Indistinguishable encoding for bidirectional quantum key distribution: Theory to experiment

JESNI SHAMSUL SHAARI¹,² and SURYADI SOEKARDJO¹

¹ Department of Physics, International Islamic University Malaysia (IIUM), Jalan Sultan Ahmad Shah, Bandar Indera Mahkota - 25200 Kuantan, Pahang, Malaysia
² Institute of Mathematical Research (INSPEM), University Putra Malaysia - 43400 UPM Serdang, Selangor, Malaysia

received 10 June 2017; accepted in final form 3 February 2018
published online 26 February 2018

PACS 03.67.Dd – Quantum cryptography and communication security
PACS 03.67.Hk – Quantum communication

Abstract – We present a bidirectional quantum key distribution protocol with minimal encoding operations derived from the use of only two “nonorthogonal” unitary transformations selected from two mutually unbiased unitary bases. Differently from many bidirectional protocols, these transformations are indistinguishable in principle for a single use. Along with its decoding procedure, it is unique compared to its “orthogonal encoding” predecessors. Given the nature of such protocols where key rates are usually dependent on two different types of error rates, we define a more relevant notion of security threshold for such protocols to allow for proper comparisons to be made. The current protocol outperforms its predecessor in terms of security as the amount of information an eavesdropper can glean is limited by the indistinguishability of the transformations. We further propose adaptations for a practical scenario and report on a proof of concept experimental scheme based on polarised photons from an attenuated pulsed laser for qubits, demonstrating the feasibility of such a protocol.

Copyright © EPLA, 2018

Introduction. – Quantum cryptography, or more specifically quantum key distribution (QKD) provides for a solution to the courier problem of distributing secret keys between two parties to be utilised for a one-time pad cryptographic protocol. Arguably a first rather direct practical application of quantum physics, QKD’s security is guaranteed by physical laws. It saw its debut in the famous BB84 [1] protocol, where one party, commonly referred to as Alice would send a photon prepared in one of two mutually unbiased bases (MUBs) over a quantum channel to another, Bob, for his measurements to determine the state sent. This is a straightforward scenario of “prepare and measure”, i.e., Alice prepares a quantum state while Bob measures. An adversary, Eve, would not be able to determine the states sent without inducing any errors. The amount of information Eve may have gleaned though can be inferred from the error between Alice and Bob and, below a prescribed threshold, a secret key can nevertheless be distilled by the legitimate parties. This is done by first correcting any errors between them using error corrections (EC) codes and Eve’s knowledge of the key can be reduced to arbitrarily low levels using privacy amplification (PA) procedures (we refer to [2,3] for excellent reviews on quantum cryptography).

While variants of the first QKD protocol has seen much development, a departure from the prepare and measure scenario was imagined in a QKD protocol making bidirectional use of the quantum channel between Alice and Bob, sometimes referred to as two-way QKD schemes (we shall use the terms bidirectional and two-way interchangeably). It was first reported in 2003 in [4] as the “ping-pong” protocol. The protocol later saw its evolution into various forms, improving on security and some on practicality [5–8]. The essential feature of such protocols is the encoding of information by Alice, who applies unitary transformations on qubits received from (and prepared by) Bob before resubmitting them to him. Bob would later measure them in the same basis he prepared them and can distinguish between the transformations used as they would not affect the qubits’ bases. Information bits for secret key generation is derived from the different transformations; in clear contrast to BB84-like schemes where bits for the same purpose is simply based on the states themselves. Hence, while prepare and measure schemes

60001-p1
require an eavesdropper to estimate the state of a traveling qubit between the legitimate parties for successful eavesdropping, two-way protocols challenge eavesdroppers to estimate the evolution of an unknown state as it travels to and fro between Alice and Bob. The realised practical implementations include those reported in [9] with entangled photons, [10,11] with weak (attenuated) pulsed laser as photon sources and even using telecommunication wavelengths in [12] to cite a few. An excellent review for the two-way protocol akin to that of [6–8] can be found in [13].

However, in all these, the unitary transformations had mostly been limited to the identity operator \( \mathbb{I} \) and \( iY \) (\( Y \) is one of the Pauli matrices). In principle, the Pauli matrices along with the identity operator can in fact be distinguished perfectly, even for a single use [14]. Reference [15] referred to these transformations as a set of orthogonal unitaries. While this does not hinder an eavesdropper to ascertain without ambiguity the transformations executed by Alice, it does result in the former introducing errors should measurements be made on the received states instead of encoding. To this effect the legitimate parties would randomly interlude their encoding/decoding runs with prepare and measure runs where Bob’s prepared states are, with a certain probability, measured by Alice, akin to a BB84 scenario and is referred to as the control mode (CM). The encoding/decoding runs are denoted as the encoding mode (EM). Hence the security of the protocol mainly reduces to Eve’s inability to determine conclusively the traveling qubits’ states randomly prepared by Bob in one of two MUBs. The “encryption” process is still delegated to the encoding of bits in qubit states.

It is clear that prepare and measure schemes deliver by capitalising on “imperfect state estimations”. One could expect that, in an analogous way, these two-way schemes would rely on “imperfect estimation of unitary transformation” as part of its working engine. This, however, is not the case. The idea of Alice actually using transformations which are in principle indistinguishable for a single use for encoding purpose was only first noted in [16]. The transformations would be selected randomly from two mutually unbiased bases of orthogonal qubit unitaries (a term used in [15]). A study, more focused on QKD for such two-way protocols using qubits selected from two MUBs with a number of four of such “nonorthogonal unitaries” [17] for encoding purposes was reported in [18]. This exercise would thus allow Alice’s encoding to be seen as an encryption as well.

A proper formalization for the structure of such unitaries was studied as mutually unbiased unitary bases (MUUBs) in [19]. Limiting our consideration to operators on a 2-dimensional Hilbert space, two orthogonal bases, \( B_0 \) and \( B_1 \), for some \( n \)-dimensional subspace of \( 2 \times 2 \) matrices are defined as sets of MUUBs when

\[
\left| \text{Tr}(B_{ij}^\dagger B_{ij}^\prime) \right|^2 = C, \quad \forall B_{ij}^0 \in B_0, B_{ij}^1 \in B_1,
\]

for \( i, j = 1, \ldots, n \) and some constant \( C \neq 0 \). \( C \) equals 1 and 2 for \( n = 4 \) and \( n = 2 \), respectively [19]. It was also reported then that the fidelity of discriminating transformations selected randomly from such a complete set of MUUBs for the \( n = 4 \) subspace, is equal to that of estimating a completely unknown unitary transformation in \( SU(2) \).

In this work, we describe and analyse a bidirectional QKD protocol which uses a minimal number of indistinguishable unitary transformations for encodings where each encoding is selected from two different MUUBs. Given the use of only 2 unitary operators, differently from [18], the very decoding procedure by Bob would be radically different from previously reported two-way protocols. Beginning with an ideal protocol, we brief on its merits in a depolarising channel and provide a security analysis against an eavesdropper committed to a collective attack. While the protocol’s decoding procedure would result in only a quarter of the qubits sent to be used as a raw key, its security threshold demonstrates its clear advantage over its predecessor, the protocol of [8]. We shall see in the following sections how the protocol allows for secret key extraction for larger regions of errors in the communication channels. We further report on an experimental proof of concept for the protocol revealing its feasibility.

**Bidirectional QKD with two mutually unbiased unitaries.** – The protocol is based on the same bidirectional use of the quantum channel where Bob sends to Alice a qubit prepared in a basis of his choice. Alice would then encode using one of two unitary transformations before submitting to Bob for his measurements. Let us consider unitary transformations described as rotations around the \( y \) axis of the Poincaré sphere given by

\[
R_y(\zeta) = \cos(\zeta/2) \mathbb{I} - i \sin(\zeta/2) Y.
\]

We choose only two angles for \( \zeta \) in this work, namely, \( \zeta = 0 \) (corresponding to a passive operation) and \( \zeta = -\pi/2 \) which corresponds to flipping states between the mutually unbiased orthonormal \( X \) and \( Z \) bases. The transformations are in fact elements taken from either of two sets of MUUB [18], \{\( \mathbb{I}, Y \)\} and \{\( R_y(\pm\pi/2) \)\} with respect to one another,

\[
\left| \text{Tr}(R_y(\pm\pi/2)) \right|^2 = \left| \text{Tr}(Y R_y(\pm\pi/2)) \right|^2 = 2.
\]

The indistinguishability of these two transformations can be seen from the indistinguishability of an input state from its output. Given an arbitrary state \( |\psi\rangle = \cos(\theta/2) |0\rangle + \exp(i\phi) \sin(\theta/2) |1\rangle \), we can quickly observe that the overlap

\[
|\langle \psi | R_y(-\pi/2) |\psi\rangle |^2 = [1 + \sin^2(\theta) \sin^2(\phi)]/2
\]

has a minimum value of 1/2. This minimum value is in fact the square of the inner product for two states coming from two MUBs. Any state lying on the equator of the Poincaré sphere would hence provide for minimal overlap; thus we let Bob prepare a state randomly selected from the basis defined by \{\( |0\rangle = \cos(\theta/2) |0\rangle + \sin(\theta/2) |1\rangle \),\( |1\rangle = \cos(\theta/2) |1\rangle - \sin(\theta/2) |0\rangle \)\}.
\[ |1^\theta \rangle = \sin(\theta/2)|0\rangle - \cos(\theta/2)|1\rangle \] to be submitted to Alice for her encoding (transformation).

Once Alice has executed her transformation, the resulting state would be forwarded to Bob for which he shall commit to a measurement in either the same basis he prepared or one rotated by \( \pi/2 \). Writing Bob’s prepared and resulting measured state as \(|\psi_f\rangle\) and \(|\psi_b\rangle\), respectively, with \( i, j \in \{0, -\pi/2\} \) and \( i \neq j \), Bob can only conclusively infer Alice’s encoding to not be \( R_y(i) \) (hence \( R_y(j) \)) provided \( \langle \psi_b | R_y(i) | \psi_f \rangle = 0 \). As an example, if Bob prepares the computational state \(|0\rangle\) and his measurement resulted in \(|1\rangle\), then he concludes that Alice could not have used the passive identity operation, and thus infers the other. Or, if a measurement had been made in the \( X \) basis instead and yields a state orthogonal to \( R_y(-\pi/2)|0\rangle\), then he concludes Alice did not use \( R_y(-\pi/2) \), but \( I \) instead. This decoding procedure is inspired very much by the SARG protocol [20]. Discounting all inconclusive results and assigning the logical value “0” to \( I \) and “1” to \( R_y(-\pi/2) \), we can see how Alice and Bob can share a common string of bits. A typical run for the protocol can be summarised in the following steps:

1) Bob randomly selects a value for the angle \( \theta \) and defines a basis, \( \{|0^\theta\rangle, |1^\theta\rangle\}\).
2) Bob submits a state randomly selected from the defined basis to Alice (forward path).
3) Alice would randomly choose either \( R_y(0) \) or \( R_y(-\pi/2) \) to operate on Bob’s qubit and returns it to Bob (backward path).
4) Bob would randomly measure the received qubit in either the same basis he prepared it in or one rotated by \( \pi/2 \) and discard runs for which his measurement result does not allow him to infer Alice’s encoding conclusively.

Bob’s announcement of the discarded runs over an authenticated channel should allow for Alice and him to share a raw key. This shared string must obviously be subjected to EC to correct any errors and PA to ensure its secrecy. The rate for the latter would be ascertained in the follow-up section. We should note that while Bob’s decoding is successful for only \( 1/4 \) of the total qubits used, this should not dispel the protocol’s advantage in terms of its security threshold where it is able to generate secret keys for larger domains of error rates in the channels, compared to its predecessor as we shall see shortly.

**Security analysis.** — Taking the conventional approach to security analysis of bidirectional QKD systems, Eve’s strategy is to attack the qubits en route twice, once in the forward path (from Bob to Alice) and once in the backward path (from Alice back to Bob). This is well known to be due to the uninformative, completely mixed state of Bob’s qubit, \( \rho_B \), in the individual paths. We shall analyze the protocol based on the methods of [21,22]. Each of Bob’s traveling state in the forward path would independently be made to interact with Eve’s ancilla. Eve is then allowed to have access to the entire state in the backward path (after encoding) to extract information and no constraint is set on how she may do this. This is ultimately a very pessimistic stand and with the attack being identical for every run, Eve is in fact committed to a collective attack scenario. We do however, reasonably require Eve’s strategy to simulate a depolarising channel like [22]. This means that Bob’s qubit, irrespective of the basis chosen, should experience the same amount of noise, essentially undergoing a symmetric attack [2]. Also, like [22], we shall begin with Bob’s state in one basis only, and then show that the information Eve should gain for any of Bob’s choice of basis is the same.

We begin by writing the interaction between Eve’s ancillae, \(|E\rangle\), and the traveling qubit (in the computational basis for simplicity) in the forward path as:

\[
U|b\rangle|E\rangle = |b\rangle|E_b\rangle + |b^\perp\rangle|E_{b^\perp}\rangle
\]

with \( b \in \{0,1\} \) and \( 0 = 1 \) (1 = 0). Unitarity of the interaction necessitates

\[
\langle E_{b^\perp}|E_b\rangle + \langle E_b|E_{b^\perp}\rangle = 1, \langle E_{b^\perp}|E_{b^\perp}\rangle + \langle E_b|E_b\rangle = 0
\]

and we let \( \langle E_b|E_{b^\perp}\rangle = F \), \( \langle E_{b^\perp}|E_{b^\perp}\rangle = Q \) and \( F + Q = 1 \). It is worth noting that, with proper choices for phases, one can ensure all of Eve’s scalar products are reals and we let \( \langle E_b|E_{b^\perp}\rangle = F \cos x \) and \( \langle E_{b^\perp}|E_{b^\perp}\rangle = Q \cos y \) [2].

Now, the value \( Q \) is really the probability of Bob’s state being projected to one that is orthogonal to which he sent. Admittedly, we have not defined the current protocol to allow for measurements of qubits in the forward path, thus making \( Q \) inaccessible. However, this is easily remedied if we should include some form of CM similar to that of [8]. We shall return to this point later.

The state of the system (Bob’s qubit after Eve’s attack in the forward path) subsequent to Alice’s encoding can be written as

\[
\rho_{BE} = [U_{\rho B} U^\dagger + R_y^E (U_{\rho B} U^\dagger) R_y^{E \dagger}] / 2,
\]

where \( \rho_B = I/2 \otimes |E\rangle\langle E| \) and \( R_y^E = R_y(-\pi/2) \otimes I_E \) with \( I_E \) being the identity on Eve’s Hilbert space. Eve’s access to the state on the backward path provides her with information of the key, \( I_E \), which is given by \( S(\rho_{BE}) = 1 - 1/2 \). \( S(\rho) \) is the von Neuman entropy given by \( -\text{tr} \log_{2} \rho \) for a state \( \rho \). We calculate the entropy through the eigenvalues, \( \lambda_i \), for \( \rho \), with \( S(\rho) = -\sum \lambda_i \log_{2} \lambda_i \).

In ascertaining the eigenvalues of \( \rho_{BE} \), we adopt the method in [22] by calculating the eigenvalues of its Gram matrix representation [23]. \( G^{BE} \) is given as

\[
G^{BE} = \frac{1}{4} \begin{pmatrix}
1 & 0 & 1/\sqrt{2} & \alpha/\sqrt{2} \\
0 & 1 & -\alpha/\sqrt{2} & 1/\sqrt{2} \\
1/\sqrt{2} & -\alpha/\sqrt{2} & 1 & 0 \\
\alpha/\sqrt{2} & 1/\sqrt{2} & 0 & 1
\end{pmatrix}
\]
with \( \alpha = (F \cos x - Q \cos y) \). The eigenvalues for \( G^{BE} \) (which are equal to those of \( \rho^{BE} \) including its multiplicities, each being 2) are then given by
\[
\lambda_{\pm} = (2 \pm \sqrt{2(F \cos x - Q \cos y)^2 + 2})/8. \tag{9}
\]
Eve’s information gain, \( I_E \), can thus be written as
\[
I_E = S(\rho^{BE}) - 1 = h[(2 - a\sqrt{2})/4] \tag{10}
\]
with \( a = \sqrt{(F \cos x - Q \cos y)^2 + 1} \) and \( h(x) = -x \log_2 x - (1 - x) \log_2 (1 - x) \) being the Shannon binary entropic function.

Using the same approach as above, it is not difficult to show that Eve’s information gain is actually the same for any state Bob could send (constrained to those on the equator of the Poincaré sphere) and thus this analysis is valid for the protocol as described above where Bob can send any such states (details are provided in the supplementary material Supplementary material.pdf (SM)). Insisting on the same disturbance for any of the states sent by Bob, the value for \( Q = 1 - F \) would be given by [2] and we can eventually write
\[
1 - 2Q(1 + \cos y) = F \cos x - Q \cos y. \tag{11}
\]
Hence, \( a = \sqrt{1 - 2Q(1 + \cos y)^2 + 1} \). We can immediately observe that Eve’s best strategy to maximise her information would be to maximise \( \cos y \); ensuring \( Q \) be kept minimal. Thus for a fixed \( Q \), let \( \cos y = 1 \) (which then fixes \( x \)) and we have \( a = \sqrt{(1 - 4Q)^2 + 1} \). It is evident that Eve achieves maximum information, approximately 0.6 when \( Q = 0.25 \) and is equal to the von Neumann entropy for a mixture of two states derived from two MUBs.

**Security thresholds.** Unlike its prepare and measure cousins, it is well understood that the secret key rate for two way protocols would depend on 2 parameters of errors, namely the error in the forward path, \( Q \), which informs the legitimate parties of Eve’s gain, thus the rate for PA, and the error in the EM, \( Q_{AB} \) which tells of the cost in bits for error correction purposes. A “security threshold” can only be determined after both \( Q \) and \( Q_{AB} \) are ascertained. Derived from different processes, there is no a priori reason to assume the two errors are related by some straightforward mathematical relationship [13] (even if both channels are depolarising). To date, to the best of our knowledge, security thresholds for two-way protocols are usually drawn based on some noise model linking the two (ref. [13] as a quick example), thus lacking in generality.

The notion of security threshold, commonly understood as a point denoting the value for error in the channel such that beyond it no secure key can be extracted must give way to the idea of curves in a plane defined by \( Q \) and \( Q_{AB} \) separating regions where key extraction is possible and otherwise. We define hence, a security threshold as the area for the region of the said plane where secret key extraction is possible; i.e., where the secret key rate is greater than zero. We take the maximum values for \( Q \) and \( Q_{AB} \) for the total region as where Eve’s information gain is maximum and Alice-Bob’s mutual information is minimal, respectively. Secret key rates can be written as \( 1 - I_E - h(Q_{AB}) \) [24].

In order to have an idea of the protocol’s merit, we compare it to the earlier “orthogonal” protocol of [8], (in some literature referred to as LM05)\(^1\). Within the depolarising channel framework, Eve’s gain for LM05 is given as \( h(1 - 2Q) \) [21,22]. We calculate and compare the secure key rates (per raw key bit) for varying values of both \( Q \) and \( Q_{AB} \), presented as contour plots in fig. 1.

The contour plot of fig. 1(a) represents the current protocol while fig. 1(b) is for LM05. The insets show Eve’s

\(^1\)We consider this as a fair comparison given that the two have essentially identical topologies as well number of states and transformations used.
gain for each protocol, respectively. The figures clearly demonstrate how utilising these nonorthogonal transformations suppresses Eve’s information, quite drastically in fact, as we observe the region (defined by \( Q \) and \( Q_{AB} \)) for extractable secure key is the greatest for the current protocol. A direct numerical integration (using a mathematical software) gives the security thresholds for the current protocol and LM05 as \( \approx 0.037 \) and \( \approx 0.017 \), respectively. The security threshold of the current protocol being roughly double to that of LM05 literally means the former is able to extract secret keys for a larger possible set of error pairs, \( (Q, Q_{AB}) \), compared to LM05. It is not unimaginable that various implementation of the protocols may result in having a variation in the errors. This can be seen as Eve’s varying attack strategies. As an example, an attack which leaves no error in EM for LM05 whilst an error rate of 25% in CM would render LM05 completely insecure. On the other hand, such errors would still allow for a positive key rate to be extracted for the current protocol.

We now return to the issue of the inaccessibility of the value \( Q \). As noted in [15], protocols like LM05 using orthogonal unitary transformation requires a CM. In principle, given the fact that Alice’s encoding in the current protocol cannot be ascertained perfectly by Eve, even for a maximal attack (\( Q = 0.25 \)) the CM is, to a certain extent obsolete. A naive way of putting this would be to say that a key can still be distilled, without knowing \( Q \) provided the error in Bob’s (raw) key is less than a certain \( Q_{AB}^{max} \). Assuming Eve has maximal information independent of errors in the raw key, we can simply calculate \( Q_{AB}^{max} \) as follows: Alice and Bob can have a positive key rate provided

\[
h(Q_{AB}^{max}) < 1 - \max(I_E), \text{ i.e., } Q_{AB}^{max} \approx 7\%.
\]

Thus in some sense, having a semblance of CM for the current protocol would only provide for a better key rate as Eve’s information gain can be ascertained properly.

However, as we shall see shortly, practical considerations may delegate the estimation of \( Q \) to a more critical role, especially given possible physical realisations where polarised photons are used for qubits and waveplates for transformations.

**A practical protocol.** — Let us consider a practical implementation of the protocol using the polarisation degree of photons as qubits. Realistic implementations of unitary transformations process pulses of photons independently of the actual number of photons. This of course exposes the protocol to a Quantum Man in the Middle attack where Eve could hijack Bob’s photon en route and estimate Alice’s transformations perfectly using a bright pulse before encoding Bob’s photon accordingly to be submitted to him. The solution to this problem is the use of CM. The CM itself should of course involve a finite number of bases, say \( n \), used for prepreparations and measurements; lest the probability for Alice’s and Bob’s aforementioned bases to agree on would approach zero in CM.

We can thus imagine adding a step such that with probability \( c \), Alice executes a CM where she would measure the incoming qubit in a basis selected from \( n \) pre-agreed bases. Bob should then include these \( n \) bases in his EM so that with probability \( c/n \), a CM is successful and Alice and Bob may estimate errors in the forward path. This immediately provides Alice and Bob with a means to access \( Q \) and thus estimate Eve’s information gain and the security analysis of the previous section holds. For simplicity, however, we do not consider imperfections to the extent of having multiphoton pulses nor do we consider channel losses in this work. For practical purposes, we set \( n = 2 \), corresponding to the conventional CM where the bases used are mutually unbiased. For simplicity, we further set Bob’s number of basis in EM to be 2 as well and correspond to the same bases for CM.

**Experimental proof of concept.** — In the following we report on an experimental implementation of the practical protocol described above. The setup is basically a proof of principle with modest apparatus utilising polarised photons derived from the \( X \) (diagonal) and the \( Z \) (rectilinear) bases from attenuated laser pulses as qubits and half-wave plates for the encoding process. These should be rather conventional; for example, the former is quite standard in QKD experiments or the latter for orthogonal/ nonorthogonal unitary implementation in [9,17]. While we do simulate the presence of Eve by introducing noise on the forward and backward paths (“artificial depolarisation” akin to that in [9]), it is important to stress that this is not meant to be a full scale secure implementation. For example, rather than have Bob randomly select between bases for his qubits, we allow the protocol to be executed with Bob choosing one bases for a certain number of runs and another for the other runs; as is the case for Alice’s encoding. We also do not execute the classical aspect of a QKD protocol such as authenticating the users (Alice and Bob), error correction of Alice-Bob’s strings and privacy amplification.

Figure 2 shows the schematic of the experimental setup which comprises of three main parts; namely Bob’s, Eve’s and Alice’s sites. Bob’s site consists of a photon state preparation setup as well as a measurement setup to analyse incoming photons in the backward path. At Bob’s site, photon states were generated by a strongly attenuated laser and the polarisation of the photons can be set by using a zero-order half-wave plate (\( \text{H}_{1/4} \)). The polarised photon is then transmitted to Alice’s site via free-space (forward-path). At her site, Alice passively switches between CM and EM using a 50/50 beam splitter (BS). In CM, Alice would measure the incoming photon directly in the forward-path using a polarising beam splitter, \( \text{P}_{1} \), detectors, \( \text{D}_{1,2} \), and a wave plate (\( \text{H}_{2} \)). In the experiment, for the sake of simplicity, we always set Alice’s measurement bases to be equal to Bob’s preparation bases. Obiously a full fledged implementation would require Alice to measure in either the rectilinear or diagonal bases randomly where half would eventually be discarded. In the EM mode, Alice would need to realise the \( \mathbb{I} \) and \( R_{y}(-\pi/2) \) operators.
A pair of half-wave plates, \( H_{6,7} \) is used for the purpose before forwarding the qubit to a mirror, thus returning it to Bob via free space in the backward path.

The incoming polarisation encoded photons from Alice are finally analysed at Bob’s site using a polarising beam splitter, \( P_1 \), detectors, \( D_{3,4} \) and the zero-order half-wave plate (\( H_9 \)) set in either the same bases the qubits were originally prepared or one rotated to the other basis.

The existence of the eavesdropper in the forward path and backward path is simulated by introducing noise in the communication system when the photons traverse Eve’s site. This is done by virtue of “artificial depolarisation” channels; \( i.e. \), using pairs of half-wave plates \( H_{2,3} \) and \( H_{4,5} \) in the forward and backward paths, respectively. It is important to note that we do not require the errors in the forward path to be equal to that in the backward nor do we require the errors in EM to be trivially related to that in CM; thus discarding the usual models of noise considered for two-way QKD.

We use two independent personal computers equipped with PCIe field-programmable gate array card (FPGA; National Instruments PCIe-7853) to control and synchronise all active equipment in the experiment as well as for data acquisition purposes. Further details of the experimental setup are provided in the SM.

**Experimental results.** Data were collected for each “noise” setting where in each one, we would have a pair of (averaged) errors, \( i.e. \), one from CM and the other from EM. In the case for EM, choosing only data which in principle would provide Bob with conclusive inference of Alice’s encodings, we consider which of the cases tally with the actual encoding used by Alice and which do not (errors). Averaging the results over all states (by Bob) and encoding (by Alice) used, we arrive at an averaged error rate for the EM. Data providing error rates for CM is quite straightforward as we only compare the states sent by Bob to those measured in CM. As argued earlier, that one may not know \textit{a priori} the relationship between the errors in CM and EM (assuming there is one), we do not presume plotting the more conventional “information curves” for Eve’s gain (which is a function of \( Q \)) and Alice-Bob’s (which is a function of \( Q_{AB} \)). Instead, points are plotted based on these error rates as \( Q_{AB} \) vs. \( Q \). This is illustrated in fig. 3. We include the contour lines of the previous fig. 1 to exhibit which of the points fall below the security threshold and which beyond. The values accompanying the points are just the value for the corresponding (in theory) secret key rates calculated using the secret key rate formula. We note that in principle a proper finite key analysis may be required for a strict treatment of the key bits with respect to security.

While the points that occupy the secure region in the figure (positive secret key rate) reflect a very small sample of points that can, in principle be achieved experimentally, we believe that these results already point out to the feasible and practical picture of our protocol.

**Conclusions.** Bidirectional or two-way QKD has certainly been a topic of interest for more than a decade now; ranging from entanglement-based protocols, nonentangled versions to even continuous variables framework [25]. These protocols essentially have a common topology; where one party sends quantum states to another who would encode with a transformation before sending it back to the sender for his decoding measurement. Building on this, we demonstrate the simplest way forward for such protocols to actually embody the essence of introducing an element of ambiguity into Eve’s estimation of the encoding itself to deter her; rather than solely relying on the use of nonorthogonal qubit states. Towards this end, we make use of two unitary transformations selected from two different MUUBs for encoding purposes. The critical difference between the current work and earlier protocols...
making use of two orthogonal unitaries is in the current protocol’s use of two indistinguishable transformations that naturally suppresses Eve’s information gain. In order for one party to make conclusive statements of the other’s encoding, the protocol subscribes to a decoding procedure, inspired by the SARG protocol [20]. While the protocol only allows for 1/4 of qubits sent to generate a (raw) key, the theoretical analysis based on collective attacks, coupled with a more relevant definition for security threshold, has provided a promising picture for the protocol’s security compared to its predecessor. The current protocol’s ability to extract a secret key for larger regions of errors in the communication channels cannot be underestimated and may have implications in practical implementations. As a quick example, implementations which see errors on a channel as a function of distance between Alice and Bob should possibly even allow for larger secure distances to be achieved compared to LM05.

We have also executed an experimental setup for a proof of concept of the protocol using weak photon pulses traversing artificial depolarising channels between the legitimate parties with a pair of half-wave plates for the encoding transformation. While we do not commit to actually distilling a secret key, we have demonstrated its feasibility given a very modest setup. A full scale protocol with actual secret key extraction is hence very possible given some addendum to the setup. This should include the randomisation of Bob’s choice for preparation and measurement, Alice’s choice for encoding as well as a proper execution of error correction and privacy amplification protocols.

Given its promising security, we hope that the future would see a more involved analysis of such a protocol. As an example, it would be interesting to analyse the protocol’s security based strictly on Eve’s estimation of the unknown transformation and the disturbance she would cause thereof using a quantum instrument [15]; similar to the suggestion made in the mentioned work. Such an analysis would circumvent the need for the value of $Q$, and consequently, the CM would, at least in principle, be obsolete. Realistic issues too should eventually be addressed. A quick example would be the issue of multiphoton pulses coupled with channel losses and how the current protocol would perform given such imperfections. On a more fundamental note, we believe, this work should engender further interest, especially regarding the role of indistinguishable unitary transformations and even MUUBs within the context of quantum cryptography and quantum information as a whole.

***

JSS would like to thank Stefano Mancini (UNICAM) and Qing-Yu Cai (WIPM) for helpful discussions and for financial support by the Ministry of Higher Education (Malaysia) under the Fundamental Research Grant Scheme FRGS14-152-0393. Both authors would like to thank Abdul Adhim (XMU) for his assistance in constructing the figure related to the experimental setup (fig. 2) and M. Ridza Wahiddin (IIUM) for his encouragement and support of the work.

REFERENCES

[1] Bennett C. H. and Brassard G., in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York) 1984, pp. 175–179.
[2] Gisin N., Ribordy G., Tittel W. and Zbinden H., Rev. Mod. Phys., 74 (2002) 145.
[3] Lo Hoi-kwong, Curty M. and Tamaki Kiyoshi, Nat. Photon., 8 (2014) 595604.
[4] Bostrom K. and Felbinger T., Phys. Rev. Lett., 89 (2002) 187902.
[5] Cai Q.-Y. and Li B.-W., Chin. Phys. Lett., 21 (2004) 601.
[6] Fu-Guo Deng and Gui Lu Long, Phys. Rev. A, 69 (2004) 052319.
[7] Fu-Guo Deng and Gui Lu Long, Phys. Rev. A, 70 (2004) 012311.
[8] Lucamarini M. and Mancini S., Phys. Rev. Lett., 94 (2005) 140501.
[9] Cerè A., Lucamarini M., Di Giuseppe G. and Tombesi P., Phys. Rev. Lett., 96 (2006) 200501.
[10] Khir Abdul M. F., Mohd Zain M. N., Soekardo S., Saharudin S. and Shaari S., Opt. Eng., 51 (2012) 045006.
[11] Khir Abdul M. F., Mohd Zain M. N., Bahari I., Soekardjo S. and Shaari S., Opt. Commun., 285 (2012) 842.
[12] Kumar K., Lucamarini M., Di Giuseppe G., Natali R., Mancini G. and Tombesi P., Phys. Rev. A, 77 (2008) 022304.
[13] Lucamarini M. and Mancini S., Theor. Comput. Sci., 560 (2014) 1.
[14] D’Ariano G. M., Lo Presti Paolopiacido and Paris M. G. A., Phys. Rev. Lett., 87 (2001) 270404.
[15] Bisio A., Chiribella G., D’Ariano G. M. and Perinotti P., Phys. Rev. A, 82 (2010) 062305.
[16] Chiribella G., D’Ariano G. M. and Perinotti P., Phys. Rev. Lett., 101 (2008) 180504.
[17] Laing A., Rudolph T. and Obrien J. L., Phys. Rev. Lett., 102 (2009) 160502.
[18] Shaari S., Phys. Lett. A, 378 (2014).
[19] Shaari J. S., Nasir R. N. M. and Mancini S., Phys. Rev. A, 94 (2016) 052328.
[20] Scarani V., Acin A., Ribordy G. and Gisin N., Phys. Rev. Lett., 92 (2004) 057901.
[21] Lu Hua, Fung Chi-Hang Fred, Ma Xiongfeng and Cai Qing-Yu, Phys. Rev. A, 84 (2011) 042344.
[22] Henao Ivan C. and Sierra Roberto M., Phys. Rev. A, 92 (2015) 052317.
[23] Joza R. and Schlienz J., Phys. Rev. A, 62 (2000) 012301.
[24] Devetak I. and Winter A., Proc. R. Soc. A, 461 (2005) 207.
[25] Pirandola S., Mancini S., Lloyd S. and Braunstein S. L., Nat. Phys., 4 (2008) 726.