Eavesdropping on BB84 using $\mathcal{PT}$-symmetry

Author: Nicolas Werner
Facultat de Física, Universitat de Barcelona,
Diagonal 645, 08028 Barcelona, Spain.
email: nicoptimist@gmail.com

Advisor: Bruno Julia Diaz

Abstract: In this work we present the well known BB84 quantum key distribution protocol and we study how could Eve intercept the shared key, assuming that Alice and Bob are able to communicate over the quantum channel with the use of single qubits. Our approach takes advantage of the state of $\mathcal{PT}$-symmetric quantum theory to enhance eavesdropping success.

I. INTRODUCTION

Daily secure communications work with complexity-based key distribution protocols, such as RSA (see [1]). In other words, when two people (whom we call Alice and Bob) share a key using a public channel, the security against an eavesdropper (whom we call Eve) relies on the complexity of the problem that the eavesdropper needs to solve to find the key. However, given the present development of quantum computation, these "complex problems" are likely to become solvable in little time, which may let two options: increasing the lengths of the exchanged keys, that is not always practical, or moving to quantum key distribution (QKD), which puts a physical bound to eavesdroppers' information gain. That is, a bound not only based on Eve's computing capacities, but also based on the laws of quantum mechanics. In this work, we present the most known example of the latter, the BB84 protocol ([2, 3]).

Ever since the protocol was introduced, different eavesdropping attacks have been developed, being photon number splitting attacks the most efficient. These are based on a technical issue when performing BB84: single photon pulses are difficult to control. Instead, multiple coherent photons are sent (weak laser pulses), some of which can be kept by the eavesdropper. However, in here we think of attacking the protocol assuming that it is performed by sending a product state of single qubits, using results from $\mathcal{PT}$-symmetric quantum theory.

This work is structured as follows: in Section II we give a detailed explanation of the BB84 protocol. In Section III we present a rather simple method of eavesdropping, then we make an introduction to $\mathcal{PT}$-symmetric quantum mechanics (III A) and, finally, we show how it could -theoretically- be used to outperform the first method (III B). Some conclusions are given in Section IV.

II. THE BB84 PROTOCOL

The goal of this protocol is that Alice and Bob securely perform key exchange through a public channel. First, let us mention the two results it is based on:

Proposition 1 ([3]). *In any attempt to distinguish between two non-orthogonal quantum states, information gain (in the sense of von Neumann entropy) is only possible at expense of introducing noise to the signal.*

Theorem 1 (No-cloning, [3]). *Let $|\varphi\rangle$ be an unknown state from a set of states S. If the states in S are non-orthogonal, it is not possible to build a device that makes a copy of $|\varphi\rangle$.*

And the protocol is the following:

1. Alice randomly generates two strings of classical bits, a and b, of length $(4+\delta)n$, where n is the length of the final shared key and δ is a parameter that controls the chances of success.

2. Alice encodes these strings into a product state made of $(4+\delta)n$ qubits. For every qubit, she works with one of the following orthonormal basis Z, X:

$$Z\begin{cases}|\psi_{00}\rangle = |0\rangle \\ |\psi_{10}\rangle = |1\rangle\end{cases}, X\begin{cases}|\psi_{01}\rangle = (|0\rangle + |1\rangle)/\sqrt{2} \\ |\psi_{11}\rangle = (|0\rangle - |1\rangle)/\sqrt{2}\end{cases}.$$

   She reads $a = (a_i)$ and $b = (b_i)$ in parallel and does the following at each step:

   • If $b_i = 0$, she encodes a_i creating the state $|\psi_{a_i 0}\rangle$.
   • If $b_i = 1$, she encodes a_i creating the state $|\psi_{a_i 1}\rangle$.

   This results into the product state

$$|\psi\rangle = \bigotimes_{i=1}^{(4+\delta)n} |\psi_{a_i b_i}\rangle .$$

   Notice that the states in Z are not orthogonal to those in X. Also, this can be replaced by $(4+\delta)n$ rounds of a single state from $Z \cup X$. To ease the notation, we write $|a_i b_i\rangle$ for $|\psi_{a_i b_i}\rangle$.

3. Alice sends $|\psi\rangle$ to Bob through the public channel. He receives $\varepsilon(|\psi\rangle\langle\psi|)$, where $|\psi\rangle\langle\psi|$ is the density matrix of the state and ε refers both to the noise of the public channel and the noise caused by Eve (we do not work on any further considerations about noise). Bob publicly announces the reception of the state.

4. Bob creates an arbitrary bit string b' of length $(4+\delta)n$ and performs a measurement on each qubit, using Z or X as determined by b'. He stores his measurements in a bit string a' and destroys the post-measurement product state.

5. Alice and Bob meet on the public channel and compare b and b'. When $b_i = b'_i$, they *expect* to be holding the same bit: $a_i = a'_i$. Because, ideally, a pure state was created and then it was measured with respect to the basis it belonged.

   They choose $2n$ indexes where the key exchange was successful. If there are less, they abort the protocol. δ is chosen big enough so that there is high probability of finding $2n$ matches (see Subsection II A). This step is called *basis reconciliation.*

6. Finally, Alice and Bob must check security, since channel noise and eavesdropping may have interfered. Pure states may have turned into non-pure, thus giving the chance for Bob to get a flipped measurement. To do so, they both publish a subset of n bits from the $2n$ selected (from a and a') and compare. If the coincidence ratio is not sufficiently high for them, they abort the protocol. Otherwise, Alice and Bob have successfully shared a key of n bits.

Now we take Eve's perspective, who wants to eavesdrop the key. For every qubit $|a_i b_i\rangle$ she would like to know b_i before the state is destroyed, that is, the basis in which it was encoded. This would allow her to measure the qubit using the appropriate basis, take all its information and then send a copy to Bob in order to remain hidden. The first way to do this, would be to discriminate if the qubit belongs to X or Z, but Proposition 1 and non-orthogonality between X and Z ensure that she will make herself (statistically) visible in any attempt of it. The other way would be to store a copy of the qubit and wait until Alice and Bob do basis reconciliation in order to know b. But Theorem 1 guarantees this is not an option.

A. Chances of success

There are two steps where the protocol can be aborted. One happens when Alice and Bob exchange n bits from a and a' respectively and check security. Statistics are easy: a coincidence ratio is previously fixed according to the desired security, under which the protocol is aborted.

The other step is basis reconciliation. For the protocol to move on, there must be not less than $2n$ coincidences among the $(4+\delta)n$ pairs of bits that are compared. But what are the chances?

b and b' are randomly generated. Considering the i-th bit, there is probability $1/2$ of coincidence, since there are 4 cases with equal probability, two of success and two of non-success. Hence, the process of comparing all $(4+\delta)n$ pairs of bits can be regarded as flipping a fair coin $(4+\delta)n$ times. The probability of having $m \geq 2n$ matches is given by a binomial distribution:

$$P(m \geq 2n) = \frac{1}{2^{(4+\delta)n}} \sum_{i=2n}^{(4+\delta)n} \binom{(4+\delta)n}{i}. \qquad (1)$$

Table I shows some computations for the chances of basis reconciliation.

$n=2$		
δ	$(4+\delta)n$	$P(m \geq 2n)$
0	8	0.63672
1	10	0.82812
2	12	0.92700
3	14	0.97131

$n=4$		
δ	$(4+\delta)n$	$P(m \geq 2n)$
0	16	0.59819
1	20	0.86841
2	24	0.96804
3	28	0.99373

$n=6$		
δ	$(4+\delta)n$	$P(m \geq 2n)$
0	24	0.58059
1	30	0.89976
2	36	0.98559
3	42	0.99856

$n=8$		
δ	$(4+\delta)n$	$P(m \geq 2n)$
0	32	0.56997
1	40	0.92307
2	48	0.99336
3	56	0.99966

TABLE I: Chances of basis reconciliation for different values of δ and n, see equation (1). Computations are done using the `binom.cdf( , , )` function from `scipy` python library.

III. EAVESDROPPING

Just as a framework, we present a naive approach for eavesdropping, not making big efforts in hiding from Alice and Bob and also neglecting channel noise.

Let Eve perform a measurement with respect to one of the basis X and Z on an intercepted key qubit $|\psi_{a_i b_i}\rangle$. There are two equally possible scenarios at this point: (i), if she takes the right basis (the one indicated by b_i), she gets the bit that was actually encoded. Ideally, she is then able reproduce the same state $|\psi_{a_i b_i}\rangle$ and send it to Bob, so he won't notice the eavesdropping. And (ii), if Eve takes the wrong basis to perform her measurements, what she gets is 0 or 1 with probability $1/2$. Furthermore, when she tries to rebuild the state $|\psi_{a_i b_i}\rangle$, she encodes this random bit in a state from the wrong basis she chose. Then she sends this new product state $|\psi'\rangle$ to Bob. Because this is one of the key bits, Bob measures $|\psi_{a_i b_i}\rangle$ with the basis it does not belong to, thus having $1/2$ of chances of error ($a_i \neq a'_i$), which may be noticed at the security check.

Now, consider the n bits which constitute the key (after basis reconciliation and security check). On each of these, Eve has probability $1/2$ of using the right basis and, when using the wrong one, she has again probability $1/2$ to get

the right bit. All in all, she expects a 75% of success:

$$P_{✓} = P(✓/_{\text{i}})\frac{1}{2} + P(✓/_{\text{ii}})\frac{1}{2} = 1\times\frac{1}{2} + \frac{1}{2}\times\frac{1}{2} = 75\%.$$

In the following, we -theoretically- improve this ratio with the use of $\mathcal{PT}$-symmetric quantum mechanics. We show a way in which Eve may be able to discriminate between one of the states and the other three without destroying them.

A. $\mathcal{PT}$-symmetry

We somehow extend the standard margins of quantum mechanics, allowing non hermitian hamiltonians. We move to another class of operators, the so called *$\mathcal{PT}$-symmetric operators*. This class does not contain all hermitian operators. What actually holds is that $\{\mathcal{PT}-symmetric\ op.\} \cap \{hermitian\ op.\} = \{real\ and\ symmetric\ op.\}$.

To present $\mathcal{PT}$-symmetric quantum mechanics, we must first introduce $\mathcal{P}$, the *parity operator*, and $\mathcal{T}$, the *time reversal operator*. They are defined by the following properties:

$$\begin{cases} \mathcal{P}\hat{x}\mathcal{P} = -\hat{x} \\ \mathcal{P}\hat{p}\mathcal{P} = -\hat{p} \end{cases} \qquad \begin{cases} \mathcal{T}\hat{x}\mathcal{T} = \hat{x} \\ \mathcal{T}\hat{p}\mathcal{T} = -\hat{p} \\ \mathcal{T}i\mathcal{T} = -i \end{cases} .$$

For the latter, antilinearity is a consequence of the first two requested properties and the fact that $[x,p] = i\hbar\,\mathbf{1}$.

Also, we recall that *given any physical quantum theory, (i) it must possess a Hilbert space of state vectors with an inner product, (ii) its time evolution must be unitary, that is, norms given by the inner product must be preserved in time, and (iii) hamiltonians must have real spectrum.*

In [7] it is proved that hamiltonians satisfying $[\mathcal{H},\mathcal{PT}] = 0$ have real spectrum. The commuting condition is denoted $\mathcal{H} = \mathcal{H}^{\mathcal{PT}}$ and it is said that $\mathcal{H}$ has *unbroken $\mathcal{PT}$-symmetry*. Also in [7], with the use of a special operator $\mathcal{C}$, a new inner product is defined over the Hilbert Space spanned by the hamiltonians' eigenstates, and it is shown that time evolution is still unitary. As for the eigenstates of these hamiltonians, orthogonality with respect to the usual inner product is lost in general. For our concern, we restrict ourselves to the following two dimensional $\mathcal{PT}$-symmetric hamiltonians (see [8] for a more general two dimensional form):

$$\mathcal{H} = \begin{pmatrix} re^{i\theta} & s \\ s & re^{-i\theta} \end{pmatrix},$$

where r, s, θ are real parameters. The $\mathcal{PT}$-symmetry of this hamiltonian remains unbroken only when $s^2 \geq r^2\sin^2\theta$. Hence, when this inequality holds, a parameter α may be defined such that $\sin(\alpha) = \frac{r}{s}\sin(\theta)$. For any two states λ, μ, the inner product is defined as

$$\langle\lambda|\mu\rangle_{\mathcal{CPT}} := (\mathcal{CPT}\lambda)^T\cdot\mu = \lambda^T(\mathcal{CPT})^T\cdot\mu\ , \quad \text{where}$$
$$\mathcal{C} = \frac{1}{\cos(\alpha)}\begin{pmatrix} i\sin(\alpha) & 1 \\ 1 & -i\sin(\alpha) \end{pmatrix}.$$

In [7] it is shown that for any state $|\mu\rangle$ the product $\langle\mu|\mu\rangle_{\mathcal{CPT}}$ is real, non-negative and vanishes if, and only if, $|\mu\rangle = 0$. Also, the norm of a state is defined as always: $||\,|\mu\rangle\,||_{\mathcal{CPT}} := \sqrt{\langle\mu|\mu\rangle_{\mathcal{CPT}}}$. We will omit the $\mathcal{CPT}$ subscript from now on.

B. Attacking protocol

Eve intercepts one of the four states involved in the BB84 protocol, $|a_ib_i\rangle \in \{|00\rangle, |10\rangle, |01\rangle, |11\rangle\}$. First, she applies the following gate:

$$R = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix},$$

so one of the following transformations occurs:

$$\begin{aligned} |00\rangle = |0\rangle &\longmapsto |0\rangle =: |00^*\rangle \\ |10\rangle = |1\rangle &\longmapsto i\,|1\rangle =: |10^*\rangle \end{aligned}$$

$$\begin{aligned} |01\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} &\longmapsto \frac{|0\rangle + i\,|1\rangle}{\sqrt{2}} =: |01^*\rangle \\ |11\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} &\longmapsto \frac{|0\rangle - i\,|1\rangle}{\sqrt{2}} =: |11^*\rangle\,. \end{aligned}$$

According to the new inner product, we have

$$\begin{aligned} \langle 01^*| &= (\mathcal{CPT}\,|01^*\rangle)^T \\ &= \left[\frac{1}{\cos(\alpha)}\begin{pmatrix} i\sin(\alpha) & 1 \\ 1 & -i\sin(\alpha) \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\mathcal{T}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix}\right]^T \\ &= \frac{1}{\cos(\alpha)}\left[\begin{pmatrix} i\sin(\alpha) & 1 \\ 1 & -i\sin(\alpha) \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix}\right]^T \\ &= \frac{1}{\sqrt{2}\cos(\alpha)}\left[\begin{pmatrix} 1 & i\sin(\alpha) \\ -i\sin(\alpha) & 1 \end{pmatrix}\begin{pmatrix} 1 \\ -i \end{pmatrix}\right]^T \\ &= \frac{1+\sin(\alpha)}{\sqrt{2}\cos(\alpha)}\begin{pmatrix} 1 \\ -i \end{pmatrix}^T . \end{aligned} \tag{2}$$

In the same way, we get

$$\langle 11^*| = \frac{1-\sin(\alpha)}{\sqrt{2}\cos(\alpha)} \begin{pmatrix} 1 \\ i \end{pmatrix}^T , \tag{3}$$

$$\langle 00^*| = \frac{1}{\cos(\alpha)} \begin{pmatrix} 1 \\ -i\sin(\alpha) \end{pmatrix}^T , \tag{4}$$

$$\langle 10^*| = \frac{1}{\cos(\alpha)} \begin{pmatrix} \sin(\alpha) \\ -i \end{pmatrix}^T . \tag{5}$$

And it follows that

$$\langle 01^*|11^*\rangle = \frac{1+\sin(\alpha)}{\sqrt{2}\cos(\alpha)} \begin{pmatrix} 1 \\ -i \end{pmatrix}^T \begin{pmatrix} 1 \\ -i \end{pmatrix} = 0. \tag{6}$$

This $\mathcal{PT}$-orthogonality allows us to build the following $\mathcal{PT}$-projectors:

$$P_1 = \frac{|01^*\rangle\langle 01^*|}{\langle 01^*|01^*\rangle} = \frac{1}{2}\begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix}, \tag{7}$$

$$P_2 = \frac{|11^*\rangle\langle 11^*|}{\langle 11^*|11^*\rangle} = \frac{1}{2}\begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}. \tag{8}$$

We define a measuring operator as $\mathcal{M} := P_1 - P_2$. From [7], we know that $\mathcal{M}$ is a $\mathcal{PT}$-observable (has real spectrum) because it fulfills $\mathcal{M}^T = \mathcal{CPT}\mathcal{M}\mathcal{CPT}$. Recall that $\mathcal{M}$'s eigenstates are $|01^*\rangle$, with eigenvalue 1, and $|11^*\rangle$, with eigenvalue -1, that are orthogonal with respect to our new inner product but not with respect the usual one.

This non-orthogonality in the usual Hermitian sense, puts us in a frame where the measuring devices we are used to no longer work. $\mathcal{CPT}$ measuring devices are still under development (see [11]). Let's see, however, the possible benefits. From (2), (3), (4) and (5) we compute the following $\mathcal{CPT}$-products:

$$\begin{aligned}
\langle 01^*|00^*\rangle &= \langle 01^*|10^*\rangle = \frac{1+\sin(\alpha)}{\sqrt{2}\cos(\alpha)} , \\
\langle 11^*|00^*\rangle &= -\langle 11^*|10^*\rangle = \frac{1-\sin(\alpha)}{\sqrt{2}\cos(\alpha)} , \\
\langle 01^*|01^*\rangle &= \frac{1+\sin(\alpha)}{\cos(\alpha)} , \\
\langle 11^*|11^*\rangle &= \frac{1-\sin(\alpha)}{\cos(\alpha)} , \\
\langle 00^*|00^*\rangle &= \langle 10^*|10^*\rangle = \frac{1}{\cos(\alpha)} .
\end{aligned} \tag{9}$$

From here we compute the cosines between states:

$$\begin{aligned}
\cos(|01^*\rangle, |00^*\rangle) &= \frac{\langle 01^*|00^*\rangle}{\sqrt{\langle 01^*|01^*\rangle}\sqrt{\langle 00^*|00^*\rangle}} \\
&= \sqrt{\frac{1+\sin(\alpha)}{2}} ,
\end{aligned} \tag{10}$$

$$\cos(|01^*\rangle, |10^*\rangle) = \sqrt{\frac{1+\sin(\alpha)}{2}} , \tag{11}$$

$$\cos(|11^*\rangle, |00^*\rangle) = \sqrt{\frac{1-\sin(\alpha)}{2}} , \tag{12}$$

$$\cos(|11^*\rangle, |10^*\rangle) = -\sqrt{\frac{1-\sin(\alpha)}{2}} . \tag{13}$$

So, when $\alpha \to \frac{\pi}{2}$, (10) and (11) tend to 1, and (12) and (13) vanish. Recall that $\alpha = \pm\frac{\pi}{2}$ are the "break-points" of the $\mathcal{PT}$-symmetry of the hamiltonian. Getting close to these might not be feasible on an experiment. However, we assume that we have a $\mathcal{PT}$-symmetric device that is able to perform measurements according to $\mathcal{M}$, and that it allows us to take values of α so that we can assume $\alpha \simeq \frac{\pi}{2}$. Also, recall that for any two normalized states $|\varphi\rangle, |\phi\rangle$:

$$|\varphi\rangle = |\phi\rangle \;\Leftrightarrow\; 0 = ||\,|\varphi\rangle - |\phi\rangle\,||^2 = 2 - \langle\varphi|\phi\rangle - \overline{\langle\varphi|\phi\rangle}.$$

In our case, using (10) and (11), we have

$$\begin{aligned}
&\left|\left| \frac{|01^*\rangle}{\sqrt{\langle 01^*|01^*\rangle}} - \frac{|00^*\rangle}{\sqrt{\langle 00^*|00^*\rangle}} \right|\right|^2 \\
&\qquad = 2\left(1 - \sqrt{\frac{1+\sin(\alpha)}{2}}\right),
\end{aligned} \tag{14}$$

$$\begin{aligned}
&\left|\left| \frac{|01^*\rangle}{\sqrt{\langle 01^*|01^*\rangle}} - \frac{|10^*\rangle}{\sqrt{\langle 10^*|10^*\rangle}} \right|\right|^2 \\
&\qquad = 2\left(1 - \sqrt{\frac{1+\sin(\alpha)}{2}}\right).
\end{aligned} \tag{15}$$

Both expressions vanish as $\alpha \to \frac{\pi}{2}$. That is, by taking the states normalized and by adjusting the $\mathcal{CPT}$-product, the state $|01^*\rangle$ becomes almost equal to the states $|00^*\rangle, |10^*\rangle$. Also, from equations (12) and (13), the state $|11^*\rangle$ becomes almost orthogonal to them. With this in hand, we go back to the attacking protocol itself. After applying the R gate, Eve measures according to $\mathcal{M}$, so there are four equally probable scenarios:

(i) $R\,|a_i b_i\rangle = |00^*\rangle$. When measuring according to $\mathcal{M}$, the measure leads to the same result as if we were measuring $|11^*\rangle$, with probability $p \simeq 1$. That is, the measure has outcome 1 with probability $p \simeq 1$.

(ii) $R\,|a_i b_i\rangle = |10^*\rangle$. Similarly, the outcome for $\mathcal{M}$ is 1 with probability $p \simeq 1$.

(iii) $R\,|a_i b_i\rangle = |01^*\rangle$. In this case, because of the definition of $\mathcal{M}$ the outcome is 1 with probability $p = 1$.

(iv) $R\,|a_i b_i\rangle = |11^*\rangle$. Finally, this is the only case in which, by definition, the outcome is -1 with probability $p = 1$.

So, if she gets a -1, she already knows that she had the $|11^*\rangle$ state in hands, so she knows that the encoded bit was 1 in the X basis. She has the right bit and she is able to send Bob a copy of the state.

If the outcome is 1, she knows that the state belongs to $\{|00^*\rangle, |10^*\rangle, |01^*\rangle\}$ (with equally distributed probability). Notice that, with probability close to one, the state is not destroyed. In this case, she first applies R^{-1} in order to go back to the set $\{|00\rangle, |10\rangle, |01\rangle\}$. Now, because there are two possible states from Z and only one from X, Eve performs an hermitian measurement according to the Z basis. The conditioned chances of success are

$$P(\checkmark/_{\mathcal{M}\,=\,1}) = \frac{2}{3}\times 1 + \frac{1}{3}\times\frac{1}{2} = \frac{5}{6}.$$

So, all in all, the chances of success are

$$\begin{aligned} P_{\checkmark} =& \frac{1}{4}P(\checkmark/_{\mathcal{M}=-1}) + \frac{3}{4}P(\checkmark/_{\mathcal{M}=1}) \\ =& \frac{1}{4} + \frac{3}{4}\times\frac{5}{6} = 87.5\%. \end{aligned}$$

IV. CONCLUSIONS

We have shown in detail how the BB84 works and also two ways of eavesdropping on it. While the naive 75%-approach is feasible, the second one may take some more time of experimental research before it can be performed (see [11]). It could happen that measuring with such a $\mathcal{PT}$-symmetric device involves transformations that have non-zero probability of destroying the state before any information is taken. Also, bringing α close to the breakpoints $\pm\frac{\pi}{2}$ is likely to be difficult to implement on an experiment, because we are getting close to the hamiltonian not having real spectrum.

Recent works are discussing possible solutions for these issues. In [9] it is shown that, considering our hamiltonian, there is a point in time evolution in which non orthogonal states become orthogonal (in the hermitian sense). At this time, these two states could be discriminated with the use of current devices. Moreover, in [12] they show how to simulate such a time evolution on a single qubit with the use on ancillary states. It must be studied, nevertheless, how all four states evolve in time and see what are the chances of eavesdropping.

Acknowledgments

I would like to express my gratitude to my advisor, Bruno Julia, for seeing me every week over the past few months, solving my doubts and giving me confidence. It has been and exciting journey to me. And I would also like to thank my close family, as they gave me the chance of living in this city and pursuing my studies.

[1] W. Trappe, L.C. Washington, *Introduction to Cryptography with Coding Theory (2nd Edition)*, Prentice-Hall, (2005).
[2] C.H. Bennett, G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, Theoretical Computer Science, Vol. 560 (Part 1), 2014, pp. 7-11, (1984).
[3] M. Nielsen, I. Chuang, *Quantum computation and quantum information*, Cambridge University Press (2010).
[4] Y. Balytsky, M. Raavi, A. Pinchuk, S.Y. Chang, *$\mathcal{PT}$-Symmetric Quantum State Discrimination for Attack on BB84 Quantum Key Distribution* (conference paper), University of Colorado Springs, CO 80918, USA, (2021).
[5] A. Chefles, *Unambiguous Discrimination Between Linearly-Independent Quantum States*, Phys. Lett. A 239 (1998) 339-347.
[6] A. Ekert, B. Huttner, G.M. Palma, A. Peres, *Eavesdropping on quantum-cryptographical systems*, Phys. Rev. A 50 (1994) 1047.
[7] C.M. Bender, *Introduction to PT-Symmetric Quantum theory*, Contemp. Phys. 46:277-292, (2005).
[8] C.M. Bender, P.N. Meisinger, Q. Wang, *Finite-Dimensional $\mathcal{PT}$-Symmetric Hamiltonians*, arXiv 0303174 (2003).
[9] C.M. Bender et al., *$\mathcal{PT}$-symmetric quantum state discrimination*, Philos. Trans. R. Soc. A371, 20120160 (2013).
[10] C.M. Bender, D.C. Brody, H.F. Jones, *Complex Extension of Quantum Mechanics*, Phys. Rev. Lett. 89: 270402 (2002).
[11] Y.T. Wang et al., *Experimental investigation of state distinguishability in parity-time symmetric quantum dynamics*, Phys. Rev. Lett. 124(23): 230402, (2020).
[12] J. Wen et al., *Experimental demonstration of a digital quantum simulation of a general $\mathcal{PT}$-symmetric system*, Phys. Rev. A 99: 062122 (2019).
[13] D. Stucki et al., *Long term performance of the SwissQuantum quantum key distribution network in a field environment*, New J. Phys. 13: 123001 (2011).
[14] B. Fröhlich et al., *Long-distance quantum key distribution secure against coherent attacks*, Optica 4: 163-167 (2017).
[15] A. Niederberger, V. Scarani, and N. Gisin, *Photon-number-splitting versus cloning attacks in practical implementations of the Bennett-Brassard 1984 protocol for quantum cryptography*, Phys. Rev. A 71: 042316 (2005).