$\mathcal{PT}$-Symmetric Quantum State Discrimination for Attack on BB84 Quantum Key Distribution

Yaroslav Balytskyi[1], Manohar Raavi[2], Anatoliy Pinchuk[1], Sang-Yoon Chang[2]

[1] University of Colorado Colorado Springs, CO 80918, USA
Department of Physics and Energy Science
{ybalytsk,apinchuk}@uccs.edu
[2] University of Colorado Colorado Springs, CO 80918, USA
Department of Computer Science
{mraavi,schang2}@uccs.edu

Abstract. Quantum Key Distribution or QKD provides symmetric key distribution using the quantum mechanics/channels with new security properties. The security of QKD relies on the difficulty of the quantum state discrimination problem. We discover that the recent developments in $\mathcal{PT}$ symmetry can be used to expedite the quantum state discrimination problem and therefore to attack the BB84 QKD scheme. We analyze the security of the BB84 scheme and show that the attack significantly increases the eavesdropping success rate over the previous Hermitian quantum state discrimination approach. We design and analyze the approaches to attack BB84 QKD protocol exploiting an extra degree of freedom provided by the $\mathcal{PT}$-symmetric quantum mechanics.

1 Introduction

Security and cryptographic mechanisms rely on the secret key between the authorized sender and receiver for the confidentiality or integrity protections. While public-key cryptography offers mechanisms to exchange keys so that the outcome of the public-key exchange yields the symmetric keys, the traditional public-key key exchange based on RSA and Diffie-Hellman Key Exchange are in risk because of the emerging quantum computing. The advancement of quantum computing is both in practice (proof-of-concept quantum computers, e.g., IBM [12] and Google [16]) and in the algorithms building on quantum computers (e.g., Shor's algorithm, Ref. [22]). While such quantum computing developments can be used for expediting the solving of the problems for beneficial purposes, it can also find its uses for breaking the traditional cryptographic ciphers. The traditional hardness problems anchoring the security of such key exchange algorithms, such as prime factorization problem, can be solved in polynomial time by the attackers equipped with quantum computers. National Institute of Standards Technology (NIST), traditionally influential in standardizing and facilitating the deployment of cryptographic ciphers, e.g., DES, AES, is therefore currently in the multi-year process of standardizing quantum-resistant key exchange ciphers.

More recent developments for key exchange/distribution use the sender-receiver channels, including those using quantum channels/mechanics, Ref. [8,23] or wireless signal channels in radio-frequency (RF), Ref. [9], or in electrical field propagation, Ref. [13]. We focus our study on the emerging Quantum Key Distribution (QKD) which exchanges quantum bits (qubits) between the sender and the receiver over a quantum channel, such as one based on optical communications, Ref. [10,17,11]. QKD provides a unique security property that the authorized sender and receiver can detect if the qubit transmissions have been accessed/eavesdropped and the key compromised so that the sender and receiver can distinguish between the secret key vs. the eavesdropped key.

Unlike the classical public key cryptography, QKD is based on the difficulty of the physical problem of the quantum state discrimination, Ref. [2], and on the no-cloning theorem, Ref. [25]. The goal of the quantum state discrimination is to find in which state the qubit is, and consists of finding an optimal observable and strategy of measurements. The no-cloning theorem ensures that an eavesdropper as able to do the measurement only once, since the qubit cannot be perfectly copied. Since the security of QKD is based on the laws of physics rather than on the hard mathematical problem, it is information-theoretically secure as opposed to assuming a computational bound on the attacker.

We apply the state of the art research on $\mathcal{PT}$-symmetric quantum mechanics and discover a novel method to increase the eavesdropping success rate of the attacker against BB84 QKD protocol. $\mathcal{PT}$ symmetry enables the attacker to discriminate the quantum states with higher probability, enabling the advanced attack to learn the exchanged keys. We construct three approaches for the attack on BB84 in theory and analyze the practicality and implementation options.

The rest of the paper is organized as follows. Section 2 provides the primer and the background in BB84 QKD protocol as well as a comparison between the regular Hermitian quantum mechanics vs. the $\mathcal{PT}$ symmetric one. Section 3 explains how $\mathcal{PT}$ symmetry can advance the quantum state discrimination and, building on that, Section 4 describes the three approaches in attacking BB84 and analyzes them. Section 5 discusses the related work focusing on the QKD in practice and the litearture studying QKD in information-theoretical security. Lastly, Section 6 concludes the paper.

2 A Primer on QKD and $\mathcal{PT}$ Symetry vs. Hermitian Quantum Mechanics

2.1 BB84 QKD Protocol

While in the classical communications the information is encoded in classical bits, in quantum communications, the information is encoded in qubits. This allows to detect the presence of the adversary trying to learn the key since the applied measurement changes the state of the qubit. By comparing the randomly chosen measurements, sender and receiver can detect the presence of an evesdropper in the channel.

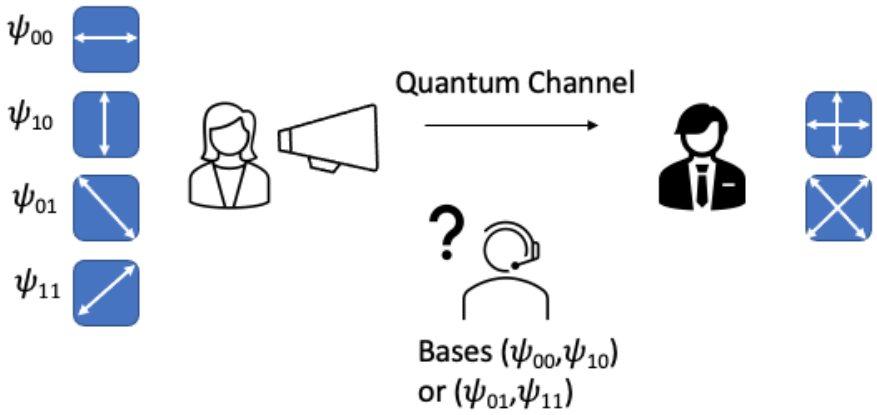

Fig. 1: An illustration of the BB84 protocol for the qubit transmission for the key exchange. The sender Alice (left) transmits the qubits in one of the four states, e.g., ψ_{00}, while the receiver Bob (right) uses either of the two bases to make measurements on the received qubits.

BB84 QKD protocol, Ref. [8], uses the set of two bases:

$$\begin{cases} |\psi_{00}\rangle = |0\rangle \\ |\psi_{10}\rangle = |1\rangle \end{cases} \quad and \quad \begin{cases} |\psi_{01}\rangle = |+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \\ |\psi_{11}\rangle = |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}} \end{cases} \tag{1}$$

Note, the conversion between the first and second basis can done by the Hadamard gate:

$$\mathcal{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Alice generates two threads of random classical bits, a and b, of equal length l and encodes them using the bases in Eqn. 1, by the following block of qubits:

$$|\psi\rangle = \bigotimes_{i=1}^{l} |\psi_{a_i b_i}\rangle$$

which is sent through an open channel to Bob, as illustrated in Fig. 1. Bob generates the thread of random classical bits c of the same length l and makes a measurement in the basis specified by c. Then, Alice and Bob through an open classical channel establish in which cases the classical bits from b and c coincide using the results of the measurements in these cases as the shared secret key and discard the rest.

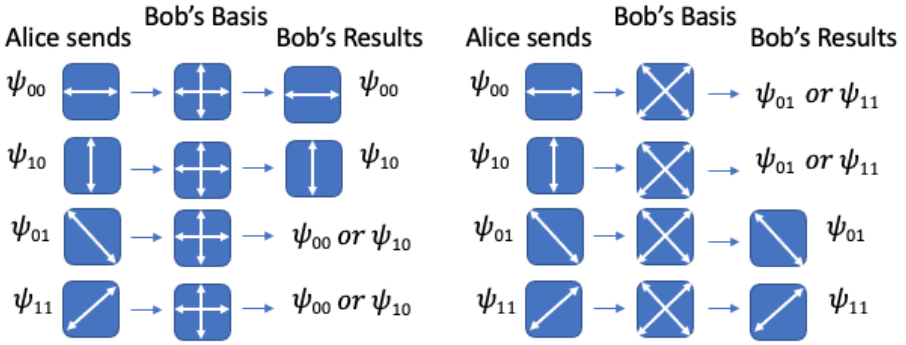

Fig. 2: An illustration of four states used in the BB84 protocol and the Bob's receiving/measurement process. The first column shows the sender Alice's state; the second column corresponds to the receiver Bob's basis; and the third column shows the Bob's measurement/decoding result. If Bob's basis matches and aligns with Alice's state, then Bob can correctly decode the qubit with a probability of 1. If Bob's basis does not match/align with Alice's state, the it becomes a coin toss with Bob's decoding between the two states, i.e., the correct qubit with 0.5 probability. *After* the qubits have been transmitted (not shown in the diagram), the sender shares the bases she used for each of the the qubit transmission so that the receiver and the sender know which qubits were delivered successfully with the matching state/base. These qubits are used to construct the secret key.

To demonstrate an advantage of the $\mathcal{PT}$-symmetric quantum mechanics over the Hermitian one for an attack on BB84, we consider the simplest Eve's attack in both approaches.

In the conventional Hermitian quantum mechanics, Eve who is trying to learn the key guesses the basis correctly in 50% of the cases, and in the other 50% of the cases the results of her measurements becomes a coin toss with a random output, Fig.2. Therefore, on average, Eve is able to guess 75% of the bits correctly sent by Alice to Bob.

The attacker on BB84 has to discriminate between the four possible states which are used for the encryption and this is a difficult problem in the Hermitian quantum mechanics. Even in the case of two non-orthogonal quantum states, it is not possible to discriminate between them by a single measurement.

BB84 and QKD in general rely on both the quantum state discrimination problem and the no-cloning theorem. Our research focuses on a $\mathcal{PT}$-symmetric quantum state discrimination to enhance the eavesdropping rate.

2.2 $\mathcal{PT}$ Symmetry vs. Hermitian

$\mathcal{PT}$-symmetric quantum mechanics is a complex extension of the regular Hermitian quantum mechanics, Refs. [5,6,19], and provides additional opportunities

to solve the quantum state discrimination problem. In this approach, the condition of Hermiticity of the Hamiltonian, $\mathcal{H} = \mathcal{H}^{\dagger}$, is replaced by a more general requirement of $\mathcal{PT}$ symmetry. The Hamiltonian $\mathcal{H}$ is defined as $\mathcal{PT}$- symmetric if it satisfies the requirement $\mathcal{H} = \mathcal{H}^{\mathcal{PT}}$.

The action of the parity operator $\mathcal{P}$ changes the sign of the quantum-mechanical coordinate $\hat{x}$ and the momentum $\hat{p}$ operators:

$$\mathcal{P}\hat{x}\mathcal{P} = -\hat{x}; \quad \mathcal{P}\hat{p}\mathcal{P} = -\hat{p}$$

Up to the unitary transformation, $\mathcal{P}$ operator is defined as:

$$\mathcal{P} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

The anti-linear time-reversal operator $\mathcal{T}$ flips the signs of $\hat{p}$ and the imaginary unit i while leaving $\hat{x}$ invariant:

$$\mathcal{T}\hat{x}\mathcal{T} = \hat{x}; \quad \mathcal{T}\hat{p}\mathcal{T} = -\hat{p}; \quad \mathcal{T}i\mathcal{T} = -i$$

In comparison with the Hermitian case, a remarkable property of $\mathcal{PT}$-symmetric Hamiltonian is that in addition to governing the time evolution of the quantum state, it allows to manipulate an inner product of two states providing an extra degree of freedom.

Firstly, it can be exploited for speeding up the quantum evolution. After being theoretically predicted, Ref. [7], this effect was demonstrated experimentally Ref. [28]. Secondly, this additional degree of freedom plays a crucial role for the quantum state discrimination problem enabling, *in principle*, single-measurement two-state quantum state discrimination, Ref. [4].

However, such an approach involves a similarity transformation of the initial Hilbert space in which the state vectors are defined into a space spanned by the eigenvectors of the $\mathcal{PT}$-symmetric Hamiltonian. This transformation can be only done with the efficiency less than one, and the measurement may produce a null result. Consequently, even though *in principle* $\mathcal{PT}$-symmetric quantum state discrimination involves a single measurement to discriminate $N = 2$ states, it can provide inconclusive results (provides definite results with a probability less than one) even in the absence of the noise. This feature of $\mathcal{PT}$-symmetric quantum discrimination resembles an unambiguous state discrimination developed in the framework of the regular Hermitian quantum mechanics, Ref. [15].

$\mathcal{PT}$-symmetric devices for quantum state discrimination are currently under experimental investigation, Ref. [24], promising practical implementations in the near future. In Section 5, we provide an estimate on the efficiency η which has to be achieved in such devices in order to be of practical relevance for an attack on BB84.

Our Contributions. Using the novel $\mathcal{PT}$-symmetric quantum state discrimination, Ref. [4], we show how to achieve an enhancement of the eavesdropping rate for an attack on BB84 by approximately 10.5% in comparison with the regular Hermitian case.

3 Using $\mathcal{PT}$ Symmetry for the Quantum State Discrimination Problem

In this section, we apply $\mathcal{PT}$ symmetry for quantum state discrimination problem which in turn can be used for attacking BB84. The Hamiltonian satisfying the requirement of $\mathcal{PT}$-symmetry has the following general form, Ref. [4]:

$$H = H^{\mathcal{PT}} = \begin{pmatrix} re^{i\theta} & s \\ s & re^{-i\theta} \end{pmatrix} \tag{2}$$

where r, s and θ are real parameters. The α parameter defined by the parameters of $\mathcal{PT}$-symmetric Hamiltonian, Eqn.(2), $\sin(\alpha) = \frac{r}{s}\sin(\theta)$ manifests an additional degree of freedom provided by $\mathcal{PT}$-symmetry. Variation of the α allows to manipulate an inner product of two quantum states.

In comparison with the Hermitian quantum mechanics, $\mathcal{PT}$-symmetric quantum mechanics has an additional $\mathcal{C}$ operator which depends on the α parameter:

$$\mathcal{C} = \frac{1}{\cos(\alpha)} \begin{pmatrix} i\sin(\alpha) & 1 \\ 1 & -i\sin(\alpha) \end{pmatrix} \tag{3}$$

In the limit $\alpha \to 0$ this operator coincides with the regular $\mathcal{P}$ operator. The $\mathcal{CPT}$ scalar product of two vectors $|\lambda\rangle$ and $|\mu\rangle$, in the $\mathcal{PT}$-symmetric quantum mechanics, is defined as:

$$\langle\lambda|\mu\rangle = (\mathcal{CPT}\lambda)^T \cdot \mu \tag{4}$$

where T refers to the transposition of a matrix.

Unlike the Hermitian case where the scalar product is fixed, variation of the matrix elements in $\mathcal{PT}$-symmetric Hamiltonian, Eqn.(2), transforms non-orthogonal vectors into orthogonal ones, Ref. [7].

In the case when the number of states is $N = 2$, $\mathcal{PT}$-symmetric quantum mechanics provides two alternative solutions for the state discrimination, Ref. [4]:

- *Solution 1: Adjusting $\mathcal{PT}$-symmetric Hamiltonian in order to make two quantum states orthogonal under the $\mathcal{CPT}$ scalar product.*
- *Solution 2: Evolving two quantum states by the $\mathcal{PT}$-symmetric Hamiltonian to make them orthogonal by a regular Hermitian scalar product.*

Solution 1 uses the variation of α parameter to adjust the $\mathcal{CPT}$ scalar product, Eqn. 4 while *Solution 2* takes advantage of the fact that $H \neq H^\dagger$ and effectively the Hermitian scalar product is changed by the following matrix, Ref. [4]:

$$\cos^2(\alpha)\, e^{iH^\dagger t} e^{-iHt} = \begin{pmatrix} \cos^2(\omega t - \alpha) + \sin^2(\omega t) & -2i\sin^2(\omega t)\sin(\alpha) \\ 2i\sin^2(\omega t)\sin(\alpha) & \cos^2(\omega t + \alpha) + \sin^2(\omega t) \end{pmatrix} \tag{5}$$

Note, in the limit $\alpha \to 0$ it reduces to the unit matrix and coincides with the regular Hermitian case. In our solution described in the Section 4, we consider attacks on BB84 exploiting both these solutions and different parts of the parameter space of the $\mathcal{PT}$-symmetric Hamiltonian, Eqn. 2.

4 Attack on BB84

In this section, we propose three alternative attack approaches and show that with the use of $\mathcal{PT}$-symmetric quantum mechanics it is possible to correctly guess the fraction $\frac{5\eta}{6}$ of the encoded bits sent by Alice to Bob in comparison with $\frac{3}{4}$ in a regular Hermitian case, where η is the efficiency of the similarity transformation mentioned in Section 1. Although all these three approaches give the same efficiency for an attacker in theory, they have different implications when implementing them in practice.

4.1 Approach 1: Unambiguous exclusion of one of the states

First, we consider an option which allows to unambiguously exclude one of the states, Ref. [3].

In $\mathcal{PT}$-symmetric quantum mechanics the Hilbert space can effectively by curved similarly to black hole curving the space in general relativity, Ref. [7]. This makes the positions on the Bloch sphere in-equivalent. First, application of the following gate:

$$R_1 = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

allows to convert our states to a form convenient for the subsequent $\mathcal{CPT}$ measurement:

$$\begin{cases} |\psi_{00}\rangle \to |0\rangle \\ |\psi_{10}\rangle \to |1\rangle \end{cases} \quad \text{and} \quad \begin{cases} |\psi_{01}\rangle \to \frac{|0\rangle + i|1\rangle}{\sqrt{2}} \\ |\psi_{11}\rangle \to \frac{|0\rangle - i|1\rangle}{\sqrt{2}} \end{cases}$$

Now, observe that the $\mathcal{CPT}$ scalar product of the transformed states $|\psi_{01}\rangle$ and $|\psi_{11}\rangle$ vanishes for an arbitrary value of the α parameter:

$$\left(\langle\psi_{01}|\psi_{11}\rangle\right)_{\mathcal{CPT}} = 0$$

since

$$\left(\langle\psi_{01}|\right)_{\mathcal{CPT}} = \frac{(1+\sin(\alpha))}{\sqrt{2}\cos(\alpha)} \begin{pmatrix} 1 \\ -i \end{pmatrix}^T$$

This allows to build the following $\mathcal{CPT}$ projection operators:

$$P_1^1 = \left(\frac{|\psi_{01}\rangle\langle\psi_{01}|}{\langle\psi_{01}|\psi_{01}\rangle}\right)_{\mathcal{CPT}} = \frac{1}{2}\begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix}$$

$$P_2^1 = \left(\frac{|\psi_{11}\rangle\langle\psi_{11}|}{\langle\psi_{11}|\psi_{11}\rangle}\right)_{\mathcal{CPT}} = \frac{1}{2}\begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}$$

which are the $\mathcal{CPT}$ observables since:

$$\left[\mathcal{CPT}, P_{1,2}^1\right] = 0$$

and the corresponding $\mathcal{CPT}$ measurement:

$$\hat{\mathcal{M}}_1 = P_1^1 - P_2^1$$

The corresponding cosines of angles between our transformed states take the form:

$$\cos^2\left(|\psi_{01}\rangle, |\psi_{00}\rangle\right) = \cos^2\left(|\psi_{01}\rangle, |\psi_{10}\rangle\right) = \frac{1+\sin\left(\alpha\right)}{2}$$

$$\cos^2\left(|\psi_{11}\rangle, |\psi_{00}\rangle\right) = \cos^2\left(|\psi_{11}\rangle, |\psi_{10}\rangle\right) = \frac{1-\sin\left(\alpha\right)}{2}$$

$$\cos^2\left(|\psi_{01}\rangle, |\psi_{11}\rangle\right) = 0$$

Taking the limit $\alpha \to \pm\frac{\pi}{2}$, one of two states $|\psi_{01}\rangle$ or $|\psi_{11}\rangle$ can be eliminated depending on the $\pm$ sign chosen. For example, if we take the limit $\alpha \to \frac{\pi}{2}$, the measurement produces the result $\mathcal{M}_1 = -1$ only in the case when the state is $|\psi_{11}\rangle$ and the result $\mathcal{M}_1 = 1$ means that the qubit is in one of the three states, $|\psi_{00}\rangle$, $|\psi_{10}\rangle$ or $|\psi_{01}\rangle$.

Therefore, an application of this approach would provide an attacker an unambiguous knowledge of an encoded state in 25% of the cases. On average, if Eve guesses the base wrongly which happens in 50% of the time, she can correctly guess the state of the qubit in fraction of $\frac{2}{3}$ of the cases in comparison with $\frac{1}{2}$ in the Hermitian case. Therefore, on average, Eve correctly guesses the encoded bit in $\frac{5\eta}{6}$ of the cases.

However, such an approach involves taking the limit $\alpha \to \pm\frac{\pi}{2}$ meaning that the absolute values of the matrix elements of the $\mathcal{PT}$-symmetric Hamiltonian have to be large, and exactly at $\alpha = \pm\frac{\pi}{2}$ the $\mathcal{C}$ operator, Eqn. 3, and metrics, Eqn. 4, become singular (the so-called $\mathcal{PT}$-symmetry breaking point).

As a result, this approach may be challenging for the practical implementation. Therefore, we consider an alternative solution in the next subsection which involves moderate values of the α parameter and the $\mathcal{CPT}$ measurements.

4.2 Approach 2: $\mathcal{CPT}$ measurement with $\alpha \not\to \pm\frac{\pi}{2}$

We show that it is possible to achieve the same average result without taking the limit $\alpha \to \pm\frac{\pi}{2}$. To exploit the fact of that the Hilbert space is curved, we apply the following gate:

$$R_2 = \begin{pmatrix} \cos\left(\frac{\rho}{2}\right) & i\sin\left(\frac{\rho}{2}\right) \\ i\sin\left(\frac{\rho}{2}\right) & \cos\left(\frac{\rho}{2}\right) \end{pmatrix} \tag{6}$$

and adjust the value of ρ to put our states in the convenient positions for the subsequent $\mathcal{CPT}$ measurement.

After application of this gate, the angles between our reference states in terms of the $\mathcal{CPT}$ scalar product become:

$$\cos\left(|\psi_{00}\rangle, |\psi_{10}\rangle\right) = \frac{\sin\left(\alpha\right)\sin\left(\rho\right)}{\sqrt{1-\cos^2\left(\rho\right)\sin^2\left(\alpha\right)}}$$

$$\cos\left(|\psi_{00}\rangle, |\psi_{01}\rangle\right) = \frac{1+\sin\left(\alpha\right)\left(\sin\left(\rho\right)+\cos\left(\rho\right)\right)}{\sqrt{2\left(1+\cos\left(\rho\right)\sin\left(\alpha\right)\right)\left(1+\sin\left(\rho\right)\sin\left(\alpha\right)\right)}}$$

$$\cos\left(|\psi_{00}\rangle, |\psi_{11}\rangle\right) = \frac{1+\sin\left(\alpha\right)\left(\cos\left(\rho\right)-\sin\left(\rho\right)\right)}{\sqrt{2\left(1+\cos\left(\rho\right)\sin\left(\alpha\right)\right)\left(1-\sin\left(\rho\right)\sin\left(\alpha\right)\right)}}$$

$$\cos\left(|\psi_{10}\rangle, |\psi_{11}\rangle\right) = \frac{1-\sin\left(\alpha\right)\left(\sin\left(\rho\right)+\cos\left(\rho\right)\right)}{\sqrt{2\left(1-\cos\left(\rho\right)\sin\left(\alpha\right)\right)\left(1-\sin\left(\rho\right)\sin\left(\alpha\right)\right)}}$$

$$\cos\left(|\psi_{01}\rangle, |\psi_{11}\rangle\right) = \frac{\sin\left(\alpha\right)\cos\left(\rho\right)}{\sqrt{1-\sin^2\left(\rho\right)\sin^2\left(\alpha\right)}}$$

$$\cos\left(|\psi_{10}\rangle, |\psi_{01}\rangle\right) = \frac{1+\sin\left(\alpha\right)\left(\sin\left(\rho\right)-\cos\left(\rho\right)\right)}{\sqrt{2\left(1-\cos\left(\rho\right)\sin\left(\alpha\right)\right)\left(1+\sin\left(\rho\right)\sin\left(\alpha\right)\right)}}$$

$$\cos\left(|\psi_{10}\rangle, |\psi_{11}\rangle\right) = \frac{1-\sin\left(\alpha\right)\left(\sin\left(\rho\right)+\cos\left(\rho\right)\right)}{\sqrt{2\left(1-\cos\left(\rho\right)\sin\left(\alpha\right)\right)\left(1-\sin\left(\rho\right)\sin\left(\alpha\right)\right)}}$$

$$\cos\left(|\psi_{01}\rangle, |\psi_{11}\rangle\right) = \frac{\sin\left(\alpha\right)\cos\left(\rho\right)}{\sqrt{1-\sin^2\left(\rho\right)\sin^2\left(\alpha\right)}}$$

Plugging $\alpha = \frac{\pi}{4}$ and $\rho = \frac{3\pi}{4}$ makes $\cos\left(|\psi_{00}\rangle, |\psi_{11}\rangle\right) = 0$. This allows to build the following projection operators:

$$P_1^2 = \left(\frac{|\psi_{00}\rangle\langle\psi_{00}|}{\langle\psi_{00}|\psi_{00}\rangle}\right)_{\mathcal{CPT}} = \frac{1}{2}\begin{pmatrix} 1-\frac{\sin(\rho)}{1+\cos(\rho)\sin(\alpha)} & \frac{-i(\cos(\rho)+\sin(\alpha)+\cos(\rho)\sin(\alpha))}{1+\cos(\rho)\sin(\alpha)} \\ \frac{i(\cos(\rho)+\sin(\alpha)+\cos(\rho)\sin(\alpha))}{1+\cos(\rho)\sin(\alpha)} & 1+\frac{\sin(\rho)}{1+\cos(\rho)\sin(\alpha)} \end{pmatrix}$$

$$P_2^2 = \left(\frac{|\psi_{11}\rangle\langle\psi_{11}|}{\langle\psi_{11}|\psi_{11}\rangle}\right)_{\mathcal{CPT}} = \frac{1}{2}\begin{pmatrix} 1+\frac{\sin(\rho)}{1+\cos(\rho)\sin(\alpha)} & \frac{i(\cos(\rho)+\sin(\alpha)+\cos(\rho)\sin(\alpha))}{1+\cos(\rho)\sin(\alpha)} \\ \frac{-i(\cos(\rho)+\sin(\alpha)+\cos(\rho)\sin(\alpha))}{1+\cos(\rho)\sin(\alpha)} & 1-\frac{\sin(\rho)}{1+\cos(\rho)\sin(\alpha)} \end{pmatrix}$$

which are also the $\mathcal{CPT}$ observables:

$$\left[\mathcal{CPT}, P_{1,2}^2\right] = 0$$

Then, applying the following measurement:

$$\hat{\mathcal{M}}_2 = P_1^2 - P_2^2$$

and identifying the result of the measurement $\mathcal{M}_2$ with the value of the encoded bit as:

$$\begin{cases} \mathcal{M}_2 = 1 \Rightarrow a = 0 \\ \mathcal{M}_2 = -1 \Rightarrow a = 1 \end{cases}$$

allows to correctly guess the encoded bit in $\frac{5\eta}{6}$ fraction of the cases.

However, one potential disadvantage of such an approach is that in practice it may be simpler to implement the Hermitian measurements instead of the $\mathcal{CPT}$ one. Therefore, we consider one additional option which involves Hermitian measurements instead.

4.3 Approach 3: Evolution and the Hermitian measurements

We use an alternative *Solution 2* of the $\mathcal{PT}$-symmetric quantum state discrimination problem involving the non-Hermitian evolution resulting in an effective change of the Hermitian scalar product, Eqn. 5.

First, we apply the same gate as we used before, Eqn. 6, which puts two of our states in the convenient positions for the further Hamiltonian evolution with $\sigma = \frac{\pi}{4}$:

$$|\psi_{00}\rangle \to \begin{pmatrix} \cos\left(\frac{\pi-2\sigma}{4}\right) \\ -i\sin\left(\frac{\pi-2\sigma}{4}\right) \end{pmatrix};\ |\psi_{11}\rangle \to \begin{pmatrix} \cos\left(\frac{\pi+2\sigma}{4}\right) \\ -i\sin\left(\frac{\pi+2\sigma}{4}\right) \end{pmatrix}$$

The Hamiltonian evolution is performed for a time τ given by the equation:

$$\sin^2(\omega\tau) = \frac{\cos^2\alpha\cos\sigma}{2\sin\alpha - 2\sin^2\alpha\cos\sigma} \tag{7}$$

As a result, $\langle\psi_{00}|\psi_{11}\rangle_{Hermitian} = 0$ and analogously to the *Approach 2* this allows to couple the two bases.

After the time given by an Eqn. 7 our four states are converted to:

$$|\psi_{a_i,b_i}\rangle \to e^{-iH\tau}|\psi_{a_i,b_i}\rangle$$

where the evolution operator is given by:

$$e^{-iH\tau} = \frac{e^{-ir\cos(\theta)\tau}}{\cos(\alpha)} \begin{pmatrix} \cos(\omega\tau-\alpha) & -i\sin(\omega\tau) \\ -i\sin(\omega\tau) & \cos(\omega\tau+\alpha) \end{pmatrix}$$

The resulting Hermitian projection operators are:

$$P^3_{1,2} = \left(\frac{|\psi_{00,11}\rangle\langle\psi_{00,11}|}{\langle\psi_{00,11}|\psi_{00,11}\rangle}\right)_{Hermitian} \tag{8}$$

Analogously, the measurement is constructed as

$$\mathcal{M}_3 = P^3_1 - P^3_2$$

And we identify the result of the measurement $\mathcal{M}_3 = 1$ as $a_i = 0$ and $\mathcal{M}_3 = -1$ as $a_i = 1$.

Note, the $\mathcal{PT}$-symmetric Hamiltonian evolution preserves the $\mathcal{CPT}$ norm of the states since $[\mathcal{C}, H] = 0$ but changes the Hermitian norm of the states. Therefore, we normalize our states in the projection operators in Eqn. 8 correspondingly.

Now we need to find an optimal value of parameter α in such a way that it minimizes the average error in determining which bit was encoded by Alice. Performing an analogous calculations to the *Approach 2* and expressing the cosines between the evolved states which now are governed by Eqn. 5, we plot the corresponding average probability of correct guessing in Fig. 3. Note, there is a minimal value of the parameter α which makes such Hamiltonian evolution possible such that $\sin^2(\omega\tau) \leq 1$ in Eqn. 7. Additionally, note that this minimal

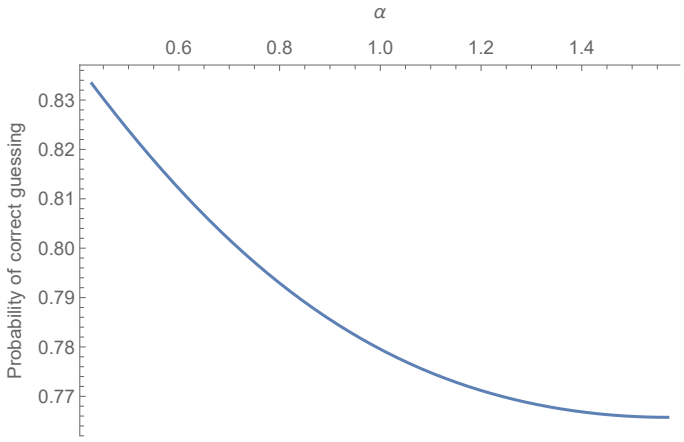

Fig. 3: The probability of correct guessing of the encoded bit as a function of the α parameter. For $\alpha < \tan^{-1}\left(\sqrt{\frac{1}{2}\left(\sqrt{2}-1\right)}\right)$, solution does not exist.

value of α corresponds to the biggest possible value of probability of correct guessing in this approach and which is the same as in the previously considered *Approaches 1* and *2* and equals $\frac{5\eta}{6}$. This optimal value equals:

$$\alpha_{Optimal} = \tan^{-1}\left(\sqrt{\frac{1}{2}\left(\sqrt{2}-1\right)}\right) \approx 0.427079$$

4.4 Comparison Between Three Approaches

All three approaches give the same *average* probability of the eavesdropper to correctly guess the encoded bit of $\frac{5\eta}{6}$. However, the *Approach 1* has an advantage that in 25% of the cases allows to *unambiguously* determine the state which is used for encoding the bit.

However, *Approach 1* requires the parameters of the $\mathcal{PT}$-symmetric Hamiltonian, Eqn. 2, to be close to the the $\mathcal{PT}$-symmetry breaking point which may be challenging for the practical implementation.

Approach 2 involves moderate values of the α parameter and should be therefore simpler for the practical implementation.

However, currently many of the $\mathcal{PT}$-symmetric Hamiltonians are implemented as on optical devices where the Hermitian measurements are simpler to implement, Refs. [14,20,26,29]. Therefore, the *Approach 3* uses an intermediate values of the α parameter far from the the $\mathcal{PT}$-symmetry breaking point as well as the Hermitian measurements.

Finally, we estimate the required efficiency of such devices in order for these *Approaches* to be relevant in practice. The efficiency of the $\mathcal{PT}$-symmetric quan-

tum state discriminator has to satisfy the requirement:

$$\frac{5p}{6} > \frac{3}{4} \Rightarrow \eta > 90\%.$$

The most recent experimental implementation on the $\mathcal{PT}$-symmetric quantum discrimination, Ref. [24], provides a practical experimental platform for the future studies but does not investigate the efficiency for this purpose.

5 Related Work

In this section, we discuss the related work in QKD and, more specifically, its practical relevance in implementations and how it offers information-theoretic security.

5.1 QKD in Practice

Over the past few years, QKD has gained attention for its unique security benefits. Continuous research to find the practical relevance yielded in multiple simulations, implementations, and modeling frameworks, Refs. [17,27,18]. Decoy-state QKD uses attenuated coherent light sources in place of perfect single photon sources and is used in the experiments conducted in Refs. [17,27]. It helps detection of photon-splitting eavesdropping and can be used in high loss channels. The authors in Ref. [27] demonstrated the first experimental implementation of decoy-state QKD over telecom fiber. The experimentation include implementations of one-decoy protocol over 15km telecom fiber and weak+vacuum protocol over 60km of telecom fiber. The authors in Ref. [17] demonstrated the possibility of global-scale quantum networks by successfully performing decoy-state QKD, using BB84, between a ground observation station and a satellite at an altitude of around 500KM. The empirical experiments in these work highlight the unique security benefits by QKD. Furthermore, the first measurement-device-independent (MDI) QKD realization in the free-space over the 19.2km in atmosphere, Ref. [11], has been demonstrated approaching a practical satellite-based QKD.

Other work facilitate the practical implementations by providing a framework building on QKD security relying on the use of a single-photon source and fundamental laws of security. Device imperfections and practical implementation limitations play a huge role in keeping QKD security intact. The authors in Ref. [18] proposed a modeling framework that helps as a reference for BB84 QKD. The proposed framework identifies the device imperfections, engineering limitations, and design trade-offs.

Our approaches can be used to enhance an eavesdropping rate in these and similar devices. Therefore, while constructing the QKD in practice, one has to keep in mind these possibilities if an efficient $\mathcal{PT}$-symmetric device for quantum state discrimination is implemented on practice.

5.2 QKD for Information-Theoretic Security

According to Shannon, Ref. [21], the system is defined to achieve *perfect secrecy* if the mutual information between the ciphertext and the plaintext is zero: $I(\mathcal{C}, \mathcal{M}) = 0$. As a result, the amount of entropy in the key must be greater or equal than that in the message, $H(\mathcal{K}) \geq H(\mathcal{M})$. *One-time pad* encryption by the Vernam cipher, Ref. [1], fulfills this condition and is provably secure encryption scheme. However, for its execution, it requires a large key to be exchanged between the communicating parties, which prohibits its deployment in many computing/networking applications.

QKD provides a unique opportunity to meet this challenge and make Vernam cipher of practical relevance. For example, in Ref. [11] more than 3.5×10^6 sifted keys were exchanged over the distance of approximately 20 km through the atmosphere in 13.4 hours. Nevertheless, QKD can also provide the keys for any other symmetric-key cryptosystems.

Furthermore, the no-cloning theorem preserves the information-theoretic security. The no-cloning theorem on which the security of the QKD rely, Ref. [25], is based on the linearity of quantum mechanics and applies both to the Hermitian as well as the $\mathcal{PT}$-symmetric quantum mechanics since they differ by the symmetry properties of the Hamiltonian and are both linear. However, as we show in this paper, the eavesdropping efficiency in the $\mathcal{PT}$-symmetric quantum mechanics can be higher in comparison with the Hermitian one if the corresponding device is implemented with sufficient efficiency.

6 Conclusion

Recent advances in quantum mechanics and the $\mathcal{PT}$- symmetric quantum state discrimination can be exploited for attacking and eavesdropping on the key transmissions in the BB84 QKD protocol. We construct three approaches for attacking BB84, all of which have the same performances for guessing the secret bit at $\frac{5\eta}{6}$.

While our contributions and validations are theoretical, we analyze the practicality and the relevance of our work. The choice between the *Approach 1, 2* or *3* depends on the accessibility of the $\mathcal{CPT}$ and Hermitian measurements as well as the availability of the parameter space of the $\mathcal{PT}$-symmetric Hamiltonian, Eqn. 2. As QKD becomes more viable and popular with generating/sharing the keys for securing the next-generation systems, our work informs the security of QKD and facilitates greater research in the direction. We also call for greater research bridging physics/quantum mechanics and cybersecurity as we prepare for the quantum computing era.

References

1. *G. S. Vernam, Trans. Am. Inst. Electr. Eng.* **XLV**, 295 (1926).
2. Joonwoo Bae and Leong-Chuan Kwek. Quantum state discrimination and its applications. *Journal of Physics A: Mathematical and Theoretical*, 48(8):083001, 2015.

3. Yaroslav Balytskyi, Manohar Raavi, Anatoliy Pinchuk, and Sang-Yoon Chang. Pt-symmetric unambiguous distinguishing of three quantum states.
4. Carl M Bender, Dorje C Brody, João Caldeira, Uwe Günther, Bernhard K Meister, and Boris F Samsonov. Pt-symmetric quantum state discrimination. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 371(1989):20120160, 2013.
5. Carl M Bender, Dorje C Brody, and Hugh F Jones. Complex extension of quantum mechanics. *Physical Review Letters*, 89(27):270401, 2002.
6. Carl M Bender, Dorje C Brody, and Hugh F Jones. Must a hamiltonian be hermitian? *American Journal of Physics*, 71(11):1095–1102, 2003.
7. Carl M Bender, Dorje C Brody, Hugh F Jones, and Bernhard K Meister. Faster than hermitian quantum mechanics. *Physical Review Letters*, 98(4):040403, 2007.
8. Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *arXiv preprint arXiv:2003.06557*, 2020.
9. Matthieu Bloch and Joo Barros. *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, USA, 1st edition, 2011.
10. WT Buttler, RJ Hughes, Paul G Kwiat, SK Lamoreaux, GG Luther, GL Morgan, JE Nordholt, CG Peterson, and CM Simmons. Practical free-space quantum key distribution over 1 km. *Physical Review Letters*, 81(15):3283, 1998.
11. Yuan Cao, Yu-Huai Li, Kui-Xing Yang, Yang-Fan Jiang, Shuang-Lin Li, Xiao-Long Hu, Maimaiti Abulizi, Cheng-Long Li, Weijun Zhang, Qi-Chao Sun, et al. Long-distance free-space measurement-device-independent quantum key distribution. *Physical Review Letters*, 125(26):260503, 2020.
12. Davide Castelvecchi. IBM's quantum cloud computer goes commercial. *Nature News*, 543(7644):159, 2017.
13. Sang-Yoon Chang, Yih-Chun Hu, Hans Anderson, Ting Fu, and Evelyn Huang. Body area network security: Robust key establishment using human body channel. In *3rd USENIX Workshop on Health Security and Privacy (HealthSec 12)*, Bellevue, WA, August 2012. USENIX Association. URL: `https://www.usenix.org/conference/healthsec12/workshop-program/presentation/Chang`.
14. A Guo, GJ Salamo, D Duchesne, R Morandotti, M Volatier-Ravat, V Aimez, GA Siviloglou, and DN Christodoulides. Observation of p t-symmetry breaking in complex optical potentials. *Physical Review Letters*, 103(9):093902, 2009.
15. Igor D Ivanovic. How to differentiate between non-orthogonal states. *Physics Letters A*, 123(6):257–259, 1987.
16. Julian Kelly. A preview of Bristlecone, Google's new quantum processor. *Google Research Blog*, 5, 2018.
17. Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, and et al. Satellite-to-ground quantum key distribution. *Nature*, 549(7670):43–47, Aug 2017. URL: `http://dx.doi.org/10.1038/nature23655`, `doi:10.1038/nature23655`.
18. Logan O Mailloux, Jeffrey D Morris, Michael R Grimaila, Douglas D Hodson, David R Jacques, John M Colombi, Colin V Mclaughlin, and Jennifer A Holes. A modeling framework for studying quantum key distribution system implementation nonidealities. *IEEE Access*, 3:110–130, 2015.
19. Ali Mostafazadeh. Pseudo-hermiticity versus pt-symmetry iii: Equivalence of pseudo-hermiticity and the presence of antilinear symmetries. *Journal of Mathematical Physics*, 43(8):3944–3951, 2002.
20. Christian E Rüter, Konstantinos G Makris, Ramy El-Ganainy, Demetrios N Christodoulides, Mordechai Segev, and Detlef Kip. Observation of parity–time symmetry in optics. *Nature physics*, 6(3):192–195, 2010.

21. Claude E Shannon. Communication theory of secrecy systems. *The Bell system technical journal*, 28(4):656–715, 1949.
22. Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.
23. Peter W. Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444, Jul 2000. URL: `https://link.aps.org/doi/10.1103/PhysRevLett.85.441`, `doi:10.1103/PhysRevLett.85.441`.
24. Yi-Tao Wang, Zhi-Peng Li, Shang Yu, Zhi-Jin Ke, Wei Liu, Yu Meng, Yuan-Ze Yang, Jian-Shun Tang, Chuan-Feng Li, and Guang-Can Guo. Experimental investigation of state distinguishability in parity-time symmetric quantum dynamics. *Physical Review Letters*, 124(23):230402, 2020.
25. William K Wootters and Wojciech H Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.
26. KF Zhao, M Schaden, and Z Wu. Enhanced magnetic resonance signal of spin-polarized rb atoms near surfaces of coated cells. *Physical Review A*, 81(4):042903, 2010.
27. Yi Zhao, Bing Qi, Xiongfeng Ma, Hoi-Kwong Lo, and Li Qian. Simulation and implementation of decoy state quantum key distribution over 60km telecom fiber. In *2006 IEEE International Symposium on Information Theory*, pages 2094–2098. IEEE, 2006.
28. Chao Zheng, Liang Hao, and Gui Lu Long. Observation of a fast evolution in a parity-time-symmetric system. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 371(1989):20120053, 2013.
29. AA Zyablovsky, Aleksei P Vinogradov, Aleksandr Aleksandrovich Pukhov, Aleksandr Viktorovich Dorofeenko, and A Abramovich Lisyansky. Pt-symmetry in optics. *Physics-Uspekhi*, 57(11):1063, 2014.