

Integrated-optical realizations of quantum key distribution over maximally unbiased bases

Moshe Nazarathy, Igor Tzeliker, Yuval Regev, Meir Orenstein, Matty Katz*
Department of Electrical Engineering, Technion, Israel Institute of Technology
*Department of Computer Science, Technion, Israel Institute of Technology

Abstract

Quantum Key Distribution (QKD) protocols based on higher-order MUBs (Maximally Unbiased Bases), potentially displaying improved range-security performance, are optically realized for higher (>2) dimensions and/or for multiple (>2) transmission and detection bases, inspired by analogies with the DPSK (Differential Phase Shift Keying) and PPM (Pulse Position Modulation) formats of classical optical communication. In particular we introduce optical realizations for (i): a six-state protocol in qubit space, employing an extra phase modulated interferometer in the transmitter, detecting the photon in the PPM basis of three consecutive time-slots. (ii): a 16-state MUB protocol in four dimensions, based on differential phase encoding over four adjacent time-slots. The transmitter (Alice) and receiver (Bob) for this system are realized using generalized Mach-Zehnder interferometers with four delay arms, and three phase modulators, further requiring a quantum Hadamard-4 gate, realized using four cross-connected directional couplers, to be implemented as an integrated-optical circuit. The conception and analysis of these optical realizations of abstract higher-order QKD MUB-based protocols, is inspired by a novel insight into the structure of the MUB set, constructed by modulating a generator matrix (typically a Hadamard matrix) with a set of phasemasks. The operating characteristics (OC) of these generalized protocols are derived in terms of three simple figures of merit, the Eve Detect (or Disturbance) Rate (EDR), the Eve Information Rate (EIR) and the Key Creation Rate.

I. Introduction

Quantum Key Distribution (QKD) systems based on optical modulation, transmission and detection of single-photon states [1-2], derive their security from the quantum-mechanical laws of nature (uncertainty and no-cloning principles) rather than relying on the conjectured computational complexity of classical cryptographic algorithms. First proposed in [3] and demonstrated in [4] over the modest transmission distance of 30 cm, experimental demonstrations of optical QKD have gradually evolved to longer distances for point-to-point fiber-optic and free-space transmis-

sion as well as for multiplexed or multiple access communications, e.g.[5-21], to the point where such systems are commencing transition from the laboratory stage to actual field deployment. Theoretically evaluating the “safe” transmission range over which unconditional security is maintained, as well as proposing systems with extended “safe” range, are still outstanding analysis and design objectives of QKD research. Evidently, the range-security trade-off is intimately coupled with the selection of optical transmission schemes. Over the fiber-optic channel, a key requirement for the optical modulation formats is that they be robust to polarization fluctuations. The QKD systems conceived so far modulate the optical attributes of polarization phase, and/or emission time, corresponding to the classical modulation formats of POLSK (Polarization Shift Keying, e.g [4,8,12]), DPSK (Differential Phase Shift Keying, e.g. [6,7,17,20]) and PPM (Pulse Position Modulation, e.g. [22-24]). We recently considered optical realizations of the six-state QKD protocol [24] based on hybrid DPSK and PPM. A similar scheme pertaining to a four-state protocol was experimentally demonstrated in [22,23]. In the seemingly unrelated domain of classical optical communication, we recently ported variants of DPSK wireless transmission using multiple (more than two) time-slots. e.g. differentially modulating and detecting the phase over a block of four-consecutive time-slots, attaining record quantum limit sensitivities [25]. A key objective of this paper is to further explore the QKD applications of such advanced DPSK+PPM modulation formats, and propose integrated-optic realizations, extending the conventional BB84 protocol to higher-dimensions and/or using more than two transmission and detection bases. Such advanced protocols were considered at the abstract level (without regard to their physical implementation) in [26]. The key underlying mathematical concept is that of Maximally Unbiased Bases (MUB) [27-29]. The conventional four-state BB84 protocol using $K = 2$ bases in $D = 2$ dimensions was extended to a six-state ($KD = 6$) protocol, and shown to provide improved security [30-32]. Moreover, in [26], multi-dimensional extensions, $D > 2$ and/or additional MUB bases, ($K \geq 2$), were shown to provide improved security performance. In this paper we introduce and analyze optical implementations of such novel multi-dimensional protocols of improved performance, based on a novel theoretical insight into multi-dimensional MUB constructions. The emerging optical structures implementing the abstract protocols include components and subsystems already present in the conventional DPSK optical realization of the BB84 protocol, namely delay-line interferometers and phase modulators, however the optical

architectures and component counts and types are extended to include multiple (more than two) delay lines and/or phase modulators, as well as resorting to a new integrated-optical implementation of a Hadamard optical gate based on coupled-waveguides (directional couplers), further to the Multi-Mode-Interference (MMI) device implementations of [33,34]. From an optical integration point of view we demonstrate that state-of-the-art integrated optic structures provide key building blocks for quantum information processing: the Hadamard optical gate and the splitting-combining optics, and possibly even the delay lines, may be realized as Planar Lightwave Circuits (PLCs), e.g. of silica-on-silicon germano-silicate types, while the phase modulators may be realized on electro-optic substrates such as LiNbO_3 . Semiconductor-based opto-electronic circuitry (e.g. InP based) can be employed to realize fully integrated QKD devices combining active phase modulators with the passive optical gates, splitters, combiners, and delay lines. Indication of the practical feasibility of our proposed integrated-optical systems, is provided by the experimental results for QKD integrated-optic circuits such as [17, 35], or [22,23] which use hybrid PLCs consisting of silica waveguides on silicon substrates, opto-mechanically coupled with LiNbO_3 phase modulators. The silica structures implementing the couplers, splitters, combiners and delay lines were temperature-tuned to statically tune the phase and balance the birefringence.

The paper is structured as follows:

In section II we review the mathematics of MUB sets, and present our key insight regarding synthesis of a MUBs set out of a single Hadamard “generator” optical gate via modulation through a set of phasemasks. Section III develops an integrated-optic implementation of the Hadamard gate, used as a building block in synthesizing the MUB matrices. Section IV reviews the MUB QKD protocol: an advanced multi-dimensional extension [26] of the BB84 protocol, based on the MUB. Section V considers a simple intercept&resend attack, introducing intuitively appealing figures of merit for protocol performance, adopting operating characteristics specifying rates for the raw key creation, for extraction of information by Eve (Eve Information Rate = EIR), and for Alice and Bob detecting Eve’s intrusion (Eve Detect Rate = EDR). Section VI presents and analyzes our novel optical realization of the six-state protocol in two-dimensions (qubit space). In section VII we introduce and analyze a novel optical realization of the 16-state protocol in four dimensions. Section VIII derives the operating characteristics of the two optical protocol realizations considered so far. The impact on the OCs of the erasure events, whereby none of the detectors click, is elucidated. A remarkable result is that the EDR and EIR, which reflect the tradeoff

between disturbance and information, sum up to unity, and the EDR is increased by the erasure effect. Section IX finally proposes an integrated optical implementation for Bob's apparatus in our final optical realization of the 16-state MUB QKD protocol, based on our Hadamard-4 integrated-optical gate and MUB synthesis of section III. The concluding discussion of section X provides comparative perspective and indicates directions for future work.

II. Maximally Unbiased Bases (MUBs)

In this section we introduce mathematical preliminaries laying the foundation for the rest of the paper. The central concept is that of mutually unbiased bases, formally defined as follows:

A Maximally Unbiased Base (MUB) Set [27-29]

$$\left\{ \left\{ |\phi_i^{(0)}\rangle \right\}_{i=1}^D, \left\{ |\phi_i^{(2)}\rangle \right\}_{i=1}^D, \dots, \left\{ |\phi_i^{(\beta)}\rangle \right\}_{i=1}^D, \dots, \left\{ |\phi_i^{(K-1)}\rangle \right\}_{i=1}^D \right\} \quad (11)$$

is a collection of K orthonormal bases of \mathbb{C}^D (D -dimensional complex Euclidean space),

$$\left| \langle \phi_i^{(\beta)} | \phi_j^{(\beta)} \rangle \right|^2 = \delta_{ij}, \quad \sum_{i=1}^D |\phi_i^{(\beta)}\rangle \langle \phi_i^{(\beta)}| = \mathbf{1}, \quad 0 \leq \beta \leq K-1 \quad (12)$$

such that any vector in any base "makes the same angle" with any vector in any other base:

$$\left| \langle \phi_i^{(\beta)} | \phi_j^{(\beta')} \rangle \right| = 1/\sqrt{D}, \quad \text{for all } i, j \text{ and all } \beta \neq \beta'. \quad (13)$$

Footnote: An infinity of MUB sets may be obtained from a given one by isometric operations on the base vectors such as multiplication by phase factors, complex-conjugation or general unitary transformations.

Notice that there are KD vectors in the MUB set, hence we sometimes refer to it as a KD -states MUB. For each dimension D we seek a construction with the maximum K . The number of bases is known to satisfy $K \leq D + 1$. A MUB set with the maximum K , i.e. containing

$$K = D + 1 \quad (14)$$

bases (i.e. $KD = (D + 1)D$ states) is referred to as *full*, whereas for $K < D + 1$, the base set is

called *partial*. A sufficient condition for the existence of a full MUB set is that $D = p^r$ (integer power of a prime dimension), [29], however the maximal K is not known for any other composite number. Even when a full MUB set exists, it is sometimes useful to utilize a partial MUB set by discarding certain bases. The two MUB sets described below play a key role in this paper:

6-state MUB set: $K = 3, D = 2$: This is the full MUB for a two-state (qubit) system:

$$\left\{ \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}, \left\{ \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right\}, \left\{ \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ j \end{bmatrix}, \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -j \end{bmatrix} \right\} \right\}$$

Interpreting these MUB vectors as polarization Jones vectors, the first two bases correspond to linear polarizations respectively aligned with the canonical axes, and rotated $\pm 45^\circ$, in fact forming a four-state partial MUB in \mathbb{R}^2 , shown in Fig. 1, complemented to a full MUB set by the third complex-valued base, corresponding to the two orthogonal circular polarizations. On the Poincare sphere these three bases correspond to the three orthogonal axes of Stokes space.

Considering now a general MUB set, let us array its base vectors as columns of K base matrices $\{\Phi^{(0)}, \Phi^{(1)}, \dots, \Phi^{(K)}\}$ of dimension $D \times D$, each containing the D orthogonal base vectors of each base. The i -th vector of the β -th base the MUB set is the i -th column $\Phi^{(\beta)}$:

$$\text{Col}_i \Phi^{(\beta)} = |\phi_i^{(\beta)}\rangle \quad (15)$$

20-state MUB set: For $D = 4$, $K = 5$, one possible full 20-state MUB set, in the matrix notation just introduced, is

$$\Phi^{(0)} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \Phi^{(1)} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, \quad \Phi^{(2)} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ j & j & -j & -j \\ -j & -j & j & j \end{bmatrix}, \quad \Phi^{(3)} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ j & j & -j & j \\ -j & -j & j & j \\ 1 & 1 & 1 & 1 \end{bmatrix}, \quad \Phi^{(4)} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ j & -j & j & -j \\ -1 & -1 & 1 & 1 \\ j & -j & -j & j \end{bmatrix} \quad (16)$$

Consistent with the MUB property, the columns within each matrix are orthogonal, while the projection of any column of one matrix onto any column of another matrix has absolute value $1/2$.

In particular we note that the zeroth base is the unity matrix of dimension 4, $\Phi^{(0)} = \mathbf{1}_4$, and that the first base is (up to a constant) equal to Hadamard matrix of order 4: $\Phi^{(1)} = \frac{1}{2}H_4$

Some relevant properties of the Hadamard and MUB matrices are relegated to Appendix A.

We have conceived a key novel construction for MUB sets of dimension $D = 2^r$, underlying the optical realizations to be explored in this paper: Our synthesis of MUB matrices is based on *phase-masks defined as diagonal unitary matrices*, i.e. matrices with phase factors along their diagonal:

$$\Lambda = \text{Diag}[e^{j\theta_0}, e^{j\theta_1}, \dots, e^{j\theta_{D-1}}] \quad (17)$$

Our new observation is that *MUBs may be constructed by multiplying a certain unitary matrix \mathbf{W}_D , called the MUB generator, by a suitable set of phase masks. In cases of interest here the MUB generator is a Hadamard matrix, $\mathbf{W}_D = \hat{\mathbf{H}}_D$* . Prior to exploring the physical realizations,

let us clarify the mathematical details: Our claim is that exist MUB sets of dimension containing $K \leq D + 1$ bases, with their basis matrices (apart from the zeroth one which is unity) expressible as follows:

$$\Phi^{(0)} = \mathbf{1}_D, \Phi^{(1)} = \mathbf{W}_D, \Phi^{(\beta)} = \Lambda_\beta \mathbf{W}_D \quad 2 \leq \beta \leq K-1 \leq D, \quad (18)$$

where $\{\Lambda_\beta\}$ is a set of phase-masks. The MUB generator, \mathbf{W}_D , might consist of a normalized Hadamard matrix, as demonstrated below for $D = 2, 4$, or for higher dimensions a generalized Fourier transform matrix (a Kronecker product of DFT matrices), or most generally a certain unitary matrix, however we shall not further pursue the higher-dimensional MUBs here, since our focus is rather on low-dimensionality optical realizations, as the implementation complexity tends to become excessive for $D > 4$

The particular MUB set of eqs. 16, for $D=4$, was actually generated from a Hadamard-4 matrix, constructing the MUB matrices as follows (as readily verified by matrix multiplication):

$$\Phi^{(0)} = \mathbf{1}_4, \Phi^{(1)} = \frac{1}{2}\mathbf{H}_4 = \hat{\mathbf{H}}_4 \quad \Phi^{(\beta)} = \Lambda_\beta \Phi^{(1)} = \Lambda_\beta \hat{\mathbf{H}}_4, \beta = 2, 3, 4 \quad (19)$$

where $\{\Lambda_\beta\}$ are phase masks given by

$$\Lambda_2 = \text{Diag}[1, 1, j, -j], \quad \Lambda_3 = \text{Diag}[1, -j, -j, -1], \quad \Lambda_4 = \text{Diag}[1, j, -1, j] \quad (20)$$

In fact the last expression in eq. 19 holds for $\beta = 1$ as well, once a trivial phase mask,

$$\Lambda_1 = \text{Diag}[1, 1, 1, 1] = \mathbf{1}_4, \text{ is introduced, such that } \Phi^{(1)} = \Lambda_1 \Phi^{(1)}.$$

The four phase masks used in constructing the $D=4$ MUB set, are then of the form

$$\Lambda_\beta = \text{Diag}\left[e^{j\theta_0^{(\beta)}}, e^{j\theta_1^{(\beta)}}, e^{j\theta_2^{(\beta)}}, e^{j\theta_3^{(\beta)}}\right], \quad (21)$$

with their phases given by

$$\begin{aligned} \{\theta_0^{(1)}, \theta_1^{(1)}, \theta_2^{(1)}, \theta_3^{(1)}\} &= \{0, 0, 0, 0\}, \quad \{\theta_0^{(2)}, \theta_1^{(2)}, \theta_2^{(2)}, \theta_3^{(2)}\} = \{0, 0, \pi/2, -\pi/2\} \\ \{\theta_0^{(3)}, \theta_1^{(3)}, \theta_2^{(3)}, \theta_3^{(3)}\} &= \{0, -\pi/2, -\pi/2, 0\}, \quad \{\theta_0^{(4)}, \theta_1^{(4)}, \theta_2^{(4)}, \theta_3^{(4)}\} = \{0, \pi/2, -\pi, \pi/2\} \end{aligned} \quad (21a)$$

Finally, we note that the six-state MUB is seen to exhibits a phase-mask-times-generator structure as well, with generator $\mathbf{w}_2 = \hat{\mathbf{H}}_2$ and phase mask $\Lambda_2 = \text{Diag}[1, j]$:

$$\Phi^{(0)} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \mathbf{1}_2, \quad \Phi^{(1)} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \hat{\mathbf{H}}_2, \quad \Phi^{(2)} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ j & -j \end{bmatrix} = \Lambda_2 \Phi^{(1)} \quad (22)$$

Relating now the math to the physics, the six-state MUB of eq. 22 is implemented in integrated optics by the cascade of a phaseshifting section (the phase mask) and a directional coupler (the

back end of a conventional Mach-Zehnder Delay interferometer), while 16-state MUB $\{\Phi^{(1)}, \Phi^{(2)}, \Phi^{(3)}, \Phi^{(4)}\}$ of eq. 19 (excluding $\Phi^{(0)}$ which is unity) will be realized in the next section by the cascade of a phaseshifting section with an optical Hadamard gate forming the back-end of a generalized Mach-Zehnder Interferometer (IF). It is now apparent that an optical Hadamard gate synthesizing the transfer matrix \hat{H}_4 constitutes a key building block in the MUB constructions underlying the novel QKD physical realization introduced in this paper. The integrated-optic realization of the Hadamard-4 gate is discussed next.

III. Integrated-optic realization of the Hadamard-4 gate and 16-state MUB

Higher-order Hadamard matrices were realized by means of optical circuits interconnecting the lowest order Hadamard-2 devices, as demonstrated in [33] for a Hadamard-8 gate. However, we have not located in the literature integrated-optical realizations (based on either MMI or other device types) of the order-4 Hadamard gate, namely an optical 4-port with spatial transfer function equal to the Hadamard matrix.

Footnote: Our spatial Hadamard gate is not to be confused with Hadamard code generation in the temporal domain, as used for code-based photonic routers [36].

We now propose a seemingly novel relatively simple integrated-optic realization of such Hadamard-4 gate. Referring to Fig. 2, such gate is first conceptually synthesized by a suitable interconnection of four Hadamard-2 modules, \hat{H}_2 as well as two “swap” modules X :

$$\hat{H}_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (23)$$

To establish that Fig. 2 indeed abstractly synthesizes the Hadamard-4 gate, we excite the system in turn with unit vector inputs, verifying that the respective columns of the \hat{H}_4 matrix emerge at the four output ports. Our optical realization of this abstract construction of the Hadamard-4 gate in terms of lower-order modules is shown in Fig. 3, wherein our preferred realization of the Hadamard-2 modules consists of 50/50 directional couplers (of half the crossover length).

Notice that the “swap” gate may be straightforwardly realized (with negligible residual cross-talk) by simply crossing two waveguides at an angle close to 90° . Another realization of the “swap” gate might consist of a directional coupler of the crossover length (double that of the Hadamard-2 directional coupler). An alternative implementation for the Hadamard-2 devices featuring in the

overall Hadamard-4 structure, may resort to MMI devices (as in the construction in [33] for the Hadamard-8 gate in terms of Hadamard-2 MMI modules).

The MUB matrices are then realizable by following the Hadamard gate with phase-shifting sections implementing the phase masks. In fact we are rather interested in implemented the adjoints (conjugate transposes) of the MUB matrices,

$$\Phi^{(\beta)\dagger} = (\Lambda_\beta \hat{H}_4)^\dagger = \hat{H}_4 \Lambda_\beta^\dagger. \quad (24)$$

where the symmetry of the Hadamard matrix, ($\hat{H}_4^\dagger = \hat{H}_4$) was used in evaluating the adjoint.

As further depicted in Fig. 3, preceding the optical Hadamard gate by a phase-mask, and applying the negatives of the phaseshifts of eq. 21a, synthesizes transfer functions for the overall 4-port, equal to the adjoints of the MUB matrices of eq. 24. Such transfer matrices, acting as “matched filters” for the detection of MUB vectors, are key ingredients in our final optical realization of Bob’s apparatus for a 16-state MUB QKD protocol (section IX). Equipped with an understanding of MUBs and their integrated-optic synthesis, we next proceed to review abstract MUB-based QKD protocols, in preparation of considering their optical realizations.

IV. A generalization of the BB84 protocol using higher dimensional MUBs

A generalization of the well-known BB84 protocol is reviewed in this section at an abstract level (without yet addressing the optical implementation details), in essence following [26]. The protocol makes use of K MUBs in a Hilbert state space of dimension D . The BB84 and six-state protocols turn out to be special cases of the general protocol, for $D = 2$ and $K = 2, 3$.

Referring to Fig. 4, Alice randomly selects with equal prob. (probability), one of K quantum sources. The transmission hypotheses H_i are indexed by a D -ary key symbol, i , $0 \leq i \leq D - 1$, independent of α , and uniformly distributed, i.e. $\Pr\{H_i\} = 1/D$. With the α -th source, and the i -th key symbol drawn, the emitted quantum object is $|\phi_i^{(\alpha)}\rangle$, i.e. the i -th state of the α -th base of the MUB set. This state is received by Bob over the quantum channel, which is assumed ideal for the purposes of analysis in this paper (i.e. over the optical channel we assume that no photons are lost). Moreover Alice’s and Bob’s systems, including their single-photon detectors, are also assumed ideal (i.e. the detector quantum efficiency is unity and the dark current is zero). Bob’s apparatus consists of switching the incoming quantum object into one of K quantum analyzers

(measurement devices), selected at random with equal prob., independent of Alice's selection of transmission source. If Bob selects the β -th analyzer, or equivalently the β -th reception base,

$\{|\phi_j^{(\beta)}\rangle\}_{j=1}^D$, he then effects a quantum measurement of the incoming state $|\phi_i^{(\alpha)}\rangle$ in this base,

generating the index \hat{i} (an estimate of Alice's key index i) w.p. (with probability) given by

$\Pr\{\hat{i}=j\} = |\langle\phi_j^{(\beta)}|\phi_i^{(\alpha)}\rangle|^2$. The protocol's objective is to have Bob share the same key symbol as

Alice, i.e. $\hat{i}=i$, with Eve drawing minimal information while generating a maximal discernible disturbance to be detected by Alice and Bob. Assume Alice and Bob happen to have selected

identical bases, $\alpha = \beta$, which event occurs w.p. $1/K$. Then, using the α -base's orthonormality,

$\Pr\{\hat{i}=j|\alpha=\beta\} = |\langle\phi_j^{(\alpha)}|\phi_i^{(\alpha)}\rangle|^2 = \delta_{ij}$ i.e. setting $j = i$ yields $\Pr\{\hat{i}=i|\alpha=\beta\} = 1$

Therefore, when the bases are matched we have an error-free quantum channel. Now assume

that Alice and Bob happen to have drawn different bases, $\alpha \neq \beta$ then state $|\phi_i^{(\alpha)}\rangle$ transmitted by Alice's is analyzed in Bob β -th measurement basis, yielding the output index j w.p.

$\Pr\{\hat{i}=j|\alpha \neq \beta\} = |\langle\phi_j^{(\beta)}|\phi_i^{(\alpha)}\rangle|^2 = 1/D$, (25)

as follows from the MUB defining property (eq. 13). It is apparent that whenever the transmit and receive bases are mismatched ($\alpha \neq \beta$), all outputs j are equally likely, regardless of the transmit

key symbol i , Bob's apparatus then behaves as a fair quantum roulette (uniform distribution of outputs). Now, as in the BB84 protocol, the core procedure is the quantum transmission, of a sequence of key symbols, with Alice and Bob keeping record of their independently drawn bases.

At the end of transmission the two parties exchange over a public channel the lists of their respective bases, discarding all key symbols transmitted and received with mismatched bases. Then, in the absence of channel impairments (losses, noise) and intrusion by Eve, the symbols obtained

with matched bases are expected to be received error-free, i.e. $\hat{i} = i$ with i the transmitted symbol and \hat{i} the detected one. We assert that for a lossless quantum channel and matched bases

($\alpha = \beta$), errors ($\hat{i} \neq i$) may only occur as a result of intrusion by Eve. This is readily verified in the next section for the most naive Intercept&Resend (I&R) attack, whereby Eve acts a repeater, detecting the transmitted quantum object using an apparatus identical to Bob's and retransmitting

it using an apparatus identical to Alice's. More sophisticated attacks on a KD -state protocol of arbitrary dimension were considered in [26].

Footnote: Most generally, it is desired that for a lossy channel, i.e. when there is a finite QSER (Quantum Symbol Error Rate) $\Pr\{\hat{i} \neq i\}$, the QSER be always enhanced whatever Eve's attack is. Quantifying the increase in QSER vs. the information drawn by Eve, for the most general attacks is a heavy information-theoretic topic, outside the scope of this paper.

V. Operating characteristics of the MUB protocol in the wake of an I&R attack

We now derive the operating characteristics of the MUB protocol, under an I&R attack, namely the tradeoffs between the prob. that the disturbance introduced by Eve gets her detected by Alice and Bob, vs. the prob. that Eve extracts information, vs. the key creation rate.

It may be shown that, without loss of generality, Eve might conduct her I&R attack by retransmitting in the same basis, labelled ε , as she used for detection, as well as repeating the same symbol she detected, labelled r . Now given that $\alpha = \beta$, if Eve randomly draws the correct base, $\varepsilon = \alpha = \beta$ (which occurs w.p. $1/K$) then there is no way for Alice and Bob to detect Eve, who shares the key information without getting detected, i.e. we have $r = i = \hat{i}$. On the other hand, w.p. $1 - 1/K$, Eve draws the wrong base, $\varepsilon \neq \alpha = \beta$. Consider now a specific value ε for Eve's mismatched base index. Then Alice induces in Eve's analyzer a fair quantum roulette w.p. $1/D$ for Eve to draw $r = i$, i.e. Eve gets the wrong key symbol, $r \neq i$, w.p. $1 - 1/D$. She then retransmits an incorrect state $|\phi_r^{(\varepsilon)}\rangle$ rather than Alice's original state $|\phi_i^{(\alpha)}\rangle$. Recalling that at the end Alice and Bob restrict the processing to matched bases, $\alpha = \beta$, then Eve is seen to have transmitted a state $|\phi_r^{(\varepsilon)}\rangle$, out of the ε -th MUB base, which differs from Bob's analysis base (the α -th one). Thus, Eve induces a fair quantum roulette in Bob's analyzer, such that Bob's detected index \hat{i} is now uniformly distributed. In particular $\hat{i} = i$ occurs w.p. $1/D$, in which case Eve goes again undetected. However, she is more likely to get detected by the presence of an error, when no error was expected by Alice and Bob, as they have their bases matched. The prob. P_D that Eve's disturbance is detected by the two parties, equals the error prob. under Eve's attack when Alice and Bob's bases are matched. This prob., called EDR (Eve-Detect-Rate) is given by

$$P_D \equiv \Pr\{\hat{i} \neq i | \text{Eve}, \alpha = \beta\} = (1 - 1/K)(1 - 1/D), \quad (26)$$

interpreted as follows: $(1 - 1/K)$ is the prob. that Eve's base be mismatched, while $(1 - 1/D)$ is the prob that Eve's mismatched base induces in Bob a symbol $\hat{i} \neq i$ (the prob. that $\hat{i}=i$ is $1/D$). A second key figure of merit is the prob. that Eve get the correct key symbol, called *Eve's Information Rate* (EIR), evaluated as follows:

$$P_I \equiv \Pr\{r=i|\text{Eve}, \alpha=\beta\} = \left(1 - \frac{1}{K}\right)\frac{1}{D} + \frac{1}{K} = \frac{1}{K} + \frac{1}{D} - \frac{1}{KD} \quad (27)$$

The mid expression is interpreted as follows: the term $1/K$ is the probability that Eve's base be matched, in which case she draws the correct information. When her base is mismatched, occurring w.p. $1 - 1/K$, all values r (in particular the correct one) are equally likely w.p. $1/D$.

A third useful parameter is the total prob. of Alice conveying the correct key symbol to Bob (in the absence of Eve), defined as the *Key Creation Rate* (KCR):

$$P_C \equiv \Pr\{\hat{i}=i\} = 1/K \quad (28)$$

equal to the prob. that the two bases, that are uniformly and independently drawn, coincide.

Footnote: Notice that this is a raw key creation rate, prior to error correction and privacy amplification.

In fact P_D vs. P_I may be viewed as measures of the tradeoff between the disturbance induced by Eve vs. the information extracted by her. Notice that P_D is monotonic increasing in K, D while P_I is monotonic decreasing, indicative of the advantage of increasing K, D , as it is intuitively plausible that protocols with higher P_D and lower P_I enjoy a better security, at least against the I&R attack. On the other hand, a disadvantage of increasing K is that Alice's and Bob's bases are matched a smaller fraction of time, reducing the key creation rate, P_C (eq.28).

It may be argued that increasing security at the expense of key creation rate is a worthwhile trade-off (the key transfer takes longer but is safe). Perhaps a more serious drawback of increasing K, D is that the complexity of realizing the multi-dimensional protocol increases along with it. For this reason we shall only consider modest dimensional values, namely $D = 2, 4$, as going higher would yield diminishing returns in the EPR, while incurring excessive complexity.

Adding up eqs. 26 and 27 yields the remarkable observation that the EDR and EIR complement to unity (i.e. one of P_D, P_I is redundant):

$$P_D(K, D) = 1 - P_I(K, D). \quad (29)$$

The rhs may be interpreted as Eve's SER (Symbol Error Rate), $SER_{Eve} \equiv 1 - P_I$, whereas the lhs is Bob's SER, $SER_{Bob} = P_D$. Remarkably $SER_{Eve} = SER_{Bob}$, interpreted as follows: *The error rate caused by Eve's disturbance, enabling the two parties to detect her, equals the fraction of symbol stream passing through Eve without gaining her information about the key.*

The three rates P_D, P_I and P_C (just two of them being independent) form an *Operating Characteristics (OC)* vector: $[P_D, P_I, P_C]$, plotted in Fig. 5 for a full MUBs ($K = D + 1$) as a function of the dimension D . Surveying some special cases, the 4-state BB84 protocol is obtained from the MUB QKD protocol, for $D = 2 = K$. Its OC is

$$[P_D, P_I, P_C]_{4\text{-state}} = [1/4, 3/4, 1/2] \quad (30)$$

The next case to consider is $D = 2, K = 3$ i.e a protocol using the full MUB set possible for a qubit system - three maximally unbiased bases, called in the literature [30,31] the *6-state protocol* ($KD = 6$) In a polarization signalling context, the two linear polarization bases are augmented with a 3rd base consisting of the two circular polarizations, yielding the full 6-state MUB with OC

$$[P_D, P_I, P_C]_{6\text{-state}} = [1/3, 2/3, 1/3]. \quad (31)$$

We remark that the four-state (BB84) protocol may be viewed as a special case of the six-state protocol, obtained by discarding one of the three bases of the full six-state MUB, but there is leeway as to which of the three bases to retain. In elementary descriptions of BB84, it is the first two bases that are retained ("linear" and "inclined" linear polarizations), whereas polarization-based optical implementations often resort to the first and last base ("linear" and "circular"), while phase-encoded optical realizations of BB84 use the second and third bases. Recently, integrated-optic phase-based implementations were introduced realizing the first and second bases [22,23]. In this paper we propose novel integrated-optic implementations of manageable complexity for the six-state protocol as well as for MUB QKD protocols with $D = 4$ and $K = 2, 4$, namely

8-states and 16-states protocols. The corresponding OCs are

$$D = 4, K = 2: [P_D, P_I, P_C]_{8\text{-state}} = [3/8, 5/8, 1/2] \quad (32a)$$

$$D = 4, K = 4: [P_D, P_I, P_C]_{16\text{-state}} = [9/16, 7/16, 1/4] \quad (33a)$$

It is apparent that compared with BB84, the 16-state protocol appears significantly more secure, though more sluggish: the chance of detecting Eve more than doubled, while Eve's information rate was reduced by more than 40%, albeit at the expense of halving the rate of key creation.

We end this section with the caveat that our introduction of the OC as a highly intuitive measure of security is to be supplanted by rigorous security studies, under more sophisticated attacks, e.g. as in [30-32], in order to formally establish our conjecture that increasing the MUB dimension is beneficial to security. In this respect we note that [30-32] all conclude that the six-state protocol is more reliable, tolerating a higher error rate than the four-state BB84 protocol. Having established the desirability of going to “higher orders” (increased D, K) we proceed in the remainder of the paper to introduce novel optical realizations of the 6, 16 and 8-state protocols.

VI. Integrated-optic realization of the six-state protocol

An optical realization of six-state QKD protocol was proposed in a recent publication [24], where it was interpreted in terms of the DPSK (Differential Phase Shift Keying) and PPM (Pulse Position Modulation) optical modulation formats. When applied to single photon transmission, these modulation formats may be represented in the PPM base $\{|0\rangle, |1\rangle, \dots, |t\rangle, \dots\}$, with $|i\rangle$ a quantum state, wherein the photon is temporally confined to time-slot i (the time axis is divided into regularly spaced slots). In phase-encoding realizations of the BB84 four-state protocol (e.g. [5-7,20]) (henceforth called BB84-DPSK) the four transmitted states are $\{\pm|0\rangle + |1\rangle\}$, $\{\pm j|0\rangle + |1\rangle\}$.

Footnote: In the DPSK version used here, it is the late time slot, $|1\rangle$, that provides the phase reference for the early time slot, $|0\rangle$, a convention opposite to that used in conventional DPSK, wherein the early slot is the reference. Notice that for simplicity, these states were stated unnormalized (their norm is not necessarily unity). It is seen that the “in-phase” states $\{\pm|0\rangle + |1\rangle\}$, called here “Re DPSK”, are orthogonal hence form a basis of the qubit space, and so are last two “quadrature” states, $\{\pm j|0\rangle + |1\rangle\}$, called here “Im DPSK”, however between them the two bases are mutually unbiased.

In a recent alternative optical realization of a four-state protocol [22,23], the Im DPSK states are replaced by two PPM states, transmitting one of the four states $\pm|0\rangle + |1\rangle$, $|0\rangle, |1\rangle$. Again, the first two DPSK Re states form an orthogonal base of the qubit space $\text{span}\{|0\rangle, |1\rangle\}$, and so do the last two PPM states, while these two-dimensional bases are mutually unbiased.

The four-state and six-state MUB protocols abstractly refer to dimension $D = 2$ (qubit) state spaces, however upon modeling the optical realization of these protocols, the qubit spaces are viewed as subspaces of a larger six-dim. Hilbert state space spanned by the PPM basis vectors,

$$\mathbb{H} = \text{span}\{|u_0\rangle, |u_1\rangle, |u_2\rangle, |d_0\rangle, |d_1\rangle, |d_2\rangle\} \quad (34)$$

with the index $t = 0, 1, 2$ denoting the time slot, while u/d designates the up / down branch.

In this section we propose a novel optical implementation for the six-state protocol abstractly introduced in [30], improving upon the optical realization suggested in [24], in essence providing an extension to the full six states MUB of the DPSK four-state protocols (BB84-DPSK and of the scheme of [22,23]). The novel proposed optical realization (Fig. 4) further builds upon the scheme of [22,23], extended here to augment the four-states treated there with the remaining two Im DPSK states. Compared with the conventional BB84-DPSK scheme, Alice now uses two coupled IFs, rather than a single one. As in [22,23] the first IF is symmetric, with no relative delay between its two arms, and its PM effects a relative phase shift of $\phi \in \{0, \pi/2, \pi\}$ between the two arms. This first IF acts as a three-state switch, as controlled by ϕ , in effect directing the light to either the upper or the lower port, or splitting it with equal power between the two ports. The second IF applies a relative time delay T sec (one discrete-time unit) and a relative phaseshift $\theta \in \{0, \pi/2, \pi, 3\pi/2\}$ between its two arms, much as in BB84-DPSK, but unlike in [22,23], where no phaseshift was used in the 2nd IF.

The principle of operation of Alice's states generator is as follows:

(i) upon setting the first IF phase to $\phi = \pi/2$, light is split between the two output ports of the mid-coupler, such that system functions as in the conventional DPSK realization of BB84, generating one of the four DPSK basis states $\{\pm |u_0\rangle + |u_1\rangle\}$, $\{\pm j|u_0\rangle + |u_1\rangle\}$, as selected by the phase setting θ of the second IF. (ii) Upon setting $\phi = 0$ in the first IF, light is switched to the upper output port of the mid-coupler, traversing the longer delay in the upper arm of the second IF, yielding the "late PPM" state, $|u_1\rangle$. (iii) Upon setting $\phi = \pi$, light is switched to lower upper port of the mid-coupler, traversing the shorter delay in the lower IF arm, yielding the "early PPM" state, $|u_0\rangle$. The six possible states at Alice's output are then

$$\{\{\pm |u_0\rangle + |u_1\rangle\}, \{\pm j|u_0\rangle + |u_1\rangle\}, \{|u_0\rangle, |u_1\rangle\}\},$$

comprising four DPSK states (two quadratures), DPSK Re, $\{\pm |u_0\rangle + |u_1\rangle\}$ and DPSK Im $\{\pm j|u_0\rangle + |u_1\rangle\}$, as well as two PPM states, $\{|u_0\rangle, |u_1\rangle\}$, altogether forming a full six-state MUB set in the qubit ($D = 2$) space $\text{span}\{|u_0\rangle, |u_1\rangle\}$, which is a subspace embedded within the six-dimensional space \mathcal{H} (eq. 34). Bob's functionality and the overall basic protocol (without error correction / privacy amplification) are now stated:

(i) Alice randomly transmits one of two base states, indexed by $i \in \{0, 1\}$, out of three possible bases (indexed by $\alpha = 0, 1, 2$): PPM / DPSK Re / DPSK Im

(ii) Bob randomly selects an analysis base (indexed by $\beta = 0, 1, 2$) out of the same set:

(a) If he selected DPSK Re/Im, he then measures both detectors during the “mid” slot 1. Let the index of the clicking detector be $\hat{i} \in \{0, 1\}$

(b) If he selected PPM, he then measures the upper detector during the early/late slots 0,2.

(iii) Bob and Alice publicly share the bases indexes α, β each used in each 3-slot block.

When their bases coincide ($\alpha = \beta$), they record the transmit/receive bits i, \hat{i} as raw key bits.

(iv) They compare a small fraction of their raw key bits. An elevated error rate in these bits is indicative of Eve’s attack (for ideal channel and devices, we have $i = \hat{i}$, unless Eve attacks).

The measurement probabilities for the detectors clicking during the relevant time slots, for all 9 possible combinations of transmission/detection bases are summarized in Table 1, the entries of which are the absolute squares of the probability amplitudes of the various time slots at the upper and lower ports, obtained by straightforwardly though tediously, propagating Alice’s quantum states through Bob’s apparatus. The salient feature is that whenever Alice and Bob’s base selections are matched ($\alpha = \beta$: the diagonal blocks in the table), the prob. of getting the wrong symbol is zero, though there is a finite prob. of getting an inconclusive result (?). However, whenever Alice and Bob are mismatched in their selections of bases, ($\alpha \neq \beta$: the off-diagonal blocks in the table) then Bob is equally biased to read the right or wrong symbol, though the two probabilities are not 1/2, though they are equal, as there is a finite prob. for an inconclusive result as well. The table then indicates that the system indeed operates in the MUB “spirit”, barring the complication that there are finite probabilities that the photon be lost, an event indicated by the erasure symbol (?), not due to absorption but inherent in the system design, as the photon may wander off to the wrong slot, as Bob’s apparatus smears Alice’s two-slot states over a 3-slot window.

The functioning of the DPSK portion of the protocol is actually identical to that of conventional four-state BB84-DPSK. As for the PPM base, if both Alice and Bob selected it, then, given that “PPM early” was transmitted, a photon can never be received in slot 2, and given that “PPM late” was transmitted, a photon can never be received in slot 0. So, assume Alice sends a PPM photon which is not lost but is conclusively detected by Bob in the PPM basis, in either slots 0 or 2. Once

he subsequently lets Alice know over the public channel that he did detect a photon in the PPM base, then upon consulting her records Alice knows exactly the slot that Bob's detector clicked in (if she transmitted PPM early/late then Bob's detector ought to have clicked in the 0/2 slot, respectively), i.e. Alice and Bob do manage to share a key bit over the PPM modulated photon.

VII. Optical realization of the sixteen-state MUB protocol

Fig. 7 indicates an optical implementation of the $D = K = 4$, 16-state MUB protocol.

Alice's system consists of the cascade of a 1:4 splitter, a phase-shifting section, a delay section and a 4:1 combiner. The 1:4 splitter distributes the optical field of the incoming single mode fiber over four single mode output waveguide ports. A phase-shifting section consists of four PMs applying the respective phaseshifts $\gamma_0, \gamma_1, \gamma_2, \gamma_3 \in \{0, \pi/2, \pi, 3\pi/2\}$, as determined by indexing a lookup table according to the output of a random number generator producing a pair of integers (i, α) , independently and uniformly distributed over the ranges $0 \leq i \leq 3$, $1 \leq \alpha \leq 4$. The phases lookup table is constructed such that the state vector at the PM outputs equal the i -th base vector of the α -th base, equivalently expressible (see eq. 15) as the i -th column of α -th MUB matrix.

Alice's transmitted vector is then

$$\mathbf{a} \equiv [e^{j\gamma_0}, e^{j\gamma_1}, e^{j\gamma_2}, e^{j\gamma_3}]^T = \text{Col}_i \Phi^{(\alpha)} \quad (35)$$

Footnote: Rows and columns of matrices are labelled here starting from 0.

The four phaseshifts are then the angles of the four complex elements of the i -th column of the α -th MUB matrix: $\gamma_r = \angle[\text{Col}_i \Phi^{(\alpha)}]_r = \angle \Phi_{ri}^{(\alpha)}$, $1 \leq r \leq 4$.

Next, a delay section applies the respective delays of $3T, 2T, T, 0$ onto the four PM output ports, followed by combining the four delayed outputs into the Alice's output fiber. The cascade of the delay section and the 4:1 combiner acts as a parallel-to-serial converter, serializing the state vector of eq. 35.

Bob's system consists of the cascade of a 1:4 splitter, a delay section, a phase-shifting section, an optical Hadamard gate and four single-photon detectors. The 1:4 splitter feeds Bob's phase-shifting section consisting of four PMs applying phaseshifts selectable out of the set $\{0, \pi/2, \pi, 3\pi/2\}$, as determined by indexing a lookup table according to the output of a random number generator producing an integer β uniformly distributed over the range $1 \leq \beta \leq 4$.

Bob's phaseshifts are actually the additive inverses of the quad of phases tabulated in of eq. 21a,

$$\{-\theta_0^{(\beta)}, -\theta_1^{(\beta)}, -\theta_2^{(\beta)}, -\theta_3^{(\beta)}\}. \quad (36)$$

This ensures that the transfer matrix of the PM section equals the conjugate of the β -th phase mask (eq. 20),

$$\Lambda_{\beta}^{\dagger} = \text{Diag}\left[e^{-j\theta_0^{(\beta)}}, e^{-j\theta_1^{(\beta)}}, e^{-j\theta_2^{(\beta)}}, e^{-j\theta_3^{(\beta)}}\right]. \quad (37)$$

The output of the phase-shifting section is fed into a "Hadamard-4" quantum gate, which is a linear optical system with four input ports and four output ports (ideally unitary upon neglecting excess losses), implementing the \hat{H}_4 mapping of input to output optical field complex amplitudes. The integrated optical implementation of this Hadamard gate warrants special attention and will be addressed in section IX. The four Hadamard gate outputs are terminated in single-photon detectors. For ideal lossless reception of a single photon transmission and no dark current, at most one of these detectors will click in each time slot. Our proposed "physical protocol" (i.e. optical realization of the abstract MUB protocol) is based on detecting the photon state emerging out of the Hadamard gate *just during the fourth time slot* (labeled $t = 3$). We denote the index of the clicking detector by $\hat{i} \in \{0, 1, 2, 3\}$, (with the erasure symbol ? indicating that no detector or more than one detector clicks) as this index is Bob's estimate of the key index i drawn in Alice's machine. The physical protocol description now follows:

(i) Alice independently and uniformly draws two random numbers $0 \leq i \leq 3$, $1 \leq \alpha \leq 4$ and applies the phaseshifts given by eq. 36 to its four PMs, in effect transmitting the i -th column vector of the α -th MUB matrix (eq. 35).

(ii) Bob performs a quantum measurement as follows:

(a) He uniformly draws a random number $1 \leq \beta \leq 4$ independently of Alice, and applies to its four PMs the phaseshifts given by eq. 36, in effect realizing for the phase shifting section a transfer matrix given by the conjugate of the β -th phase mask (eq. 37).

(b) He then measures the presence of a photon at his four detectors during the fourth time-slot, labeled $t = 3$. Whenever precisely one of the four detectors clicks, Bob records the index \hat{i} of the clicking detector.

(iii) Bob and Alice publicly exchange their respective base indexes α and β (but keep their respective key indexes i, \hat{i} secret). Whenever their bases coincide, i.e. $\alpha = \beta$, they register i, \hat{i} as raw key indexes.

(iv) They compare a small fraction of their raw key indexes. An elevated error rate in these bits is indicative of Eve's attack (for ideal channel and devices, we have $i = \hat{i}$, unless Eve attacks).

We now show that the physical protocol just described indeed provides an optical realization (for $D = 4$ and $K = 4$) of the abstract MUB protocol generically reviewed in section IV. Notice that the tapped delay line in Eve's system generates 4-slots long optical states, but the subsequent convolution with Bob's tapped delay lines spreads the received states over 7 time slots. The proper Hilbert state space in which to analyze the system is 28-dim. (7 time-slots, $0 \leq t \leq 6$ times 4 spatial ports $0 \leq s \leq 3$): $\mathbf{H} = \text{span}\{|u_t^s\rangle\}$ where $|u_t^s\rangle$ is the space-time basis vector representing the photon being in time slot t at spatial port s . We shall not reproduce here the formal derivation in full, but shall cover its key elements.

The overall output state is obtained by propagating the single photon input state $|u_0^0\rangle$ in sequence through Alice's and Bob's various modules. Referring to Fig. 7, Alice's state at reference plane II (at the output of her PM section), during time slot $t = 0$, is

$$|\Psi_a\rangle = 2^{-1}(a_0|u_0^0\rangle + a_1|u_0^1\rangle + a_2|u_0^2\rangle + a_3|u_0^3\rangle), \quad (37a)$$

where $a_s = e^{j\gamma_s}$, and the factor of half is due to the preceding splitter. Represented as a 4-tuple of coordinates, this state is $|\Psi_a\rangle \leftrightarrow 2^{-1}[a_0, a_1, a_2, a_3] = 2^{-1}\mathbf{a}$, where \mathbf{a} is Alice's transmitted state:

$$\mathbf{a} \equiv [a_0, a_1, a_2, a_3]^T = [e^{j\gamma_0}, e^{j\gamma_1}, e^{j\gamma_2}, e^{j\gamma_3}]^T = \text{Col}_I \Phi^{(\alpha)} \quad (37b)$$

Now consider Bob's state at plane VI, the tapped delay line output (= the PM section input), and sample this state in the fourth time slot (labeled by $t = 3$) i.e. project it onto the sub-space spanned by $\{|u_3^0\rangle, |u_3^1\rangle, |u_3^2\rangle, |u_3^3\rangle\}$. The time-sampled state $b_0|u_3^0\rangle + b_1|u_3^1\rangle + b_2|u_3^2\rangle + b_3|u_3^3\rangle$ is represented by the 4-tuple $\mathbf{b} = [b_0, a_1, a_2, a_3]^T$, called Bob's received state. Fig. 8 graphically demonstrates that Bob's received state is proportional to Alice's transmitted state:

$$\mathbf{b} = 2^{-2}\mathbf{a} = 2^{-3}\text{Col}_i\Phi^{(\alpha)} \quad (38)$$

where in last equality eq. 37b was substituted. In effect the back-end of Alice's system and the front-end of Bob's system, combined with the sampling during the fourth slot, act as back-to-back parallel-to-serial and serial-to-parallel converters, that cascade to an identity operation (up to a constant and a delay). Hence, Alice's phase modulated vector \mathbf{a} (the i -th MUB vector of the α -th basis) is essentially reproduced during slot 3 at Bob's PM input, \mathbf{b} . Continuing to represent the spatial quantum states during time-slot $t = 3$, by 4-tuple vectors, and the operators by 4x4 matrices, we are interested in the state at the detector's input, denoted by \mathbf{d} . As indicated in Fig. 7, the transformation from \mathbf{b} to \mathbf{d} is the cascade of Bob's PM section with the optical Hadamard-4 gate, seen in eq. 24 to equal the conjugate transpose of the MUB base matrix: $\Phi^{(\beta)\dagger} = \hat{\mathbf{H}}_4\Lambda_\beta^\dagger$.

It follows that Bob's photodetector input state is $\mathbf{d} = \Phi^{(\beta)\dagger}\mathbf{b}$. In a sense, the transfer matrix $\Phi^{(\beta)\dagger}$ in the back-end of Bob's apparatus, may be considered a filter matched to the β -th basis. Indeed, substituting eq. 38 into the last equation, we see that the input to this filter

is the i -th column of the α -th basis:

$$\mathbf{d} = \Phi^{(\beta)\dagger}\mathbf{b} = 2^{-3}\Phi^{(\beta)\dagger}\text{Col}_i\Phi^{(\alpha)} = \text{Col}_i 2^{-3}\Phi^{(\beta)\dagger}\Phi^{(\alpha)} \quad (39)$$

When, $\beta = \alpha$, i.e. Alice and Bob draw matched bases, we show that Bob's matched matrix actually reconstructs Alice's transmission state, as only the i -th component of \mathbf{d} is non-zero, i.e. just the i -th detector possibly clicks (w.p. given by the $|d_i|^2$). Indeed, setting $\beta = \alpha$ in eq. 39 yields

$$\mathbf{d} = 2^{-3}\Phi^{(\alpha)\dagger}\text{Col}_i\Phi^{(\alpha)} \quad (40)$$

but the i -th column of the unitary symmetric matrix $\Phi^{(\alpha)}$ is orthogonal to each of the other columns (=rows). Formally,

$$\mathbf{d} = \text{Col}_i 2^{-3}\Phi^{(\alpha)\dagger}\Phi^{(\alpha)} = \text{Col}_i 2^{-3}\mathbf{1}_4 \quad (41)$$

i.e. when Alice transmits key index i then Bob's state at the detectors, \mathbf{d} , is given by a unit vector with 1 in its i -th place times the constant 2^{-3} , i.e. the i -th detector clicks w.p.

$$\Pr\{i\text{-th detector clicks}|\alpha=\beta, i\text{-th state transmitted}\} = 2^{-6} \quad (42)$$

while the other detectors never click during slot 3. The erasure prob. is now quite high, given by

$$\Pr\{\text{no detector clicks}|\alpha=\beta, i\text{-th state transmitted}\} = 1 - 2^{-6} = 63/64 \quad (43)$$

Now, if Alice's and Bob's random draws of bases happen to be mismatched, $\beta \neq \alpha$, we are back to eq. 39, re-written as

$$\mathbf{d} = \text{Col}_i 2^{-3} \Phi^{(\beta)\dagger} \Phi^{(\alpha)} = \text{Col}_i G^{(\beta\alpha)} \quad (44)$$

wherein we defined $G^{(\beta\alpha)} \equiv 2^{-3} \Phi^{(\beta)\dagger} \Phi^{(\alpha)}$ as a scaled cross-gramian of the two matrices. As seen in eq. 51b, the cross-gramian is an unbiased matrix, then so is $G^{(\beta\alpha)}$ which differs from it by the constant 2^{-3} :

$$G^{(\beta\alpha)} \in \text{UB}_{4 \times 4}[2^{-3}/\sqrt{4}] = \text{UB}_{4 \times 4}[2^{-4}] \quad (45)$$

We then have $|[G^{(\beta\alpha)}]_{ri}| = 2^{-4}$ then evidently the i -th column of $G^{(\beta\alpha)}$ is also unbiased:

$\mathbf{d} \in \text{UB}_{4 \times 1}[2^{-4}]$. It follows that all (squared) components $|d_i|^2$, have the same absolute value:

$$\Pr\{j\text{-th detector clicks}|\alpha \neq \beta, i\text{-th state transmitted}\} = |d_j|^2 = 2^{-8} \quad (46)$$

These four equal probabilities (squares of prob. amplitudes) indicate that the output is uniform such that there is a prob. of that one of the four detectors click during slot 3, i.e. we have a fair quantum roulette, w.p. 2^{-8} , and with erasure erasure prob.

$$\Pr\{\text{no detector clicks}|\alpha \neq \beta, i\text{-th state transmitted}\} = 1 - 4 \cdot 2^{-8} = 63/64 \quad (47)$$

In summary when the bases are matched, we have an ideal quantum channel, whereas when the bases are mismatched we have a fair quantum roulette, i.e. the optical system described in this section indeed implements the abstract MUB protocol for $D = 4$ and $K = 4$.

It turns out that the realization complexity may actually be somewhat improved by saving a couple of PMs: As the phases of the four time slots are relative, and an overall phase factor is inconsequential, it actually suffices to use just three PMs rather than four in each system, e.g. the bottom PM in Alice's system and the top PM in Bob's system may be removed, and the lookup table for the phases be corrected accordingly, subtracting out of the three remaining phases the phase originally assigned to the modulator that was removed. While on the topic of phase modulation, we remark that Alice's transmission states may be considered to be a generalized form of DPSK, called multi-symbol or multi-chip DPSK [25]. In such modulation format, which might be more appropriately called here multi-slot DPSK, the phase is differentially modulated over a

sliding block of more than two slots, as in conventional DPSK. In our case we use $D = 4$ slots, selecting the phases of three of these slots, relative to the phase of a reference slot, consistent with the implementation remark above. The difference with respect to multi-slot DPSK of classical communication is that in the current quantum system each four-slot DPSK block carries a single photon, and moreover unlike in the classical case the current system does not resort to overlap of transmission blocks (the 4 slot blocks are disjoint, each carrying a single photon).

VIII. Operating characteristics of the six-state and 16-state optical realizations

A distinctive feature of the optical protocol realizations introduced in section VI, absent in the theoretical abstract version of the MUB protocol of section V, is the finite prob. of inconclusive events, whereby no detector clicks, e.g. the entries marked by the erasure symbol (?) in Table 1. The erasure is an inherent feature of the optical implementations of the 6 and 16 states protocols, due to the temporal spreading of received photon state over additional time-slots by Bob's IF, while photon detection is performed just over one or two of these time slots. This allows for a finite prob. that the photon end up in the unmeasured slots, i.e. go undetected, even for ideal channel and devices. In particular, in the BB84-DPSK optical implementation, Alice's 2-slot photon states are spread out by Bob's apparatus over 3 slots, with only slot 1 used for DPSK analysis, and only slots 0,2 used for PPM analysis. In the optical realization of the 16-state protocol, Alice's 4-slot photon states are spread out by Bob over 7 slots, with just slot 3 used for analysis.

In fact, the definition of erasure event may be generalized to include all the cases when the analysis is inconclusive, i.e. the case of more than one detector clicking may also be considered erasure (?), as is the case of no detector clicking. This extended definition may account in principle for system non-idealities as well - losses and impairments over the optical channel and/or end-systems (e.g. detector dark current). Here we focus on the quantum limits in the wake of the erasure due to the inherent structure of the physical protocol even for a lossless channel and ideal devices. A detailed derivation of the averaged EDR, EIR and KCR operating characteristics with erasure is outside the scope of the paper, however we just mention the key conclusions: (i) *the KCR and EIR are always diminished by erasure*. The decrease in key creation rate is obvious - photons are lost. The decrease in EIR may be interpreted as an effective decrease in Eve's key creation rate (much like Bob experiences a decrease in his key creation rate due to erasure)

(ii) Quite remarkably, *for all MUB protocols, regardless of their erasure rates,*

the average EDR and EIR complement to unity:

$$\bar{P}_D + \bar{P}_I = 1. \quad (48)$$

Such complementarity was seen to hold in the erasure-free special case (eq. 29), but it turns out that it generally holds in the wake of erasure, inducing a push-pull effect: the EIR decreases while the EDR increases, such that both of these two parameters move in beneficial directions (higher chance of detecting Eve, less information extracted by her). Applying the detailed OC formulas, not reproduced here, yields the following OCs for the 4,6,16-state integrated-optic implementations of the MUB protocols. For comparison we also listed the 4-state abstract protocol OC without erasure (e.g. for a polarization-oriented realization of BB84):

$$[P_D^{\text{no?}}, P_I^{\text{no?}}, P_C^{\text{no?}}]_{4\text{-state}} = [1/4, 3/4, 1/2]$$

$$[\bar{P}_D, \bar{P}_I, \bar{P}_C]_{4\text{-state}} = [3/4, 1/4, 1/8]$$

$$[\bar{P}_D, \bar{P}_I, \bar{P}_C]_{6\text{-state}} = [5/6, 1/6, 5/72] = [0.83, 0.17, 0.07] \quad (49)$$

$$[\bar{P}_D, \bar{P}_I, \bar{P}_C]_{16\text{-state}} = [1017/1024, 7/1024, 1/256] = [0.993, 0.007, 0.004] \quad (50)$$

It is apparent that the key creation rate diminishes significantly as we go to higher orders, however, beneficially, the EDR is improved, approaching unity (e.g. 99.3% for 16-state), i.e. Alice and Bob are almost certain to detect Eve even in a single usage of the channel, and along with it, the EIR, i.e. the rate at which Eve extracts information, gets very low (0.7% of 16 state).

If indeed the heuristic figures of merit EDR/EIR are good indicators of the protocol's reliability (which is yet to be rigorously justified by further information-theoretic studies), then these results indicate the desirability of resorting to higher order optical realizations of the MUB protocols, such as introduced here for the six-state and 16-state protocols.

IX. Integrated optic realization of 16-state system with the Hadamard quantum gate

All the ingredients are now in place to fully specify the integrated-optic implementation of Bob's apparatus for the 16-state MUB based protocol with $K = 4$ bases in $D = 4$ dimensions (Fig. 9). A key building block, already reviewed, is the integrated-optic Hadamard-4 quantum gate, cascaded with a phase mask (Fig. 3), synthesizing the adjoint MUB bases.

Notice that the second swap stage in Fig. 2 was actually discarded in the optical realization of Fig. 9: rather than crossing the output waveguides, we may simply exchange the labels of the two mid detectors, i.e. the single-photon detectors are now re-labeled as $j = 0, 2, 1, 3$ from top to bottom.

Effectively, it is the signalling wires leading from the two mid detectors that are crossed over, instead of having the waveguides leading to these detectors crossing over.

X. Discussion

In this paper we departed from the BB84 quantum key distribution protocol, conceiving novel integrated-optic implementations of advanced QKD MUB protocols. While recent quantum-theoretic studies [30-32] indicate that protocols of extended dimension and/or using more bases should in principle provide the benefit of enhanced security, the mission of precisely evaluating the security bounds, and quantifying the security improvement under a variety of attacks, is still outstanding. Our focus here has been on integrated-optic system design and straightforward quantum modeling: we proposed and analyzed novel integrated-optical implementations such higher-order abstract protocols, based on our novel theoretical insight identifying MUB constructions in terms of products of phase masks and a generator matrix such as the Hadamard matrix. To enable such systems we further developed two requisite integrated optic components, realizing quantum gates. Compared with the BB84 protocol, which uses an MZI and a PM in each of Alice's and Bob's systems, the novel protocols using generalized interferometer structures are more complex, yet the complexity seems manageable for up to four dimensions.

Our novel optical DPSK/PPM realization of the six-state protocol required two coupled interferometers on Bob's side, while on Alice's side the photon is to be detected in three time slots rather than one. Our novel 16-state system was implemented with four-arm interferometers, using four PMs for both Alice and Bob, as well as requiring a novel 4-port Hadamard optical gate, which we proposed to realize by cross-connecting four directional couplers.

It would be tempting to consider alternative implementations of the Hadamard-4 gates e.g. by means of a single-waveguide MMI devices. The feasibility of such integrated-optical synthesis of key optical gates will be discussed elsewhere along with alternative implementations based on coupled waveguides and modal drop modules (mode-selective couplers)

We note that the 16-state MUB set optically realized here is still partial - the full MUB set in four dimensions was seen to contain 5 bases i.e. a total of 20 states. In fact, we have further designed an optical implementation for the full MUB protocol, however its description must be relegated to another paper. We just remark here that the four "DPSK" bases are now to be augmented with a fifth PPM basis $\{|u_0^0\rangle, |u_1^0\rangle, |u_2^0\rangle, |u_3^0\rangle\}$. To generate these four additional PPM states further to the

16 DPSK states, as well as switching between these states, essentially requires an extra Hadamard gate in Alice's system. Moreover, whenever Bob selects the PPM base, he must detect the photon in four additional time slots.

While quantum modeling of optical systems implementing the six-state and 16-state protocol accounts for the extended observation interval, it still suffers from the deficiency that it addresses the unused interferometer ports in a simplistic way by means of projectors. A more rigorous Fock-space analysis is called for to refine the modeling. Another issue to be further explored is whether the "erased" photons straying in the unused time-slots may be used by Eve to gain some advantage. It should be mentioned that such issues, requiring further study, are not unique to our extended realizations, but apply to the conventional BB84-DPSK realization as well.

In terms of optical integration, the Hadamard and MMI device and the phase modulators may be realized as PLCs (Planar Lightwave Circuits) on silica-on-silicon, extrapolating the device fabrication techniques described in [22,23] for a modified four-state protocol.

We remark that as explored in [24], DPSK/PPM-like schemes of the types discussed there and further elaborated here, enjoy the beneficial property of polarization-independence, as the polarization state hardly varies over the differential-phase encoded adjacent time-slots. This indicates that the schemes described provide a one-way alternative to the two-way "plug-and-play" schemes based on self-compensating round-trip polarization modulation (e.g. [8,12,14]).

It is hoped that this paper will advance the theoretical knowledge and practical feasibility of integrated-optic QKD systems, enabling improved trade-offs between security and range over fiber-optic and free-space optical channels.

Appendix

For further reference we recall the following properties of the Hadamard matrix of order D :

\mathbf{H}_D is a real-valued matrix with elements ± 1 and all ones in the first row and column; symmetry: $\mathbf{H}_D = \mathbf{H}_D^\dagger$; introducing a normalized Hadamard matrix $\hat{\mathbf{H}}_D \equiv \frac{1}{\sqrt{D}}\mathbf{H}_D$, we have unitarity:

$\hat{\mathbf{H}}_D \hat{\mathbf{H}}_D^\dagger = \hat{\mathbf{H}}_D^2 = \mathbf{1}_D$ (here † is the conjugate transpose).

The MUB matrix properties are best formulated in terms of the following definitions:

*The **gramian** of a square matrix M is the matrix $M^\dagger M$. The adjoint product $P^\dagger Q$ of two matrices P, Q is called **cross-gramian**. A matrix $M = [M_{ij}]$ is called **unbiased** if the absolute values*

of all its elements are equal: $|M_{ij}| = \text{const}$. The set of unbiased $M \times N$ matrices with common absolute value a of their elements is denoted $\text{UB}_{M \times N}[a]$.

Let $\mathbf{M} = c\mathbf{U}$ be equal a unitary $D \times D$ matrix times a constant, and let M be unbiased, then we have $|U_{ij}| = 1/\sqrt{D}$, and $M \in \text{UB}_{D \times D}[c/\sqrt{D}]$.

The following property readily stems from the MUB definition and the MUB matrices unitarity:

A collection of $D \times D$ matrices $\{\Phi^{(0)}, \Phi^{(1)}, \dots, \Phi^{(K-1)}\}$ is a MUB set iff the following two properties hold: (i) Each base matrix is unitary, i.e. its gramian is the identity:

$$\Phi^{(\alpha)\dagger} \Phi^{(\alpha)} = \mathbf{1}_D. \quad (51a)$$

(ii) The cross-gramians of any two distinct base matrices are unitary unbiased matrices:

$$\Phi^{(\alpha)\dagger} \Phi^{(\beta)} \in \text{UB}_{D \times D}[1/\sqrt{D}], \quad \Phi^{(\beta)\dagger} \Phi^{(\alpha)} \in \text{UB}_{D \times D}[1/\sqrt{D}], \quad \alpha \neq \beta \quad (51b)$$

The evaluation of (cross)-gramians then provides a convenient test for the MUB property.

XI. References

- [1] M. Nielsen and I. Chuang, Quantum Computation and Quantum Information, Cambridge Univ. Press, 2000.
- [2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Modern Phys.*, 74, 145-196, (2002).
- [3] C.H. Bennett, G. Brassard "Quantum cryptography: public key distribution and coin tossing", In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York, 1984), p. 175.
- [4] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, "Experimental Quantum Cryptography," *J. Crypt.*, vol. 5, no. 3 (1992).
- [5] Hugo Zbinden "Experimental quantum cryptography"- book chapter in *Introduction to quantum computation and information*, editors Hoi-Kwong Lo, Sandu Popescu, Tim Spiller, World Scientific, 1999.
- [6] P.D. Townsend, J.G. Rarity and P.R. Tapster, "Single photon interference in 10Km long optical fiber interferometer," *Electron. Lett.*, 29, 634-635 (1993).
- [7] P.D. Townsend, J.G. Rarity, and P.R. Tapster, "Enhanced single photon fringe visibility in a 10 km-long prototype quantum cryptography channel," *Electron. Lett.* 29, 1993, 1291-1292.

- [8] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, "Plug&play systems for quantum cryptography," *Appl. Phys. Lett.*, 70, 793-795 (1997).
- [9] P.D. Townsend, "Quantum Cryptography on multi-user optical fiber networks," *Nature*, 385, 47-49 (1997).
- [10] P.D. Townsend, "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing," *Electron. Lett.*, 33, 188-190 (1997).
- [11] W. T. Buttler, R. J. Hughes, P. G. Kwiat, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, "Free-space quantum-key distribution," *Phys. Rev. A* 57, 2379–2382 (1998).
- [12] D. Bethune, and W. Risk, "An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light," *IEEE J. Quant. Electron.*, 36, 340-347 (2000).
- [13] J. G. Rarity, P. R. Tapster and P. M. Gorman, "Practical free-space quantum key distribution over 10km in daylight and at night," *J. Mod. Phys.* 48, 1887-1901 (2001).
- [14] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug&play system," *New J. of Physics*, 4, 41.1-41.8 (2002).
- [15] P. Toliver, et. al, "Experimental investigation of quantum key distribution through transparent optical switch elements," *Photon. Tech. Lett.*, 15, 1669-1671 (2003).
- [16] H. Kosaka, A. Tomita, Y. Nambu, T. Kimura, and K. Nakamura, "Single-photon interference experiment over 100 Km for quantum cryptography system using balanced gated-mode photon detector," *Electron. Lett.*, 39, 1199-1201 (2003).
- [17] T. Honjo, K. Inoue and H. Takahashi, "Differential phase-shift quantum key distribution experiment with a planar light-wave circuit Mach-Zehnder interferometer," *Opt. Lett.*, 29, p. 2797-2799 (2004).
- [18] M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster and J. G. Rarity, "A step towards global key distribution," *Nature*, 419, 450-450 (2002).
- [19] K. J. Gordon, V. Fernandez, P. D. Townsend and G. S. Buller, "A short wavelength gigahertz clocked fiberoptic quantum key distribution system," *IEEE J. Quantum Electron.* 40, 900-908 (2004).

- [20] C. Gobby, Z.L. Yuan and A.J. Shields., “Quantum key distribution over 122 Km of standard telecom fiber,” *Appl. Phys. Lett.*, 84, 3762-3764, (2004).
- [21] T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka, and K. Nakamura, Single-photon interference over 150 Km transmission using silica-based integrated optic interferometers for quantum cryptography, *Jpn. J. Appl. Phys.* 43 pp.L1217-L1219(2004)
- [22] Y. Nambu, T. Hatanaka, and K. Nakamura, Planar lightwave circuits for quantum cryptographic systems, <http://arxiv.org/abs/quant-ph/0307074>
- [23] Y. Nambu, T. Hatanaka, and K. Nakamura, BB84 Quantum Key Distribution System based on silica-based planar lightwave circuits, *Jpn. J. Appl. Phys.* 43 pp.L1109-L1110 (2004) <http://arxiv.org/abs/quant-ph/0404015>
- [24] Moshe Nazarathy, “Quantum Key Distribution over the fiber-optic channel by means of Pulse Position Modulation,” *Opt. Lett.*, 30, 1533-1535 (2005).
- [25] Moshe Nazarathy and Erez Simony, “Multi-Chip Differential Phase Encoded Optical Transmission”, *Photon. Technol. Lett.*, 17, 1133-1135 (2005).
- [26] N.J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, “Security of quantum key distribution using d-level systems,” *Phys. Rev. Lett.*, Vol. 88, pp. 127902-1-4, (2002).
- [27] J. Swinger, “Unitary operator bases,” *Proc. Nat. Acad. Sci. U.S.A.*, 46, 570-579 (1960).
- [28] W. K. Wootters and B.D. Fields, “Optimal state-determination by mutually unbiased measurements,” *Ann. Phys.* 191, 363 (1989).
- [29] A. Klappenecker and M. Rotteler, “Constructions of mutually unbiased bases,” [quant-ph/0309120](http://arxiv.org/abs/quant-ph/0309120).
- [30] D. Bruss, Optimal Eavesdropping in Quantum Cryptography with Six State, *Phys. Rev. Lett.* 81, 3018 (1998). [quant-ph-98050019](http://arxiv.org/abs/quant-ph/98050019)
- [31] H. Bechmann-Pasquinucci and N. Gisin, “Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography,” *Phys. Rev. A.*, vol. 59, pp.4238-4248, (1999).
- [32] D. Gottesman and Hoi-Kwong Lo, Proof of security of quantum key distribution with two-way classical communications, *IEEE Trans. Info. Theory* 49, 457-475 (2003), [quant-ph/0105121](http://arxiv.org/abs/quant-ph/0105121).

- [33] A.R. Gupta et. al., "Synthesis of Hadamard transformers by use of multimode interference optical waveguides," *Appl. Opt.*, 42, 2730-2738, (2003).
- [34] L.B. Soldano et. al., "Optical multi-mode interference devices based on self-imaging: principles and applications," *Journ. Lightwave Technol.*, 13, 615-627, (1995).
- [35] G. Bonfrate, M. Harlow, C. Ford, G. Maxwell and P.D. Townsend, "Asymmetric Mach-Zehnder germano-silicate channel waveguide interferometers for quantum cryptographic systems," *Electron. Lett.*, 37, 846-847 (2001).
- [36] G. Cincotti, "Design of Optical Full Encoders/Decoders for Code-Based Photonic Routers" *Journ. Lightwave Technol.*, 22, 1642-1650, (2004).

Table 1:

TRANSMISSION DETECTION			<i>ALICE</i>					
			PPM $\alpha=0$		DPSK Re $\alpha=1$		DPSK Im $\alpha=2$	
			$ u_0\rangle$	$ u_1\rangle$	$ u_0\rangle + u_1\rangle$	$- u_0\rangle + u_1\rangle$	$j u_0\rangle + u_1\rangle$	$-j u_0\rangle + u_1\rangle$
<i>BOB</i>	PPM $\beta=0$	<i>up early</i>	1/8	0	1/16	1/16	1/16	1/16
		<i>up late</i>	0	1/8	1/16	1/16	1/16	1/16
		?	7/8	7/8	7/8	7/8	7/8	7/8
	DPSK Re $\beta=1$	<i>up mid</i>	1/8	1/8	1/4	0	1/8	1/8
		<i>down mid</i>	1/8	1/8	0	1/4	1/8	1/8
		?	3/4	3/4	3/4	3/4	3/4	3/4
	DPSK Im $\beta=2$	<i>up mid</i>	1/8	1/8	1/8	1/8	1/4	0
		<i>down mid</i>	1/8	1/8	1/8	1/8	0	1/4
		?	3/4	3/4	3/4	3/4	3/4	3/4

Table 1: Detection probabilities for the optical DPSK/PPM realization of the six-state QKD protocol. The main entries are the probabilities that a certain detector click in certain time slot: *up/down mid* means upper/lower detector clicking during time-slot 1; *up early/late* means the upper detector clicking during slot 0/2; The erasure symbol ? designates an inconclusive measurement whereby no detector clicks. The six columns correspond to the transmitted states the six-state protocol, stated unnormalized. The columns are partitioned in pairs corresponding to the transmission bases α , while the rows are partitioned in triplets corresponding to the detection bases β .

XII. Figures and figure captions

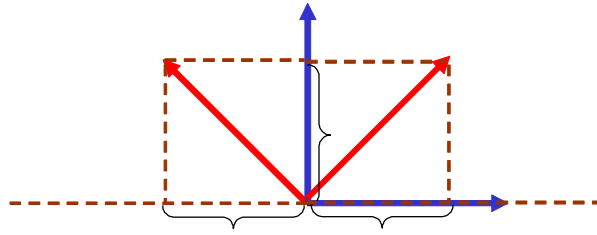


Fig. 1: $K = 2$ partial MUB (Maximally Unbiased bases) for dimension $D = 2$. One base coincides with the canonical axes of \mathbf{R}^2 , the other is obtained by ccw rotating the canonical axes by 45° . The MUB property amounts to the projections of any vector of one base onto any other vector of the other base having the same lengths.

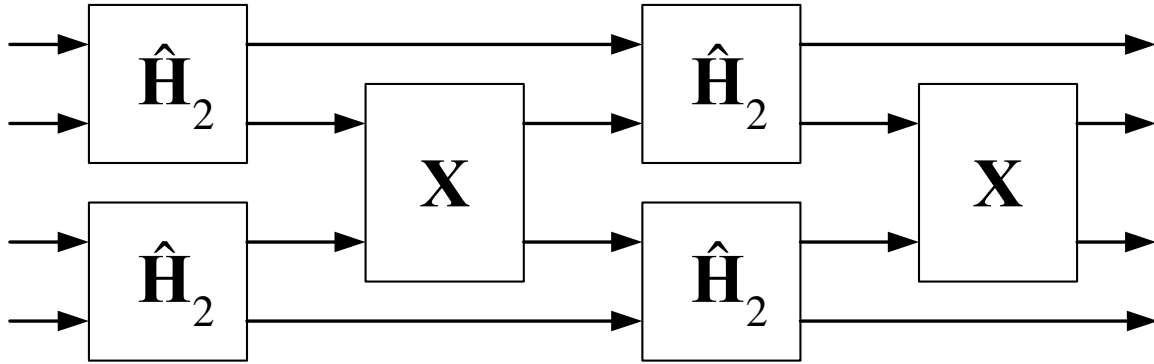


Fig. 2: Abstract realization of the Hadamard-4 gate in terms of Hadamard-2 and swap gates.

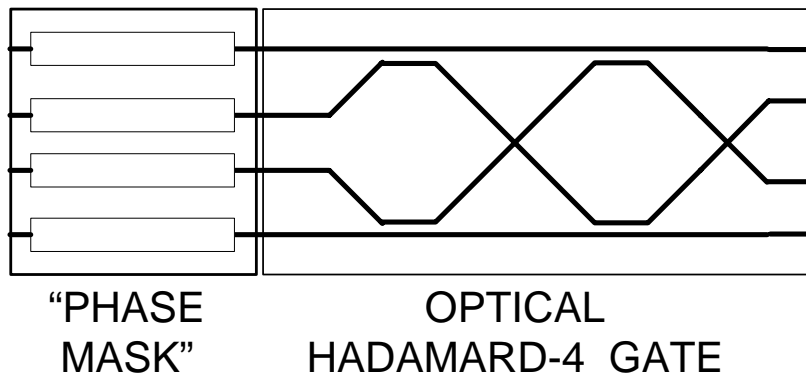


Fig. 3: Integrated-optical implementation of the Hadamard-4 optical gate and of the 16-state adjoint MUB transfer matrices. The Hadamard-4 gate is realized as a PLC cross-connecting four 50/50 directional couplers as shown, realizing the optical signal processing and flow of Fig. 2. The “Phase Mask” section consists of four phase modulators applying the static phaseshifts $\{-\theta_0^{(\beta)}, -\theta_1^{(\beta)}, -\theta_2^{(\beta)}, -\theta_3^{(\beta)}\}$ (the negatives of the values in eq. 21a). The details of the PM electrode structures are not shown. The overall the integrated-optic 4-port implements the adjoint MUB transfer matrices $\Phi^{(\beta)\dagger}$, $\beta = 1, 2, 3, 4$ (eq. 24), providing a key optical building block for the MUB-based protocol explored in this paper. The phase mask section may be butt-coupled to the Hadamard gate in one hybridized structure (similar to the experimental demonstration of [22,23]). Alternatively, InP based PLCs may be employed to combine the two active and passive sections on a single substrate.

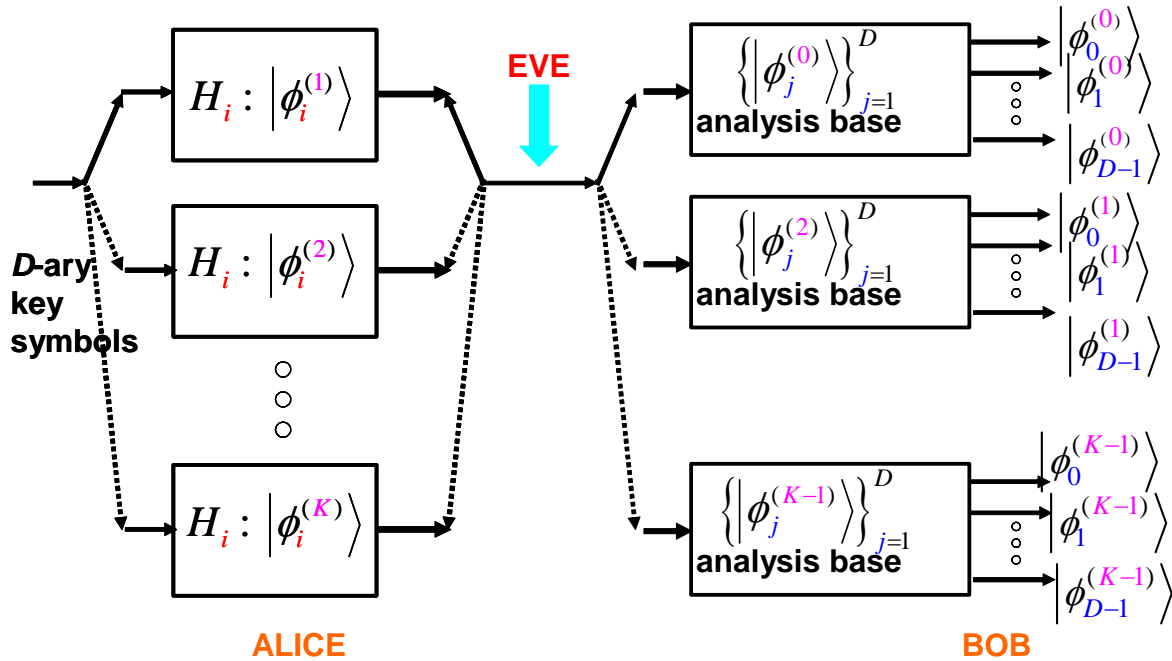


Fig. 4: Abstract description of a general MUB-based QKD protocol using K bases in D dimensional Hilbert space. The well-known BB84 protocol is a special case for $D = 2 = K$. Alice transmits one of KD states, by drawing one of K bases of a MUB set, then drawing one state, i , out of the D orthogonal states of the selected base. Bob randomly switches in an analysis base out of the same MUB set and measures Alice's transmitted state. The sample space of outputs of each analyzer is shown as the collection of its base states, but in actuality the measurement output is just a D -ary index, \hat{i} , labeling the post-measurement state.

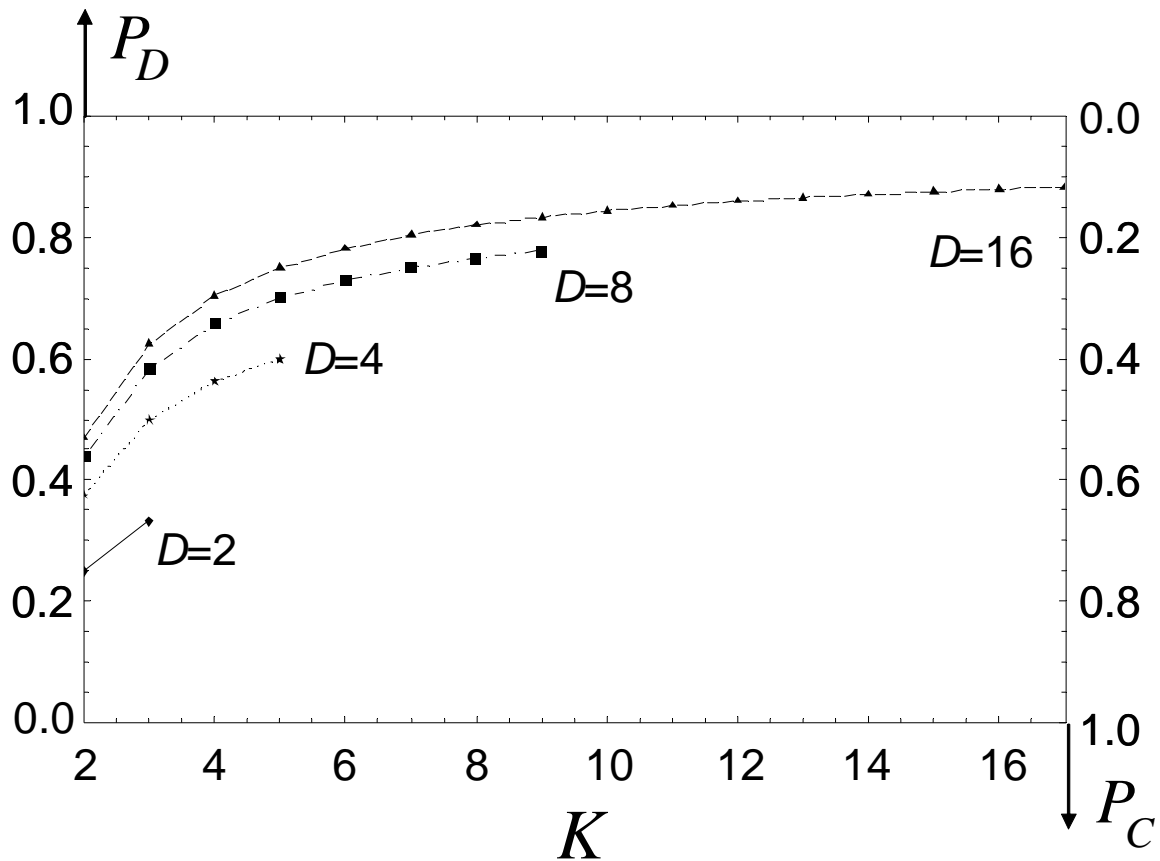


Fig. 5: Operating Characteristics (OC) of the MUB based protocol: The EDR (Eve Detection Rate) P_D and EIR (Eve Information Rate) probabilities P_I as a function of the the number of bases K ., for powers-of-two dimensions. Notice that there are at most $D + 1$ bases of dimension D in a MUB set. The third parameter $P_c = 1/K$ of the OC, is not plotted as its graph is evident. Notice that since $P_D + P_C = 1$ it suffices to invert the scale for P_C .

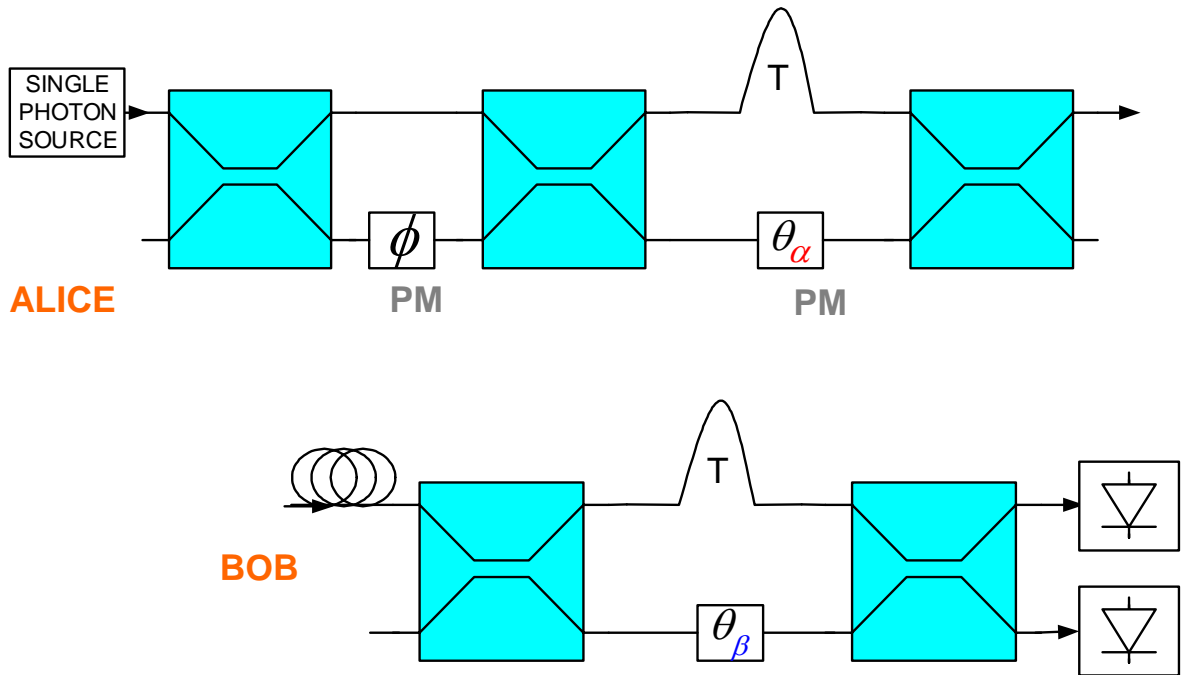


Fig. 6: Optical realization of the six-state QKD protocol ($D = 2, K = 3$). Compared to the DPSK implementation of the BB84 protocol, Alice's apparatus uses two coupled MZIs (Mach-Zehnder Interferometers) whereas Bob's apparatus contains the same electro-optical hardware as in the BB84 DPSK scheme, however the photon is detected over three adjacent time-slots as well.

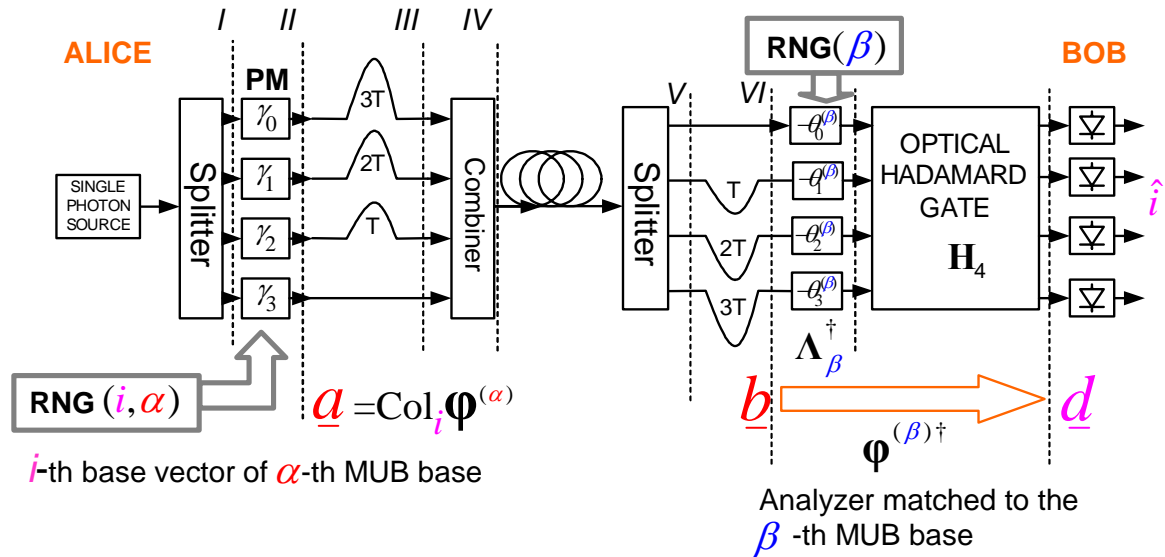


Fig. 7: Optical implementation of the 16-state MUB QKD protocol. In Alice's system, a single-photon source is split to feed four PMs (phase modulators) followed by four regularly spaced delays the outputs of which are combined into the transmission fiber. The PMs are driven by phaseshifts the combinations of which are controlled by a Random Number Generator (RNG), generating the output vector \mathbf{a} , out of the 16 base states of the $D = 4 = K$ MUB set. In Bob's apparatus the received photon is split along four delays followed by a PM section, followed by an optical Hadamard gate, feeding four single photon detectors. The four PMs implement the conjugate of the one of four phase masks associated with the MUB set, as selected by Bob's RNG. The cascade of PM section and Optical Hadamard Gate acts as an analyzer matched to the β -th base. Finally, the received key symbol is index \hat{i} of the clicking detector during time slot $t = 3$

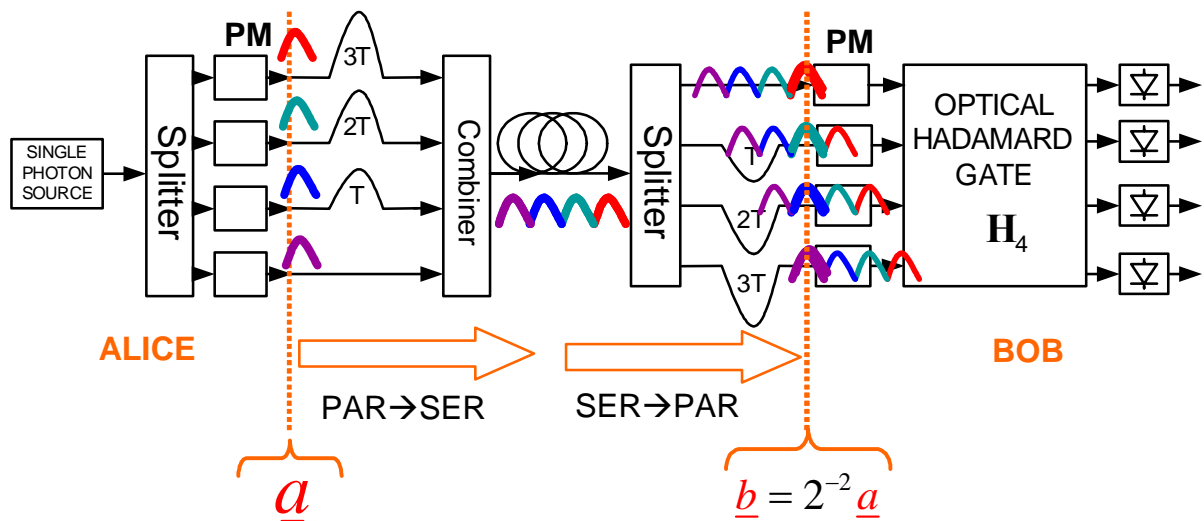


Fig. 8: Operational details of the 16-state MUB protocol optical realization of the previous figure: The parallel-to-serial and serial-to-parallel conversions, together with sampling in time-slot $t = 3$ reproduce, (up to a constant 2^{-2} and a delay) at the input of Bob's PM section, the state vector \underline{a} generated at the output of Alice's PM section.

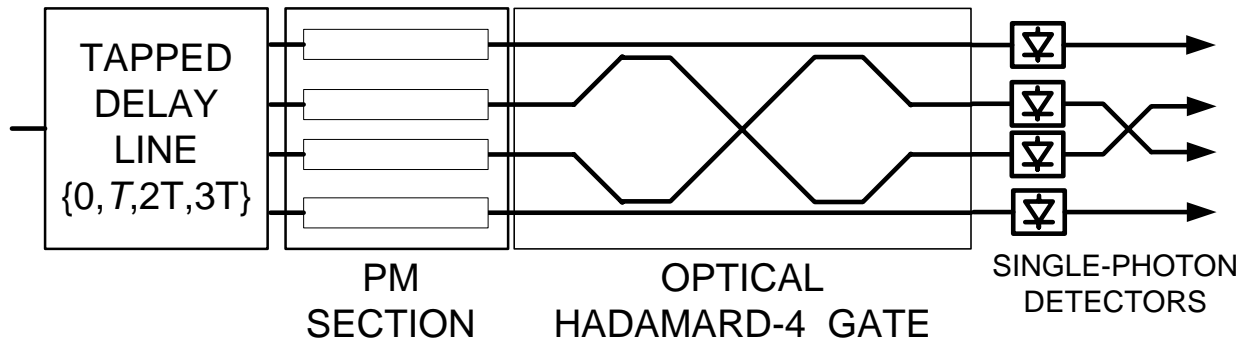


Fig. 9: Optical implementation of Bob's apparatus for the 16-state MUB protocol, including a modified version of the integrated-optic Hadamard-4 gate PLC described in Fig. 3. The other sections of Bob's apparatus (the PM section implementing the phase mask, and the tapped delay line) are shown in schematic form. In the version of Hadamard-4 gate used here, the waveguides leading to the two mid outputs do not cross over. Instead, the terminals of the mid pair of single-photon detectors are crossed, effectively implementing the rightmost swap module of Fig. 2 in the electrical rather than the optical domain.