A complete characterization of the optimal unitary attacks in quantum cryptography with a refined optimality criteria involving the attacker’s Hilbert space only

Atanu Acharyya\textsuperscript{1,a} and Goutam Paul\textsuperscript{2,b}

\textsuperscript{1} Applied Statistics Unit, Indian Statistical Institute, Kolkata 700 108, India
\textsuperscript{2} Cryptology and Security Research Unit, R. C. Bose Centre for Cryptology and Security, Indian Statistical Institute, Kolkata 700 108, India

Received 21 October 2020 / Accepted 8 June 2021 / Published online 31 July 2021
© The Author(s), under exclusive licence to EDP Sciences, SIF and Springer-Verlag GmbH Germany, part of Springer Nature 2021, corrected publication 2021

Abstract. Fuchs et al. (Phys Rev A 56:1163, 1997, https://doi.org/10.1103/PhysRevA.56.1163) suggested an optimal attack on the BB84 protocol, where the necessary and sufficient condition for optimality involves the joint Hilbert space of the sender and the attacker. In this work, we propose a refined optimality criteria involving the Hilbert space of the attacker only. It reveals that the optimal (non-zero) overlaps between the attackers post-interactions states must be equal and numerically the same as the difference between the fidelity and the disturbance at the receiving end. That amount turns out to be the same as the reduction (factor) in Bell violation when estimated for the equivalent entanglement-based protocol. Further, a series of necessary and sufficient conditions unveil the structure of the optimal states which therefore are the only and all possible optimal interactions. These optimal states are the same as the outputs of an optimal phase-covariant cloner. We also demonstrate various methods to derive optimal unitary evolutions that an eavesdropper is interested to know in order to mount an optimal attack. The final key-rate is computed and plotted as well.

1 Introduction

The power of quantum theory \cite{1} is better manifested through the manipulation of quantum information for secure electronic communication \cite{2,3}. The most interesting application is perhaps quantum key distribution that started its journey through the BB84 protocol \cite{4}. The protocol can establish an information-theoretically secure secret key between two distant parties. Alice encodes a stream of classical bits (cbits) into an ensemble of quantum bits (qubits) using two mutually unbiased bases (MUBs). She then transmits the qubits one-by-one over a quantum channel. Bob, at the receiving end, measures individually in one of the encoding bases, chosen randomly. Later they reconcile bases publicly over an authenticated classical channel to filtrate a sifted key.

A third party (Eve) is allowed to tamper the quantum channel. However, any approach to learn the state of the qubit introduces an error which is further detectable by the recipient. The legitimate parties can estimate the quantum bit error rate (QBER) by discussing over the public channel on a part of the sifted key. Within a threshold value QBER\textsuperscript{⋆}, a classical post-processing (CPP) is faithful to filter a shared secret on which Eve has virtually no information.

An advanced eavesdropping model \cite{5} is to extract the information of a transmitted qubit via an ancilla qubit by interacting unitarily. Given that the attacker is allowed to defer her measurement until after basis reconciliation, an one-way (OW) CPP is faithful if the estimated QBER remains below the critical value 0.1464 where the secret key-rate becomes zero. The authors could estimate the maximum knowledge gain (KG) by an attacker that eventually appeared a tight bound due to an witness interaction. Nonetheless, there could be infinitely many such saturating candidates (interactions) which are unitarily equivalent \cite{6}. In that attack model, a candidate interaction must pass a formal verification of optimality, viz., a necessary and sufficient condition (NSC) \cite{5} involving the joint Hilbert space of the sender and the attacker.
Our contributions

We suggest here a necessary and sufficient condition for optimality that involves the Hilbert space of the attacker only. The verification is easier to perform than that in Ref. [5]. This new criteria explicitly depicts the geometry of the optimal states. We find its direct connection with the equivalent entanglement-based protocol and with optimal phase-covariant (pc) cloner [7].

To be precise, an optimal attack is characterized by the non-zero overlaps between various post-interaction states of Eve’s ancilla. The optimal overlap must equate the fidelity less than the disturbance incurred at Bob’s end. We show that the amount is the same as the reduction (factor) in the CHSH sum [8,9] for an equivalent amount. We show that the amount is the same as the reduction (factor) in the CHSH sum [8,9] for an equivalent amount.

The optimal PIJSs are in sync with the outputs obtained by an optimal pc-cloner [7].

We carry on through a chain of NSCs to derive infinitely many optimal interactions, and therefore without ambiguity, these are the only and all possible optimal interactions. Their connection with the optimal states derived in Ref. [6] is also established unitarily.

An optimal post-interaction joint state (PIJS) clearly exhibits an one-to-one correspondence with the optimal measurement of Eve. Thus, Eves measurement setup determines her interaction and vice versa. Relation between Eve’s optimal measurements for the two encoding bases is established here for the sake of completeness. The optimal PIJSs are in sync with the outputs obtained by an optimal pc-cloner [7].

We then consider the task of characterizing the optimal unitary attacks, i.e., to derive the optimal unitary operators. First, we describe the basic approach to find an optimal unitary for a given pair of optimal PIJSs, which faces some technical difficulties like basis completion issue in an arbitrary measurement basis for Eve. We bypass these hurdles in an elegant analytical approach to obtain an optimal unitary fit for an initial state (IS) when Eve measures in the computational basis. We show the methods to find any of its infinitely many siblings. Further, we explain the ways to get optimal unitaries for an arbitrary IS and then for arbitrary measurement basis used by Eve. We exemplify these methods to understand the intricacies. Essentially we have characterized the whole space of optimal unitary attacks.

The strength of the protocol and the attack model gets judged by several parameters, e.g., the maximum tolerable disturbance, key-rate etc. Considering certain lack of clarity in the existing literature, we are motivated to emphasise here on finding the key-rate for the sifted key as well for the final key. While the former one depends on the bipartite mutual informations, the latter one involves the amount of discarded fraction during the privacy amplification stage. We calculate all these ingredients and plot them in diagrams.

Overall, our objective here remained to augment the completeness of the existing literature by addressing some minute details of the art of optimal eavesdropping in quantum cryptography. We have added a rigorous mathematical structure to fine tune the gaps found in the existing literature. Some connections across various other related mechanisms are also made explicit and stronger.

Paper outline

The section-wise work-flow is as follows. Section 2 is dedicated to quickly recall the framework of optimal eavesdropping [5], the optimal interactions [6], and the interrelation between Eves optimal measurements across the two MUBs. Moreover, we have established explicit connection with the cloning mechanism by directly comparing the optimal states.

The main results are briefly described in Sects. 3–4, while the derivations are deferred until in Sect. 6. The new NSC and the optimal states are discussed in Sect. 3, while Sect. 4 deals with characterizing the optimal unitary evolutions. Section 5 is left to discuss the final key-rate. We conclude by summarizing the new findings and their implications.

2 Elements of optimal eavesdropping

Here we brief the attack model, the objective functions to be optimized and their bounds, and the optimal states after an interaction. We exhibit some direct connections that a practical attack has with Bell violation and with an optimal pc-cloner.

2.1 Alice’s encoding

For encoding, Alice uses two orthonormal bases conjugate to each other: the computational basis, and the Hadamard basis. The basis states correspond to the eigenstates of the phase-flip operator σz and bit-flip operator σx, respectively. The following notations for the bases and their states are used interchangeably throughout the paper (Table 1).

Here, β denotes the conjugate of a basis β. The Hadamard transform H := 1/√2 (σz + σx) flips the bases (H : β → β) while the basis states can be written with respect to the computational basis elements as |a⟩β = Hβ(a) for α = 0, 1.

The orthogonal counterpart of a state |a⟩ is denoted by |a ⊕ 1⟩ or |a⟩. Alice encodes the cbit 0 into a qubit in state |x⟩ or |u⟩, and encodes 1 into |y⟩ or |v⟩.

2.2 The attack model

Eve attacks the quantum channel with an intention to indirectly learn the transmitted qubits one-by-one. She attaches a probe in state |e⟩ ∈ HE to Alice’s qubit that was transmitted in state |αβ⟩ ∈ HA. She evolves the joint system unitarily (U) from the pre-interaction

---

1 Although new contribution, these interrelations are better fitted in this recapitulation section only.
be grouped into two mutually orthogonal sets [5]: the IVs share real-valued inner products, they can 
encode in $\mathbf{R}^2$. These two states with Eve share 
disturbed set [5]. Consequently, he finds the 
channel producing a QBER $D_\beta$ for an encoding basis $\beta$.

Now, consider Alice sent the state $|a\rangle^\beta$. When Bob 
receives the same state, we denote the corresponding state $|\xi_a\rangle^\beta$ of Eve’s ancilla as the 
fidelity state. When Bob finds the state altered, we denote Eve’s state $|\zeta_a\rangle^\beta$ as the 
disturbed state. These two states with Eve share 
no overlap. Similarly, when Alice sends $|\bar{a}\rangle^\beta$, Eve’s 
states $|\xi_a\rangle$ and $|\zeta_a\rangle$ are mutually orthogonal.

In a fixed basis, when these four interaction vec-
tors (IVs) share real-valued inner products, they can 
be grouped into two mutually orthogonal sets [5]: the 
fidelity set $\{|\xi_a\rangle, |\xi_\lambda\rangle\}$, and the disturbed set $\{|\zeta_a\rangle, |\zeta_\lambda\rangle\}$. Clearly, a two-qubit probe 
suffices to describe Eve’s four-dimensional Hilbert space $H_E = R^2 \otimes \mathbb{C}^2$ that spans these 
four states.

To distinguish these four states, she needs to incor-
porate a generalized measurement with four outcomes. 
Thus, her measurement is considered to be a positive 
operator-valued measure (POVM): a resolution of unity into 
non-negative Hermitian operators [10–12]. Denote 
her POVMs $\{E_\lambda\}$ or $\{F_\lambda\}$ depending on whether Alice 
encodes in $xy$ or $uv$ basis. Denote them commonly as 
$\{M_\lambda\}^D$, where an outcome is labeled by $\lambda \in \{0, 1, 2, 3\}$. She then interprets the outcome following a strategy 
which is a rule for Eve to assign a guess for the state of the signal sent by Alice.

2 We use $F_\beta$ and $1 - D_\beta$ interchangeably.

### 2.3 Functions to be optimized

After the measurement by Eve and Bob, each of the 
three parties is left with a classical random variable, 
denoted here as $A, B$, and $E$, for Alice, Bob, and Eve, 
respectively. For a permissible QBER, all the legiti-
mate parties are concerned about, is the secret key-rate 
(SKR) which is the ratio of the length of the final secret 
key and the sifted key. No analytic expression is known 
for the SKR, except a lower bound [13] which depends 
on the bipartite mutual informations (MI): $\text{MI}_{AE}$ and $\text{MI}_{EB}$. Minimizing SKR amounts to maximizing $\text{MI}_{AE}$ 
which in turn is an appropriate candidate to estimate 
Eve’s knowledge gain from measurement outcomes as it 
captures the reduction of entropy in Alice’s random 
variable due to Eve’s knowledge from outcomes. A closely related, but easier to estimate quantifier is her information gain (IG) [5]. The optimal MI is found to be a concave function of the optimal IG.

An optimal interaction is the one that can maxi-
mize her knowledge gain in both the bases. However, 
acquiring the maximum knowledge depends on the right 
choice of the measurement, called an optimal measure-
ment.

For BB84 protocol, for equal prior, both IG and MI 
are a function of three parameters: two density opera-
tors $\rho_a^\beta$, $\rho_\lambda^\beta$ and the POVM $\{M_\lambda\}^D$. For a fixed QBER $D_\beta$ in each bases, a global maxima exists for each of 
the functions IG and MI in each of the bases and is 
attainable [5].

\[ \text{IG}_\beta^* = 2\sqrt{D_\beta(1-D_\beta)}, \quad \text{MI}_\beta^* = \frac{1}{2} \phi(\text{IG}_\beta^*) , \]

for the concave function \( \phi(z) := (1 + z) \ln(1 + z) + (1 - z) \ln(1 - z) \).

The upper bounds for both IG and MI are attainable in 
each of the bases for independently chosen error rates $D_{xy}$ and $D_{uv}$ that is incurred across the bases.

Finding an optimal POVM for such interaction vectors 
correspond to a rather easier optimization problem: 
maximize IG over all POVMs [10]. An upper bound 
exists and is achievable in each of the encoding bases. In 
$xy$ basis, the maximum IG is attained by the orthon-
ormal eigenprojectors $\{E_\lambda := |E_\lambda\rangle\langle E_\lambda|\}$ of the Hermitian $\rho_x - \rho_y$. 
For equal prior (and not necessarily for unequal prior), the same measurement optimizes both IG and 
MI for an optimal interaction.

### 2.4 The optimal states after an interaction

An optimal interaction induces a restriction on the 
interaction vectors. Optimal IVs must satisfy some nec-
essary and sufficient conditions [5]. Deriving optimal 
IVs from these conditions remained a harder task [done 
in Sect. 3]. Nevertheless, a judicious bet on a specific 
choice of IVs passed the verification [5].

Although, there could be various other choices [6], 
ininitely many for each of the encoding bases, they are
Alice uses one of the two MUBs, \( \beta \), to encode a cbit 'a' into a qubit \(|a\rangle\). Eve attaches an ancilla \(|e\rangle\) and evolves the joint system unitarily \(|\xi\rangle\) that creates an entangled state \(|S_\beta\rangle\). Bob measures the received qubit in basis \( \beta' \) to get the cbit \( b \), and keeps it if the bases are matched. After basis reconciliation, Eve measures her ancilla in the POVM basis \(|\langle M_\lambda\rangle\rangle\). She interprets her outcome \( \lambda \) by a strategy and bet for \( a_\lambda \) to guess Alice’s cbit. When Eve’s choices for the unitary and the measurement are optimal, she guesses the key best while not forcing to abort the protocol.

Fig. 1 A schematic diagram for an optimal eavesdropping on BB84 protocol

unitarily equivalent. In \( xy \) basis, the optimal IVs of Eve can be expressed in her orthonormal measurement basis \(|E_\lambda\rangle\rangle\) as follows:

\[
|\xi^+_y\rangle = \mathcal{D}_{uv}^+ |E_0\rangle + \mathcal{D}_{uv}^- |E_1\rangle,
|\xi^-_y\rangle = \mathcal{D}_{uv}^- |E_0\rangle + \mathcal{D}_{uv}^+ |E_1\rangle.
\]

Note that, an optimal IV is a superposition of two measurement directions having amplitudes \( \mathcal{D}_{uv}^+ \) and \( \mathcal{D}_{uv}^- \) defined as

\[
\mathcal{D}_{uv}^\pm := \frac{\sqrt{1-D_\beta} \pm \sqrt{D_\beta}}{\sqrt{2}}.
\] (4)

Similarly, the general expression representing the optimal IVs in \( uv \) basis is as follows:

\[
|\xi^+_u\rangle = \mathcal{D}_{uv}^+ |F_0\rangle + \mathcal{D}_{xy}^- |F_1\rangle,
|\xi^-_u\rangle = \mathcal{D}_{uv}^- |F_0\rangle + \mathcal{D}_{xy}^+ |F_1\rangle.
\]

Any specification of the orthonormal basis \(|E_\lambda\rangle\rangle\) (or \(|F_\lambda\rangle\rangle\)) provides a specific instance of optimal IVs in computational basis, e.g., the optimal IVs due to Fuchs et al. [5]. Due to varied choices of the eigenbasis, there are infinitely many setups of the optimal IVs when expressed in the computational basis. A one-to-one correspondence between the optimal IVs in each basis can be established (Sect. 6) since the optimal measurement directions \(|E_\lambda\rangle\rangle\) in \( xy \) basis are interrelated to the optimal measurement directions \(|F_\lambda\rangle\rangle\) in \( uv \) basis as follows:

\[
2|F_0\rangle = |E_0\rangle + |E_1\rangle + |E_2\rangle + |E_3\rangle,
2|F_1\rangle = |E_0\rangle - |E_1\rangle - |E_2\rangle - |E_3\rangle,
2|F_2\rangle = |E_0\rangle - |E_1\rangle - |E_2\rangle + |E_3\rangle,
2|F_3\rangle = |E_0\rangle - |E_1\rangle + |E_2\rangle - |E_3\rangle.
\] (6)

For instance, the measurement basis \(|E_\lambda\rangle\rangle\) = \{|00\rangle, |11\rangle, |10\rangle, |01\rangle\} fixes the measurement basis \(|F_\lambda\rangle\rangle\) = \{|00\rangle, |11\rangle, |10\rangle, |01\rangle\} for Eve. This choice of the permuted computational basis retains the symmetry in Eve’s measurement basis \(|E_\lambda\rangle\rangle, |F_\lambda\rangle\rangle\) across the two encoding bases \( xy, uv \). The corresponding IVs in Eqs. (3) and (5) represent the optimal states chosen by Fuchs et al.

Optimal strategy: Strategy of Eve can now be determined as follows. As Alice declares her basis to be \( \beta \in \{0,1\} \), Eve measures her ancilla in basis \(|M_\lambda\rangle\rangle\) and interprets her measurement outcome in terms of a guess on Alice’s bit. For +ve outcome, which occurs for \( \lambda = 0,2 \), she bets on 0, whereas, for -ve outcome, which occurs for \( \lambda = 1,3 \), she bets on 1.

To mount an optimal attack, Eve performs a suitable interaction (the allowed unitaries can be found in Sect. 4), measures accordingly after basis reconciliation, and finally guesses the signal applying her strategy. Figure 1 provides a schematic view of the attack model.

2.5 Practical eavesdropping: the secure zone

A practical eavesdropping should ideally leave the error rate symmetric across the two bases, i.e., \( D_{xy} = D_{uv} = D \). Otherwise, the legitimate parties can detect the difference during the error-estimation phase, and thereby detect the presence of a malevolent party. For a QBER
\( = D \), the maximum amount of the IG in both the bases reaches \( 2 \sqrt{D(1 - D)} \) and is achievable [5].

Due to symmetric eavesdropping, the quantum channel between Alice–Bob and that between Alice–Eve can be interpreted as a binary symmetric channel with data-flipping rate \( D \) and \( D_E = \frac{1}{2} - \sqrt{D(1 - D)} \), respectively. Thus, at error-rate \( D \), the respective bipartite mutual informations become

\[
\begin{align*}
\text{MI}_{AB} &= 1 - H(D) = \frac{1}{2} \phi (1 - 2D), \\
\text{MI}_{AE} &= 1 - H(D_E) = \frac{1}{2} \phi (2 \sqrt{D(1 - D)}),
\end{align*}
\]

when expressed in bits per sifted-photon (bpsp). Here, \( H(D) \) stands for the entropy of a binary random variable assuming values \( D \) and \( 1 - D \).

The sifted key-rate \( R^{\text{sif}} \) is bounded below by the difference \( \text{MI}_{AB} - \text{MI}_{AE} \). For a QBER \( D \), it amounts to \( R^{\text{sif}} = H(D_E) - H(D) \) bpsp. It decreases with growing QBER and vanishes when the two MIs coincide which happens at the threshold (Fig. 2)

\[
D^* = \frac{1}{2} \left( 1 - \frac{1}{\sqrt{2}} \right) \approx 0.1464. \tag{7}
\]

Beyond this tolerable rate, an OW-CPP may not guarantee to filtrate a secure key. Within the secure zone \( D \in [0, D^*) \), key-filtration is guaranteed because Bob possess more information on Alice’s bit than Eve does.

Following the optimal strategy, Eve can glean \( (1 - H(D_E)) \) bits per sifted-photon of the transmission with fidelity \( 1 - D_E \) in lieu of introducing an error-rate \( D \) at Bob’s end. The distinguishing advantage for an optimal attack is \( \sqrt{D(1 - D)} \).

2.6 Connecting Bell violation and cloning

An optimal attack on the prepare-and-measure (p&m) scheme that we considered here has some interesting connections with the optimal attack on its entanglement-based (eb) counterpart as well with optimal cloning mechanisms.

In the eb protocol, the legitimate parties observe a Bell violation so far the estimated QBER remains in the secure zone of the p&m scheme [5]. An optimal attack with QBER \( D \) reduces the CHSH correlation coefficient to \( \eta_D 2 \sqrt{2} \) for \( \eta_D := 1 - 2D \). An optimal attack also leaves Bob with the Bloch vectors contracted by a factor of \( \eta_D \).

An optimal attack on the p&m scheme can also be achieved via an optimal phase-covariant cloner [7]. The cloner is asymmetric since it creates two clones of the senders state: a degraded copy for her own with fidelity \( \left( \frac{1}{2} + \sqrt{D(1 - D)} \right) \), and a superior copy for Bob with fidelity \( 1 - D \). At the threshold QBER, both the fidelity for Bob and Eve reaches the maximum of \( 1 - D^* = \frac{1}{2} \left( 1 + \frac{1}{\sqrt{2}} \right) \), i.e., 85.36%, both in cloning and

![Fig. 2 Sifted key-rate for one-way classical post-processing](image-url)

Plotted: optimal Information Gain, bipartite Mutual Informations, and the secret key-rate. The graph of \( \text{MI}_{AE} \) reveals the information-disturbance trade-off. For QBER \( D^* = 0.1464 \), \( \text{MI}_{AB} \) and \( \text{MI}_{AE} \) coincides, and the key-rate drops to zero. Below this error rate, an OW-CPP is faithful.

3 A necessary and sufficient condition for optimality and deriving optimal interaction vectors

Optimality of an interaction require a certificate, e.g., a necessary and sufficient condition [5]. The verification involves the post-interaction joint states in the joint Hilbert space. Here we suggest a refined NSC involving the states of Eve only that makes the verification easier. The journey also leads to derive the optimal IVs.

3.1 A Necessary and sufficient condition due to Fuchs et al. [5]

Consider the optimality of the post-interaction states (2). For Alices symbol \( a^d \in \{ x, y, u, v \} \), denote the PIJS symbol \( S^a_{xy} \) as \( X, Y, U, V \), respectively. The NSC [5, Eqs. (38,39)] for optimality in xy basis involves the following four states defined over the joint Hilbert space of Bob and Eve.

\[
|W_{\lambda a} \rangle := B_a \otimes \sqrt{E_X} |W\rangle. \tag{8}
\]
Here, a choice of the variables \( W \in \{ U, V \} \) and \( a \in \{ u, v \} \) will lead to one of the four possible equations. Bob uses the projectors \( B_a := |a\rangle\langle a| \).

For optimal knowledge gain in the \( xy \) basis, the inner products \( \langle U_{\lambda a} | V_{\lambda a} \rangle \) and \( \langle U_{\lambda a} | V_{\lambda a} \rangle \) must be real and have the same sign \( \varepsilon_\lambda \in \pm 1 \). Checking optimality is essentially to check the following parallelism:

\[
|U_{\lambda a}\rangle \| |V_{\lambda a}\rangle \text{ and } |U_{\lambda a}\rangle \parallel |V_{\lambda a}\rangle.
\]

The post-interaction joint states \( |X\rangle, |Y\rangle \) turn out to be optimal for Eve with a POVM \( \{ E_\lambda \} \) iff the following conditions are satisfied:

\[
\sqrt{D_{uv}} \langle U_{\lambda a} \rangle = \varepsilon_\lambda \sqrt{1 - D_{uv}} \langle V_{\lambda a} \rangle, \quad (9.u)
\]
\[
\sqrt{D_{uv}} \langle V_{\lambda a} \rangle = \varepsilon_\lambda \sqrt{1 - D_{uv}} \langle U_{\lambda a} \rangle. \quad (9.v)
\]

Similarly, analogous conditions hold for the optimality of the post-interaction joint states in the \( uv \) basis.

### 3.2 A new necessary and sufficient condition toward completely characterizing Eve’s optimal states

Now, we move from this NSC to derive a refined one. In this pursuit, we move through a series of \( \text{iff} \) conditions that eventually derives the optimal IVs in terms of the optimal measurement basis.

The following observation is going to help finding a refined certificate for optimality.

**Lemma 1.** The post-interaction states of Eve exhibit an interrelation involving the overlap between the two undisturbed states and that between the two disturbed states.

\[
(1 - D_{xy}) \langle \xi_x | \zeta_y \rangle + D_{xy} \langle \xi_x | \zeta_y \rangle = 2 \mathcal{D}_{uv}^+ \mathcal{D}_{uv}^{-}.
\]

The result follows by considering the inter-relations (25) between the IVs across the bases, while imposing the normalization constraint on \( |\xi_u\rangle \). The result agrees with [14]. However, we provide more powerful statement on its individual overlaps in the following.

Here we derive a series of \( \text{iff} \) conditions for an interaction to be optimal. The following conditions are equivalent.

**Theorem 1.** The set of interaction vectors in the \( xy \) basis is optimal along with the projectors \( E_\lambda := |E_\lambda \rangle \langle E_\lambda| \) for measurement \( \text{iff} \) any of the following conditions hold:

1. The overlap between the measurement direction \( |E_\lambda\rangle \) in the \( xy \) basis and the interaction vectors in the \( uv \) basis are related in the following way:

\[
\langle E_\lambda | \xi_u \rangle = \varepsilon_\lambda \langle E_\lambda | \zeta_u \rangle,
\]
\[
\langle E_\lambda | \xi_v \rangle = \varepsilon_\lambda \langle E_\lambda | \zeta_v \rangle. \quad (10)
\]

**Corollary 1.** The overlap between the interaction vectors in the \( xy \) basis satisfy the following condition:

\[
\langle \xi_x | \zeta_y \rangle = \varepsilon_\lambda = 1 - 2 D_{uv}. \quad (11)
\]

2. The overlaps between the measurement direction \( |E_\lambda\rangle \) in the \( xy \) basis and the interaction vectors in the same basis must maintain the following ratio:

\[
\frac{\langle E_\lambda | \xi_x \rangle}{\langle E_\lambda | \xi_y \rangle} = \frac{\langle E_\lambda | \zeta_x \rangle}{\langle E_\lambda | \zeta_y \rangle} = \frac{\mathcal{D}_{uv}^+}{\mathcal{D}_{uv}^{-}} \varepsilon_\lambda. \quad (12)
\]

Here, we improvise to the following notation

\[
\mathcal{T}_{uv}(\pm, \varepsilon_\lambda) = \frac{1}{\sqrt{2}} \left( \sqrt{1 - D_{uv}^2} \pm \varepsilon_\lambda \sqrt{D_{uv}} \right). \quad (13)
\]

It becomes \( \mathcal{D}_{uv}^+ \), or, \( \mathcal{D}_{uv}^- \), depending on whether \( \varepsilon_\lambda \) becomes +1, or, −1, respectively.

3. The interaction vectors in the \( xy \) basis can be expressed in an orthonormal basis \( \{|E^+_\lambda\rangle, |E^-_\lambda\rangle, |E^{+\prime}_\lambda\rangle, |E^{-\prime}_\lambda\rangle\} \) as follows:

\[
|\xi_x\rangle = \mathcal{D}_{uv}^+ |E^+_\lambda\rangle + \mathcal{D}_{uv}^- |E^-_\lambda\rangle,
\]
\[
|\xi_y\rangle = \mathcal{D}_{uv}^+ |E^+_\lambda\rangle + \mathcal{D}_{uv}^- |E^-_\lambda\rangle,
\]
\[
|\zeta_x\rangle = \mathcal{D}_{uv}^+ |E^{+\prime}_\lambda\rangle + \mathcal{D}_{uv}^- |E^{-\prime}_\lambda\rangle,
\]
\[
|\zeta_y\rangle = \mathcal{D}_{uv}^+ |E^{+\prime}_\lambda\rangle + \mathcal{D}_{uv}^- |E^{-\prime}_\lambda\rangle. \quad (14)
\]

The basis vectors \( \{|E^+_\lambda\rangle, |E^{+\prime}_\lambda\rangle\} \) correspond to some unitary transform \( R^\pm \) of those two measurement directions \( |E_\lambda\rangle \) that provide \( \pm\varepsilon_\lambda \) outcomes.

The above four \( \text{iff} \) conditions in Theorem 1 are equivalent, in the sense that any of them can be derived [see Sect. 6] from the other one, directly, or via some of the remaining conditions as sketched below.

![Diagram](https://example.com/diagram)

**3.3 Explaining the \( \text{iff} \) conditions**

Let’s explain the essence of the four \( \text{iff} \) conditions described in Theorem 1 involving the optimality of the four interaction vectors in the \( xy \) basis.

The 1st \( \text{iff} \) condition says that the overlap between a measurement direction \( |E_\lambda\rangle \) and a fidelity state corresponding to Alice’s signal \( u \) (or \( v \)) is the same in magnitude as the overlap between that measurement direction and the disturbed state corresponding to Alice’s signal \( v \) (or \( u \)), except that they differ in sign \( \varepsilon_\lambda \).
The 2nd iff condition says that the ratio of the overlaps between a measurement direction and the undisturbed states are the same as the ratio of the overlaps between the measurement direction and the disturbed states. The ratio becomes $\mathcal{D}_{uv}^+ / \mathcal{D}_{uv}^-$ or its inverse depending on whether the measurement outcome is positive or negative in sign.

The 3rd iff condition provides the optimal interaction vectors, and therefore are the only and all possible optimal IVs. They are unitarily equivalent to those in Ref. [6, Eq.(38)], as established in Sect. 6.2.2.

The iff condition in Corollary 1, which is a byproduct of the 1st iff condition of Theorem 1, restricts Eve’s optimal states to have a specific orientation in the four-dimensional Hilbert space. To be more specific, when Alice encodes is $xy$ basis, the overlap between the two fidelity states must be the same as the overlap between the two disturbed states and is equal to $(1 - 2D_{uv})$.

The new NSC and its significance: The necessary and sufficient condition in Corollary 1 can be used as a working formula to verify whether a given set of IVs is optimal or not. It’s efficient due to easy verification, it’s simple as it involves Eve’s states only than the joint Hilbert space as in Ref. [5], it’s intuitive as it demands a specific configuration of the states in Eve’s Hilbert space.

An optimal attack is essentially characterized by the optimal overlap, called here as optimal syndrome, that amounts to $1 - 2D$ for a symmetric attack. It exhibits interesting links between various other approaches for eavesdropping. Although the connection between Bell violation and optimal state discrimination is known [5], we find the connection more explicit here with respect to the optimal syndrome. For a specific error-rate $D$, the fraction of reduction in the optimal CHSH-sum in an $eb$ scheme is precisely the optimal syndrome in the $p&m$ scheme. The Bloch vector at the receiving end shrinks by the same factor.

4 Characterizing optimal unitary evolutions

Given the optimal post-interaction joint states $|X^*\rangle, |Y^*\rangle$, we wish to find an optimal unitary for a suitable initial state $|\psi_0\rangle$ of Eve’s ancilla. Mathematically speaking, the task is to solve the following equations.

$$U_{\psi_0}^{AE} |0\rangle_A |\psi_0\rangle_E = |X^*\rangle, \quad U_{\psi_0}^{AE} |1\rangle_A |\psi_0\rangle_E = |Y^*\rangle.$$  

(15)

Although the same unitary serves the purpose in the conjugate basis, the measurement setup generally differs.

Getting a specific optimal unitary $U_{\psi_0}$ from a given pair of post-interaction joint states, i.e., solving Eq. (15), can be done by the following basis completion method.

By introducing some auxiliary states, an unitary evolution $U_{\psi_0}$ can be viewed as a linear transformation that maps an orthonormal basis $\{|0\rangle_A |\psi_i\rangle_E\}_{i \in \{0,1,2,3\}}$ to the orthonormal basis $\{|X_i\rangle, |Y_i\rangle\}_{i \in \{0,1,2,3\}}$, where $|X_0\rangle = |X^*\rangle, |Y_0\rangle = |Y^*\rangle$.

$$U_{\psi_0} |0\rangle_A |\psi_i\rangle_E = |X_i\rangle, \quad U_{\psi_0} |1\rangle_A |\psi_i\rangle_E = |Y_i\rangle,$$

$\forall i \in \{0,1,2,3\}$.

Then a solution for the optimal unitary can be given by

$$U_{\psi_0} = \sum_{i=0}^{3} (|X_i\rangle \langle 0_A | + |Y_i\rangle \langle 1_A |) |\psi_i\rangle \langle E|.$$  

(16)

which can further be factored [see Sect. 6.3.2] in two unitaries as

$$U_{\psi_0} = \mathcal{W}^{AE}_{X,Y} (1^A_2 \otimes W^{E^\dagger}_{\psi_0}).$$  

(17)

The first unitary $\mathcal{W}^{AE}_{X,Y}$, that depends on the PIJSs $|X^*\rangle, |Y^*\rangle$, is defined as

$$\mathcal{W}^{AE}_{X,Y} := \sum_{i=0}^{3} |X_i\rangle \langle 0_A | i_E | + |Y_i\rangle \langle 1_A | i_E |,$$

(18)Mat

which has the following matrix representation

$$\begin{bmatrix}
|X_0\rangle, |X_1\rangle, |X_2\rangle, |X_3\rangle, & |Y_0\rangle, |Y_1\rangle, |Y_2\rangle, |Y_3\rangle
\end{bmatrix}.$$  

(18.Mat)

The local unitary $\mathcal{W}$, that depends on the initial state $|\psi_0\rangle$, is defined as follows

$$\mathcal{W}^{E}_{\psi_0} = \sum_{i=0}^{3} |\psi_i\rangle \langle i_E |$$

(19)

which has the following matrix representation

$$\begin{bmatrix}
|\psi_0\rangle, |\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle
\end{bmatrix}.$$  

(19.Mat)

We observe from Eq. (17) that an optimal unitary is a product of two unitaries. In order to evolve the joint system from the initial state $|a\rangle|c\rangle$, the part of it first transforms Eve’s initial state to $|00\rangle$ leaving Alice’s part invariant, and then the second part creates the required entanglement between Alice and Eve’s states.

Equations (2) and (3) together depict that Eve’s measurement setup $M$ is in one-to-one correspondence with the post-interaction joint states $|X^M\rangle, |Y^M\rangle$. Moreover, the factorization (17) indicates that a joint unitary $U$ is two-parametric: the initial state $IS$ of Eve’s ancilla, and Eve’s measurement setup $M$. While the earlier one (IS) controls the unitary $U^{IS}_{\psi_0}$, the later one ($M$) determines $\mathcal{W}^{X,Y}_E$. Nevertheless, $U \equiv U^{IS}_M$ represent an infinite collection of unitaries.

When Eve measures in four-dimensional computational basis $\{ |00\rangle, |01\rangle, |10\rangle, |11\rangle \}$ denote the optimal post-interaction joint states as $|X^c\rangle, |Y^c\rangle$ and are
described in Table 2. Let’s consider the problem of getting an optimal unitary that evolves an initial state of Eve’s ancilla along with the captured signal state into these post-interaction joint states. As discussed earlier, it corresponds to the problem of basis completion: once in the eight-dimensional space of optimal PIJSs, and once in the four-dimensional space of the initial state. To avoid any technical difficulty (e.g., numerical, or, trial-and-error approach) with basis completion, we address briefly a unique analytical approach.

The crux is to view the post-interaction joint states $|X\rangle^C$ and $|Y\rangle^C$ to be resulted out of an action of two sub-matrices $U_x := (|00\rangle\langle 11|) \otimes I_2$ and $U_y := (|10\rangle\langle 01|) \otimes \sigma_x$, respectively, on some specific initial state

$$|\Delta\Omega\rangle_E := |\Delta_{xy}\rangle_{E_1}|\Omega_{uv}\rangle_{E_2}, \quad (20)$$

where the individual factor states are defined for a chosen basis $\beta \in \{xy, uv\}$ as follows

$$|\Delta\beta\rangle := \sqrt{F_\beta}|0\rangle + \sqrt{D_\beta}|1\rangle,$$

$$|\Omega\rangle_\beta := \mathbb{H}|\Delta\beta\rangle = \mathbb{D}_\beta|0\rangle + \mathbb{D}_\beta|1\rangle. \quad (21)$$

The optimal unitary $U$ eventually becomes the partitioned matrix $[U_x, U_y]$ with the block-matrix form as follows

$$U^C_{\Delta\Omega} = \begin{bmatrix}
1_2 & \cdots & \cdots & \cdots \\
\cdots & \cdots & \cdots & \cdots \\
\cdots & \cdots & \sigma_x & \cdots \\
\cdots & \cdots & \cdots & \cdots \\
1_2 & \cdots & \cdots & \cdots
\end{bmatrix}, \quad (22)$$

The 2-dim submatrices $1_2$ (identity) and $\sigma_x$ (Pauli X-spin) operate on the second qubit of Eve’s probe.

However, the same states $|X\rangle^C$, and $|Y\rangle^C$ can also be produced by some other unitary acting on the same joint initial states $|0\rangle_A|\Delta\Omega\rangle_E$ and $|1\rangle_A|\Delta\Omega\rangle_E$, respectively. Eventually, there are infinitely many such unitary evolutions for the same post-interaction joint states and the same initial state, as evident from Eq. (17). The arbitration is twofold: on $\mathcal{W}_{X,Y}$ or $\mathcal{W}_{\psi_0}$, which in turn corresponds to various choices of the auxiliary states $\{\langle X_i|,|Y_i|\}_{i=1,2,3}$ or $\{|\psi_i\rangle\}_{i=1,2,3}$, respectively. The later arbitration, for instance, is technically achieved by post-multiplying the unitary in Eq. (22) by some $I_2 \otimes \Gamma_{\psi_0}^{\pm}$, where the local unitary $\Gamma_{\psi_0}^{\pm}$ leaves $|\psi_0\rangle$ unchanged while makes new choices for the auxiliary states $|\psi_i\rangle_{i=1,2,3}$. For instance, the following choice

$$\Gamma_{\psi_0}^{\pm} = \begin{bmatrix}
1 & \cdots & \cdots & \cdots \\
\sqrt{2} & \cdots & \cdots & \cdots \\
\cdots & \cdots & 1 & \cdots \\
\cdots & \cdots & \cdots & \cdots \\
1 & \sqrt{2} & \cdots & \cdots
\end{bmatrix},$$

will affect the (2nd, 4th) and (6th, 8th) columns of the unitary $U^C_{\Delta\Omega}$. Naturally, the unitary in Eq. (22) is the simplest among its infinitely many siblings.

Moreover, the same PIJSs $|X\rangle^C$, and $|Y\rangle^C$ can be produced by a newer family of unitary evolutions if we consider a different initial state of Eve’s ancilla. Getting an optimal unitary for a different initial state corresponds to finding a local unitary that transforms the earlier initial state to a newer one, as formulated in Eq. (27). For instance, consider finding the optimal unitary for the initial state $|0\rangle_E$ which in turn is a unitary tweak $A_{xy} \otimes \mathbb{H}$ of the initial state in Eq. (20) for the two-dimensional unitary $A_\beta = \sqrt{1-D_\beta}\sigma_x + \sqrt{D_\beta}\sigma_x$. The desired optimal unitary $U^C_{\Delta\Omega}$ is given in Table 2.

We can now interrelate our unique approach with the rudimentary basis completion method. One can now directly read the auxiliary basis states $\{\langle X_i|,|Y_i|\}$ from the columns of the unitary $U^C_{\Delta\Omega}$ by fixing the other auxiliary basis states $\{|\psi_i\rangle\}$ to enforce $\mathcal{W}_{\psi_0}$ to be the identity matrix. It is so because the unitary $U^C_{\Delta\Omega}$ represents the matrix in Eq. (18.Mat).

Finally, consider finding optimal unitaries in a different measurement basis other than the computational basis. Eve’s new measurement basis $\{E_\lambda\}$ is a unitary transformation $|E_\lambda\rangle = \mathbf{M}_{xy}(\lambda)$ of the computational basis. For instance, consider the unitary transformation $\mathbf{M}_{xy} = (|E_0\rangle\langle E_1|,|E_2\rangle\langle E_3|)$, as mentioned in Table 2. Corresponding optimal PIJSs $\{\langle X\rangle^M,\langle Y\rangle^M\}$ and an optimal unitary ($U^M$) can be obtained by operating $(I_2 \otimes \mathbf{M})$ on those in the computational basis, and are described in Table 2.

5 Classical post-processing

If the disturbance $D$ is within the threshold, one-way classical post-processing can be considered to filtrate into a secret key. Although we have already calculated the key-rate for the sifted key, the final key-rate is relevant to get an idea of how much more data is to be sacrificed. For our optimal states [5,6] for incoherent eavesdropping on the BB84 protocol, here we compute the related parameters.

For $QBER=D$, Bob knows $I_{AB} = 1 - H(D)$ fraction of Alice’s bit-string correctly. The remaining $H(D)$ fraction is erroneous due to Eve and is either discarded or corrected. In case of err-discard, they remove at least $H(D)$ fraction of the sifted key.

Eve’s knowledge on the final key can be made arbitrarily small by properly choosing the fraction $\tau(D)$ of the reconciled key to be discarded [15] during privacy amplification.

Thus, the key-rate for the final key depends on the two quantities: $MI_{AB}$, and the discarded fraction $\tau(D)$. Depending on whether the error is corrected or discarded, the final key-rate boils down to computing the followings.

$$R_{\text{corr}}^\text{fin} := I_{AB}(D) - (1 - D)\tau(D) - D,$$

$$R_{\text{disc}}^\text{fin} := I_{AB}(D) - (1 - D)\tau(D) - D,$$

$$I_{AB} = 1 - H(D).$$
5.1 Discarded fraction for our optimal states

Based on a criteria for strong security [15], a condition on the discarded fraction in order to reduce Eve’s knowledge (Shannon information) on the final key is as follows [14,16]. For individual attack, for an error-rate $D$, Eve knows less than $\frac{1}{m^2}$ bits of the final key provided

$$\tau_D \geq 1 + \log_2(P_2^{(c)}).$$  \hspace{1cm} (23)

Here, $P_2^{(c)}$ is the maximum average collision probability of Eve’s knowledge per bit of the reconciled key. When Alice prepares her signals in the $xy$ basis, the collision probability of order 2 averaged over Eve’s measurement knowledge $\lambda$ is defined as follows.

$$(P_2^{(c)})_{xy} = \sum_{\lambda} P_\lambda \left( P_{x|x\lambda}^2 + P_{y|y\lambda}^2 \right).$$

Considering Eve’s optimal states in the $xy$ basis, the posterior probabilities become [6]

$$P_{x|x\lambda} = \frac{1}{2} \pm \sqrt{D_{uv}(1-D_{uv})},$$  \hspace{1cm} (24a)

$$P_{y|y\lambda} = \frac{1}{2} \pm \sqrt{D_{uv}(1-D_{uv})}, \ \forall \lambda.$$

Thus,

$$P_{x|x\lambda}^2 + P_{y|y\lambda}^2 = \frac{1}{2} + 2D_{uv}(1-D_{uv}), \ \forall \lambda.$$

Thereby, the average collision probability becomes

$$(P_2^{(c)})_{xy} = \frac{1}{2} (1 + 4D_{uv} - 4D_{uv}^2).$$

Hence, considering equal errors $D$ across the two bases, the right-hand side for the inequality in Eq. (23) becomes

$$1 + \log_2(P_2^{(c)}) \geq \log_2(1 + 4D - 4D^2).$$  \hspace{1cm} (24)

Clearly, for our optimal states, the discarded fraction saturates the Lütkenhaus bound [14,17].

5.2 Final key-rate for our optimal states

From the expression of $\tau(D)$ as calculated above, one can calculate the key-rate for the final key as follows.

$$R_{\text{corr}} = \log_2(1 + 4D - 4D^2),$$

$$R_{\text{disc}} = 1 - H(D) - \log_2(1 + 4D - 4D^2) - D.$$  \hspace{1cm} (25)

These are plotted in Fig. 3. As evident, the final key-rate becomes 10.5% when error is discarded, and 11.5% when error is corrected.

6 Proofs and technical details

Here we sketch a broad outline to prove the claims in the earlier sections.

6.1 Proofs for Sect. 2

Although Sect. 2 mainly recapitulates the background knowledge, to maintain the flow of ideas we have kept two newly found results therein. We prove them here.

6.1.1 Interrelating optimal POVMs across the two MUBs

Here we sketch an outline to prove Eq. (6) that interrelates two optimal POVMs in the conjugate bases. Note that the conjugate relation between the two encoding bases gets inherited to a similar conjugate relation between the post-interaction joint states across two MUBs. The later conjugate relation in turn produces an inter-relation between the two sets of interaction vectors across the two MUBs [5]. In this relation, one can directly plug in the optimal interaction vectors as expressed in Eqs. (3, 5) and a simple algebra would eventually lead to Eq. (6). The technical details are as follows.

Since the conjugate relation for the encoding bases inherits to the post-interaction joint state, the interaction vectors in each of the encoding bases get interrelated as follows.

$$2\sqrt{F_{uv}(\xi_\alpha)} = \sqrt{F_{xy}(|\xi_x\rangle + |\xi_y\rangle)} + \sqrt{D_{xy}(|\xi_x\rangle + |\xi_y\rangle)},$$  \hspace{1cm} (26.F+)

$$2\sqrt{F_{uv}(\xi_\alpha)} = \sqrt{F_{xy}(|\xi_x\rangle + |\xi_y\rangle)} - \sqrt{D_{xy}(|\xi_x\rangle + |\xi_y\rangle)},$$  \hspace{1cm} (26.F–)

$$2\sqrt{D_{uv}(\xi_\alpha)} = \sqrt{F_{xy}(|\xi_x\rangle - |\xi_y\rangle)} + \sqrt{D_{xy}(|\xi_x\rangle - |\xi_y\rangle)},$$  \hspace{1cm} (26.D+)

$$2\sqrt{D_{uv}(\xi_\alpha)} = \sqrt{D_{xy}(|\xi_0\rangle - |\xi_\xi\rangle)}.$$  \hspace{1cm} (26.D–)

The sum and difference between the fidelity states (and similarly for the disturbed states) in $uv$ basis are written in terms of the Eve’s states in $xy$ basis.

$$\sqrt{F_{uv}(|\xi_\alpha\rangle + |\xi_\alpha\rangle)} = \sqrt{F_{xy}(|\xi_x\rangle + |\xi_y\rangle)},$$  \hspace{1cm} (26.F+)

$$\sqrt{F_{uv}(|\xi_\alpha\rangle - |\xi_\alpha\rangle)} = \sqrt{D_{xy}(|\xi_x\rangle + |\xi_y\rangle)},$$  \hspace{1cm} (26.F–)

$$\sqrt{D_{uv}(|\xi_\alpha\rangle + |\xi_\alpha\rangle)} = \sqrt{F_{xy}(|\xi_x\rangle - |\xi_y\rangle)},$$  \hspace{1cm} (26.D+)

$$\sqrt{D_{uv}(|\xi_\alpha\rangle - |\xi_\alpha\rangle)} = \sqrt{D_{xy}(|\xi_0\rangle - |\xi_\xi\rangle)}.$$  \hspace{1cm} (26.D–)

Now, we use the optimal interaction vectors for $xy$ and $uv$ basis as in Eqs. (3, 5) to find the sum and difference of the parity IVs (disturbed or undisturbed) and feed them back into Eq. (26) to get the following relations:

$$|F_0\rangle + |F_1\rangle = |E_0\rangle + |E_1\rangle,$$  \hspace{1cm} (26.1+)

$$|F_0\rangle - |F_1\rangle = |E_0\rangle - |E_1\rangle,$$  \hspace{1cm} (26.1–)

$$|F_2\rangle + |F_3\rangle = |E_2\rangle + |E_3\rangle,$$  \hspace{1cm} (26.2+)

$$|F_2\rangle - |F_3\rangle = |E_2\rangle - |E_3\rangle.$$  \hspace{1cm} (26.2–)

Getting the relation between the optimal measurement directions in Eq. (6) is now obvious.
In these expressions, the amplitude of each compos-

The PIJSs in two different measurement basis

| $|X\rangle^C$ | $|Y\rangle^C$ | $|X\rangle^M$ | $|Y\rangle^M$ |
|---|---|---|---|
| $\sqrt{F_{xy}} \hat{p}_{xy}^+$ | $\sqrt{D_{xy}} \hat{p}_{xy}$ | $\sqrt{D_{xy}} (-\frac{\sqrt{3}}{3} \hat{p}_{xy} - \frac{1}{\sqrt{3}} \hat{p}_{uv})$ | $\sqrt{D_{xy}} (-\frac{\sqrt{3}}{3} \hat{p}_{xy} + \frac{1}{\sqrt{3}} \hat{p}_{uv})$ |
| $\sqrt{F_{xy}} \hat{p}_{xy}$ | $\sqrt{D_{xy}} \hat{p}_{xy}$ | $\sqrt{D_{xy}} (-\frac{\sqrt{3}}{3} \hat{p}_{xy} + \frac{1}{\sqrt{3}} \hat{p}_{uv})$ | $\sqrt{D_{xy}} (-\frac{\sqrt{3}}{3} \hat{p}_{xy} - \frac{1}{\sqrt{3}} \hat{p}_{uv})$ |
| $\sqrt{F_{xy}} \hat{p}_{xy}$ | $\sqrt{D_{xy}} \hat{p}_{xy}$ | $\sqrt{D_{xy}} (-\frac{\sqrt{3}}{3} \hat{p}_{xy} + \frac{1}{\sqrt{3}} \hat{p}_{uv})$ | $\sqrt{D_{xy}} (-\frac{\sqrt{3}}{3} \hat{p}_{xy} - \frac{1}{\sqrt{3}} \hat{p}_{uv})$ |
| $\sqrt{F_{xy}} \hat{p}_{xy}$ | $\sqrt{D_{xy}} \hat{p}_{xy}$ | $\sqrt{D_{xy}} (-\frac{\sqrt{3}}{3} \hat{p}_{xy} + \frac{1}{\sqrt{3}} \hat{p}_{uv})$ | $\sqrt{D_{xy}} (-\frac{\sqrt{3}}{3} \hat{p}_{xy} - \frac{1}{\sqrt{3}} \hat{p}_{uv})$ |
| $\sqrt{F_{xy}} \hat{p}_{xy}$ | $\sqrt{D_{xy}} \hat{p}_{xy}$ | $\sqrt{D_{xy}} (-\frac{\sqrt{3}}{3} \hat{p}_{xy} + \frac{1}{\sqrt{3}} \hat{p}_{uv})$ | $\sqrt{D_{xy}} (-\frac{\sqrt{3}}{3} \hat{p}_{xy} - \frac{1}{\sqrt{3}} \hat{p}_{uv})$ |
| $\sqrt{F_{xy}} \hat{p}_{xy}$ | $\sqrt{D_{xy}} \hat{p}_{xy}$ | $\sqrt{D_{xy}} (-\frac{\sqrt{3}}{3} \hat{p}_{xy} + \frac{1}{\sqrt{3}} \hat{p}_{uv})$ | $\sqrt{D_{xy}} (-\frac{\sqrt{3}}{3} \hat{p}_{xy} - \frac{1}{\sqrt{3}} \hat{p}_{uv})$ |
| $\sqrt{F_{xy}} \hat{p}_{xy}$ | $\sqrt{D_{xy}} \hat{p}_{xy}$ | $\sqrt{D_{xy}} (-\frac{\sqrt{3}}{3} \hat{p}_{xy} + \frac{1}{\sqrt{3}} \hat{p}_{uv})$ | $\sqrt{D_{xy}} (-\frac{\sqrt{3}}{3} \hat{p}_{xy} - \frac{1}{\sqrt{3}} \hat{p}_{uv})$ |
| $\sqrt{F_{xy}} \hat{p}_{xy}$ | $\sqrt{D_{xy}} \hat{p}_{xy}$ | $\sqrt{D_{xy}} (-\frac{\sqrt{3}}{3} \hat{p}_{xy} + \frac{1}{\sqrt{3}} \hat{p}_{uv})$ | $\sqrt{D_{xy}} (-\frac{\sqrt{3}}{3} \hat{p}_{xy} - \frac{1}{\sqrt{3}} \hat{p}_{uv})$ |
| $\sqrt{F_{xy}} \hat{p}_{xy}$ | $\sqrt{D_{xy}} \hat{p}_{xy}$ | $\sqrt{D_{xy}} (-\frac{\sqrt{3}}{3} \hat{p}_{xy} + \frac{1}{\sqrt{3}} \hat{p}_{uv})$ | $\sqrt{D_{xy}} (-\frac{\sqrt{3}}{3} \hat{p}_{xy} - \frac{1}{\sqrt{3}} \hat{p}_{uv})$ |
| $\sqrt{F_{xy}} \hat{p}_{xy}$ | $\sqrt{D_{xy}} \hat{p}_{xy}$ | $\sqrt{D_{xy}} (-\frac{\sqrt{3}}{3} \hat{p}_{xy} + \frac{1}{\sqrt{3}} \hat{p}_{uv})$ | $\sqrt{D_{xy}} (-\frac{\sqrt{3}}{3} \hat{p}_{xy} - \frac{1}{\sqrt{3}} \hat{p}_{uv})$ |

An optimal unitary when Eve measures in the four-dimensional computational basis (C)

$$U_{00}^C = \begin{pmatrix} \sqrt{F_{xy}} [-\hat{p}_{xy} - \hat{p}_{uv}] & \sqrt{D_{xy}} [-\hat{p}_{xy} + \hat{p}_{uv}] \\ \sqrt{D_{xy}} [-\hat{p}_{xy} + \hat{p}_{uv}] & \sqrt{F_{xy}} [-\hat{p}_{xy} - \hat{p}_{uv}] \end{pmatrix} \begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix},$$

An optimal unitary when Eve measures in the $R$-rotated computational basis (M)

$$U_{00}^M = \begin{pmatrix} R_A & R_B \\ R_C & R_D \end{pmatrix} \begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix},$$

with $R = \begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{2}}{2} & -\frac{1}{2} & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & \frac{1}{2} & \frac{\sqrt{2}}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{2}}{2} & \frac{1}{2} & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & -\frac{1}{2} & -\frac{\sqrt{2}}{2} & \frac{1}{2} \end{pmatrix}$.

The initial state of Eve’s probe is chosen as $|00\rangle$ for both the measurement setups

$\hat{D}^+$ and $\hat{D}^-$ represent null submatrix of order 2

6.1.2 Optimal PIJSs in the p&m scheme versus the output of an optimal phase-covariant cloner

For the p&m scheme, considering an attack leveraging equal QBER=D across the two encoding bases, the post-interaction joint states become

$$U|0\rangle|e\rangle = \sqrt{1-D} |0\rangle (\hat{D}^+|E_0\rangle + \hat{D}^-|E_1\rangle) + \sqrt{D} |1\rangle (\hat{D}^+|E_2\rangle + \hat{D}^-|E_3\rangle),$$

$$U|1\rangle|e\rangle = \sqrt{1-D} |1\rangle (\hat{D}^-|E_0\rangle + \hat{D}^+|E_1\rangle) + \sqrt{D} |0\rangle (\hat{D}^-|E_2\rangle + \hat{D}^+|E_3\rangle).$$

In these expressions, the amplitude of each composite state $|a\rangle|E_3\rangle$ at the maximum tolerable disturbance $D^* = \frac{1}{2} \left( 1 - \frac{1}{\sqrt{2}} \right)$ are calculated as follows.
\[ U|1\rangle|e\rangle = \frac{1}{2} \left( 1 + \frac{1}{\sqrt{2}} \right) |1\rangle|E_1\rangle + \frac{1}{2} \left( 1 - \frac{1}{\sqrt{2}} \right) |0\rangle|E_2\rangle + \frac{1}{2\sqrt{2}} (|1\rangle|E_0\rangle + |0\rangle|E_3\rangle). \]

For the measurement setup \{\{E_0\}, \{E_1\}, \{E_2\}, \{E_3\}\} = \{\{00\}, \{11\}, \{01\}, \{10\}\}, which in disguise is the Fuchs basis (except the shuffle in the last two) the optimal PJSs can then be written in the computational basis as follows.

\[ U|0\rangle|e\rangle = \frac{1}{2} \left( 1 + \frac{1}{\sqrt{2}} \right) |0\rangle|00\rangle + \frac{1}{2} \left( 1 - \frac{1}{\sqrt{2}} \right) |1\rangle|10\rangle + \frac{1}{2\sqrt{2}} (|0\rangle|11\rangle + |1\rangle|01\rangle), \]

\[ U|1\rangle|e\rangle = \frac{1}{2} \left( 1 + \frac{1}{\sqrt{2}} \right) |1\rangle|11\rangle + \frac{1}{2} \left( 1 - \frac{1}{\sqrt{2}} \right) |0\rangle|01\rangle + \frac{1}{2\sqrt{2}} (|1\rangle|00\rangle + |0\rangle|10\rangle). \]

They are same as the outputs of optimal phase-covariant cloner as in [7, Eq. (36)].

To conclude, the generalized optimal states that we derived here cover a broader spectrum than any existing analysis. A special choice of a measurement setup in our generalized scenario leads to the outputs of an optimal pc-cloner that in turn started with a particular choice of the initial condition. This way, one can use or improvise our results, and start with a specific choice of the initial conditions (and other parameters) to arrive at the initial condition specific analysis that is generally available in the existing literature.

6.2 Proofs for Sect. 3

6.2.1 Proving the necessary and sufficient conditions

Here we prove Theorem 1. The following relations involving the amplitudes \( \mathcal{G}^u_d \) and \( \mathcal{G}^u_u \) defined in Eq. (4) are heavily used in the derivations here.

\[ (\mathcal{G}^u_d)^2 - (\mathcal{G}^u_u)^2 = 2\sqrt{D_{uv}(1-D_{uv})}, \]

\[ (\mathcal{G}^u_d)^2 + (\mathcal{G}^u_u)^2 = 1, \quad 2\mathcal{G}^u_d\mathcal{G}^u_u = 1 - 2D_{uv}. \]

**Proof of the iff condition 1 of Theorem 1** The catch here is to unfold the fictitious states in Eq. (8) by using the Schmidt form of the post-interaction joint states \( |U\rangle, |V\rangle \), and feed them back into Eq. (9).

Choosing \( a = u \), Eq. (8) provides

\[ |U_{\lambda u}\rangle = B_u \otimes E_\lambda |U\rangle \]

\[ = \sqrt{1 - D_{uv}} \langle E_\lambda |\xi_u\rangle \langle |u\rangle |E_\lambda\rangle, \]

\[ |V_{\lambda u}\rangle = B_u \otimes E_\lambda |V\rangle \]

\[ = \sqrt{D_{uv}} \langle E_\lambda |\zeta_u\rangle \langle |u\rangle |E_\lambda\rangle. \]

Feeding them back into Eq. (9.u) leads to the first equality in Eq. (10).

Key-rate becomes 10.5% when error discarded, and 11.5% when error corrected.

![Fig. 3 Final key-rate for error discard and correction](image)

The second equality in Eq. (10) can similarly be derived from the iff condition (9.v) while unfolding the fictitious states in Eq. (8) for \( a = v \).

**Proof of the iff condition 2 of Theorem 1** The iff conditions in Eq. (10) can be grouped as follows:

\[ \langle E_\lambda |(|\xi_u\rangle \pm |\xi_v\rangle) = \varepsilon_\lambda \langle E_\lambda |(|\zeta_u\rangle \pm |\zeta_v\rangle). \]

Now, we look back to the interrelations between the interaction vectors in \( xy \) and \( uv \) basis, viz., use Eqs. (26.F+, 26.D+). Taking the inner product of the interaction vectors in each of these equations with the
measurement directions \(|E_\lambda\rangle\), and then taking the ratio of the like sides, we get,
\[
\frac{\langle E_\lambda | \xi_\alpha \rangle + \langle E_\lambda | \xi_\beta \rangle}{\langle E_\lambda | \xi_\gamma \rangle} = \frac{\sqrt{D_{uv}} \langle E_\lambda | \xi_\alpha \rangle + \langle E_\lambda | \xi_\beta \rangle}{\sqrt{D_{uv}} \langle E_\lambda | \xi_\gamma \rangle} = \frac{\sqrt{D_{uv}} \langle E_\lambda | \xi_\alpha \rangle}{\sqrt{D_{uv}} \langle E_\lambda | \xi_\gamma \rangle} \frac{\langle E_\lambda | \xi_\beta \rangle}{\langle E_\lambda | \xi_\gamma \rangle}.
\]

By component and dividendo, we get,
\[
\frac{\langle E_\lambda | \xi_\alpha \rangle}{\langle E_\lambda | \xi_\gamma \rangle} = \frac{\sum \lambda T_{uv}(+, \varepsilon_\alpha \rangle \langle E_\lambda | \xi_\alpha \rangle}{\sum \lambda T_{uv}(-, \varepsilon_\alpha \rangle \langle E_\lambda | \xi_\alpha \rangle} = \frac{\sum \lambda T_{uv}(+, \varepsilon_\alpha \rangle \langle E_\lambda | \xi_\beta \rangle}{\sum \lambda T_{uv}(-, \varepsilon_\alpha \rangle \langle E_\lambda | \xi_\gamma \rangle} \frac{\langle E_\lambda | \xi_\alpha \rangle}{\langle E_\lambda | \xi_\gamma \rangle}.
\]

We used here the improved notation of Eq. (13). The ratio \(T_{uv}(+, \varepsilon_\alpha \rangle \langle E_\lambda | \xi_\alpha \rangle)/T_{uv}(-, \varepsilon_\alpha \rangle \langle E_\lambda | \xi_\alpha \rangle)\) becomes \(P_{uv}/P_{uv}\) or its inverse depending on whether the sign \(\pm\) of the eigenvalue assumes \(+1\) or \(-1\), respectively.

Similarly, to establish the other ratio \(\langle E_\lambda | \xi_\alpha \rangle/\langle E_\lambda | \xi_\beta \rangle\) of Eq. (12), we consider Eqs. (26.F−, 26.D−) and follow the same procedure as above. \(\square\)

Proof of theiff condition 3 of Theorem 1 The proof follows from theiff condition 2, viz., Eq. (12). The overlaps in the ratio \(\langle E_\lambda | \xi_\alpha \rangle/\langle E_\lambda | \xi_\beta \rangle\) can be unfolded using some (complex) constant of proportion \(r_{\lambda, \xi}\) as follows.
\[
\langle E_\lambda | \xi_\alpha \rangle = r_{\lambda, \xi} T_{uv}(+, \varepsilon_\alpha \rangle \langle E_\lambda | \xi_\alpha \rangle, \quad \langle E_\lambda | \xi_\beta \rangle = r_{\lambda, \xi} T_{uv}(-, \varepsilon_\alpha \rangle \langle E_\lambda | \xi_\alpha \rangle.
\]

Note that, these overlaps constitute the components of the fidelity states when expressed in the eigenbasis \(|E_\lambda\rangle\).

Similarly, in the ratio \(\langle E_\lambda | \xi_\alpha \rangle/\langle E_\lambda | \xi_\beta \rangle\), the overlaps can be written, for some complex number \(r_{\lambda, \xi}\), in the following way.
\[
\langle E_\lambda | \xi_\alpha \rangle = r_{\lambda, \xi} T_{uv}(+, \varepsilon_\alpha \rangle \langle E_\lambda | \xi_\alpha \rangle, \quad \langle E_\lambda | \xi_\beta \rangle = r_{\lambda, \xi} T_{uv}(-, \varepsilon_\alpha \rangle \langle E_\lambda | \xi_\alpha \rangle.
\]

These are the components of the disturbed states when expressed in the eigenbasis \(|E_\lambda\rangle\).

Then we can write down the interaction vectors with respect to the eigenbasis \(|E_\lambda\rangle\) as follows.
\[
\xi_\alpha = \sum \lambda r_{\lambda, \xi} T_{uv}(+, \varepsilon_\alpha \rangle \langle E_\lambda | \xi_\alpha \rangle, \quad \xi_\beta = \sum \lambda r_{\lambda, \xi} T_{uv}(-, \varepsilon_\alpha \rangle \langle E_\lambda | \xi_\alpha \rangle,
\]
\[
\xi_\alpha = \sum \lambda r_{\lambda, \xi} T_{uv}(+, \varepsilon_\alpha \rangle \langle E_\lambda | \xi_\alpha \rangle, \quad \xi_\beta = \sum \lambda r_{\lambda, \xi} T_{uv}(-, \varepsilon_\alpha \rangle \langle E_\lambda | \xi_\alpha \rangle.
\]

But, we observe that, \(T_{uv}(+, \varepsilon_\alpha \rangle = P_{uv}, \) or, \(P_{uv}\) for \(\varepsilon_\alpha = +1\), or, \(-1\), respectively. Similarly, \(T_{uv}(-, \varepsilon_\alpha \rangle = P_{uv}, \) or, \(P_{uv}\) for \(\varepsilon_\alpha = +1,\) or, \(-1\), respectively. Thereby, in the expression of the interaction vectors, we can group the basis vectors \(|E_\lambda\rangle\) according to the sign of the measurement outcome. For instance, each of the fidelity states get two groups: \(|E_\pm\rangle\) groups the measurement directions for \(+\) or \(+\) outcomes. Similarly, the two groups for the disturbed states correspond to \(|E_\pm\rangle\).

The following equation captures the grouping:
\[
|E_\pm\rangle := \sum \lambda r_{\lambda, \xi} \langle E_\lambda | \xi_\alpha \rangle, \quad |E_\pm\rangle := \sum \lambda r_{\lambda, \xi} \langle E_\lambda | \xi_\alpha \rangle.
\]

With these grouping, the interaction vectors can be described as in Eq. (14). That the vectors \(|E_\pm\rangle\) form an orthonormal basis, can be argued as follows. As defined, the states in \(|E_\pm\rangle\) are mutually orthogonal to the states in \(|E_\pm\rangle\). Then, the normalization constraint on the fidelity (or disturbed) states together induces the normalization constraint on the states in \(|E_\pm\rangle\) (or \(|E_\pm\rangle\)). Moreover, the orthogonality of the fidelity states and the disturbed states inherits the orthogonality within the states in \(|E_\pm\rangle\) as well the orthogonality within the states in \(|E_\pm\rangle\).

The last but not the least is the fact that each of the states \(|E_\pm\rangle\) can be expressed in terms of exactly two of the measurement directions \(|E_\lambda\rangle\). It is so, the sign of the measurement outcomes are evenly distributed for an optimal interaction: two \(+\) outcomes, and two \(-\) outcomes. Had it not been this way, then, without loss of generality, let’s assume the possibility for only one \(+\) outcome. Then, each of the states \(|E_\pm\rangle\) should have only one of the measurement directions \(|E_\lambda\rangle\) in their description. While the normalization constraint on these states indicate the coefficients \(r_{\lambda, \xi}\) to be unimodular, their mutual orthogonality enforces one of these coefficients to be zero, leading to a contradiction. \(\square\)

Proof of Corollary 1 of Theorem 1 The proof follows from condition 1 of the same theorem and Lemma 1.

Clearly, an equality of the overlaps in Lemma 1 lead to the desired result (11). To establish this equality, we consider theiff conditions (10), but for optimality in \(uv\) basis, viz.
\[
\langle F_\lambda | \xi_\alpha \rangle = \langle E_\lambda | \xi_\alpha \rangle, \quad \langle F_\lambda | \xi_\beta \rangle = \langle E_\lambda | \xi_\beta \rangle.
\]

Multiplying the like sides of these two equations and adding over the measurement outcomes \(\lambda\) in \(uv\) basis, we get,
\[
\sum \lambda \langle \xi_\alpha | F_\lambda \rangle = \sum \lambda \langle \xi_\alpha | F_\lambda \rangle = \sum \lambda \langle \xi_\beta | F_\lambda \rangle = \sum \lambda \langle \xi_\beta | F_\lambda \rangle.
\]

Since the projectors \(F_\lambda\) consist a POVM, their completeness relation leads to the equality between the two overlaps \(\langle \xi_\alpha | \xi_\alpha \rangle\) and \(\langle \xi_\beta | \xi_\beta \rangle\), and consequently the desired result follows from Lemma 1. \(\square\)
Table 3: Transformation between the OLD and NEW bases that describes the interaction vectors with Eve

| OLD | NEW |
|-----|-----|
| \((|E^+_\xi\rangle, |E^-_{\xi}\rangle, |E^+_\zeta\rangle, |E^-_{\zeta}\rangle)\) | \(\downarrow\) SWAP |
| \((|E^+_\xi\rangle, |E^-_{\xi}\rangle, |E^+_\zeta\rangle, |E^-_{\zeta}\rangle)\) | \(\downarrow\) \(R\) |
| \((|E^+_\xi\rangle, |E^-_{\xi}\rangle, |E^+_\zeta\rangle, |E^-_{\zeta}\rangle)\) | \(\downarrow\) SWAP |
| \((|E^+_\xi\rangle, |E^-_{\xi}\rangle, |E^+_\zeta\rangle, |E^-_{\zeta}\rangle)\) | \(\downarrow\) SWAP |

6.2.2 The two representations of the optimal interaction vectors are unitarily equivalent

Considering Alice encoded in the \(xy\) basis, here we establish the equivalence of the optimal interaction vectors \(|\xi_x\rangle, |\xi_y\rangle, |\zeta_x\rangle, |\zeta_y\rangle\) as in Eq. (3) and those in Eq. (14).

First note that the (OLD) states in Eq. (3) are expressed in the (orthonormal) measurement basis \([|E^+_0\rangle, |E^-_1\rangle, |E^+_2\rangle, |E^-_3\rangle]\), where the superscripts \(\pm\) are introduced to track the sign of the eigenvalues. Whereas, the (NEW) states in Eq. (14) are expressed in another orthonormal basis \([|E^+_\xi\rangle, |E^-_{\xi}\rangle, |E^+_\zeta\rangle, |E^-_{\zeta}\rangle]\). Since both the bases describe the same 4-dimensional Hilbert space, they must be unitarily connected. The unitary equivalence is established in Table 3.

All the three maps are post-multiplication to transform the column-space, e.g.,

\[
\begin{align*}
(|E^+_\xi\rangle, |E^-_{\xi}\rangle, |E^+_\zeta\rangle, |E^-_{\zeta}\rangle) = (|E^+_\xi\rangle, |E^-_{\xi}\rangle, |E^+_\zeta\rangle, |E^-_{\zeta}\rangle) \text{ SWAP.}
\end{align*}
\]

The swap operation

\[
\text{SWAP} := \\
\begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
\end{bmatrix}
\]

exchanges the 2nd and the 3rd state.

The unitary \(R := \text{diag}(R^+, R^-)\) works twofold on the measurement directions: \(R^+\) rotates the subspace corresponding to the \(\pm\) outcomes.

\[
\begin{align*}
(|E^+_\xi\rangle, |E^-_{\xi}\rangle) &= (|E^+_0\rangle, |E^-_2\rangle) R^+, \\
(|E^-_{\xi}\rangle, |E^+_\xi\rangle) &= (|E^-_1\rangle, |E^+_3\rangle) R^-.
\end{align*}
\]

Therefore, we get the following interrelation between the two orthonormal bases describing the NEW and OLD optimal IVs:

\[
\text{NEW} \xrightarrow{\text{SWAP}} R \xrightarrow{\text{SWAP}} \text{OLD}
\]

Hence, the equivalence follows.

6.3 Proofs for Sect. 4

6.3.1 Getting an optimal unitary along with an initial state when Eve measures in the computational basis

First, we find the optimal IVs and the optimal PIJSs as Eve measures in the computational basis.

Her optimal IVs (3) can then be expressed as follows:

\[
\begin{align*}
|\xi^+_y\rangle^C &= |0\rangle_{E_1} |\Omega_{uv}\rangle_{E_2}, \\
|\xi^-_y\rangle^C &= (1/2) |E_1^x \otimes E_2^x\rangle |\xi^+_y\rangle^C, \\
|\zeta^+_y\rangle^C &= |1\rangle_{E_1} |\Omega_{uv}\rangle_{E_2}, \\
|\zeta^-_y\rangle^C &= (1/2) |E_1^x \otimes E_2^x\rangle |\zeta^+_y\rangle^C.
\end{align*}
\]

Here the state \(|\Omega_{uv}\rangle\) is as defined in Eq. (21).

Therefore, the optimal PIJSs in the \(xy\) basis can be expressed as follows

\[
\begin{align*}
|X^*\rangle^C &= |\Phi_{xy}\rangle_{AE_1} |\Omega_{uv}\rangle_{E_2}, \\
|Y^*\rangle^C &= |\Psi_{xy}\rangle_{AE_1} \otimes E_2^x |\Omega_{uv}\rangle_{E_2},
\end{align*}
\]

where

\[
\begin{align*}
|\Phi_{xy}\rangle_{AE_1} &= \sqrt{1-D_{xy}} |0\rangle_{AE_1} + \sqrt{D_{xy}} |1\rangle_{AE_1}, \\
|\Psi_{xy}\rangle_{AE_1} &= \sqrt{1-D_{xy}} |0\rangle_{AE_1} + \sqrt{D_{xy}} |1\rangle_{AE_1}.
\end{align*}
\]

To get an optimal unitary, we need to rewrite the post-interaction joint states in matrix-vector form. First, note that the entangled states from the subsystem AE_1 can be expressed in matrix-vector form as follows

\[
\begin{align*}
|\Phi_{xy}\rangle_{AE_1} &= W^A_{x} E_1 |\Delta_{xy}\rangle_{E_1}, \\
|\Psi_{xy}\rangle_{AE_1} &= W^A_{y} E_1 |\Delta_{xy}\rangle_{E_1},
\end{align*}
\]

with the \(4 \times 2\) matrices

\[
\begin{align*}
W^A_{x} &= |0\rangle_{AE_1} |0\rangle_{E_1} + |1\rangle_{AE_1} |1\rangle_{E_1}, \\
W^A_{y} &= |0\rangle_{AE_1} |0\rangle_{E_1} + |1\rangle_{AE_1} |1\rangle_{E_1}.
\end{align*}
\]

Therefore, the optimal PIJSs in the \(xy\) basis can be expressed in matrix-vector form as follows:

\[
\begin{align*}
|X^*\rangle^C &= |U_{xy} A E_1 |\Delta_{xy}\rangle_{E_1} |\Omega_{uv}\rangle_{E_2}, \\
|Y^*\rangle^C &= |U_{xy} A E_1 |\Delta_{xy}\rangle_{E_1} |\Omega_{uv}\rangle_{E_2},
\end{align*}
\]

with the \(8 \times 4\) matrices

\[
\begin{align*}
U^A_{xy} &= W^A_{x} E_1 \otimes 1^2_{E_2}, \\
U^A_{xy} &= W^A_{y} E_1 \otimes 1^2_{E_2}.
\end{align*}
\]

Then, for an initial state

\[
|\Delta_{\Omega}\rangle_E := |\Delta_{xy}\rangle_{E_1} |\Omega_{uv}\rangle_{E_2},
\]

\[
\text{SWAP}
\]
an optimal unitary can be given as

\[ U_{AE}^{\star} = U_x^{AE}(0)_{A} + U_y^{AE}(1)_{A} \]

\[ = W_x^{AE}(0)_{A} \otimes 1_2^{E_2} + W_y^{AE}(1)_{A} \otimes \sigma_x^{E_2} \]

\[ = (|00\rangle_{AE}, |00\rangle + |11\rangle)_{AE}(01)_{A} \otimes 1_2^{E_2} \]

\[ + (|10\rangle_{AE}, |10\rangle + |01\rangle)_{AE}(11)_{A} \otimes \sigma_x^{E_2}. \]

6.3.2 Factorization of an optimal unitary

The optimal unitary in Eq. (16) can be factored in the following way

\[
U_{\psi_0} = \sum_{a=0}^{1} \sum_{i=0}^{3} |S_a\rangle \langle a_A| \psi_i |E\rangle \\
= \sum_{a=0}^{1} \sum_{i=0}^{3} |S_a\rangle \langle a_A| \langle i|E|i\rangle \langle \psi_i |E\rangle \\
= \sum_{a=0}^{1} \sum_{i=0}^{3} |S_a\rangle \langle a_A| \langle i|E|i\rangle \sum_{i=0}^{3} 1_2 \otimes |i\rangle E \langle \psi_i |. 
\]

6.3.3 Various optimal unitaries for a fixed initial state

Here we explain how to find alternate optimal unitaries for a fixed initial state \(|\psi_0\rangle\). We completely characterize the two-level arbitration.

**Theorem 2** For a given initial state \(|\psi_0\rangle\), let an optimal unitary be known as \(U_{\psi_0}\). For the same initial state, a new optimal unitary \(U_{\psi_0}^{\prime}\) can be found in one of the following ways.

1. A change in the auxiliary states spanning the orthogonal complement of the initial state \(|\psi_0\rangle\), such that

\[ U_{\psi_0}^{\prime} = U_{\psi_0}(1_2 \otimes \Gamma_{\psi_0}^{\perp}). \]

The local unitary \(\Gamma_{\psi_0}^{\perp} = \left[ \begin{array}{c} 1 \\ \Lambda_{0}^{\perp} \end{array} \right] \) makes an alternate choice \(W_{\psi_0}^{\prime}\) for \(W_{\psi_0}\):

\[ W_{\psi_0}^{\prime} = W_{\psi_0} \Gamma_{\psi_0}^{\perp} = \left[ \begin{array}{c} |\psi_0\rangle \\ |\psi_1\rangle^{\prime} \\ |\psi_2\rangle^{\prime} \\ |\psi_3\rangle^{\prime} \end{array} \right]. \]

For a suitable choice of \(\Lambda_{0}^{\perp}\) as a three-dimensional unitary, \(\Gamma_{\psi_0}^{\perp}\) transforms the auxiliary states \(|\psi_1\rangle_{1,2,3}\) to the new ones \(|\psi_1\rangle_{1,2,3}^{\prime}\), while leaving \(|\psi_0\rangle\) intact.

2. Changing the auxiliary states spanning the orthogonal complement of the post-interaction joint states \(|X^{\perp}\rangle, |Y^{\perp}\rangle\), such that

\[ U_{\psi_0}^{\prime} = W_{XY}^{\prime} W_{\psi_0} = W_{XY} \Gamma_{X^{\perp}Y^{\perp}} W_{\psi_0}. \]

The global unitary

\[ \Gamma_{X^{\perp}Y^{\perp}} = diag (\Gamma_{X^{\perp}}, \Gamma_{Y^{\perp}}) \]

transforms \(U_{XY}\) to a new one \(U_{XY}^{\prime} = U_{XY} \Gamma_{X^{\perp}Y^{\perp}}\) having the following matrix representation

\[
\begin{bmatrix}
|X^{\perp}\rangle |X^{\perp}_1\rangle |X^{\perp}_2\rangle |X^{\perp}_3\rangle |Y^{\perp}\rangle |Y^{\perp}_1\rangle |Y^{\perp}_2\rangle |Y^{\perp}_3\rangle
\end{bmatrix},
\]

by changing the auxiliary states \(|X_i\rangle, |Y_i\rangle\) for \(i = 1, 2, 3\) while leaving the optimal PIJSs \(|X^{\perp}\rangle, |Y^{\perp}\rangle\) intact.

3. due to a change in both of the above auxiliary states.

Note that, the first rule doesn’t require the factorization. Given an optimal unitary, an alternate solution can be found by post-multiplying the former by \(1_2 \otimes \Gamma_{\psi_0}^{\perp}\).

6.3.4 Optimal unitary for a different initial state

A global unitary evolves the joint system as follows:

\[ U_{\psi_0}^{\star} (|a\rangle_A |e\rangle_E) = |S_a\rangle_{AE}. \]

For \(a \in \{x, y\}\), the PIJSs \(S_a \in \{X, Y\}\) get fixed by fixing the measurement directions \(M\). However, the same PIJS \(|S_a\rangle_{AE}\) can be produced for a different IS and a different unitary:

\[ U_{\psi_0}^{\star} (|a\rangle_A |f\rangle_E) = |S_a\rangle_{AE}. \]

Given an unitary \(U_{\psi_0}^{\star}\), one can find an unitary \(U_{\psi_0}^{\star}\) by knowing the local unitary that transforms \(|e\rangle \rightarrow |f\rangle\).

**Theorem 3** If an unitary \(U_e\) is known for some initial state \(|e\rangle\), one can find an unitary \(U_{\psi_0}^{\star}\) for some other initial state \(|f\rangle\), just by knowing the local unitary \(T_{ef}\) that transforms \(|e\rangle \rightarrow |f\rangle\).

\[ U_{\psi_0}^{\star} = U_e \left( 1_2^A \otimes T_{ef}^{E_1} \right). \]

**Proof** Since \(|f\rangle = T_{ef}|e\rangle\), we get

\[ U_{\psi_0}^{\star} (|a\rangle_A |f\rangle_E) = |S_a\rangle_{AE} = U_e (|a\rangle_A |e\rangle_E) \]

\[ = U_e (|a\rangle_A \otimes T_{ef}^{E_1} |f\rangle_E) \]

\[ = U_e \left( 1_2^A \otimes T_{ef}^{E_1} \right) |a\rangle_A |f\rangle_E. \]

And the result follows.

\[ \square \]

For instance, consider the task to find an optimal unitary for the initial state \(|\Delta\rangle_E = |\Delta_{xy}\rangle_{E_1} |\Delta_{uv}\rangle_{E_2}\), which is a small tweak \(T_{ef} = 1_2 \otimes \mathbb{H} : |\Delta\rangle_E \rightarrow |\Delta\rangle_E\) of the earlier initial state \(|\Delta\rangle_E\) (19). Then, the global unitary is transformed as follows

\[ \mathcal{U}_{\Delta \Delta} = \mathcal{U}_{\Delta \Delta} \left( 1_2^A \otimes 1_2^{E_1} \otimes \mathbb{H}^{E_2} \right). \]
The corresponding matrix is a tweak of the one in Eq. (22) while each inner sub-matrix $I_2, \sigma_x$ gets post-multiplied by the Hadamard transformation $H$.

A more involved example would be finding an optimal unitary for the initial state $|\phi^+_xy\rangle := \frac{|00\rangle + |11\rangle}{\sqrt{2}}$. Since this maximally entangled state can be obtained by applying an unitary $T = c\sigma_y (H \otimes I_2)$ (a Hadamard on the first qubit followed by a CNOT operation) on the state $|00\rangle$, an optimal unitary for the former state ($U^C_{\phi^+}$) is obtained from an optimal unitary for the latter state ($U^C_{\phi^0}$) by applying the unitary transform

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ \sigma_x & -\sigma_x \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ \sigma_x & -\sigma_x \end{bmatrix}.$$

### 6.3.5 Eve’s optimal unitary versus measurement setup

Let us understand the change in the optimal unitary as Eve’s measurement setup changes from the computational basis to a different one. Note that, a new measurement basis $\{E_{\lambda} \}$ is a unitary transformation $M_{xy} := \{|E_0\}, |E_1\rangle, |E_2\rangle, |E_3\rangle\}$ of the computational basis $\{|\lambda\rangle\}$, i.e., $|E_{\lambda}\rangle \equiv M_{xy}|\lambda\rangle$. We have used $M$ and $M_{xy}$ interchangeably for Eve’s measurement.

**Theorem 4** For an arbitrary measurement $\{M \equiv M_{xy}\}$ with Eve, the following retrospective effects could be observed on the optimal IVs, the optimal PIJSs, and the optimal global unitary.

1. **The optimal IVs of Eve are changed as follows:**

$$|IV^x_{xy}\rangle^M = M_{xy}|IV^x_{xy}\rangle^C. \ (28)$$

2. **The optimal PIJSs are transformed as follows:**

$$|S_{a}\rangle^M = (I_2 \otimes M_{xy})|S_{a}\rangle^C, \quad a = x, y. \ (29)$$

3. **The global unitary gets tweaked as follows:**

$$U^M = (I_2 \otimes M_{xy}) U^C. \ (30)$$

**Proof** The first two claims are straight-forward, while the last claim is proved below.

$$U^M |0\rangle_A |\psi_0\rangle_E = |X\rangle^M = (I_2 \otimes M_{xy}) |X\rangle^C = (I_2 \otimes M_{xy}) U^C |0\rangle_A |\psi_0\rangle_E.$$

And similarly for other possible states. $\square$

Note that, a permutation of the measurement basis (e.g., $M_{xy} = \{|00\rangle, |11\rangle, |10\rangle, |01\rangle\}$) or a phase shift (e.g., $|E_{\lambda}\rangle \rightarrow -|E_{\lambda}\rangle$) doesn’t change the measurement statistics, despite a small tweak $(I_2 \otimes M_{xy})$ on the optimal unitary. Thus, we consider the overall effect due to such changes as equivalent. An effective change in the measurement basis corresponds to those unitary transformations on the four-dimensional computational basis, which contains at least a row having more than one non-zero entries.

### 6.4 Technical details for Sect. 2

#### 6.4.1 Fidelity of Eve’s state discrimination

An optimal attack on the p&m scheme leaves Eve with an optimal state-discriminate problem [12]. For a specific encoding basis, the four different post-interaction states of Eve’s ancilla can be grouped into two mutually orthogonal sets: one with the two fidelity states, and the other with the two disturbed states. Since Eve can discriminate these orthogonal sets (whether disturbed or not), all she is left with is to distinguish the two states in a set, e.g., distinguishing $|\xi_a\rangle$ from $|\xi_b\rangle$, or, distinguishing $|\zeta_a\rangle$ from $|\zeta_b\rangle$. Following the optimal strategy, Eve can distinguish the two such parity states (fidelity or disturbed) with probability [18]

$$F^E_\beta = \frac{1}{2} + \frac{1}{2} \sqrt{1 - |\langle \xi_a^\beta | \xi_b^\beta \rangle|^2} = \frac{1}{2} + \frac{1}{2} \sqrt{1 - (1 - 2D^2)}$$

Now, some results used in practical eavesdropping are elaborated here for better understanding.

#### 6.4.2 Secret-key rate

The secrecy capacity $C_s$ of the quantum channel between Alice and Bob is defined [13] as the maximum rate at which Alice can reliably send information to Bob leaving Eve’s information on that data arbitrarily small. A necessary and sufficient condition for a positive secret-key rate is not known, but a lower bound is known [13]. For a more general scenario, considering the knowledge gain of Eve over Bob’s data ($I_{EB}$) due to public discussion over the supplementary classical channel, one can lower bound the secrecy capacity [19] by the following formula

$$C_s \geq \max\{I_{AB} - I_{AE}, I_{AB} - I_{EB}\}.$$

Thus the legitimate parties should consider the channel unsafe and abort the transmission whenever

$$I_{AB} \leq \min\{I_{AE}, I_{EB}\}.$$

On the other hand, the legitimate parties can establish a secret key following some one-way CPP, iff $I_{AB} > I_{AE}$ or $I_{AB} > I_{EB}$. For an optimal symmetric attack, $I_{AE} = I_{EB}$. Therefore, Alice and Bob lives in the secure zone whenever $I_{AB} > I_{AE}$. The difference $I_{AB} - I_{AE}$ captures the secret-key rate.

#### 6.4.3 Optimal attack and contraction in Bloch vectors

The state $|a\rangle^\beta$ of a two-level quantum system (qubit) corresponds to a Bloch vector $a^\beta$ on the surface of the
Poincaré sphere. Alices’ density operator \( \rho_A = |a\rangle^\beta \langle a| \) is a convex combination \( \frac{1}{2} (1 + a_\beta \cdot \sigma) \) of the Pauli operators. For the BB84 protocol, the states in the \( Z \) and the \( X \) bases correspond to the Bloch vectors \((0,0,\pm 1) \) and \((\pm 1,0,0) \), respectively. Therefore, Alice sends the density operators \( \frac{1}{2} (1 \pm \sigma_s) \) (for, \( s \in \{z, x\} \)) to Bob. But, due to eavesdropping, Bob receives the density

\[
\rho_B = F|a\rangle^\beta \langle a| + D|\bar{a}\rangle^\beta \langle \bar{a}| \\
= F \cdot \frac{1}{2} (1 + a_\beta \cdot \sigma) + D \cdot \frac{1}{2} (1 - a_\beta \cdot \sigma) \\
= \frac{1}{2} (1 + (F - D) a_\beta \cdot \sigma)
\]

While Alice sends the density \( \frac{1}{2} (1 + a \cdot \sigma) \), Bob receives \( \frac{1}{2} (1 + \eta_\sigma a \cdot \sigma) \) with \( \eta_\sigma = 1 - 2D \). To be specific, the density operators \( \frac{1}{2} (1 \pm \sigma_s) \) (for, \( s \in \{z, x\} \)) from Alice get perturbed to \( \frac{1}{2} (1 \pm \eta_\sigma \sigma_s) \) when it reaches Bob. Thus, eavesdropping shrinks the Bloch vectors by a factor of \( \eta_\sigma = 1 - 2D \).

6.4.4 Optimal state-discrimination versus Bell-violation

An optimal state-discrimination-based attack on a \( pk\&m \) scheme has some intriguing connection with Bell-violation in an equivalent \( eb \) scheme and is discussed here.

The \( pk\&m \) scheme has its equivalent \( eb \) counterpart where Alice prepares a maximally entangled state \( |\phi\rangle = \frac{1}{\sqrt{2}} \left( |00\rangle + |11\rangle \right) \) and send one of the particles to Bob. Both the parties measure the observables \( \sigma_z, \sigma_x \), chosen randomly.

The security of the \( eb \) scheme is linked to the tests of quantum nonlocality [5]. Presence of non-locality is a certificate for OW-CPP. The degree of non-locality depends on the estimated value of the CHSH polynomial for which the legitimate parties sacrifice a subset of their particles. Alice measures one of the observables \( \sigma_z, \sigma_x \) chosen randomly, while Bob measures one of the observables \( \sigma_z', \sigma_x' \), chosen randomly. The binary measurement outcomes \( a_i, b_j \in \{-1, +1\} \) are used to estimate the CHSH correlation-coefficient which in turn is the expected value of the product of the outcomes.

\[
S := E(a_1, b_1) + E(a_1, b_2) + E(a_2, b_1) - E(a_2, b_2).
\]

Due to some channel error \( D \), each of the correlations \( E(a_i, b_j | D) \) get reduced from its error-free counterpart \( E(a_i, b_j) \) by a factor of \( 1 - 2D \):

\[
E(a_i, b_j | D) = F \cdot E(a_i, b_j) - D \cdot E(a_i, b_j) \\
= (1 - 2D) \cdot E(a_i, b_j).
\]

Consequently, \( S_D = (1 - 2D) S_0 \).

The CHSH inequality forbids the correlation coefficient \( S \) to exceed 2 for local operations and classical communication. However, for an error-free quantum channel, this inequality is violated and the correlation amount reaches the maximum of \( 2 \sqrt{2} \). Then, in a quantum channel with error \( D \), the maximum amount of violation becomes \( S_D = (1 - 2D) 2 \sqrt{2} \). In order to maintain quantum non-locality, this reduced sum must exceed 2, which happens precisely for \( D < D^* \) as in Eq. (7).

7 Conclusion and Final remarks

We have characterized the optimal attacks on the BB84 protocol exhaustively, where an attacker entangles a two-qubit probe per transmitted signal. We have considered the generalized asymmetric error rates across the two MUBs in order to uncover all possible choices for an attacker, while a symmetric attack automatically becomes a special case. A necessary and sufficient condition is derived here to testify the optimality of an interaction performed by an eavesdropper. As it unveils, an optimal attack corresponds to a specific configuration of the attacker’s post-interaction states: that the overlap between the two disturbed states is the same as the overlap between the two undisturbed states and is equal to the difference between the fidelity and the disturbance at the receiving end. Interestingly enough, the optimal overlap is the same as the reduction in Bell violation in the equivalent entanglement-based scheme. We have shown explicitly that the optimal states of the joint system can also be obtained by an optimal phase-covariant cloning mechanism, and vice versa.

For practical purposes, all an eavesdropper requires is the optimal unitary to evolve the joint system and the corresponding measurement that she must perform to glean the maximum information. We have developed the methods to characterize the optimal unitaries and demonstrated via examples. Our method could figure out the simplest one out of the infinite family of optimal unitaries in a most natural fashion. As an optimal unitary is parameterized by the error-rate, an attacker may first fix the QBER she wishes to introduce and choose an optimal unitary (not unique) for a specific choice of her measurement and the initial state. An attacker would like to choose such unitaries which, if feasible, is easier to design than its siblings. The techniques developed here to identify the optimal unitary evolutions are generic and can also be employed with other QKD protocols, e.g., in [20], where the optimal states with an eavesdropper is known. We also address the quality of the classical post-processing by finding the rate at which the final key could be produced.

Acknowledgements The authors acknowledge Dr. Guruprasad Kar for his technical suggestions.

Author contributions

GP formulated the problem of characterizing the optimal unitary evolutions and closely monitored the
progress. AA worked out the NSC and the optimal unitary evolution.

Data Availability Statement This manuscript has no associated data or the data will not be deposited. [Authors’ comment: There are no external or experimental data associated with this manuscript.]

References

1. B.-G. Englert, Eur. Phys. J. D 67, 238 (2013). https://doi.org/10.1140/epjd/e2013-40486-5
2. R. Alléaume, C. Branciard, J. Bouda, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, N. Lütkenhaus, C. Monyk, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, A. Zeilinger, Theor. Comput. Sci. 560, 62–81 (2014). https://doi.org/10.1016/j.tcs.2014.09.018
3. P. Zoller, Th. Beth, D. Binosi, R. Blatt, H. Briegel, D. Bruss, T. Calarco, J.I. Cirac, D. Deutsch, J. Eisert, A. Ekert, C. Fabre, N. Gisin, P. Grangier, M. Grassl, S. Haroche, A. Imamoglu, A. Karlson, J. Kempe, L. Kouwenhoven, S. Kröll, G. Leuchs, M. Lewenstein, D. Loss, N. Lütkenhaus, S. Massar, J.E. Mooij, M.B. Plenio, E. Polzik, S. Popescu, G. Rempe, A. Sergienko, D. Suter, J. Twamley, G. Wendin, R. Werner, A. Winter, J. Wrachtrup, A. Zeilinger, Eur. Phys. J. D 36, 203–228 (2005). https://doi.org/10.1140/epjd/e2005-00251-1
4. C.H. Bennett, G. Brassard, in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing vol. 1, pp. 175–179 (1984)
5. C.A. Fuchs, N. Gisin, R.B. Griffiths, C.S. Niu, A. Peres, Phys. Rev. A 56, 1163 (1997). https://doi.org/10.1103/PhysRevA.56.1163
6. A. Acharyya, G. Paul, Phys. Rev. A 95, 022326 (2017). https://doi.org/10.1103/PhysRevA.95.022326
7. D. Bruß, M. Cinchetti, G. Mauro D’Ariano, C. Macchiavello, Phys. Rev. A 62, 012302 (2000). https://doi.org/10.1103/PhysRevA.62.012302
8. J.F. Clauser, M.A. Home, A. Shimony, R.A. Holt, Phys. Rev. Lett. 23, 880 (1969). https://doi.org/10.1103/PhysRevLett.23.880
9. B.S. Cirel’son, Lett. Math. Phys. 4, 93 (1980). https://doi.org/10.1007/BF00417500
10. C.A. Fuchs, in Proceedings of the Fourth Workshop on Physics and Computation, pp. 229–259 (1996). arXiv:quant-ph/9611010
11. M.A. Nielsen, I.L. Chuang, Quantum Computation and Quantum Information (Cambridge University Press, Cambridge, 2002)
12. D.S. Barnett, S. Croke, Adv. Opt. Photon. 1, 238–278 (2009). https://doi.org/10.1364/AOP.1.000238
13. I. Csiszár, J. Körner, IEEE Trans. Inf. Theory 24(3), 339–348 (1978). https://doi.org/10.1109/TIT.1978.1055892
14. I.M. Herbauts, S. Bettelli, H. Hübel, M. Peev, Eur. Phys. J. D 46, 395–406 (2008). https://doi.org/10.1140/epjd/e2008-00002-x
15. C.H. Bennett, G. Brassard, C. Crepeau, U.M. Maurer, IEEE Trans. Inf. Theory 41, 1915–1923 (1995). https://doi.org/10.1109/18.476316
16. N. Lütkenhaus, Phys. Rev. A 54, 97–111 (1996). https://doi.org/10.1103/PhysRevA.54.97
17. N. Lütkenhaus, Phys. Rev. A 59, 3301–3319 (1999). https://doi.org/10.1103/PhysRevA.59.3301
18. C.W. Helstrom, Quantum Detection and Estimation Theory (Academic Press, New York, 1976), pp. 80–84
19. A.K. Ekert, B. Huttner, G.M. Palma, A. Peres, Phys. Rev. A 50, 1047 (1994). https://doi.org/10.1103/PhysRevA.50.1047
20. D. Bruß, Phys. Rev. Lett. 81, 3018–3021 (1998). https://doi.org/10.1103/PhysRevLett.81.3018