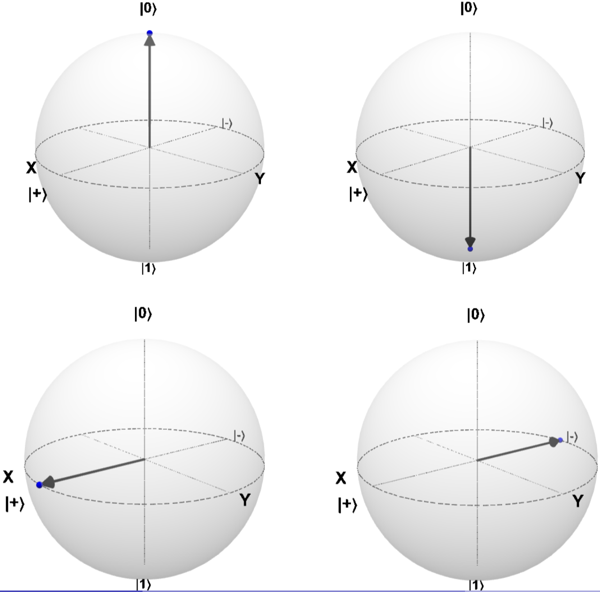
Bloch sphere



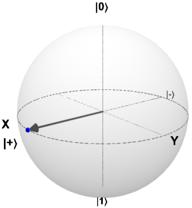




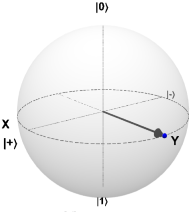
Bloch sphere



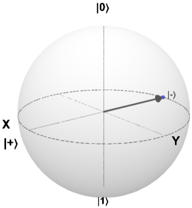
Phase



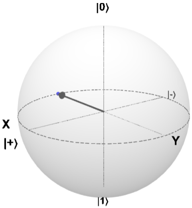
$$|+\rangle = |0\rangle + e^{i0}\,|1\rangle$$



$$|0\rangle + e^{i\frac{\pi}{2}}\,|1\rangle$$



$$|-\rangle = |0\rangle + e^{i\pi}\,|1\rangle$$



$$|0\rangle + e^{i\frac{3\pi}{2}}\,|1\rangle$$

Compound Systems

How do we describe a system composed of two different qubits? As the **Tensor product** of Hilbert spaces.

$$\text{If } \left|\psi\right\rangle, \left|\phi\right\rangle \in \mathcal{H} \quad \text{then} \quad \left|\psi\phi\right\rangle \in \mathcal{H} \otimes \mathcal{H}$$

$\mathcal{H}_2 \otimes \mathcal{H}_2$ is a **four-dimensional Hilbert space**.

Dot product in a compound space

Given $\left|\psi\psi'\right\rangle$ and $\left|\phi\phi'\right\rangle$, the dot product is defined as

$$\left\langle\psi\psi'|\phi\phi'\right\rangle = \left\langle\psi|\phi\right\rangle \left\langle\psi'\phi'\right\rangle$$

Second Postulate: Unitary Transformations

II Postulate

The evolution of a **closed** quantum system is described by a **unitary transformation**. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on t_1 and t_2:

$$|\psi'\rangle = U\,|\psi\rangle$$

Second Postulate: Unitary Transformations

II Postulate

The evolution of a **closed** quantum system is described by a **unitary transformation**. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on t_1 and t_2:

$$|\psi'\rangle = U\,|\psi\rangle$$

- **Closed**: without interaction with the environment, i.e. without exchanging with the environment any energy, information, etc..

Second Postulate: Unitary Transformations

II Postulate

The evolution of a **closed** quantum system is described by a **unitary transformation**. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on t_1 and t_2:

$$|\psi'\rangle = U\,|\psi\rangle$$

- **Closed**: without interaction with the environment, i.e. without exchanging with the environment any energy, information, etc..
- **Unitary tranformation** on a Hilbert space $\mathcal{H}_n$: A $n \times n$ matrix such that its *adjoint* it's also its *inverse*:

$$UU^H = U^H U = UU^-1 = I$$

A useful property

Unitary Matrices preserve dot product

Given $|\psi\rangle$, $|\phi\rangle$ with dot product x, for a unitary matrix U holds:

$$\langle\psi|\phi\rangle = x$$
$$\langle U\psi|U\phi\rangle = \langle\psi|U^H U|\phi\rangle = \langle\psi|\phi\rangle = x$$

A useful property

Unitary Matrices preserve dot product

Given $|\psi\rangle$, $|\phi\rangle$ with dot product x, for a unitary matrix U holds:

$$\langle\psi|\phi\rangle = x$$
$$\langle U\psi|U\phi\rangle = \langle\psi|U^H U|\phi\rangle = \langle\psi|\phi\rangle = x$$

Corollary

If $|\psi\rangle$ is a unit vector, $U|\psi\rangle$ will also be a unit vector.

$$\langle U\psi|U\psi\rangle = \langle\psi|\psi\rangle = 1$$

Third Postulate: Measurements

III Postulate

If a state $|\psi\rangle = \alpha\,|b_0\rangle + \beta\,|b_1\rangle$ gets **measured** in the base $\{b_0, b_1\}$, it will **collapse**

- In state $|b_0\rangle$ with probability $\|\alpha\|^2$
- In state $|b_1\rangle$ with probability $\|\beta\|^2$.

Third Postulate: Measurements

III Postulate

If a state $|\psi\rangle = \alpha\,|b_0\rangle + \beta\,|b_1\rangle$ gets **measured** in the base $\{b_0, b_1\}$, it will **collapse**

- In state $|b_0\rangle$ with probability $\|\alpha\|^2$
- In state $|b_1\rangle$ with probability $\|\beta\|^2$.

If $|0\rangle$ gets measured in the computational basis $\{|0\rangle, |1\rangle\}$, it will **always** result in $|0\rangle$.

Third Postulate: Measurements

III Postulate

If a state $|\psi\rangle = \alpha |b_0\rangle + \beta |b_1\rangle$ gets **measured** in the base $\{b_0, b_1\}$, it will **collapse**

- In state $|b_0\rangle$ with probability $\|\alpha\|^2$
- In state $|b_1\rangle$ with probability $\|\beta\|^2$.

If $|0\rangle$ gets measured in the computational basis $\{|0\rangle, |1\rangle\}$, it will **always** result in $|0\rangle$.

If $|+\rangle = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle$ gets measured in the computational basis $\{|0\rangle, |1\rangle\}$, it will result in $|0\rangle$ or $|1\rangle$ with probability 0.5 each.

Third Postulate: Measurements

III Postulate

If a state $|\psi\rangle = \alpha|b_0\rangle + \beta|b_1\rangle$ gets **measured** in the base $\{b_0, b_1\}$, it will **collapse**

- In state $|b_0\rangle$ with probability $\|\alpha\|^2$
- In state $|b_1\rangle$ with probability $\|\beta\|^2$.

If $|0\rangle$ gets measured in the computational basis $\{|0\rangle, |1\rangle\}$, it will **always** result in $|0\rangle$.

If $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ gets measured in the computational basis $\{|0\rangle, |1\rangle\}$, it will result in $|0\rangle$ or $|1\rangle$ with probability 0.5 each.

Since $|0\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle$, measuring $|0\rangle$ in the hadamard basis $\{|+\rangle, |-\rangle\}$ will result in $|+\rangle$ or $|-\rangle$ with probability 0.5 each.

Takeaway

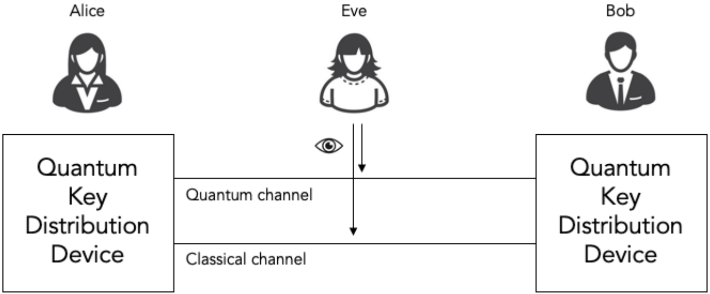
To understand the quantum cryptographic protocols, two properties will be useful:

- The evolution of a quantum system is described by a **unitary matrix**, and unitary matrices preserve the inner product.
- When the $|0\rangle$ and $|1\rangle$ states are **measured** in the computational basis, will give with probability 1 the outcome $|0\rangle$ and $|1\rangle$, respectively. When measured in the Hadamard basis, will give outcome $|+\rangle$ or $|-\rangle$ with probability $\frac{1}{2}$ each. The inverse is true for the $|+\rangle$ and $|-\rangle$ states.

Quantum Key Distribution Protocols

Two communicating parties, Alice and Bob, want to establish a shared **secret k** $\in \{0, 1\}^N$, $N \geq 0$ for secure communication. They do not share any prior information, but can make use of:

- A **classical**, (public) channel, that can be passively monitored but not tampered with by an attacker.
- A **quantum** channel, that can be tampered with by an attacker, but by its nature can not be passively monitored.



Information gains implies disturbance

Theorem

In any attempt to distinguish between two **non-orthogonal** quantum states, information gain is only possible at the expense of **introducing disturbance** to the signal.

Eve, having intercepted a qubit $q \in \{|\psi\rangle, |\phi\rangle\}$ would like to apply a unitary transformation U such that:

$$U(|\psi a\rangle) = |\psi b\rangle$$
$$U(|\phi a\rangle) = |\phi b'\rangle$$

Information gains implies disturbance

Theorem

In any attempt to distinguish between two **non-orthogonal** quantum states, information gain is only possible at the expense of **introducing disturbance** to the signal.

Eve, having intercepted a qubit $q \in \{|\psi\rangle, |\phi\rangle\}$ would like to apply a unitary transformation U such that:

$$U(|\psi a\rangle) = |\psi b\rangle$$
$$U(|\phi a\rangle) = |\phi b'\rangle$$

But, since unitary transformation preserve inner products:

$$\langle \psi a | \phi a \rangle$$

Information gains implies disturbance

Theorem

In any attempt to distinguish between two **non-orthogonal** quantum states, information gain is only possible at the expense of **introducing disturbance** to the signal.

Eve, having intercepted a qubit $q \in \{|\psi\rangle, |\phi\rangle\}$ would like to apply a unitary transformation U such that:

$$U(|\psi a\rangle) = |\psi b\rangle$$
$$U(|\phi a\rangle) = |\phi b'\rangle$$

But, since unitary transformation preserve inner products:

$$\langle \psi a | \phi a\rangle = \langle \psi | \phi \rangle \langle a | a \rangle$$

Information gains implies disturbance

Theorem

In any attempt to distinguish between two **non-orthogonal** quantum states, information gain is only possible at the expense of **introducing disturbance** to the signal.

Eve, having intercepted a qubit $q \in \{|\psi\rangle, |\phi\rangle\}$ would like to apply a unitary transformation U such that:

$$U(|\psi a\rangle) = |\psi b\rangle$$
$$U(|\phi a\rangle) = |\phi b'\rangle$$

But, since unitary transformation preserve inner products:

$$\langle \psi a | \phi a \rangle = \langle \psi | \phi \rangle \langle a | a \rangle = \langle \psi | \phi \rangle \langle b | b' \rangle = \langle \psi b | \phi b' \rangle$$

Information gains implies disturbance

Theorem

In any attempt to distinguish between two **non-orthogonal** quantum states, information gain is only possible at the expense of **introducing disturbance** to the signal.

Eve, having intercepted a qubit $q \in \{|\psi\rangle, |\phi\rangle\}$ would like to apply a unitary transformation U such that:

$$U(|\psi a\rangle) = |\psi b\rangle$$
$$U(|\phi a\rangle) = |\phi b'\rangle$$

But, since unitary transformation preserve inner products:

$$\langle \psi a|\phi a\rangle = \langle \psi|\phi\rangle \langle a|a\rangle = \langle \psi|\phi\rangle \langle b|b'\rangle = \langle \psi b|\phi b'\rangle$$
$$\langle a|a\rangle = \langle b|b'\rangle$$

Information gains implies disturbance

Theorem

In any attempt to distinguish between two **non-orthogonal** quantum states, information gain is only possible at the expense of **introducing disturbance** to the signal.

Eve, having intercepted a qubit $q \in \{|\psi\rangle, |\phi\rangle\}$ would like to apply a unitary transformation U such that:

$$U(|\psi a\rangle) = |\psi b\rangle$$
$$U(|\phi a\rangle) = |\phi b'\rangle$$

But, since unitary transformation preserve inner products:

$$\langle \psi a|\phi a\rangle = \langle \psi|\phi\rangle \langle a|a\rangle = \langle \psi|\phi\rangle \langle b|b'\rangle = \langle \psi b|\phi b'\rangle$$
$$\langle a|a\rangle = \langle b|b'\rangle = 1$$

Information gains implies disturbance

Theorem

In any attempt to distinguish between two **non-orthogonal** quantum states, information gain is only possible at the expense of **introducing disturbance** to the signal.

Eve, having intercepted a qubit $q \in \{|\psi\rangle, |\phi\rangle\}$ would like to apply a unitary transformation U such that:

$$U(|\psi a\rangle) = |\psi b\rangle$$
$$U(|\phi a\rangle) = |\phi b'\rangle$$

But, since unitary transformation preserve inner products:

$$\langle \psi a | \phi a \rangle = \langle \psi | \phi \rangle \langle a | a \rangle = \langle \psi | \phi \rangle \langle b | b' \rangle = \langle \psi b | \phi b' \rangle$$
$$\langle a | a \rangle = \langle b | b' \rangle = 1$$

$|b\rangle$ and $|b'\rangle$ must be equal!

The BB84 Protocol

First Phase: Quantum transmission

1. Alice creates a random string of bits $\mathbf{d} \in \{0,1\}^n$, and a random string of bases $\mathbf{b} \in \{\boxplus, \boxtimes\}^n$, where $n > N$.

The BB84 Protocol

First Phase: Quantum transmission

1. Alice creates a random string of bits $\mathbf{d} \in \{0, 1\}^n$, and a random string of bases $\mathbf{b} \in \{\boxplus, \boxtimes\}^n$, where $n > N$.
2. Alice sends to Bob the sequence of qubits $|\phi_i\rangle = |\phi_{b_i d_i}\rangle$, where

$$|\phi_{\boxplus 0}\rangle = |0\rangle \qquad |\phi_{\boxtimes 0}\rangle = |+\rangle$$
$$|\phi_{\boxplus 1}\rangle = |1\rangle \qquad |\phi_{\boxtimes 1}\rangle = |-\rangle$$

The BB84 Protocol

First Phase: Quantum transmission

1. Alice creates a random string of bits $\mathbf{d} \in \{0,1\}^n$, and a random string of bases $\mathbf{b} \in \{\boxplus, \boxtimes\}^n$, where $n > N$.
2. Alice sends to Bob the sequence of qubits $|\phi_i\rangle = |\phi_{b_i d_i}\rangle$, where

$$|\phi_{\boxplus 0}\rangle = |0\rangle \qquad |\phi_{\boxtimes 0}\rangle = |+\rangle$$
$$|\phi_{\boxplus 1}\rangle = |1\rangle \qquad |\phi_{\boxtimes 1}\rangle = |-\rangle$$

3. Bob creates a random string of bases $\mathbf{b}' \in \{\boxplus, \boxtimes\}^n$, and measures each $|\phi_i\rangle$ in the bases b'_i. When he measures $|0\rangle$ or $|+\rangle$, he stores 0, when he measures $|1\rangle$ or $|-\rangle$, he stores 1. Doing so he obtains a string of bits $\mathbf{d}' \in \{0,1\}^n$, that will contain some errors with respect to the original $\mathbf{d}$.

Second Phase: Public discussion

Alice and Bob will keep only the correct bits, $\mathbf{k} \subseteq \mathbf{b}$

The BB84 Protocol

First Phase: Quantum transmission

Alice has $\mathbf{d}$ and $\mathbf{b}$, Bob has $\mathbf{d}'$ and $\mathbf{b}'$.

Second Phase: Public discussion

1. Alice sends $\mathbf{b}$ over the public channel, Bob confronts it with $\mathbf{b}'$, and answers to Alice the set $S = \{i \mid b_i = b'_i\}$. Only the corresponding qubits have been correctly measured, and the others are discarded.

The BB84 Protocol

First Phase: Quantum transmission

Alice has $\mathbf{d}$ and $\mathbf{b}$, Bob has $\mathbf{d}'$ and $\mathbf{b}'$.

Second Phase: Public discussion

1. Alice sends $\mathbf{b}$ over the public channel, Bob confronts it with $\mathbf{b}'$, and answers to Alice the set $S = \{i \mid b_i = b_i'\}$. Only the corresponding qubits have been correctly measured, and the others are discarded.
2. Alice chooses a subset oh the remaining bits in $\mathbf{d}$ and discloses their values to Bob. For each d_i in this subset, since it holds $b_i = b_i'$, it should be $d_i = d_i'$. If Bob notices discrepancies $d_i \neq d_i'$, eavesdropping is detected.

The BB84 Protocol

First Phase: Quantum transmission

Alice has $\mathbf{d}$ and $\mathbf{b}$, Bob has $\mathbf{d}'$ and $\mathbf{b}'$.

Second Phase: Public discussion

1. Alice sends $\mathbf{b}$ over the public channel, Bob confronts it with $\mathbf{b}'$, and answers to Alice the set $S = \{i \mid b_i = b'_i\}$. Only the corresponding qubits have been correctly measured, and the others are discarded.
2. Alice chooses a subset oh the remaining bits in $\mathbf{d}$ and discloses their values to Bob. For each d_i in this subset, since it holds $b_i = b'_i$, it should be $d_i = d'_i$. If Bob notices discrepancies $d_i \neq d'_i$, eavesdropping is detected.
3. The shared secret $\mathbf{k} \in \{0,1\}^N$ is the string of bits in $\mathbf{d} = \mathbf{b}'$ that have not been disclosed at step 2.

BB84 Observations

- Alice secret, **d**, is never completely disclosed. Each bit is sent "encrypted" as $|\phi_{b_i d_i}\rangle$ over the quantum channel. Later, the "key" b_i is revealed, but only **after that the quantum information** $|\phi_{b_i d_i}\rangle$ **is destroyed**.
- If Eve guesses the right base each time, her presence is undetectable, but the probability of this event decreases exponentially with n.

Eavesdropper's attacks

What can Eve do? She can intercept every qubit on the channel, measure it, and send to bob a substitute
We will examine two different attacks:

Eavesdropper's attacks

What can Eve do? She can intercept every qubit on the channel, measure it, and send to bob a substitute

We will examine two different attacks:

- **Intercept-Resend attack**: Alice sends qubit $|\psi_{bd}\rangle$, Eve chooses a basis $\hat{b}$, and measures Alice's qubit, obtaining $\hat{d}$. If $\hat{b} = b$, then $\hat{d} = d$, else $\hat{d}$ will be a random bit. Eve will send to Bob $|\psi_{\hat{b}\hat{d}}\rangle$.

Eavesdropper's attacks

What can Eve do? She can intercept every qubit on the channel, measure it, and send to bob a substitute
We will examine two different attacks:

- **Intercept-Resend attack**: Alice sends qubit $|\psi_{bd}\rangle$, Eve chooses a basis $\hat{b}$, and measures Alice's qubit, obtaining $\hat{d}$. If $\hat{b} = b$, then $\hat{d} = d$, else $\hat{d}$ will be a random bit. Eve will send to Bob $|\psi_{\hat{b}\hat{d}}\rangle$.
- **Random Substitute attack**: Alice sends qubit $|\psi_{bd}\rangle$, Eve chooses a basis $\hat{b}$ and a bit $\hat{d}$, and measures Alice's qubit. If $\hat{b} = b$, then Eve has discovered d. Independently from the measurment, Eve will send to Bob $|\psi_{\hat{b}\hat{d}}\rangle$.

PRISM Formalization: Channel

```
module ChannelResend
ch_state : [0..4];
ch_bas : [0..1];
ch_bit : [0..1];
[aliceput] (ch_state=0) ->
    (ch_state'=1) & (ch_bas'=al_bas) & (ch_bit'=al_bit);
[evemeasure] (ch_state=1) & (ch_bas=eve_bas) -> (ch_state'=2);
[evemeasure] (ch_state=1) & (ch_bas!=eve_bas) ->
    0.5 : (ch_state'=2) &(ch_bit'=0) +
    0.5 : (ch_state'=2) &(ch_bit'=1);
[eveget] (ch_state=2) -> (ch_state'=3);
[eveput] (ch_state=3) ->
    (ch_state'=4) & (ch_bas'=eve_bas) & (ch_bit'=eve_bit);
[bobget] (ch_state=4) -> (ch_state'=0);
endmodule
```

PRISM Formalization: Alice

```
const int N;
module Alice
al_state : [0..5];
al_index : [1..N];
al_bas : [0..1];
al_bit : [0..1];
[] (al_state=0) & (eve_state>0) ->
    0.5 : (al_state'=1) & (al_bas'=0) +
    0.5 : (al_state'=1) & (al_bas'=1);
[] (al_state=1) ->
    0.5 : (al_state'=2) & (al_bit'=0) +
    0.5 : (al_state'=2) & (al_bit'=1);
[aliceput] (al_state=2) -> (al_state'=3);
[reveal] (al_state=3) -> (al_state'=4);
[loop] (al_state=4) & (al_index<N) -> (al_state'=0) & (al_index'=al_index+1);
[loop] (al_state=4) & (al_index=N) -> (al_state'=5);
[stop] (al_state=4) -> (al_state'=4);
[stop] (al_state=5) -> (al_state'=5);
endmodule
```

PRISM Formalization: Bob

```
const int CHECKBIT;
module Bob
bob_state : [0..7];
bob_bas : [0..1];
bob_bit : [0..1];
[] (bob_state=0) & (eve_state>0) ->
    0.5 : (bob_state'=2) & (bob_bas'=0) +
    0.5 : (bob_state'=2) & (bob_bas'=1);
[bobget] (bob_state=2) & (bob_bas=ch_bas) -> (bob_state'=3) & (bob_bit'=ch_bit);
[bobget] (bob_state=2) & (bob_bas!=ch_bas) ->
    0.5 : (bob_bit'=ch_bit) & (bob_state'=3) +
    0.5 : (bob_bit'=1-ch_bit) & (bob_state'=3);
[reveal] (bob_state=3) & (bob_bas!=al_bas) -> (bob_state'=4);
[reveal] (bob_state=3) & (bob_bas=al_bas)  -> (bob_state'=5);
[] (bob_state=5) & (bob_bit!=al_bit) -> (bob_state'=7);
[] (bob_state=5) & (bob_bit=al_bit) -> (bob_state'=4);
[loop] (bob_state=4) & (al_index<N) -> (bob_state'=0);
[loop] (bob_state=4) & (al_index=N) -> (bob_state'=6);
[stop] (bob_state=6) -> (bob_state'=6); // no eavesdropping detected
[stop] (bob_state=7) -> (bob_state'=7); // eavesdropping detected
endmodule
```

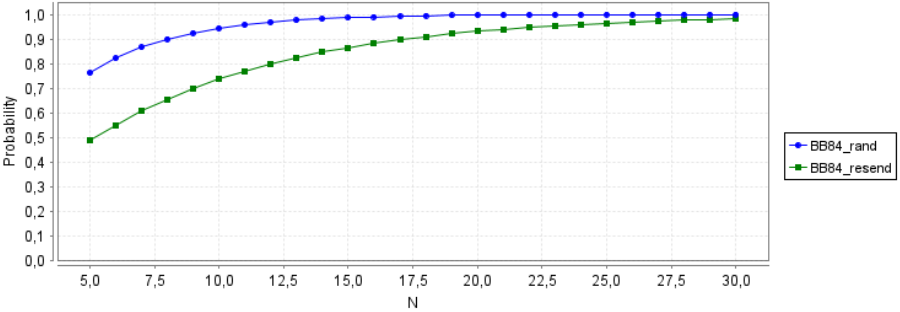
PRISM Formalization: Intercept/Resend

```
module EveResend
eve_state : [0..4];
eve_bas : [0..1];
eve_bit : [0..1];
[] (eve_state=0) ->
    0.5 : (eve_state'=1) & (eve_bas'=0) +
    0.5 : (eve_state'=1) & (eve_bas'=1);
[evemeasure] (eve_state=1) -> (eve_state'=2);
[eveget] (eve_state=2)  -> (eve_state'=3) & (eve_bit'=ch_bit) ;
[eveput] (eve_state=3) -> (eve_state'=0);
endmodule
```

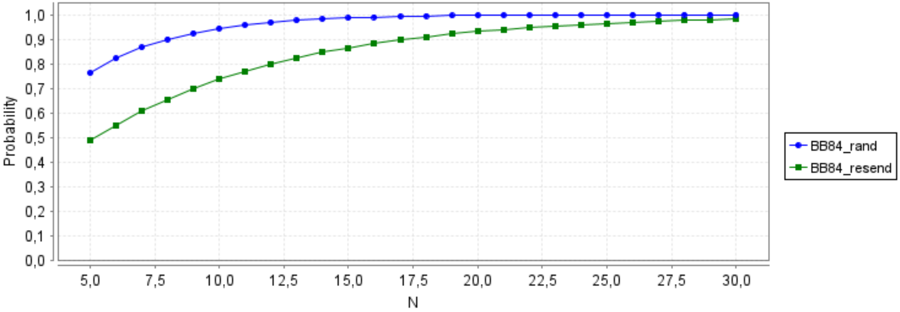
PRISM Formalization: Random Substitution

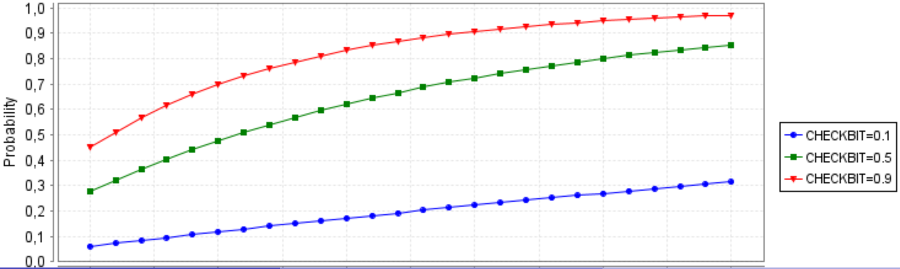
```
module EveRandom
eve_state : [0..4];
eve_bas : [0..1];
eve_bit : [0..1];
[] (eve_state=0) ->
    0.5 : (eve_state'=1) & (eve_bas'=0) +
    0.5 : (eve_state'=1) & (eve_bas'=1);
[evemeasure] (eve_state=1) -> (eve_state'=2);
[eveget] (eve_state=2)  -> (eve_state'=3) & (eve_bit'=ch_bit) ;
[] (eve_state=3) ->
    0.50: (eve_state'=4) & (eve_bit'=0) +
    0.50: (eve_state'=4) & (eve_bit'=1) ;
[eveput] (eve_state=4) -> (eve_state'=0);
endmodule
```

Eve will be detected



Eve will be detected





The B92 Protocol

First Phase: Quantum transmission

1. Alice creates a random string of bits $\mathbf{b} \in \{\boxplus, \boxtimes\}^n$, where $n > N$.
2. Alice sends to Bob the sequence of qubits $|\phi_i\rangle = |\phi_{b_i}\rangle$, where

$$|\phi_{\boxplus}\rangle = |0\rangle \qquad\qquad |\phi_{\boxtimes}\rangle = |+\rangle$$

The B92 Protocol

First Phase: Quantum transmission

1. Alice creates a random string of bits $\mathbf{b} \in \{\boxplus, \boxtimes\}^n$, where $n > N$.
2. Alice sends to Bob the sequence of qubits $|\phi_i\rangle = |\phi_{b_i}\rangle$, where

$$|\phi_{\boxplus}\rangle = |0\rangle \qquad\qquad |\phi_{\boxtimes}\rangle = |+\rangle$$

3. Bob creates a random string of bases $\mathbf{b}' \in \{\boxplus, \boxtimes\}^n$, and measures each $|\phi_i\rangle$ in the bases b'_i. Doing so he construct a sequence of bits $\mathbf{t} \in \{0, 1\}^N$, such that

$$t_i = \begin{cases} 0 \text{ if } |\phi_i\rangle, \text{ measured with } b'_i, \text{ yields } |0\rangle \text{ or } |+\rangle \\ 1 \text{ if } |\phi_i\rangle, \text{ measured with } b'_i, \text{ yields } |1\rangle \text{ or } |-\rangle \end{cases}$$

Second Phase: Public discussion

Alice and Bob will keep only the correct bits, $\mathbf{k} \subseteq \mathbf{b}$

The B92 Protocol

First Phase: Quantum transmission

Alice has $\mathbf{b}$, Bob has $\mathbf{b}'$ and $\mathbf{t}$

Second Phase: Public discussion

1. When $t_i = 1$, it means that Bob has used the wrong basis, and so he knows the original bit b_i, that is $1 - b'_i$. Bob sends $\mathbf{t}$ over the public channel, and both parties keep only the bits for which $t_i = 1$.

The B92 Protocol

First Phase: Quantum transmission

Alice has $\mathbf{b}$, Bob has $\mathbf{b}'$ and $\mathbf{t}$

Second Phase: Public discussion

1. When $t_i = 1$, it means that Bob has used the wrong basis, and so he knows the original bit b_i, that is $1 - b'_i$. Bob sends $\mathbf{t}$ over the public channel, and both parties keep only the bits for which $t_i = 1$.
2. Alice chooses a subset oh the remaining bits in $\mathbf{b}$ and discloses their values to Bob. For each b_i in this subset, it should be $b_i = 1 - b'_i$. If Bob notices discrepancies $b_i = b'_i$, eavesdropping is detected.
3. The shared secret $\mathbf{k} \in \{0, 1\}^N$ is the string of bits in $\mathbf{b} = \mathbf{1} - \mathbf{b}'$ that have not been disclosed at step 2.

B92 Observation

- Alice secret, $\vec{d}$, is never completely disclosed. Each bit is sent codified in a quantum state ($|0\rangle$ or $|+\rangle$), but these two state are not distinguishable without altering them.
- If Bob guesses the right base, he gains no information. If he uses the wrong base, he could measure a state in $\{|0\rangle, |+\rangle\}$, which gives him no information, or a state in $\{|1\rangle, |-\rangle\}$, which is surely an error. He so can deduce the basis that Alice was using.
- With respect to BB84, B92 discards more bits, as the probability of Bob gaining information is $\frac{1}{4}$.

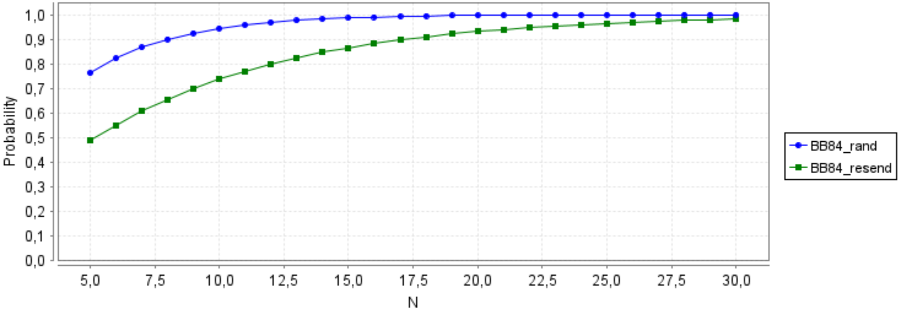
PRISM Formalization: Alice

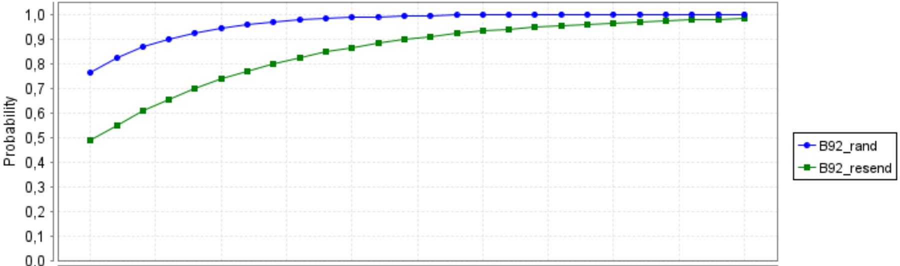
```
module Alice
al_state : [0..5];
al_index : [1..N];
al_bas : [0..1];
al_bit : [0..1];
[] (al_state=0) & (eve_state>0) ->
0.5 : (al_state'=1) & (al_bit'=0) & (al_bas'=0)+
0.5 : (al_state'=1) & (al_bit'=0) & (al_bas'=1);
[aliceput] (al_state=1) -> (al_state'=2);
[reveal] (al_state=2) -> (al_state'=3);
[loop] (al_state=3) & (al_index<N) -> (al_state'=0) & (al_index'=al_index+1);
[loop] (al_state=3) & (al_index=N) -> (al_state'=4);
[stop] (al_state=3) -> (al_state'=3);
[stop] (al_state=4) -> (al_state'=4);
endmodule
```

PRISM Formalization: Bob

```
module Bob
bob_state : [0..7];
bob_bas : [0..1];
bob_bit : [0..1];
[] (bob_state=0) & (eve_state>0) ->
    0.5 : (bob_state'=2) & (bob_bas'=0) +
    0.5 : (bob_state'=2) & (bob_bas'=1);
[bobget] (bob_state=2) & (bob_bas=ch_bas) -> (bob_state'=3) & (bob_bit'=ch_bit);
[bobget] (bob_state=2) & (bob_bas!=ch_bas) ->
    0.5 : (bob_bit'=ch_bit) & (bob_state'=3) +
    0.5 : (bob_bit'=1-ch_bit) & (bob_state'=3);
[reveal] (bob_state=3) & (bob_bit = 0) -> (bob_state'=4);
[reveal] (bob_state=3) & (bob_bit = 1)  ->  (bob_state' = 5);
[] (bob_state=5) & (bob_bas != 1 - al_bas) -> (bob_state'=7);
[] (bob_state=5) & (bob_bas = 1 - al_bas) -> (bob_state'=4);
[loop] (bob_state=4) & (al_index<N) -> (bob_state'=0);
[loop] (bob_state=4) & (al_index=N) -> (bob_state'=6);
[stop] (bob_state=6) -> (bob_state'=6); // no eavesdropping detected
[stop] (bob_state=7) -> (bob_state'=7); // eavesdropping detected
endmodule
```

BB84 and B92

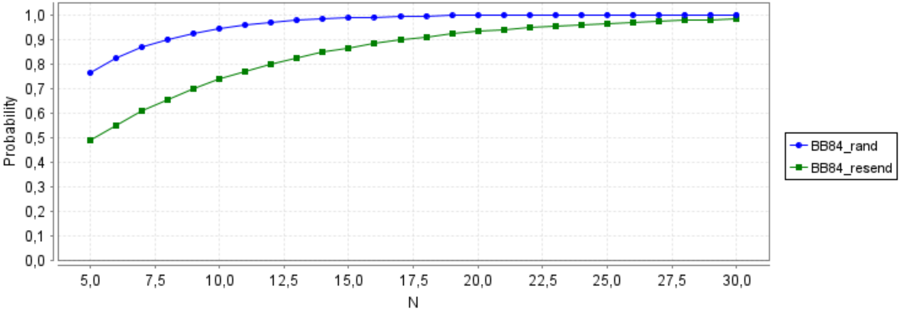

1,0
0,9
0,8
0,7
0,6
0,5
0,4
0,3
0,2
0,1
0,0
Probability
5,0
7,5
10,0
12,5
15,0
17,5
20,0
22,5
25,0
27,5
30,0
N
BB84_rand
BB84_resend


1,0
0,9
0,8
0,7
0,6
0,5
0,4
0,3
0,2
0,1
0,0
Probability
B92_rand
B92_resend

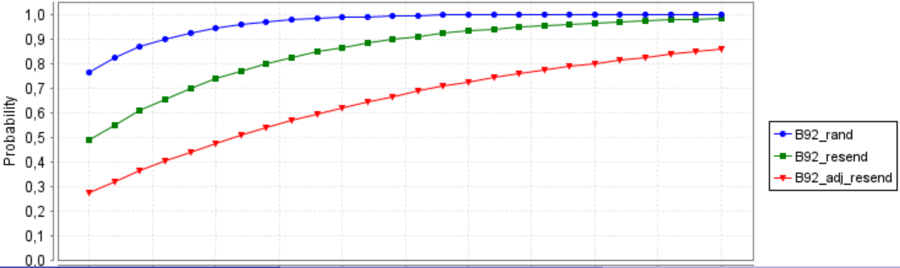
A smarter MIM attack

```
module EveClever
eve_state : [0..4];
eve_bas : [0..1];
eve_bit : [0..1];
[] (eve_state=0) ->
    0.5 : (eve_state'=1) & (eve_bas'=0) +
    0.5 : (eve_state'=1) & (eve_bas'=1);
[evemeasure] (eve_state=1) -> (eve_state'=2);
[eveget] (eve_state=2)  -> (eve_state'=3) & (eve_bit'=ch_bit) ;
[] (eve_state=3) & (eve_bit = 1) ->
    (eve_bas'=1-eve_bas) & (eve_bit'=0) & (eve_state' = 4);
[] (eve_state=3) & (eve_bit = 0) ->
    (eve_bas'=eve_bas) & (eve_bit'=0) & (eve_state' = 4);
[eveput] (eve_state=4) -> (eve_state'=0);
endmodule
```

BB84 and B92

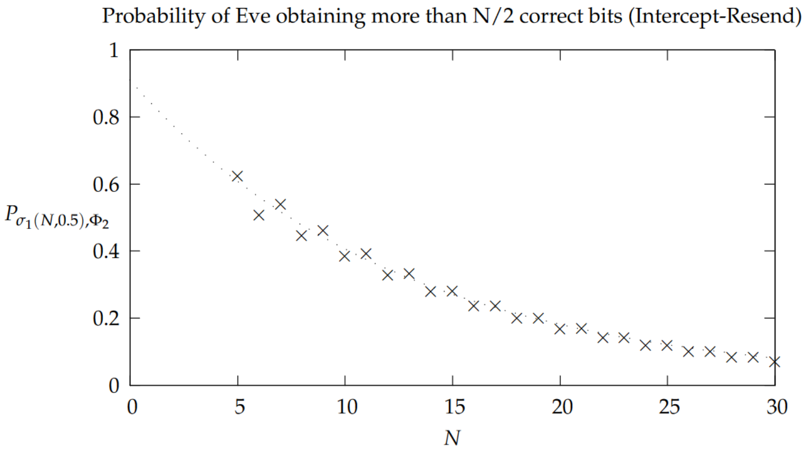


1,0
0,9
0,8
0,7
0,6
0,5
0,4
0,3
0,2
0,1
0,0
Probability
5,0
7,5
10,0
12,5
15,0
17,5
20,0
22,5
25,0
27,5
30,0
N
BB84_rand
BB84_resend

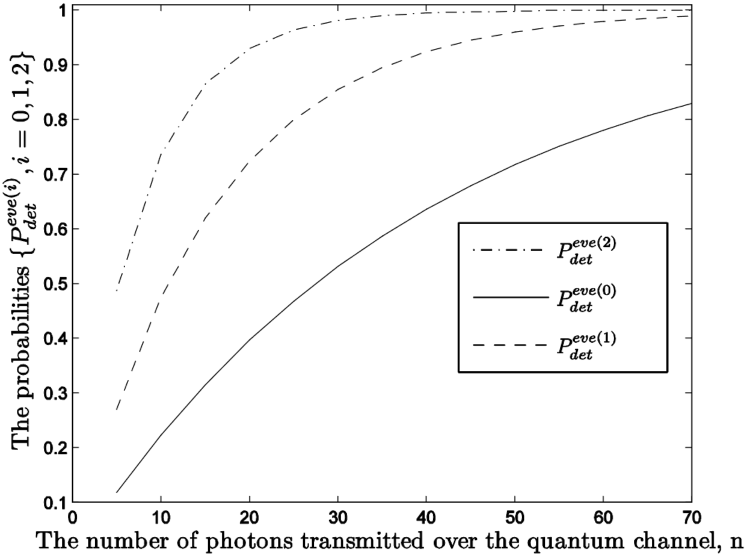


1,0
0,9
0,8
0,7
0,6
0,5
0,4
0,3
0,2
0,1
0,0
Probability
B92_rand
B92_resend
B92_adj_resend

Other interesting metrics: bits obtained by Eve



Other interesting metrics: Eve with different power



Bibliography

M. Elboukhari, M. Azizi, and A. Azizi.
Verification of quantum cryptography protocols by model checking.
International Journal of Network Security and Its Applications, 2, 10 2010.

S. Kuppam.
Modelling of quantum key distribution protocols in communicating quantum processes language with verification and analysis in PRISM.
In *Proceedings of 8th International Conference on Simulation and Modeling Methodologies, Technologies and Applications*. SCITEPRESS - Science and Technology Publications, 2018.

M. A. Nielsen and I. L. Chuang.
Quantum Computation and Quantum Information: 10th Anniversary Edition.
Cambridge University Press, 2010.

N. K. Papanikolaou.
Techniques for design and validation of quantum protocols.
PhD thesis, University of Warwick. Department of Computer Science, 2004.